Επίσημη Εφημερίδα L 333
της Ευρωπαϊκής Ένωσης

Έκδοση στην ελληνική γλώσσα

Νομοθεσία

65ο έτος

27 Δεκεμβρίου 2022

Περιεχόμενα

I *Νομοθετικές πράξεις*

ΚΑΝΟΝΙΣΜΟΙ

★ **Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011** [1] 1

ΟΔΗΓΙΕΣ

★ **Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2)** [1] 80

★ **Οδηγία (ΕΕ) 2022/2556 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, για την τροποποίηση των οδηγιών 2009/65/ΕΚ, 2009/138/ΕΚ, 2011/61/ΕΕ, 2013/36/ΕΕ, 2014/59/ΕΕ, 2014/65/ΕΕ, (ΕΕ) 2015/2366 και (ΕΕ) 2016/2341 όσον αφορά την ψηφιακή επιχειρησιακή ανθεκτικότητα για τον χρηματοοικονομικό τομέα** [1] 153

★ **Οδηγία (ΕΕ) 2022/2557 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, για την ανθεκτικότητα των κρίσιμων οντοτήτων και την κατάργηση της οδηγίας 2008/114/ΕΚ του Συμβουλίου** [1] 164

[1] Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ

EL

Οι πράξεις των οποίων οι τίτλοι έχουν τυπωθεί με λευκά στοιχεία αποτελούν πράξεις τρεχούσης διαχειρίσεως που έχουν θεσπισθεί στο πλαίσιο της γεωργικής πολιτικής και είναι γενικά περιορισμένης χρονικής ισχύος.

Οι τίτλοι όλων των υπολοίπων πράξεων έχουν τυπωθεί με μαύρα στοιχεία και επισημαίνονται με αστερίσκο.

I

(Νομοθετικές πράξεις)

ΚΑΝΟΝΙΣΜΟΙ

ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2022/2554 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

της 14ης Δεκεμβρίου 2022

σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης, και ιδίως το άρθρο 114,

Έχοντας υπόψη την πρόταση της Ευρωπαϊκής Επιτροπής,

Κατόπιν διαβίβασης του σχεδίου νομοθετικής πράξης στα εθνικά κοινοβούλια,

Έχοντας υπόψη τη γνώμη της Ευρωπαϊκής Κεντρικής Τράπεζας ([1]),

Έχοντας υπόψη τη γνώμη της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής ([2]),

Αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία ([3]),

Εκτιμώντας τα ακόλουθα:

(1) Στην ψηφιακή εποχή, οι τεχνολογίες των πληροφοριών και των επικοινωνιών (ΤΠΕ) υποστηρίζουν σύνθετα συστήματα που χρησιμοποιούνται για καθημερινές δραστηριότητες. Διασφαλίζουν την αδιάλειπτη λειτουργία των οικονομιών μας σε βασικούς τομείς, συμπεριλαμβανομένου του χρηματοοικονομικού τομέα, και ενισχύουν τη λειτουργία της εσωτερικής αγοράς. Η αυξημένη ψηφιοποίηση και διασυνδεσιμότητα εντείνουν επίσης τους κινδύνους ΤΠΕ, οι οποίοι καθιστούν την κοινωνία συνολικά —και ειδικότερα το χρηματοοικονομικό σύστημα— πιο ευάλωτη σε κυβερνοαπειλές ή διαταραχές των ΤΠΕ. Μολονότι η καθολική χρήση των συστημάτων ΤΠΕ και ο υψηλός βαθμός ψηφιοποίησης και συνδεσιμότητας αποτελούν σήμερα βασικά χαρακτηριστικά των δραστηριοτήτων των χρηματοοικονομικών οντοτήτων της Ένωσης, η ψηφιακή τους ανθεκτικότητα δεν έχει ακόμη αντιμετωπιστεί και ενσωματωθεί καλύτερα στα ευρύτερα επιχειρησιακά τους πλαίσια.

(2) Κατά τις προηγούμενες δεκαετίες, η χρήση ΤΠΕ έχει κατακτήσει καθοριστικό ρόλο στην παροχή χρηματοοικονομικών υπηρεσιών, σε σημείο που έχει πλέον αποκτήσει κρίσιμη σημασία για τη διασφάλιση των συνήθων καθημερινών λειτουργιών όλων των χρηματοοικονομικών οντοτήτων. Η ψηφιοποίηση καλύπτει πλέον, για παράδειγμα, τις πληρωμές, οι οποίες από τα μετρητά και τα έντυπα μέσα στρέφονται πλέον ολοένα και περισσότερο στη χρήση ψηφιακών λύσεων, καθώς και την εκκαθάριση και τον διακανονισμό τίτλων, τις ηλεκτρονικές και αλγοριθμικές συναλλαγές, τις πράξεις δανεισμού και χρηματοδότησης, τη χρηματοδότηση μεταξύ ομοτίμων, την αξιολόγηση πιστοληπτικής ικανότητας, τη διαχείριση

([1]) ΕΕ C 343 της 26.8.2021, σ. 1.
([2]) ΕΕ C 155 της 30.4.2021, σ. 38.
([3]) Θέση του Ευρωπαϊκού Κοινοβουλίου της 10ης Νοεμβρίου 2022 (δεν έχει ακόμη δημοσιευθεί στην Επίσημη Εφημερίδα) και απόφαση του Συμβουλίου της 28ης Νοεμβρίου 2022.

απαιτήσεων και τις υπηρεσίες υποστήριξης (back-office). Η χρήση ΤΠΕ μετασχημάτισε επίσης τον ασφαλιστικό τομέα, από την εμφάνιση ασφαλιστικών διαμεσολαβητών που προσφέρουν τις υπηρεσίες τους μέσω διαδικτύου και λειτουργούν με την InsurTech, έως την ψηφιακή ανάληψη ασφαλιστικών κινδύνων. Εκτός του υψηλού βαθμού ψηφιοποίησης σε ολόκληρο τον χρηματοοικονομικό τομέα, η ψηφιοποίηση έχει εμβαθύνει επίσης τις διασυνδέσεις και τις εξαρτήσεις εντός του χρηματοοικονομικού τομέα, καθώς και με τρίτους παρόχους υποδομών και υπηρεσιών.

(3) Σε έκθεση του 2020 σχετικά με τον συστημικό κίνδυνο στον κυβερνοχώρο, το Ευρωπαϊκό Συμβούλιο Συστημικών Κινδύνων (ΕΣΣΚ) επιβεβαίωσε τον τρόπο με τον οποίο το υφιστάμενο υψηλό επίπεδο διασυνδεσιμότητας μεταξύ των χρηματοοικονομικών οντοτήτων, των χρηματοοικονομικών αγορών και των υποδομών χρηματοοικονομικών αγορών, και ιδίως οι αλληλεξαρτήσεις των οικείων συστημάτων ΤΠΕ, θα μπορούσε να αποτελέσει συστημική ευπάθεια, δεδομένου ότι τοπικά κυβερνοπεριστατικά θα μπορούσαν να εξαπλωθούν ταχέως από οποιαδήποτε από τις περίπου 22 000 χρηματοοικονομικές οντότητες της Ένωσης σε ολόκληρο το χρηματοοικονομικό σύστημα, χωρίς να εμποδίζονται από τα γεωγραφικά σύνορα. Οι σοβαρές παραβιάσεις των ΤΠΕ που ανακύπτουν στον χρηματοοικονομικό τομέα δεν επηρεάζουν μόνο μεμονωμένες χρηματοοικονομικές οντότητες. Διευκολύνουν επίσης τη διάδοση τοπικών ευπαθειών στους διαύλους μετάδοσης και μπορούν να έχουν δυσμενείς συνέπειες για τη σταθερότητα του χρηματοοικονομικού συστήματος της Ένωσης, φέρ' ειπείν προκαλώντας εκροές ρευστότητας και συνολική απώλεια της αξιοπιστίας των χρηματοοικονομικών αγορών και της εμπιστοσύνης σε αυτές.

(4) Κατά τα τελευταία έτη, οι κίνδυνοι ΤΠΕ έχουν προσελκύσει την προσοχή διεθνών ενωσιακών και εθνικών φορέων χάραξης πολιτικής, ρυθμιστικών αρχών και οργανισμών τυποποίησης, στο πλαίσιο μιας απόπειρας να ενισχυθεί η ψηφιακή ανθεκτικότητα, να καθοριστούν πρότυπα και να συντονιστούν οι ρυθμιστικές ή εποπτικές εργασίες. Σε διεθνές επίπεδο, η Επιτροπή της Βασιλείας για την Τραπεζική Εποπτεία, η Επιτροπή Πληρωμών και Υποδομών Αγορών, το Συμβούλιο Χρηματοπιστωτικής Σταθερότητας, το Ίδρυμα Χρηματοπιστωτικής Σταθερότητας, καθώς και οι G7 και G20, έχουν θέσει ως στόχο την παροχή εργαλείων στις αρμόδιες αρχές και στους διαχειριστές αγοράς σε διάφορες δικαιοδοσίες για την ενίσχυση της ανθεκτικότητας των χρηματοοικονομικών τους συστημάτων. Το έργο αυτό υπαγορεύθηκε επίσης από την ανάγκη να ληφθούν δεόντως υπόψη οι κίνδυνοι ΤΠΕ στο πλαίσιο ενός εξαιρετικά διασυνδεδεμένου παγκόσμιου χρηματοοικονομικού συστήματος και να επιδιωχθεί μεγαλύτερη συνοχή των σχετικών βέλτιστων πρακτικών.

(5) Παρά την ανάληψη ενωσιακών και εθνικών πολιτικών και νομοθετικών πρωτοβουλιών, οι κίνδυνοι ΤΠΕ εξακολουθούν να συνιστούν πρόκληση για την επιχειρησιακή ανθεκτικότητα, τις επιδόσεις και τη σταθερότητα του χρηματοοικονομικού συστήματος της Ένωσης. Οι μεταρρυθμίσεις που ακολούθησαν τη χρηματοοικονομική κρίση του 2008 ενίσχυσαν πρωτίστως τη χρηματοοικονομική ανθεκτικότητα του χρηματοοικονομικού τομέα της Ένωσης και είχε ως στόχο τη διασφάλιση της ανταγωνιστικότητας και της σταθερότητας της Ένωσης από την οπτική γωνία της οικονομίας, της προληπτικής εποπτείας και της δεοντολογίας της αγοράς. Μολονότι η ασφάλεια των ΤΠΕ και η ψηφιακή ανθεκτικότητα αποτελούν μέρος του επιχειρησιακού κινδύνου, δεν τέθηκαν δεόντως στο επίκεντρο του κανονιστικού θεματολογίου μετά τη χρηματοοικονομική κρίση, ενώ έχουν αναπτυχθεί μόνο σε ορισμένους τομείς του πολιτικού και κανονιστικού πλαισίου της Ένωσης για τις χρηματοοικονομικές υπηρεσίες ή μόνο σε μερικά κράτη μέλη.

(6) Στην ανακοίνωσή της της 8ης Μαρτίου 2018 με τίτλο «Σχέδιο δράσης για τη χρηματοοικονομική τεχνολογία: Για έναν πιο ανταγωνιστικό και καινοτόμο ευρωπαϊκό χρηματοπιστωτικό τομέα», η Επιτροπή επισήμανε τη θεμελιώδη σημασία της ενίσχυσης της ανθεκτικότητας του χρηματοοικονομικού τομέα της Ένωσης, μεταξύ άλλων, από επιχειρησιακής πλευράς για τη διασφάλιση της τεχνολογικής ασφάλειας και της άρτιας λειτουργίας του, καθώς και της ταχείας ανάκαμψής του από παραβιάσεις και συμβάντα που σχετίζονται με τις ΤΠΕ, ώστε να καταστεί εντέλει δυνατή η αποτελεσματική και ομαλή παροχή χρηματοοικονομικών υπηρεσιών σε ολόκληρη την Ένωση, μεταξύ άλλων υπό συνθήκες ακραίων καταστάσεων, ενώ θα διατηρείται παράλληλα η αξιοπιστία της αγοράς και η εμπιστοσύνη των καταναλωτών σε αυτήν.

(7) Τον Απρίλιο του 2019, η Ευρωπαϊκή Εποπτική Αρχή (Ευρωπαϊκή Αρχή Τραπεζών) (ΕΑΤ), η οποία συγκροτήθηκε με τον κανονισμό (ΕΕ) αριθ. 1093/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([4]), η Ευρωπαϊκή Εποπτική Αρχή (Ευρωπαϊκή Αρχή Ασφαλίσεων και Επαγγελματικών Συντάξεων) («ΕΑΑΕΣ»), η οποία συγκροτήθηκε με τον κανονισμό (ΕΕ) αριθ. 1094/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([5]), και η Ευρωπαϊκή Εποπτική Αρχή (Ευρωπαϊκή Αρχή Κινητών Αξιών και Αγορών) (ΕΑΚΑΑ), η οποία συγκροτήθηκε με τον κανονισμό (ΕΕ) αριθ. 1095/2010 του

([4]) Κανονισμός (ΕΕ) αριθ. 1093/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Νοεμβρίου 2010, σχετικά με τη σύσταση Ευρωπαϊκής Εποπτικής Αρχής (Ευρωπαϊκή Αρχή Τραπεζών), την τροποποίηση της απόφασης αριθ. 716/2009/ΕΚ και την κατάργηση της απόφασης 2009/78/ΕΚ της Επιτροπής (ΕΕ L 331 της 15.12.2010, σ. 12).

([5]) Κανονισμός (ΕΕ) αριθ. 1094/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Νοεμβρίου 2010, για τη σύσταση Ευρωπαϊκής Εποπτικής Αρχής (Ευρωπαϊκή Αρχή Ασφαλίσεων και Επαγγελματικών Συντάξεων), την τροποποίηση της απόφασης αριθ. 716/2009/ΕΚ και την κατάργηση της απόφασης 2009/79/ΕΚ της Επιτροπής (ΕΕ L 331 της 15.12.2010, σ. 48).

Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([6]) (συλλογικά γνωστές ως «Ευρωπαϊκές Εποπτικές Αρχές» ή «ΕΕΑ»), εξέδωσαν από κοινού τεχνικές γνωμοδοτήσεις, στις οποίες διατύπωναν έκκληση για συνεκτική προσέγγιση όσον αφορά τους κινδύνους ΤΠΕ στον χρηματοοικονομικό τομέα και σύσταση για ενίσχυση της ψηφιακής επιχειρησιακής ανθεκτικότητας του κλάδου των χρηματοοικονομικών υπηρεσιών, κατά τρόπο αναλογικό, μέσω ειδικής τομεακής πρωτοβουλίας της Ένωσης.

(8) Ο χρηματοοικονομικός τομέας της Ένωσης ρυθμίζεται από ενιαίο εγχειρίδιο κανόνων και διέπεται από το ευρωπαϊκό σύστημα χρηματοοικονομικής εποπτείας. Ωστόσο, οι διατάξεις που αφορούν την ψηφιακή επιχειρησιακή ανθεκτικότητα και την ασφάλεια ΤΠΕ δεν έχουν εναρμονιστεί ακόμη πλήρως ή με συνεκτικό τρόπο, παρά το γεγονός ότι η ψηφιακή επιχειρησιακή ανθεκτικότητα είναι ζωτικής σημασίας για τη διασφάλιση της χρηματοοικονομικής σταθερότητας και της ακεραιότητας της αγοράς στην ψηφιακή εποχή και είναι εξίσου σημαντική, για παράδειγμα, με τα κοινά πρότυπα προληπτικής εποπτείας ή δεοντολογίας της αγοράς. Κατά συνέπεια, το ενιαίο εγχειρίδιο κανόνων και το σύστημα εποπτείας θα πρέπει να εξελιχθούν ώστε να καλύπτουν και την ψηφιακή επιχειρησιακή ανθεκτικότητα, με την ενίσχυση των εντολών των αρμόδιων αρχών για να μπορούν να εποπτεύουν τη διαχείριση των κινδύνων ΤΠΕ στον χρηματοοικονομικό τομέα, προκειμένου να προστατεύουν την ακεραιότητα και την αποτελεσματικότητα της εσωτερικής αγοράς και να διευκολύνουν την εύρυθμη λειτουργία της.

(9) Οι νομοθετικές διαφορές και οι ανομοιόμορφες εθνικές κανονιστικές και εποπτικές προσεγγίσεις όσον αφορά τους κινδύνους ΤΠΕ εγείρουν φραγμούς στη λειτουργία της εσωτερικής αγοράς χρηματοοικονομικών υπηρεσιών, παρεμποδίζοντας με τον τρόπο αυτόν την απρόσκοπτη άσκηση της ελευθερίας εγκατάστασης και της παροχής υπηρεσιών για τις χρηματοοικονομικές οντότητες που λειτουργούν σε διασυνοριακή βάση. Είναι επίσης πιθανό να προκαλούνται στρεβλώσεις στον ανταγωνισμό μεταξύ των χρηματοοικονομικών οντοτήτων του ίδιου τύπου που δραστηριοποιούνται σε διαφορετικά κράτη μέλη. Αυτό ισχύει, ιδίως, για τομείς στους οποίους η εναρμόνιση της Ένωσης είναι εξαιρετικά περιορισμένη, όπως οι δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας, ή απούσα, όπως η παρακολούθηση των κινδύνων τρίτων παρόχων ΤΠΕ. Οι διαφορές που απορρέουν από τις εξελίξεις που προβλέπονται σε εθνικό επίπεδο θα μπορούσαν να δημιουργήσουν περαιτέρω φραγμούς για τη λειτουργία της εσωτερικής αγοράς εις βάρος των συμμετεχόντων στην αγορά και της χρηματοοικονομικής σταθερότητας.

(10) Έως τούδε, επειδή οι σχετικές με τους κινδύνους ΤΠΕ διατάξεις έχουν εξεταστεί μόνο μερικώς σε επίπεδο Ένωσης, υπάρχουν κενά ή αλληλεπικαλύψεις σε σημαντικούς τομείς, όπως η αναφορά συμβάντων που σχετίζονται με τις ΤΠΕ και οι δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας, και ασυνέπειες ως αποτέλεσμα αναδυόμενων αποκλινόντων εθνικών κανόνων ή μη αποδοτικής ως προς το κόστος εφαρμογής των αλληλεπικαλυπτόμενων κανόνων. Η κατάσταση αυτή είναι ιδιαίτερα επιζήμια για τους εντατικούς χρήστες ΤΠΕ, όπως ο χρηματοοικονομικός τομέας, δεδομένου ότι οι τεχνολογικοί κίνδυνοι δεν έχουν σύνορα και ο χρηματοοικονομικός τομέας αναπτύσσει τις υπηρεσίες του σε ευρεία διασυνοριακή βάση, τόσο εντός όσο και εκτός της Ένωσης. Οι μεμονωμένες χρηματοοικονομικές οντότητες που δραστηριοποιούνται σε διασυνοριακή βάση ή είναι κάτοχοι πολλών αδειών (π.χ. μια χρηματοοικονομική οντότητα μπορεί να διαθέτει άδεια λειτουργίας τραπεζικού ιδρύματος, επιχείρησης επενδύσεων και ιδρύματος πληρωμών, καθεμία από τις οποίες έχει εκδοθεί από διαφορετική αρμόδια αρχή σε ένα ή περισσότερα κράτη μέλη) βρίσκονται αντιμέτωπες με επιχειρησιακές προκλήσεις διότι καλούνται να αντιμετωπίσουν τους κινδύνους ΤΠΕ και να μετριάσουν τις δυσμενείς επιπτώσεις συμβάντων ΤΠΕ μεμονωμένα και με συνεκτικό και οικονομικά αποδοτικό τρόπο.

(11) Δεδομένου ότι το ενιαίο εγχειρίδιο κανόνων δεν συνοδεύεται από ολοκληρωμένο πλαίσιο για τους κινδύνους ΤΠΕ ή τους λειτουργικούς κινδύνους, απαιτείται περαιτέρω εναρμόνιση των βασικών απαιτήσεων ψηφιακής επιχειρησιακής ανθεκτικότητας για όλες τις χρηματοοικονομικές οντότητες. Η ανάπτυξη ικανοτήτων ΤΠΕ και συνολικής ανθεκτικότητας από τις χρηματοοικονομικές οντότητες, σύμφωνα με τις εν λόγω βασικές απαιτήσεις, με σκοπό την αντιμετώπιση διακοπών λειτουργίας, θα συμβάλει στη διατήρηση της σταθερότητας και της ακεραιότητας των χρηματοοικονομικών αγορών της Ένωσης και, κατ' επέκταση, στη διασφάλιση υψηλού επιπέδου προστασίας των επενδυτών και των καταναλωτών στην Ένωση. Λαμβανομένου υπόψη ότι ο παρών κανονισμός έχει ως στόχο να συμβάλει στην εύρυθμη λειτουργία της εσωτερικής αγοράς, θα πρέπει να βασίζεται στις διατάξεις του άρθρου 114 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ), όπως ερμηνεύονται σύμφωνα με την πάγια νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης (Δικαστήριο).

(12) Ο παρών κανονισμός αποσκοπεί στην ενοποίηση και την αναβάθμιση των απαιτήσεων για τους κινδύνους ΤΠΕ στο πλαίσιο των απαιτήσεων για τους λειτουργικούς κινδύνους, οι οποίες, έως το σημείο αυτό, έχουν εξεταστεί χωριστά σε διάφορες νομικές πράξεις της Ένωσης. Παρότι οι εν λόγω πράξεις κάλυπταν τις κύριες κατηγορίες χρηματοοικονομικών κινδύνων (π. χ. πιστωτικό κίνδυνο, κίνδυνο αγοράς, πιστωτικό κίνδυνο αντισυμβαλλομένου και κίνδυνο ρευστότητας, κίνδυνο συμπεριφοράς της αγοράς), δεν αντιμετώπισαν συνολικά, κατά τον χρόνο έκδοσής τους, όλες τις συνιστώσες της επιχειρησιακής ανθεκτικότητας. Οι κανόνες για λειτουργικούς κινδύνους, όταν αναπτύσσονταν περαιτέρω στις εν λόγω νομικές πράξεις της Ένωσης, ευνοούσαν συχνά την υιοθέτηση παραδοσιακής ποσοτικής προσέγγισης για την αντιμετώπιση του κινδύνου (κυρίως με την πρόβλεψη κεφαλαιακής απαίτησης για την κάλυψη των κινδύνων ΤΠΕ), αντί της έγκρισης

([6]) Κανονισμός (ΕΕ) αριθ. 1095/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Νοεμβρίου 2010, σχετικά με τη σύσταση Ευρωπαϊκής Εποπτικής Αρχής (Ευρωπαϊκή Αρχή Κινητών Αξιών και Αγορών), την τροποποίηση της απόφασης αριθ. 716/2009/ΕΚ και την κατάργηση της απόφασης 2009/77/ΕΚ (ΕΕ L 331 της 15.12.2010, σ. 84).

στοχευμένων ποιοτικών κανόνων για την προστασία, τον εντοπισμό, τον περιορισμό, την αποκατάσταση και την επιδιόρθωση συμβάντων σχετικών με τις ΤΠΕ και για τις ικανότητες αναφοράς και ψηφιακών δοκιμών. Οι εν λόγω πράξεις είχαν ως πρωταρχικό στόχο την κάλυψη και την επικαιροποίηση βασικών κανόνων προληπτικής εποπτείας, ακεραιότητας ή δεοντολογίας της αγοράς. Μέσω της ενοποίησης και της αναβάθμισης των κανόνων σχετικά με τον κίνδυνο ΤΠΕ, όλες οι διατάξεις που αφορούν τον ψηφιακό κίνδυνο στον χρηματοοικονομικό τομέα θα πρέπει να συγκεντρωθούν για πρώτη φορά με συνεκτικό τρόπο σε μια ενιαία νομοθετική πράξη. Κατά συνέπεια, ο παρών κανονισμός καλύπτει τα κενά ή διορθώνει τις ασυνέπειες που παρουσιάζουν ορισμένες από τις πρότερες νομικές πράξεις, μεταξύ άλλων σε σχέση με την ορολογία που χρησιμοποιείται σε αυτές, και αναφέρεται ρητά στους κινδύνους ΤΠΕ μέσω στοχευμένων κανόνων για τις ικανότητες διαχείρισης κινδύνων ΤΠΕ, την αναφορά συμβάντων, τις δοκιμές επιχειρησιακής ανθεκτικότητας και την παρακολούθηση των κινδύνων τρίτων παρόχων ΤΠΕ. Ως εκ τούτου, ο παρών κανονισμός θα πρέπει επίσης να ευαισθητοποιήσει σχετικά με τους κινδύνους ΤΠΕ και να αναγνωρίσει ότι τα συμβάντα ΤΠΕ και η έλλειψη επιχειρησιακής ανθεκτικότητας ενδέχεται να θέσουν σε κίνδυνο την ευρωστία των χρηματοοικονομικών οντοτήτων.

(13) Οι χρηματοοικονομικές οντότητες θα πρέπει να ακολουθούν την ίδια προσέγγιση και τους ίδιους κανόνες βάσει αρχών κατά την αντιμετώπιση των κινδύνων ΤΠΕ, λαμβάνοντας υπόψη το μέγεθός τους και το συνολικό προφίλ κινδύνου τους και τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών τους. Η συνοχή συμβάλλει στην ενίσχυση της εμπιστοσύνης στο χρηματοοικονομικό σύστημα και στη διατήρηση της σταθερότητάς του, ιδίως σε περιόδους υψηλής εξάρτησης από συστήματα, πλατφόρμες και υποδομές ΤΠΕ, η οποία συνεπάγεται αυξημένο ψηφιακό κίνδυνο. Κατά την τήρηση βασικής κυβερνοϋγιεινής θα πρέπει επίσης να αποφεύγεται η επιβολή υψηλών δαπανών στην οικονομία με την ελαχιστοποίηση των επιπτώσεων και του κόστους των διαταραχών ΤΠΕ.

(14) Ένας κανονισμός συμβάλλει στη μείωση της πολυπλοκότητας του κανονιστικού πλαισίου, ενισχύει την εποπτική σύγκλιση και αυξάνει την ασφάλεια δικαίου, ενώ βοηθά επίσης στον περιορισμό του κόστους συμμόρφωσης, ιδίως για τις χρηματοοικονομικές οντότητες που δραστηριοποιούνται διασυνοριακά, καθώς και στη μείωση των στρεβλώσεων του ανταγωνισμού. Ως εκ τούτου, η επιλογή κανονισμού για τη θέσπιση κοινού πλαισίου για την ψηφιακή επιχειρησιακή ανθεκτικότητα των χρηματοοικονομικών οντοτήτων συνιστά τον πλέον κατάλληλο τρόπο για τη διασφάλιση ομοιογενούς και συνεκτικής εφαρμογής όλων των συνιστωσών της διαχείρισης κινδύνων ΤΠΕ από τον χρηματοοικονομικό τομέα της Ένωσης.

(15) Η οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([7]) ήταν το πρώτο οριζόντιο πλαίσιο κυβερνοασφάλειας που θεσπίστηκε σε επίπεδο Ένωσης, το οποίο εφαρμόζεται επίσης σε τρεις τύπους χρηματοοικονομικών οντοτήτων, δηλαδή τα πιστωτικά ιδρύματα, τους τόπους διαπραγμάτευσης και τους κεντρικούς αντισυμβαλλομένους. Ωστόσο, αφότου ότι η οδηγία (ΕΕ) 2016/1148 θέσπισε μηχανισμό προσδιορισμού, σε εθνικό επίπεδο, των φορέων εκμετάλλευσης βασικών υπηρεσιών, μόνο ορισμένα πιστωτικά ιδρύματα, τόποι διαπραγμάτευσης και κεντρικοί αντισυμβαλλόμενοι που προσδιορίστηκαν από τα κράτη μέλη εμπίπτουν πρακτικά στο πεδίο εφαρμογής της και, κατά συνέπεια, υποχρεούνται να συμμορφώνονται με τις απαιτήσεις σχετικά με την ασφάλεια ΤΠΕ και την κοινοποίηση συμβάντων που προβλέπονται σε αυτήν. Η οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([8]) θεσπίζει ενιαίο κριτήριο για τον προσδιορισμό των οντοτήτων που εμπίπτουν στο πεδίο εφαρμογής της (κανόνας για τα ανώτατα όρια μεγέθους), διατηρώντας παράλληλα τους τρεις τύπους χρηματοοικονομικών οντοτήτων στο πεδίο εφαρμογής της.

(16) Ωστόσο, λαμβανομένου υπόψη ότι ο παρών κανονισμός αυξάνει το επίπεδο εναρμόνισης των διάφορων συνιστωσών ψηφιακής ανθεκτικότητας, με τη θέσπιση απαιτήσεων σχετικά με τη διαχείριση κινδύνων ΤΠΕ και την αναφορά συμβάντων που σχετίζονται με τις ΤΠΕ, οι οποίες είναι αυστηρότερες σε σύγκριση με τις απαιτήσεις που προβλέπονται στην ισχύουσα νομοθεσία της Ένωσης για τις χρηματοοικονομικές υπηρεσίες, αυτό το υψηλότερο επίπεδο συνιστά αυξημένη εναρμόνιση σε σύγκριση με τις απαιτήσεις που καθορίζονται στην οδηγία (ΕΕ) 2022/2555 Συνεπώς, ο παρών κανονισμός συνιστά lex specialis ως προς την οδηγία (ΕΕ) 2022/2555 Ταυτόχρονα, είναι καίριας σημασίας να διατηρηθεί ισχυρή σχέση μεταξύ του χρηματοοικονομικού τομέα και του οριζόντιου πλαισίου της Ένωσης για την κυβερνοασφάλεια, όπως ορίζεται επί του παρόντος στην οδηγία (ΕΕ) 2022/2555 ώστε να διασφαλιστεί η συνοχή με τις στρατηγικές κυβερνοασφάλειας που έχουν θεσπίσει τα κράτη μέλη και να εξασφαλιστεί η δυνατότητα ενημέρωσης των αρχών χρηματοοικονομικής εποπτείας για κυβερνοπεριστατικά τα οποία έχουν αντίκτυπο σε άλλους τομείς που καλύπτονται από την εν λόγω οδηγία.

([7]) Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση (ΕΕ L 194 της 19.7.2016, σ. 1).

([8]) Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972 και την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2) (βλέπε σελίδα 80 της παρούσας Επίσημης Εφημερίδας).

(17) Σύμφωνα με το άρθρο 4 παράγραφος 2 της Συνθήκης για την Ευρωπαϊκή Ένωση και με την επιφύλαξη του δικαστικού ελέγχου από το Δικαστήριο, ο παρών κανονισμός δεν θα πρέπει να θίγει την ευθύνη των κρατών μελών όσον αφορά τις ουσιώδεις λειτουργίες του κράτους που αφορούν τη δημόσια ασφάλεια, την άμυνα και την προστασία της εθνικής ασφάλειας, για παράδειγμα όσον αφορά την παροχή πληροφοριών που θα ήταν αντίθετες προς την προστασία της εθνικής ασφάλειας.

(18) Για να καταστεί δυνατή η διατομεακή μάθηση και να αξιοποιηθούν αποτελεσματικά οι εμπειρίες από άλλους τομείς όσον αφορά την αντιμετώπιση κυβερνοαπειλών, οι χρηματοοικονομικές οντότητες που αναφέρονται στην οδηγία (ΕΕ) 2022/2555 θα πρέπει να εξακολουθήσουν να αποτελούν μέρος του «οικοσυστήματος» της εν λόγω οδηγίας (επί παραδείγματι, ομάδα συνεργασίας και ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (CSIRT)). Οι ΕΕΑ και οι εθνικές αρμόδιες αρχές θα πρέπει να είναι σε θέση να συμμετέχουν στις συζητήσεις στρατηγικής πολιτικής και στις τεχνικές εργασίες της ομάδας συνεργασίας βάσει της εν λόγω οδηγίας και να ανταλλάσσουν πληροφορίες και να συνεργάζονται περαιτέρω με τα ενιαία κέντρα επαφής που ορίζονται ή συστήνονται σύμφωνα με την εν λόγω οδηγία. Οι αρμόδιες αρχές δυνάμει του παρόντος κανονισμού θα πρέπει επίσης να διαβουλεύονται και να συνεργάζονται με τις CSIRT. Οι αρμόδιες αρχές θα πρέπει επίσης να μπορούν να ζητούν τεχνικές συμβουλές από τις αρμόδιες αρχές που ορίζονται ή συστήνονται σύμφωνα με την οδηγία (ΕΕ) 2022/2555 και να θεσπίζουν ρυθμίσεις συνεργασίας που αποσκοπούν στη διασφάλιση αποτελεσματικών μηχανισμών συντονισμού ταχείας απόκρισης.

(19) Δεδομένων των ισχυρών διασυνδέσεων μεταξύ της ψηφιακής ανθεκτικότητας και της υλικής ανθεκτικότητας των χρηματοοικονομικών οντοτήτων, είναι αναγκαία μια συνεκτική προσέγγιση όσον αφορά την ανθεκτικότητα των κρίσιμων οντοτήτων στον παρόντα κανονισμό και στην οδηγία (ΕΕ) 2022/2557 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([9]). Δεδομένου ότι η υλική ανθεκτικότητα των χρηματοοικονομικών οντοτήτων αντιμετωπίζεται με ολοκληρωμένο τρόπο από τις υποχρεώσεις διαχείρισης και αναφοράς κινδύνων ΤΠΕ που καλύπτονται από τον παρόντα κανονισμό, οι υποχρεώσεις που ορίζονται στα κεφάλαια III και IV της οδηγίας (ΕΕ) 2022/2557 δεν θα πρέπει να εφαρμόζονται στις χρηματοοικονομικές οντότητες που εμπίπτουν στο πεδίο εφαρμογής της εν λόγω οδηγίας.

(20) Οι πάροχοι υπηρεσιών υπολογιστικού νέφους αποτελούν μία κατηγορία υποδομών που καλύπτονται από την οδηγία (ΕΕ) 2022/2555 Το ενωσιακό πλαίσιο εποπτείας («πλαίσιο εποπτείας») που θεσπίζεται με τον παρόντα κανονισμό εφαρμόζεται σε όλους τους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, συμπεριλαμβανομένων των παρόχων υπηρεσιών υπολογιστικού νέφους, όταν παρέχουν υπηρεσίες ΤΠΕ σε χρηματοοικονομικές οντότητες, και θα πρέπει να θεωρείται συμπληρωματικό της εποπτείας δυνάμει της οδηγίας (ΕΕ) 2022/2555.Επιπλέον, το πλαίσιο εποπτείας που θεσπίζεται με τον παρόντα κανονισμό θα πρέπει να καλύπτει τους παρόχους υπηρεσιών υπολογιστικού νέφους ελλείψει ενωσιακού οριζόντιου πλαισίου για τη σύσταση αρχής ψηφιακής εποπτείας.

(21) Προκειμένου να διατηρηθεί ο πλήρης έλεγχος των κινδύνων ΤΠΕ, οι χρηματοοικονομικές οντότητες χρειάζεται να διαθέτουν ολοκληρωμένες ικανότητες που να επιτρέπουν την αυστηρή και αποτελεσματική διαχείριση κινδύνων ΤΠΕ, παράλληλα με ειδικούς μηχανισμούς και πολιτικές για τον χειρισμό όλων των συμβάντων που σχετίζονται με τις ΤΠΕ και για την αναφορά μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ. Ομοίως, οι χρηματοοικονομικές οντότητες θα πρέπει να εφαρμόζουν πολιτικές για τη δοκιμή συστημάτων, δικλείδων ασφάλειας και διαδικασιών ΤΠΕ, καθώς και για τη διαχείριση των κινδύνων τρίτων παρόχων ΤΠΕ. Η βάση αναφοράς για το επίπεδο ψηφιακής επιχειρησιακής ανθεκτικότητας για τις χρηματοοικονομικές οντότητες θα πρέπει να αυξηθεί, επιτρέποντας παράλληλα αναλογική εφαρμογή των απαιτήσεων για ορισμένες χρηματοοικονομικές οντότητες, ιδίως για τις πολύ μικρές επιχειρήσεις, καθώς και για τις χρηματοοικονομικές οντότητες που υπόκεινται σε απλουστευμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ. Για να διευκολυνθεί η αποτελεσματική εποπτεία των ιδρυμάτων επαγγελματικών συνταξιοδοτικών παροχών που είναι αναλογική και ανταποκρίνεται στην ανάγκη μείωσης του διοικητικού φόρτου για τις αρμόδιες αρχές, οι σχετικές εθνικές εποπτικές ρυθμίσεις όσον αφορά τις εν λόγω χρηματοοικονομικές οντότητες θα πρέπει να λαμβάνουν υπόψη το μέγεθος και το συνολικό προφίλ κινδύνου τους και τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών τους, ακόμη και όταν σημειώνεται υπέρβαση των σχετικών κατώτατων ορίων που καθορίζονται στο άρθρο 5 της οδηγίας (ΕΕ) 2016/2341 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([10]). Ειδικότερα, οι εποπτικές δραστηριότητες θα πρέπει να επικεντρώνονται πρωτίστως στην ανάγκη αντιμετώπισης σοβαρών κινδύνων που συνδέονται με τη διαχείριση κινδύνων ΤΠΕ συγκεκριμένης οντότητας.

([9]) Οδηγία (ΕΕ) 2022/2557 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ανθεκτικότητα των κρίσιμων οντοτήτων και την κατάργηση της οδηγίας 2008/114/ΕΚ (βλέπε σελίδα 164 της παρούσας Επίσημης Εφημερίδας).

([10]) Οδηγία (ΕΕ) 2016/2341 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2016, για τις δραστηριότητες και την εποπτεία των ιδρυμάτων επαγγελματικών συνταξιοδοτικών παροχών (ΙΕΣΠ) (ΕΕ L 354 της 23.12.2016, σ. 37).

Οι αρμόδιες αρχές θα πρέπει επίσης να διατηρούν μια προσέγγιση επαγρύπνησης, αλλά αναλογική, σε σχέση με την εποπτεία των ιδρυμάτων επαγγελματικών συνταξιοδοτικών παροχών τα οποία, σύμφωνα με το άρθρο 31 της οδηγίας (ΕΕ) 2016/2341, αναθέτουν σε παρόχους υπηρεσιών σημαντικό μέρος των βασικών δραστηριοτήτων τους, όπως η διαχείριση περιουσιακών στοιχείων, οι αναλογιστικοί υπολογισμοί, η λογιστική και η διαχείριση δεδομένων.

(22) Τα κατώτατα όρια αναφοράς συμβάντων και οι ταξινομήσεις που σχετίζονται με τις ΤΠΕ παρουσιάζουν σημαντικές διαφοροποιήσεις σε εθνικό επίπεδο. Μολονότι μπορεί να επιτευχθεί κοινή βάση μέσω των σχετικών εργασιών που έχουν αναλάβει ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) που συστάθηκε με τον κανονισμό (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([11]) και η ομάδα συνεργασίας δυνάμει της οδηγίας (ΕΕ) 2022/2555 όσον αφορά τον καθορισμό κατώτατων ορίων και τη χρήση ταξινομήσεων εξακολουθούν να υπάρχουν αποκλίνουσες προσεγγίσεις ή μπορεί να προκύψουν για τις υπόλοιπες χρηματοοικονομικές οντότητες. Λόγω των εν λόγω αποκλίσεων, υπάρχουν πολλαπλές απαιτήσεις τις οποίες πρέπει να τηρούν οι χρηματοοικονομικές οντότητες, ιδίως όταν δραστηριοποιούνται σε διάφορα κράτη μέλη και όταν ανήκουν σε χρηματοοικονομικό όμιλο. Επιπλέον, οι αποκλίσεις αυτές θα μπορούσαν να παρεμποδίσουν τη δημιουργία περαιτέρω ενιαίων ή κεντρικών μηχανισμών της Ένωσης για την επιτάχυνση της διαδικασίας αναφορών και την υποστήριξη της ταχείας και ομαλής ανταλλαγής πληροφοριών μεταξύ των αρμόδιων αρχών, η οποία είναι καίριας σημασίας για την αντιμετώπιση των κινδύνων ΤΠΕ σε περίπτωση επιθέσεων μεγάλης κλίμακας με δυνητικά συστημικές συνέπειες.

(23) Για να μειωθούν ο διοικητικός φόρτος και οι ενδεχομένως αλληλεπικαλυπτόμενες υποχρεώσεις αναφοράς για ορισμένες χρηματοοικονομικές οντότητες, η απαίτηση για την αναφορά συμβάντων σύμφωνα με την οδηγία (ΕΕ) 2015/2366 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([12]) θα πρέπει να παύσει να ισχύει για τους παρόχους υπηρεσιών πληρωμών που εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού. Κατά συνέπεια, τα πιστωτικά ιδρύματα, τα ιδρύματα ηλεκτρονικού χρήματος, τα ιδρύματα πληρωμών και οι πάροχοι υπηρεσιών πληροφοριών λογαριασμού, όπως αναφέρονται στο άρθρο 33 παράγραφος 1 της εν λόγω οδηγίας, θα πρέπει από την ημερομηνία εφαρμογής του παρόντος κανονισμού να αναφέρουν, σύμφωνα με τον παρόντα κανονισμό, όλα τα λειτουργικά συμβάντα ή συμβάντα ασφάλειας που σχετίζονται με πληρωμές και τα οποία έχουν αναφερθεί προηγουμένως δυνάμει της εν λόγω οδηγίας, ανεξάρτητα αν τα εν λόγω συμβάντα σχετίζονται με τις ΤΠΕ.

(24) Προκειμένου οι αρμόδιες αρχές να είναι σε θέση να επιτελούν τους εποπτικούς ρόλους, αποκτώντας ολοκληρωμένη εικόνα ως προς τη φύση, τη συχνότητα, τη σημασία και τις επιπτώσεις των συμβάντων που σχετίζονται με τις ΤΠΕ, και να προωθούν την ανταλλαγή πληροφοριών μεταξύ των αρμόδιων δημόσιων αρχών, συμπεριλαμβανομένων των αρχών επιβολής του νόμου και των αρχών εξυγίανσης, ο παρών κανονισμός θα πρέπει να θεσπίσει ισχυρό καθεστώς αναφοράς συμβάντων που σχετίζονται με τις ΤΠΕ σύμφωνα με το οποίο οι σχετικές απαιτήσεις αντιμετωπίζουν τα σημερινά κενά του δικαίου για τις χρηματοοικονομικές υπηρεσίες και θα εξαλείψουν τις υφιστάμενες αλληλεπικαλύψεις και επαναλήψεις για την ελάφρυνση του κόστους. Είναι σημαντικό να διασφαλιστεί η εναρμόνιση του καθεστώτος αναφοράς συμβάντων που σχετίζονται με τις ΤΠΕ με την επιβολή της υποχρέωσης σε όλες τις χρηματοοικονομικές οντότητες να αναφέρουν συμβάντα στις οικείες αρμόδιες αρχές μέσω ενός ενιαίου εξορθολογισμένου πλαισίου, όπως ορίζεται στον παρόντα κανονισμό. Επιπροσθέτως, οι ΕΕΑ θα πρέπει να έχουν την αρμοδιότητα να προσδιορίζουν περαιτέρω σχετικά στοιχεία για το πλαίσιο αναφοράς συμβάντων που σχετίζονται με τις ΤΠΕ, όπως η ταξινόμηση, τα χρονοδιαγράμματα, τα σύνολα δεδομένων, τα υποδείγματα και τα εφαρμοστέα κατώτατα όρια. Προκειμένου να διασφαλιστεί πλήρης συμμόρφωση με την οδηγία (ΕΕ) 2022/2555 οι χρηματοοικονομικές οντότητες θα πρέπει να μπορούν, σε προαιρετική βάση, να γνωστοποιούν σημαντικές κυβερνοαπειλές στη σχετική αρμόδια αρχή, όταν θεωρούν ότι η απειλή είναι σημαντική για το χρηματοοικονομικό σύστημα, τους χρήστες υπηρεσιών ή τους πελάτες.

(25) Σε ορισμένους χρηματοοικονομικούς υποτομείς έχουν αναπτυχθεί απαιτήσεις δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας που καθορίζουν πλαίσια τα οποία δεν είναι πάντοτε πλήρως ευθυγραμμισμένα. Αυτό οδηγεί σε πιθανή αλληλεπικάλυψη του κόστους για τις διασυνοριακές χρηματοοικονομικές οντότητες και καθιστά περίπλοκη την αμοιβαία αναγνώριση των αποτελεσμάτων των δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας, η οποία, με τη σειρά της, μπορεί να κατακερματίσει την εσωτερική αγορά.

([11]) Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια) (ΕΕ L 151 της 7.6.2019, σ. 15).

([12]) Οδηγία (ΕΕ) 2015/2366 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2015, σχετικά με υπηρεσίες πληρωμών στην εσωτερική αγορά, την τροποποίηση των οδηγιών 2002/65/ΕΚ, 2009/110/ΕΚ και 2013/36/ΕΕ και του κανονισμού (ΕΕ) αριθ. 1093/2010 και την κατάργηση της οδηγίας 2007/64/ΕΚ (ΕΕ L 337 της 23.12.2015, σ. 35).

(26) Επιπλέον, όταν δεν απαιτούνται δοκιμές ΤΠΕ, οι ευπάθειες εξακολουθούν να μην εντοπίζονται, με αποτέλεσμα να εκθέτουν σε κινδύνους ΤΠΕ μια χρηματοοικονομική οντότητα και, εντέλει, να προκαλούν υψηλότερο κίνδυνο για τη σταθερότητα και την ακεραιότητα του χρηματοοικονομικού τομέα. Χωρίς την παρέμβαση της Ένωσης, οι δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας θα εξακολουθήσουν να είναι ανομοιογενείς και δεν θα περιλαμβάνουν σύστημα αμοιβαίας αναγνώρισης των αποτελεσμάτων των δοκιμών ΤΠΕ σε διάφορες δικαιοδοσίες. Επιπρόσθετα, λαμβανομένου υπόψη ότι είναι απίθανο άλλοι χρηματοοικονομικοί υποτομείς να υιοθετήσουν συστήματα δοκιμών σε ουσιαστική κλίμακα, θα χάσουν τα δυνητικά οφέλη πλαισίου δοκιμών, όσον αφορά την αποκάλυψη ευπαθειών και κινδύνων ΤΠΕ και τις δοκιμές των ικανοτήτων άμυνας και της επιχειρησιακής συνέχειας, που συμβάλλει στην αύξηση της εμπιστοσύνης των πελατών, των προμηθευτών και των επιχειρηματικών εταίρων. Για τη διόρθωση αυτών των αλληλεπικαλύψεων, αποκλίσεων και κενών, είναι απαραίτητο να θεσπιστούν κανόνες για ένα συντονισμένο καθεστώς δοκιμών και, με τον τρόπο αυτό, να διευκολυνθεί η αμοιβαία αναγνώριση των προηγμένων δοκιμών για χρηματοοικονομικές οντότητες που πληρούν τα κριτήρια που καθορίζονται στον παρόντα κανονισμό.

(27) Η στήριξη των χρηματοοικονομικών οντοτήτων στη χρήση υπηρεσιών ΤΠΕ οφείλεται εν μέρει στην ανάγκη προσαρμογής τους σε μια αναδυόμενη ανταγωνιστική ψηφιακή παγκόσμια οικονομία, με σκοπό την ενίσχυση της επιχειρηματικής τους απόδοσης και την κάλυψη της ζήτησης των καταναλωτών. Η φύση και η έκταση της στήριξης αυτής εξελίσσονται διαρκώς κατά τα πρόσφατα έτη, με αποτέλεσμα τη μείωση του κόστους της χρηματοοικονομικής διαμεσολάβησης, την εξασφάλιση της δυνατότητας επέκτασης των επιχειρήσεων και κλιμάκωσης όσον αφορά την ανάπτυξη χρηματοοικονομικών δραστηριοτήτων, ενώ προσφέρεται παράλληλα ευρύ φάσμα εργαλείων ΤΠΕ για τη διαχείριση πολύπλοκων εσωτερικών διαδικασιών.

(28) Η εκτεταμένη χρήση υπηρεσιών ΤΠΕ αποδεικνύεται από πολύπλοκες συμβατικές ρυθμίσεις, στο πλαίσιο των οποίων οι χρηματοοικονομικές οντότητες αντιμετωπίζουν συχνά δυσκολίες στη διαπραγμάτευση συμβατικών όρων που είναι προσαρμοσμένοι στα πρότυπα προληπτικής εποπτείας ή σε άλλες ρυθμιστικές απαιτήσεις στις οποίες υπόκεινται ή με άλλον τρόπο στην άσκηση συγκεκριμένων δικαιωμάτων, όπως δικαιώματα πρόσβασης ή ελέγχου, ακόμη και σε περίπτωση που τα δικαιώματα αυτά κατοχυρώνονται στις συμβατικές ρυθμίσεις τους. Επιπλέον, πολλές από τις εν λόγω συμβατικές ρυθμίσεις δεν προβλέπουν επαρκείς διασφαλίσεις που να επιτρέπουν την πλήρη παρακολούθηση των διαδικασιών υπεργολαβίας, στερώντας με τον τρόπο αυτόν από τη χρηματοοικονομική οντότητα την ικανότητά της να αξιολογεί τους συναφείς κινδύνους. Επιπροσθέτως, λαμβανομένου υπόψη ότι οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ παρέχουν συχνά τυποποιημένες υπηρεσίες σε διαφορετικούς τύπους πελατών, οι συμβατικές ρυθμίσεις αυτού του είδους ενδέχεται να μην ανταποκρίνονται πάντα επαρκώς στις επιμέρους ή ειδικές ανάγκες των παραγόντων του χρηματοοικονομικού κλάδου.

(29) Μολονότι το δίκαιο της Ένωσης για τις χρηματοοικονομικές υπηρεσίες περιλαμβάνει ορισμένους γενικούς κανόνες για την εξωτερική ανάθεση, η παρακολούθηση της συμβατικής διάστασης δεν θεμελιώνεται πλήρως στο δίκαιο της Ένωσης. Ελλείψει της εφαρμογής σαφών και εξειδικευμένων ενωσιακών προτύπων στις συμβατικές ρυθμίσεις που συνάπτονται με τρίτους παρόχους υπηρεσιών ΤΠΕ, η εξωτερική πηγή κινδύνων ΤΠΕ δεν αντιμετωπίζεται με ολοκληρωμένο τρόπο. Ως εκ τούτου, είναι απαραίτητο να καθοριστούν ορισμένες βασικές αρχές για την καθοδήγηση της διαχείρισης των κινδύνων τρίτων παρόχων ΤΠΕ από τις χρηματοοικονομικές οντότητες, οι οποίες είναι ιδιαίτερα σημαντικές όταν οι χρηματοοικονομικές οντότητες καταφεύγουν σε τρίτους παρόχους υπηρεσιών ΤΠΕ για την υποστήριξη των κρίσιμων ή σημαντικών λειτουργιών τους. Οι εν λόγω αρχές θα πρέπει να συνοδεύονται από ένα σύνολο βασικών συμβατικών δικαιωμάτων σε σχέση με διάφορα στοιχεία της εκτέλεσης και της καταγγελίας των συμβατικών ρυθμίσεων, με σκοπό την παροχή ορισμένων ελάχιστων διασφαλίσεων προκειμένου να ενισχύουν την ικανότητα των χρηματοοικονομικών οντοτήτων να παρακολουθούν αποτελεσματικά όλους τους κινδύνους ΤΠΕ που ανακύπτουν σε επίπεδο τρίτων παρόχων υπηρεσιών. Οι εν λόγω αρχές είναι συμπληρωματικές προς το τομεακό δίκαιο που διέπει την εξωτερική ανάθεση.

(30) Σήμερα είναι προφανής μια ορισμένη έλλειψη ομοιογένειας και σύγκλισης όσον αφορά την παρακολούθηση των κινδύνων τρίτων παρόχων ΤΠΕ και των εξαρτήσεων από τρίτους παρόχους ΤΠΕ. Παρά την καταβολή προσπαθειών για την αντιμετώπιση της εξωτερικής ανάθεσης, όπως οι κατευθυντήριες γραμμές της ΕΑΤ του 2019 και οι κατευθυντήριες γραμμές της ΕΑΚΑΑ του 2021 για την εξωτερική ανάθεση σε παρόχους υπηρεσιών υπολογιστικού νέφους, το ευρύτερο ζήτημα της καταπολέμησης του συστημικού κινδύνου που ενδέχεται να ανακύψει από την έκθεση του χρηματοοικονομικού τομέα σε περιορισμένο αριθμό κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ δεν αντιμετωπίζεται επαρκώς από το ενωσιακό δίκαιο. Η έλλειψη κανόνων σε επίπεδο Ένωσης επιδεινώνεται από την απουσία εθνικών κανόνων περί ειδικών εντολών και εργαλείων που επιτρέπουν στις αρχές χρηματοοικονομικής εποπτείας να κατανοούν δεόντως τις εξαρτήσεις από τρίτους παρόχους ΤΠΕ και να παρακολουθούν επαρκώς τους κινδύνους που ανακύπτουν λόγω της συγκέντρωσης εξαρτήσεων από τρίτους παρόχους ΤΠΕ.

(31) Λαμβανομένου υπόψη του δυνητικού συστημικού κινδύνου που συνεπάγεται η αύξηση των πρακτικών εξωτερικής ανάθεσης και η συγκέντρωση τρίτων παρόχων ΤΠΕ και έχοντας επίγνωση της ανεπάρκειας εθνικών μηχανισμών να παρέχουν στις αρχές χρηματοοικονομικής εποπτείας τα κατάλληλα εργαλεία για τη δυνατότητα ποσοτικού προσδιορισμού, χαρακτηρισμού και αποκατάστασης των επιπτώσεων των κινδύνων ΤΠΕ που αφορούν κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, είναι απαραίτητο να θεσπιστεί κατάλληλο πλαίσιο εποπτείας, το οποίο θα επιτρέπει τη διαρκή παρακολούθηση των δραστηριοτήτων τρίτων παρόχων υπηρεσιών ΤΠΕ που είναι κρίσιμοι πάροχοι υπηρεσιών ΤΠΕ σε χρηματοοικονομικές οντότητες, διασφαλίζοντας, παράλληλα, τη διατήρηση της εμπιστευτικότητας και της ασφάλειας των πελατών, πλην των χρηματοοικονομικών οντοτήτων. Ενώ η ενδοομιλική παροχή υπηρεσιών ΤΠΕ συνεπάγεται ειδικούς κινδύνους και οφέλη, δεν θα πρέπει να θεωρείται αυτομάτως λιγότερο επικίνδυνη από την παροχή υπηρεσιών ΤΠΕ από παρόχους εκτός χρηματοοικονομικού ομίλου και, ως εκ τούτου, θα πρέπει να υπόκειται στο ίδιο ρυθμιστικό πλαίσιο. Ωστόσο, όταν οι υπηρεσίες ΤΠΕ παρέχονται από τον ίδιο χρηματοοικονομικό όμιλο, οι χρηματοοικονομικές οντότητες ενδέχεται να έχουν υψηλότερο επίπεδο ελέγχου επί των ενδοομιλικών παρόχων, το οποίο θα πρέπει να λαμβάνεται υπόψη στη συνολική εκτίμηση κινδύνου.

(32) Καθώς οι κίνδυνοι ΤΠΕ εξελίσσονται και περιπλέκονται ολοένα και πιο πολύ, τα καλά μέτρα για τον εντοπισμό και την πρόληψη των κινδύνων ΤΠΕ εξαρτώνται σε μεγάλο βαθμό από την τακτική ανταλλαγή πληροφοριών σχετικά με απειλές και ευπάθειες μεταξύ των χρηματοοικονομικών οντοτήτων. Η ανταλλαγή πληροφοριών συμβάλλει στην αύξηση της ευαισθητοποίησης σχετικά με τις κυβερνοαπειλές. Αυτό με τη σειρά του ενισχύει την ικανότητα των χρηματοοικονομικών οντοτήτων να αποτρέπουν τη μετατροπή απειλών σε πραγματικά συμβάντα που σχετίζονται με τις ΤΠΕ και παρέχει στις χρηματοοικονομικές οντότητες τη δυνατότητα να περιορίζουν αποτελεσματικότερα τις επιπτώσεις των συμβάντων που σχετίζονται με τις ΤΠΕ και να ανακάμπτουν ταχύτερα. Ελλείψει καθοδήγησης σε επίπεδο Ένωσης, φαίνεται ότι η παρεμπόδιση της ανταλλαγής στοιχείων αυτού του είδους οφείλεται σε διάφορους παράγοντες, κυρίως στην αβεβαιότητα ως προς τη συμβατότητα με τους κανόνες προστασίας δεδομένων, τους αντιμονοπωλιακούς κανόνες και τους κανόνες περί ευθύνης.

(33) Επιπροσθέτως, οι αμφιβολίες ως προς το είδος των πληροφοριών που μπορούν να γνωστοποιούνται σε άλλους συμμετέχοντες στην αγορά ή σε μη εποπτικές αρχές (όπως ο ENISA, για σκοπούς ανάλυσης, ή η Ευρωπόλ, για σκοπούς επιβολής του νόμου) έχουν ως αποτέλεσμα την απόκρυψη χρήσιμων πληροφοριών. Κατά συνέπεια, η έκταση και η ποιότητα της ανταλλαγής πληροφοριών παραμένει επί του παρόντος περιορισμένη και κατακερματισμένη, με την πραγματοποίηση των σχετικών ανταλλαγών κυρίως σε τοπικό επίπεδο (μέσω εθνικών πρωτοβουλιών) και χωρίς συνεκτικές ρυθμίσεις, σε επίπεδο Ένωσης, για την ανταλλαγή πληροφοριών κατάλληλα προσαρμοσμένων στις ανάγκες ενός ενοποιημένου χρηματοοικονομικού συστήματος. Ως εκ τούτου, είναι σημαντικό να ενισχυθούν αυτοί οι δίαυλοι επικοινωνίας.

(34) Οι χρηματοοικονομικές οντότητες θα πρέπει να ενθαρρύνονται να ανταλλάσσουν μεταξύ τους πληροφορίες και στοιχεία περί κυβερνοαπειλών και να αξιοποιούν συλλογικά τις επιμέρους γνώσεις και την πρακτική εμπειρία που διαθέτουν σε στρατηγικό, τακτικό και επιχειρησιακό επίπεδο, με σκοπό την ενίσχυση των ικανοτήτων τους, ώστε να είναι σε θέση να αξιολογούν, να παρακολουθούν, να υπερασπίζονται και να αντιμετωπίζουν δεόντως κυβερνοαπειλές, συμμετέχοντας σε ρυθμίσεις ανταλλαγής πληροφοριών. Ως εκ τούτου, είναι απαραίτητο να καταστεί δυνατή η δημιουργία, σε επίπεδο Ένωσης, μηχανισμών για τη θέσπιση προαιρετικών ρυθμίσεων ανταλλαγής πληροφοριών, οι οποίοι, όταν θα εφαρμόζονται σε αξιόπιστο περιβάλλον, θα διευκολύνουν την κοινότητα του χρηματοοικονομικού κλάδου να αποτρέπει απειλές και να αντιδρά συλλογικά σε αυτές, περιορίζοντας ταχέως την εξάπλωση των κινδύνων ΤΠΕ και εμποδίζοντας την πιθανή μετάδοσή τους σε όλους τους χρηματοοικονομικούς διαύλους. Οι εν λόγω μηχανισμοί θα πρέπει να συμμορφώνονται με τους ισχύοντες κανόνες του ενωσιακού δικαίου περί ανταγωνισμού που ορίζονται στην ανακοίνωση της Επιτροπής, της 14ης Ιανουαρίου 2011, με τίτλο «Κατευθυντήριες γραμμές για την εφαρμογή του άρθρου 101 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης στις συμφωνίες οριζόντιας συνεργασίας», καθώς και με τους κανόνες της Ένωσης για την προστασία των δεδομένων, ιδίως με τον κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([13]). Θα πρέπει να λειτουργούν με βάση τη χρήση μίας ή περισσότερων από τις νομικές βάσεις που ορίζονται στο άρθρο 6 του εν λόγω κανονισμού, όπως στο πλαίσιο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα που είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, όπως αναφέρεται στο άρθρο 6 παράγραφος 1 στοιχείο στ) του εν λόγω κανονισμού, καθώς και στο πλαίσιο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα που είναι απαραίτητη για τη συμμόρφωση προς νομική υποχρέωση στην οποία υπόκειται ο υπεύθυνος επεξεργασίας, αναγκαία για την εκπλήρωση καθήκοντος το οποίο εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας, όπως αναφέρεται στο άρθρο 6 παράγραφος 1 στοιχεία γ) και ε), αντίστοιχα, του εν λόγω κανονισμού.

([13]) Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (ΕΕ L 119 της 4.5.2016, σ. 1).

(35) Προκειμένου ολόκληρος ο χρηματοοικονομικός τομέας να διατηρεί υψηλό επίπεδο ψηφιακής επιχειρησιακής ανθεκτικότητας και ταυτόχρονα να συμβαδίζει με τις τεχνολογικές εξελίξεις, ο παρών κανονισμός θα πρέπει να αντιμετωπίζει τους κινδύνους που απορρέουν από όλα τα είδη υπηρεσιών ΤΠΕ. Για τον σκοπό αυτόν, ο ορισμός των υπηρεσιών ΤΠΕ στο πλαίσιο του παρόντος κανονισμού θα πρέπει να ερμηνεύεται ευρέως, περιλαμβάνοντας τις ψηφιακές υπηρεσίες και τις υπηρεσίες δεδομένων που παρέχονται μέσω συστημάτων ΤΠΕ σε έναν ή περισσότερους εσωτερικούς ή εξωτερικούς χρήστες σε συνεχή βάση. Ο εν λόγω ορισμός θα πρέπει, για παράδειγμα, να περιλαμβάνει τις λεγόμενες «επιφυείς (over the top)» υπηρεσίες, οι οποίες εμπίπτουν στην κατηγορία των υπηρεσιών ηλεκτρονικών επικοινωνιών. Θα πρέπει να εξαιρεθεί μόνο η περιορισμένη κατηγορία παραδοσιακών αναλογικών τηλεφωνικών υπηρεσιών που χαρακτηρίζονται ως υπηρεσίες δημόσιου τηλεφωνικού δικτύου μεταγωγής (PSTN), υπηρεσίες επίγειου δικτύου, απλές παλιές τηλεφωνικές υπηρεσίες (POTS) ή υπηρεσίες σταθερής τηλεφωνίας.

(36) Παρά την ευρεία κάλυψη που επιδιώκεται με τον παρόντα κανονισμό, η εφαρμογή των κανόνων για την ψηφιακή επιχειρησιακή ανθεκτικότητα θα πρέπει να λαμβάνει υπόψη τις σημαντικές διαφορές μεταξύ των χρηματοοικονομικών οντοτήτων όσον αφορά το μέγεθος και το συνολικό προφίλ κινδύνου τους. Ως γενική αρχή, κατά την κατανομή πόρων και ικανοτήτων για την εφαρμογή του πλαισίου διαχείρισης κινδύνων ΤΠΕ, οι χρηματοοικονομικές οντότητες θα πρέπει να εξισορροπούν δεόντως τις σχετικές με τις ΤΠΕ ανάγκες τους με το μέγεθος και το συνολικό προφίλ κινδύνου των χρηματοοικονομικών οντοτήτων και τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών τους, ενώ οι αρμόδιες αρχές θα πρέπει να συνεχίσουν να αξιολογούν και να επανεξετάζουν την προσέγγιση της εν λόγω κατανομής.

(37) Οι πάροχοι υπηρεσιών πληροφοριών λογαριασμού, οι οποίοι αναφέρονται στο άρθρο 33 παράγραφος 1 της οδηγίας (ΕΕ) 2015/2366, περιλαμβάνονται ρητά στο πεδίο εφαρμογής του παρόντος κανονισμού, λαμβανομένων υπόψη της ιδιαίτερης φύσης των δραστηριοτήτων τους και των κινδύνων που απορρέουν από αυτές. Επιπλέον, τα ιδρύματα ηλεκτρονικού χρήματος και τα ιδρύματα πληρωμών που εξαιρούνται δυνάμει του άρθρου 9 παράγραφος 1 της οδηγίας 2009/110/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([14]) και του άρθρου 32 παράγραφος 1 της οδηγίας (ΕΕ) 2015/2366 περιλαμβάνονται στο πεδίο εφαρμογής του παρόντος κανονισμού, ακόμη και αν δεν τους έχει χορηγηθεί άδεια σύμφωνα με την οδηγία 2009/110/ΕΚ για την έκδοση ηλεκτρονικού χρήματος ή δεν τους έχει χορηγηθεί άδεια σύμφωνα με την οδηγία (ΕΕ) 2015/2366 για την παροχή και την εκτέλεση υπηρεσιών πληρωμών. Ωστόσο, τα γραφεία ταχυδρομικών επιταγών, που αναφέρονται στο άρθρο 2 παράγραφος 5 σημείο 3) της οδηγίας 2013/36/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([15]), εξαιρούνται από το πεδίο εφαρμογής του παρόντος κανονισμού. Η αρμόδια αρχή για τα ιδρύματα πληρωμών, τα οποία εξαιρούνται δυνάμει της οδηγίας (ΕΕ) 2015/2366, τα ιδρύματα ηλεκτρονικού χρήματος, τα οποία εξαιρούνται δυνάμει της οδηγίας 2009/110/ΕΚ, και τους παρόχους υπηρεσιών πληροφοριών λογαριασμού, όπως αναφέρονται στο άρθρο 33 παράγραφος 1 της οδηγίας (ΕΕ) 2015/2366, θα πρέπει να είναι η αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 22 της οδηγίας (ΕΕ) 2015/2366.

(38) Δεδομένου ότι οι μεγαλύτερες χρηματοοικονομικές οντότητες ενδέχεται να διαθέτουν ευρύτερους πόρους και μπορούν να κινητοποιούν άμεσα κεφάλαια για την ανάπτυξη δομών διακυβέρνησης και τη χάραξη διαφόρων εταιρικών στρατηγικών, μόνο οι χρηματοοικονομικές οντότητες που δεν είναι πολύ μικρές επιχειρήσεις κατά την έννοια του παρόντος κανονισμού θα πρέπει να υποχρεούνται να θεσπίζουν πιο πολύπλοκες ρυθμίσεις διακυβέρνησης. Οντότητες αυτού του είδους είναι καλύτερα εξοπλισμένες, ιδίως για τη δημιουργία ειδικών λειτουργιών διαχείρισης όσον αφορά τις εποπτικές ρυθμίσεις με τρίτους παρόχους υπηρεσιών ΤΠΕ ή τη διασφάλιση της διαχείρισης κρίσεων για την οργάνωση της διαχείρισης κινδύνων ΤΠΕ σύμφωνα με το μοντέλο των τριών γραμμών άμυνας ή τη δημιουργία εσωτερικού μοντέλου διαχείρισης κινδύνων και ελέγχου, καθώς και για την υποβολή του οικείου πλαισίου διαχείρισης κινδύνων ΤΠΕ σε εσωτερικές επιθεωρήσεις.

(39) Ορισμένες χρηματοοικονομικές οντότητες επωφελούνται από εξαιρέσεις ή υπόκεινται σε πολύ χαλαρό ρυθμιστικό πλαίσιο βάσει του τομεακού ενωσιακού δικαίου. Στις εν λόγω χρηματοοικονομικές οντότητες περιλαμβάνονται οι διαχειριστές οργανισμών εναλλακτικών επενδύσεων που αναφέρονται στο άρθρο 3 παράγραφος 2 της οδηγίας 2011/61/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([16]), οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις που αναφέρονται στο άρθρο 4 της οδηγίας 2009/138/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([17]) και τα ιδρύματα επαγγελματικών συνταξιοδοτικών παροχών που διαχειρίζονται συνταξιοδοτικά συστήματα τα οποία από κοινού δεν έχουν

([14]) Οδηγία 2009/110/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 16ης Σεπτεμβρίου 2009, για την ανάληψη, άσκηση και προληπτική εποπτεία της δραστηριότητας ιδρύματος ηλεκτρονικού χρήματος, την τροποποίηση των οδηγιών 2005/60/ΕΚ και 2006/48/ΕΚ και την κατάργηση της οδηγίας 2000/46/ΕΚ (ΕΕ L 267 της 10.10.2009, σ. 7).

([15]) Οδηγία 2013/36/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και το Συμβουλίου, της 26ης Ιουνίου 2013, σχετικά με την πρόσβαση στη δραστηριότητα των πιστωτικών ιδρυμάτων και την προληπτική εποπτεία των πιστωτικών ιδρυμάτων, την τροποποίηση της οδηγίας 2002/87/ΕΚ και την κατάργηση των οδηγιών 2006/48/ΕΚ και 2006/49/ΕΚ (ΕΕ L 176 της 27.6.2013, σ. 338).

([16]) Οδηγία 2011/61/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 8ης Ιουνίου 2011, σχετικά με τους διαχειριστές οργανισμών εναλλακτικών επενδύσεων και για την τροποποίηση των οδηγιών 2003/41/ΕΚ και 2009/65/ΕΚ και των κανονισμών (ΕΚ) αριθ. 1060/2009 και (ΕΕ) αριθ. 1095/2010 (ΕΕ L 174 της 1.7.2011, σ. 1).

([17]) Οδηγία 2009/138/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2009, σχετικά με την ανάληψη και την άσκηση δραστηριοτήτων ασφάλισης και αντασφάλισης (Φερεγγυότητα ΙΙ) (ΕΕ L 335 της 17.12.2009, σ. 1).

περισσότερα από 15 μέλη συνολικά. Υπό το πρίσμα των εν λόγω εξαιρέσεων, δεν θα ήταν αναλογικό να συμπεριληφθούν οι εν λόγω χρηματοοικονομικές οντότητες στο πεδίο εφαρμογής του παρόντος κανονισμού. Επιπλέον, ο παρών κανονισμός αναγνωρίζει τις ιδιαιτερότητες της δομής της αγοράς ασφαλιστικής διαμεσολάβησης, με αποτέλεσμα οι ασφαλιστικοί διαμεσολαβητές, οι αντασφαλιστικοί διαμεσολαβητές και οι ασφαλιστικοί διαμεσολαβητές που ασκούν ως δευτερεύουσα δραστηριότητα την ασφαλιστική διαμεσολάβηση, που χαρακτηρίζονται ως πολύ μικρές επιχειρήσεις ή ως μικρές ή μεσαίες επιχειρήσεις, να μην υπόκεινται στον παρόντα κανονισμό.

(40) Δεδομένου ότι οι οντότητες που αναφέρονται στο άρθρο 2 παράγραφος 5 σημεία 4) έως 23) της οδηγίας 2013/36/ΕΕ εξαιρούνται από το πεδίο εφαρμογής της εν λόγω οδηγίας, τα κράτη μέλη θα πρέπει, κατά συνέπεια, να έχουν τη δυνατότητα να εξαιρούν από την εφαρμογή του παρόντος κανονισμού τις εν λόγω οντότητες που είναι εγκατεστημένες στις αντίστοιχες επικράτειές τους.

(41) Ομοίως, προκειμένου να ευθυγραμμιστεί ο παρών κανονισμός με το πεδίο εφαρμογής της οδηγίας 2014/65/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([18]), είναι επίσης σκόπιμο να εξαιρεθούν από το πεδίο εφαρμογής του παρόντος κανονισμού τα φυσικά και νομικά πρόσωπα που αναφέρονται στα άρθρα 2 και 3 της εν λόγω οδηγίας, τα οποία επιτρέπεται να παρέχουν επενδυτικές υπηρεσίες χωρίς να χρειάζεται να λάβουν άδεια δυνάμει της οδηγίας 2014/65/ΕΕ. Ωστόσο, το άρθρο 2 της οδηγίας 2014/65/ΕΕ εξαιρεί επίσης από το πεδίο εφαρμογής της εν λόγω οδηγίας οντότητες που θεωρούνται χρηματοοικονομικές οντότητες για τους σκοπούς του παρόντος κανονισμού, όπως τα κεντρικά αποθετήρια τίτλων, οι οργανισμοί συλλογικών επενδύσεων ή οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις. Η εξαίρεση από το πεδίο εφαρμογής του παρόντος κανονισμού των προσώπων και των οντοτήτων που αναφέρονται στα άρθρα 2 και 3 της εν λόγω οδηγίας δεν θα πρέπει να περιλαμβάνει τα εν λόγω κεντρικά αποθετήρια τίτλων, οργανισμούς συλλογικών επενδύσεων ή ασφαλιστικές και αντασφαλιστικές επιχειρήσεις.

(42) Σύμφωνα με το τομεακό ενωσιακό δίκαιο, ορισμένες χρηματοοικονομικές οντότητες υπόκεινται σε λιγότερο αυστηρές απαιτήσεις ή εξαιρέσεις για λόγους οι οποίοι σχετίζονται με το μέγεθός τους ή τις υπηρεσίες που παρέχουν. Σε αυτήν την κατηγορία χρηματοοικονομικών οντοτήτων περιλαμβάνονται μικρές και μη διασυνδεδεμένες επιχειρήσεις επενδύσεων, μικρά ιδρύματα επαγγελματικών συνταξιοδοτικών παροχών που μπορούν να εξαιρεθούν από το πεδίο εφαρμογής της οδηγίας (ΕΕ) 2016/2341, υπό τις προϋποθέσεις που ορίζονται στο άρθρο 5 της εν λόγω οδηγίας από το οικείο κράτος μέλος, και διαχειρίζονται συνταξιοδοτικά συστήματα τα οποία από κοινού δεν έχουν περισσότερα από 100 μέλη συνολικά, καθώς και ιδρύματα που εξαιρούνται δυνάμει της οδηγίας 2013/36/ΕΕ. Ως εκ τούτου, σύμφωνα με την αρχή της αναλογικότητας και για να διατηρηθεί το πνεύμα του τομεακού ενωσιακού δικαίου, είναι επίσης σκόπιμο να υπαχθούν οι εν λόγω χρηματοοικονομικές οντότητες σε απλουστευμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ δυνάμει του παρόντος κανονισμού. Ο αναλογικός χαρακτήρας του πλαισίου διαχείρισης κινδύνων ΤΠΕ που καλύπτει τις εν λόγω χρηματοοικονομικές οντότητες δεν θα πρέπει να τροποποιείται από τα ρυθμιστικά τεχνικά πρότυπα που πρόκειται να εκπονηθούν από τις ΕΕΑ. Επιπλέον, σύμφωνα με την αρχή της αναλογικότητας, είναι σκόπιμο να υπαχθούν επίσης τα ιδρύματα πληρωμών που αναφέρονται στο άρθρο 32 παράγραφος 1 της οδηγίας (ΕΕ) 2015/2366 και τα ιδρύματα ηλεκτρονικού χρήματος που αναφέρονται στο άρθρο 9 της οδηγίας 2009/110/ΕΚ, σύμφωνα με τη μεταφορά των εν λόγω νομικών πράξεων της Ένωσης στο εθνικό δίκαιο, σε απλουστευμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ δυνάμει του παρόντος κανονισμού, ενώ τα ιδρύματα πληρωμών και τα ιδρύματα ηλεκτρονικού χρήματος που δεν έχουν εξαιρεθεί σύμφωνα με την αντίστοιχη μεταφορά του τομεακού δικαίου της Ένωσης στο εθνικό τους δίκαιο θα πρέπει να συμμορφώνονται με το γενικό πλαίσιο που θεσπίζεται με τον παρόντα κανονισμό.

(43) Ομοίως, οι χρηματοοικονομικές οντότητες που χαρακτηρίζονται πολύ μικρές επιχειρήσεις ή υπόκεινται στο απλουστευμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ δυνάμει του παρόντος κανονισμού δεν θα πρέπει να υποχρεούνται να καθορίζουν ρόλο για την παρακολούθηση των ρυθμίσεων που συνάπτουν με τρίτους παρόχους υπηρεσιών ΤΠΕ σχετικά με τη χρήση υπηρεσιών ΤΠΕ ή να ορίζουν ανώτερο διοικητικό στέλεχος υπεύθυνο για την εποπτεία της σχετικής έκθεσης σε κίνδυνο και τη σχετική τεκμηρίωση, να αναθέτουν την ευθύνη διαχείρισης και εποπτείας των κινδύνων ΤΠΕ σε λειτουργία ελέγχου και να διασφαλίζουν κατάλληλο επίπεδο ανεξαρτησίας της εν λόγω λειτουργίας ελέγχου, προκειμένου να αποφεύγονται συγκρούσεις συμφερόντων, να τεκμηριώνουν και να επανεξετάζουν τουλάχιστον μία φορά ετησίως το πλαίσιο διαχείρισης κινδύνων ΤΠΕ, να υποβάλλουν σε τακτική εσωτερική επιθεώρηση το πλαίσιο διαχείρισης κινδύνων ΤΠΕ, να διενεργούν εις βάθος αξιολογήσεις μετά από σημαντικές αλλαγές στις υποδομές και στις διαδικασίες των συστημάτων δικτύου και πληροφοριών τους, να προβαίνουν ανά τακτά χρονικά διαστήματα σε αναλύσεις κινδύνου για τα παρωχημένα συστήματα ΤΠΕ, να υποβάλλουν την εφαρμογή των σχεδίων αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ σε ανεξάρτητες επανεξετάσεις εσωτερικής επιθεώρησης, να διαθέτουν λειτουργία διαχείρισης κρίσεων, να επεκτείνουν τις δοκιμές επιχειρησιακής συνέχειας και τα σχέδια αντιμετώπισης και ανάκαμψης, ώστε να σχεδιάζουν σενάρια μετάβασης μεταξύ της κύριας υποδομής ΤΠΕ και των εφεδρικών εγκαταστάσεων, να υποβάλλουν στις αρμόδιες αρχές, κατόπιν αιτήματός τους,

([18]) Οδηγία 2014/65/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαΐου 2014, για τις αγορές χρηματοπιστωτικών μέσων και την τροποποίηση της οδηγίας 2002/92/ΕΚ και της οδηγίας 2011/61/ΕΕ (ΕΕ L 173 της 12.6.2014, σ. 349).

εκτίμηση των συγκεντρωτικών ετήσιων δαπανών και ζημιών οι οποίες προκαλούνται από μείζονα συμβάντα που σχετίζονται με τις ΤΠΕ, να διατηρούν εφεδρικές χωρητικότητες ΤΠΕ, να κοινοποιούν στις εθνικές αρμόδιες αρχές τις αλλαγές που εφαρμόστηκαν κατόπιν επανεξετάσεων μετά από συμβάντα που σχετίζονται με τις ΤΠΕ, να παρακολουθούν σε συνεχή βάση τις σχετικές τεχνολογικές εξελίξεις, να θεσπίζουν ολοκληρωμένο πρόγραμμα δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας ως αναπόσπαστο μέρος του πλαισίου διαχείρισης κινδύνων ΤΠΕ που προβλέπεται στον παρόντα κανονισμό ή να εγκρίνουν και να επανεξετάζουν τακτικά στρατηγική για τους κινδύνους τρίτου παρόχου ΤΠΕ. Επιπλέον, οι πολύ μικρές επιχειρήσεις θα πρέπει μόνο να υποχρεούνται να αξιολογούν την ανάγκη διατήρησης αυτών των εφεδρικών χωρητικοτήτων ΤΠΕ με βάση το προφίλ κινδύνου τους. Οι πολύ μικρές επιχειρήσεις θα πρέπει να επωφελούνται από ένα πιο ευέλικτο καθεστώς όσον αφορά τα προγράμματα δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας. Κατά την εξέταση του είδους και της συχνότητας των δοκιμών που πρέπει να διενεργούνται, θα πρέπει να εξισορροπούν δεόντως τον στόχο της διατήρησης υψηλής ψηφιακής επιχειρησιακής ανθεκτικότητας, τους διαθέσιμους πόρους και το συνολικό προφίλ κινδύνου τους. Οι πολύ μικρές επιχειρήσεις και οι χρηματοοικονομικές οντότητες που υπόκεινται στο απλουστευμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ βάσει του παρόντος κανονισμού θα πρέπει να εξαιρούνται από την απαίτηση διενέργειας προηγμένων δοκιμών σε εργαλεία, συστήματα και διαδικασίες ΤΠΕ που βασίζονται σε δοκιμές παρείσδυσης βάσει απειλών (TLPT), καθώς μόνο οι χρηματοοικονομικές οντότητες που πληρούν τα κριτήρια που καθορίζονται στον παρόντα κανονισμό θα πρέπει να υποχρεούνται να διενεργούν τις εν λόγω δοκιμές. Λόγω των περιορισμένων ικανοτήτων τους, οι πολύ μικρές επιχειρήσεις θα πρέπει να είναι σε θέση να συμφωνήσουν με τον τρίτο πάροχο υπηρεσιών ΤΠΕ να αναθέσουν τα δικαιώματα πρόσβασης, επιθεώρησης και ελέγχου της χρηματοοικονομικής οντότητας σε ανεξάρτητο τρίτο μέρος, το οποίο θα οριστεί από τον τρίτο πάροχο υπηρεσιών ΤΠΕ, υπό την προϋπόθεση ότι η χρηματοοικονομική οντότητα είναι σε θέση να ζητήσει, ανά πάσα στιγμή, όλες τις σχετικές πληροφορίες και διασφαλίσεις σχετικά με τις επιδόσεις του τρίτου παρόχου υπηρεσιών ΤΠΕ από το αντίστοιχο ανεξάρτητο τρίτο μέρος.

(44) Δεδομένου ότι μόνο οι χρηματοοικονομικές οντότητες που ταυτοποιούνται για τους σκοπούς των προηγμένων δοκιμών ψηφιακής ανθεκτικότητας θα πρέπει να υποχρεούνται να διενεργούν δοκιμές παρείσδυσης βάσει απειλών, οι διοικητικές διαδικασίες και το οικονομικό κόστος που συνεπάγεται η διενέργεια των δοκιμών αυτών θα πρέπει να βαρύνουν μικρό ποσοστό των χρηματοοικονομικών οντοτήτων.

(45) Για τους σκοπούς της διασφάλισης της πλήρους ευθυγράμμισης και της συνολικής συνοχής μεταξύ των επιχειρηματικών στρατηγικών των χρηματοοικονομικών οντοτήτων, αφενός, και της άσκησης της διαχείρισης κινδύνων ΤΠΕ, αφετέρου, τα διοικητικά όργανα των χρηματοοικονομικών οντοτήτων θα πρέπει να υποχρεούνται να επιτελούν καίριο και ενεργό ρόλο στον προσανατολισμό και στην προσαρμογή του πλαισίου διαχείρισης κινδύνων ΤΠΕ, καθώς και της συνολικής στρατηγικής για την ψηφιακή λειτουργική ανθεκτικότητα. Η προσέγγιση που οφείλουν να υιοθετούν τα διοικητικά όργανα δεν θα πρέπει να επικεντρώνεται μόνο στα μέσα διασφάλισης της ανθεκτικότητας των συστημάτων ΤΠΕ, αλλά θα πρέπει επίσης να καλύπτει τα άτομα και τις διαδικασίες μέσω μιας δέσμης πολιτικών που καλλιεργούν, σε κάθε εταιρικό επίπεδο και για το σύνολο των μελών του προσωπικού, ισχυρό αίσθημα ευαισθητοποίησης όσον αφορά τους κινδύνους στον κυβερνοχώρο, καθώς και την ανάληψη δέσμευσης για την τήρηση αυστηρής κυβερνοϋγιεινής σε όλα τα επίπεδα. Η τελική ευθύνη του διοικητικού οργάνου για τη διαχείριση κινδύνων ΤΠΕ της χρηματοοικονομικής οντότητας θα πρέπει να αποτελεί γενική αρχή της εν λόγω ολοκληρωμένης προσέγγισης, η οποία θα μετουσιώνεται περαιτέρω στη διαρκή συμμετοχή του διοικητικού οργάνου στον έλεγχο της παρακολούθησης της διαχείρισης κινδύνων ΤΠΕ.

(46) Επιπλέον, η αρχή της πλήρους και τελικής ευθύνης του διοικητικού οργάνου για τη διαχείριση κινδύνων ΤΠΕ της χρηματοοικονομικής οντότητας συμβαδίζει με την ανάγκη εξασφάλισης επιπέδου επενδύσεων που σχετίζονται με τις ΤΠΕ και συνολικού προϋπολογισμού για τη χρηματοοικονομική οντότητα που θα επιτρέψουν στη χρηματοοικονομική οντότητα να επιτύχει υψηλό επίπεδο ψηφιακής επιχειρησιακής ανθεκτικότητας.

(47) Βάσει σχετικών διεθνών, εθνικών και κλαδικών βέλτιστων πρακτικών, κατευθυντήριων γραμμών, συστάσεων και προσεγγίσεων για τη διαχείριση των κινδύνων στον κυβερνοχώρο, ο παρών κανονισμός προάγει μια σειρά αρχών που διευκολύνουν τη συνολική διάρθρωση της διαχείρισης κινδύνων ΤΠΕ. Κατά συνέπεια, στον βαθμό που οι κύριες ικανότητες τις οποίες διαθέτουν οι χρηματοοικονομικές οντότητες ανταποκρίνονται στις διάφορες λειτουργίες στη διαχείριση κινδύνων ΤΠΕ (προσδιορισμός, προστασία και πρόληψη, εντοπισμός, αντιμετώπιση και ανάκαμψη, μάθηση και εξέλιξη και επικοινωνία) που καθορίζονται στον παρόντα κανονισμό, οι χρηματοοικονομικές οντότητες θα πρέπει να εξακολουθήσουν να έχουν τη διακριτική ευχέρεια να χρησιμοποιούν μοντέλα διαχείρισης κινδύνων ΤΠΕ τα οποία πλαισιώνονται ή κατηγοριοποιούνται με διαφορετικό τρόπο.

(48) Προκειμένου να συμβαδίζουν με το εξελισσόμενο τοπίο των κυβερνοαπειλών, οι χρηματοοικονομικές οντότητες θα πρέπει να διατηρούν επικαιροποιημένα συστήματα ΤΠΕ, τα οποία είναι αξιόπιστα και ικανά να εξασφαλίζουν όχι μόνο την επεξεργασία δεδομένων που απαιτείται για τις υπηρεσίες τους, αλλά και επαρκή τεχνολογική ανθεκτικότητα που θα τους επιτρέπει να ανταποκρίνονται δεόντως στις πρόσθετες ανάγκες επεξεργασίας λόγω ακραίων συνθηκών της αγοράς ή άλλων αντίξοων καταστάσεων.

(49) Απαιτούνται αποτελεσματικά σχέδια επιχειρησιακής συνέχειας και ανάκαμψης ώστε οι χρηματοοικονομικές οντότητες να είναι σε θέση να επιλύουν άμεσα και γρήγορα συμβάντα που σχετίζονται με τις ΤΠΕ, ιδίως κυβερνοεπιθέσεις, περιορίζοντας τις ζημίες και δίνοντας προτεραιότητα στην επανέναρξη των δραστηριοτήτων και στην ανάληψη δράσεων ανάκαμψης, σύμφωνα με τις πολιτικές τους για τη δημιουργία εφεδρικών συστημάτων. Ωστόσο, η επανέναρξη αυτή δεν θα πρέπει σε καμία περίπτωση να θέτει σε κίνδυνο την ακεραιότητα και την ασφάλεια των συστημάτων δικτύου και πληροφοριών ή τη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα ή την εμπιστευτικότητα των δεδομένων.

(50) Μολονότι ο παρών κανονισμός παρέχει στις χρηματοοικονομικές οντότητες τη δυνατότητα να καθορίζουν τους στόχους τους για τον χρόνο ανάκαμψης και το σημείο ανάκαμψης με ευέλικτο τρόπο και, κατ' επέκταση, να θέτουν τέτοιους στόχους λαμβάνοντας πλήρως υπόψη τη φύση και την κρισιμότητα των σχετικών λειτουργιών, καθώς και τυχόν ειδικών επιχειρηματικών αναγκών, θα πρέπει, ωστόσο, να τις υποχρεώνει να αξιολογούν τις συνολικές δυνητικές επιπτώσεις στην αποτελεσματικότητα της αγοράς, κατά τον καθορισμό των εν λόγω στόχων.

(51) Οι φορείς διάδοσης κυβερνοεπιθέσεων τείνουν να επιδιώκουν οικονομικά οφέλη απευθείας στην πηγή, εκθέτοντας έτσι τις χρηματοοικονομικές οντότητες σε σημαντικές συνέπειες. Για να προληφθεί η απώλεια της ακεραιότητας ή της διαθεσιμότητας των συστημάτων ΤΠΕ και, ως εκ τούτου, να αποφευχθούν οι παραβιάσεις δεδομένων και η ζημία σε υλική υποδομή ΤΠΕ, η αναφορά μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ από χρηματοοικονομικές οντότητες θα πρέπει να βελτιωθεί και να εξορθολογιστεί σημαντικά. Η αναφορά συμβάντων που σχετίζονται με τις ΤΠΕ θα πρέπει να εναρμονιστεί μέσω της θέσπισης απαίτησης για όλες τις χρηματοοικονομικές οντότητες να υποβάλλουν αναφορά απευθείας στις οικείες αρμόδιες αρχές τους. Όταν μια χρηματοοικονομική οντότητα υπόκειται σε εποπτεία από περισσότερες από μία εθνικές αρμόδιες αρχές, τα κράτη μέλη θα πρέπει να ορίζουν μία μόνο αρμόδια αρχή ως αποδέκτη της εν λόγω αναφοράς. Τα πιστωτικά ιδρύματα που ταξινομούνται ως σημαντικά σύμφωνα με το άρθρο 6 παράγραφος 4 του κανονισμού (ΕΕ) αριθ. 1024/2013 του Συμβουλίου ([19]) θα πρέπει να υποβάλλουν την εν λόγω αναφορά στις εθνικές αρμόδιες αρχές, οι οποίες θα πρέπει στη συνέχεια να διαβιβάζουν την αναφορά στην Ευρωπαϊκή Κεντρική Τράπεζα (ΕΚΤ).

(52) Η απευθείας αναφορά θα πρέπει να επιτρέπει στις αρχές χρηματοοικονομικής εποπτείας να έχουν άμεση πρόσβαση σε πληροφορίες για μείζονα συμβάντα που σχετίζονται με τις ΤΠΕ. Οι αρχές χρηματοοικονομικής εποπτείας θα πρέπει με τη σειρά τους να διαβιβάζουν λεπτομέρειες σχετικά με μείζονα συμβάντα που σχετίζονται με τις ΤΠΕ σε δημόσιες μη χρηματοοικονομικές αρχές (όπως οι αρμόδιες αρχές και τα ενιαία σημεία επαφής βάσει της οδηγίας (ΕΕ) 2022/2555 εθνικές αρχές προστασίας δεδομένων και αρχές επιβολής του νόμου για μείζονα συμβάντα που σχετίζονται με τις ΤΠΕ ποινικού χαρακτήρα), προκειμένου να ενισχυθεί η ευαισθητοποίηση των εν λόγω αρχών σχετικά με αυτά τα συμβάντα και, στην περίπτωση των CSIRT, να διευκολυνθεί η άμεση συνδρομή που μπορεί να παρέχεται στις χρηματοοικονομικές οντότητες, κατά περίπτωση. Επιπλέον, τα κράτη μέλη θα πρέπει να είναι σε θέση να καθορίζουν ότι οι ίδιες οι χρηματοοικονομικές οντότητες θα πρέπει να παρέχουν τις πληροφορίες αυτές σε δημόσιες αρχές εκτός του τομέα των χρηματοοικονομικών υπηρεσιών. Οι εν λόγω ροές πληροφοριών θα πρέπει να επιτρέπουν στις χρηματοοικονομικές οντότητες να επωφελούνται άμεσα από κάθε σχετική τεχνική συμβολή, συμβουλές σχετικά με τα διορθωτικά μέτρα και επακόλουθη παρακολούθηση από τις εν λόγω αρχές. Η διοχέτευση πληροφοριών για μείζονα συμβάντα που σχετίζονται με τις ΤΠΕ θα πρέπει να είναι αμοιβαία: οι αρχές χρηματοοικονομικής εποπτείας θα πρέπει να παρέχουν στη χρηματοοικονομική οντότητα κάθε αναγκαία παρατήρηση ή καθοδήγηση, ενώ οι ΕΕΑ θα πρέπει να ανταλλάσσουν ανωνυμοποιημένα δεδομένα σχετικά με κυβερνοαπειλές και ευπάθειες που σχετίζονται με ένα συμβάν, με σκοπό την ενίσχυση της ευρύτερης συλλογικής άμυνας.

(53) Ενώ όλες οι χρηματοοικονομικές οντότητες θα πρέπει να υπόκεινται στην υποχρέωση αναφοράς συμβάντων, η απαίτηση αυτή δεν αναμένεται να τις επηρεάσει όλες με τον ίδιο τρόπο. Πράγματι, τα σχετικά κατώτατα όρια σημαντικότητας, καθώς και τα χρονοδιαγράμματα υποβολής αναφορών, θα πρέπει να προσαρμόζονται δεόντως, στο πλαίσιο των κατ' εξουσιοδότηση πράξεων που βασίζονται στα ρυθμιστικά τεχνικά πρότυπα που θα αναπτύξουν οι ΕΕΑ, με σκοπό την κάλυψη μόνο μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ. Επιπλέον, οι ιδιαιτερότητες των χρηματοοικονομικών οντοτήτων θα πρέπει να λαμβάνονται υπόψη κατά τον καθορισμό χρονοδιαγραμμάτων για τις υποχρεώσεις υποβολής αναφορών.

(54) Ο παρών κανονισμός θα πρέπει να απαιτεί από τα πιστωτικά ιδρύματα, τα ιδρύματα πληρωμών, τους παρόχους υπηρεσιών πληροφοριών λογαριασμού και τα ιδρύματα ηλεκτρονικού χρήματος να αναφέρουν όλα τα λειτουργικά συμβάντα ή τα συμβάντα ασφάλειας που σχετίζονται με πληρωμές —τα οποία έχουν αναφερθεί προηγουμένως βάσει της οδηγίας (ΕΕ) 2015/2366— ανεξάρτητα από τη φύση του συμβάντος όσον αφορά τις ΤΠΕ.

([19]) Κανονισμός (ΕΕ) αριθ. 1024/2013 του Συμβουλίου, της 15ης Οκτωβρίου 2013, για την ανάθεση ειδικών καθηκόντων στην Ευρωπαϊκή Κεντρική Τράπεζα σχετικά με τις πολιτικές που αφορούν την προληπτική εποπτεία των πιστωτικών ιδρυμάτων (ΕΕ L 287 της 29.10.2013, σ. 63).

(55) Οι ΕΕΑ θα πρέπει να επιφορτιστούν με την αξιολόγηση της σκοπιμότητας και των προϋποθέσεων για πιθανή συγκέντρωση των αναφορών συμβάντων που σχετίζονται με τις ΤΠΕ σε επίπεδο Ένωσης. Η συγκέντρωση αυτή θα μπορούσε να συνίσταται σε ενιαίο κόμβο της ΕΕ για αναφορά μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ, είτε με την άμεση παραλαβή των σχετικών εκθέσεων και την αυτόματη κοινοποίησή τους στις εθνικές αρμόδιες αρχές είτε με τη συγκέντρωση απλώς των σχετικών εκθέσεων που διαβιβάζονται από τις εθνικές αρμόδιες αρχές και την άσκηση, κατ' αυτόν τον τρόπο, συντονιστικού ρόλου. Θα πρέπει να ανατεθεί στις ΕΕΑ να εκπονήσουν, σε διαβούλευση με την ΕΚΤ και τον ENISA, κοινή έκθεση στην οποία θα διερευνάται η σκοπιμότητα της δημιουργίας ενιαίου κόμβου της ΕΕ.

(56) Για τους σκοπούς της διασφάλισης υψηλού επιπέδου ψηφιακής επιχειρησιακής ανθεκτικότητας, και σύμφωνα τόσο με τα σχετικά διεθνή πρότυπα (π.χ. τα θεμελιώδη στοιχεία της G7 για τις δοκιμές παρείσδυσης βάσει απειλών), όσο και με τα πλαίσια που εφαρμόζονται στην Ένωση, όπως το TIBER–EU, οι χρηματοοικονομικές οντότητες θα πρέπει να υποβάλλουν τακτικά σε δοκιμή τα οικεία συστήματα ΤΠΕ και το προσωπικό τους το οποίο έχει αρμοδιότητες σχετικές με τις ΤΠΕ ως προς την αποτελεσματικότητα των ικανοτήτων τους όσον αφορά την πρόληψη, τον εντοπισμό, την αντιμετώπιση και την ανάκαμψη, ώστε να αποκαλύπτουν και να αντιμετωπίζουν πιθανές ευπάθειες των ΤΠΕ. Για τη συνεκτίμηση των διαφορών που υπάρχουν τόσο μεταξύ όσο και εντός των διαφόρων χρηματοοικονομικών υποτομέων όσον αφορά το επίπεδο ετοιμότητας των χρηματοοικονομικών οντοτήτων στον τομέα της κυβερνοασφάλειας, οι δοκιμές θα πρέπει να περιλαμβάνουν ευρύ φάσμα εργαλείων και δράσεων, που εκτείνονται από την αξιολόγηση βασικών απαιτήσεων (π.χ. αξιολογήσεις και σαρώσεις ευπάθειας, αναλύσεις ανοικτής πηγής, αξιολογήσεις ασφάλειας δικτύου, αναλύσεις ελλείψεων, επισκοπήσεις υλικής ασφάλειας, λύσεις λογισμικού ερωτηματολογίων και σάρωσης, επανεξετάσεις πηγαίου κώδικα όπου αυτό είναι εφικτό, δοκιμές βάσει σεναρίων, δοκιμές συμβατότητας, δοκιμές επιδόσεων ή διατερματικές δοκιμές), έως πιο προηγμένες δοκιμές μέσω TLPT. Αυτού του είδους οι προηγμένες δοκιμές θα πρέπει να απαιτούνται μόνο από τις χρηματοοικονομικές οντότητες που παρουσιάζουν επαρκή βαθμό ωριμότητας από πλευράς ΤΠΕ, ώστε να τις διενεργούν εύλογα. Συνεπώς, οι δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας που απαιτούνται βάσει του παρόντος κανονισμού θα πρέπει να είναι πιο απαιτητικές για τις χρηματοοικονομικές οντότητες που πληρούν τα κριτήρια που καθορίζονται στον παρόντα κανονισμό (για παράδειγμα, μεγάλα, συστημικά και ώριμα για ΤΠΕ πιστωτικά ιδρύματα, χρηματιστήρια, κεντρικά αποθετήρια τίτλων και κεντρικοί αντισυμβαλλόμενοι) από ό,τι για άλλες χρηματοοικονομικές οντότητες. Ταυτόχρονα, οι δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας μέσω TLPT θα πρέπει να είναι περισσότερο σημαντικές για χρηματοοικονομικές οντότητες οι οποίες δραστηριοποιούνται σε βασικούς υποτομείς χρηματοοικονομικών υπηρεσιών και διαδραματίζουν συστημικό ρόλο (για παράδειγμα, πληρωμές, τράπεζες και εκκαθάριση και διακανονισμός) και λιγότερο σημαντικές για άλλους υποτομείς (για παράδειγμα, διαχειριστές περιουσιακών στοιχείων και οργανισμοί αξιολόγησης της πιστοληπτικής ικανότητας).

(57) Οι χρηματοοικονομικές οντότητες οι οποίες ασχολούνται με διασυνοριακές δραστηριότητες και ασκούν το δικαίωμα ελεύθερης εγκατάστασης ή παροχής υπηρεσιών εντός της Ένωσης θα πρέπει να συμμορφώνονται με ένα ενιαίο σύνολο απαιτήσεων προηγμένων δοκιμών (δηλαδή TLPT) στο κράτος μέλος προέλευσής τους που θα πρέπει να περιλαμβάνει τις υποδομές ΤΠΕ σε όλες τις δικαιοδοσίες στις οποίες δραστηριοποιείται ο διασυνοριακός χρηματοοικονομικός όμιλος εντός της Ένωσης, ώστε να διασφαλίζεται ότι αυτοί οι διασυνοριακοί χρηματοοικονομικοί όμιλοι επιβαρύνονται με το κόστος δοκιμών που σχετίζονται με τις ΤΠΕ μόνο σε μία δικαιοδοσία.

(58) Προκειμένου να αξιοποιηθεί η εμπειρογνωσία που έχει ήδη αποκτηθεί από ορισμένες αρμόδιες αρχές, ιδίως όσον αφορά την εφαρμογή του πλαισίου TIBER–EU, ο παρών κανονισμός θα πρέπει να επιτρέπει στα κράτη μέλη να ορίζουν μία μόνο δημόσια αρχή ως υπεύθυνη στον χρηματοοικονομικό τομέα, σε εθνικό επίπεδο, για όλα τα θέματα TLPT, ή στις αρμόδιες αρχές να αναθέτουν, ελλείψει τέτοιου ορισμού, την άσκηση καθηκόντων που σχετίζονται με TLPT σε άλλη εθνική χρηματοοικονομική αρμόδια αρχή.

(59) Δεδομένου ότι ο παρών κανονισμός δεν απαιτεί από τις χρηματοοικονομικές οντότητες να καλύπτουν όλες τις κρίσιμες ή σημαντικές λειτουργίες σε μία και μόνη δοκιμή παρείσδυσης βάσει απειλών, οι χρηματοοικονομικές οντότητες θα πρέπει να είναι ελεύθερες να καθορίζουν ποιες και πόσες κρίσιμες ή σημαντικές λειτουργίες θα πρέπει να περιλαμβάνονται στο πεδίο εφαρμογής της εν λόγω δοκιμής.

(60) Οι ομαδικές δοκιμές κατά την έννοια του παρόντος κανονισμού —που περιλαμβάνουν τη συμμετοχή διαφόρων χρηματοοικονομικών οντοτήτων σε μια TLPT και για τις οποίες ένας τρίτος πάροχος υπηρεσιών ΤΠΕ μπορεί να συνάψει απευθείας συμβατικές ρυθμίσεις με εξωτερικό δοκιμαστή— θα πρέπει να επιτρέπονται μόνο όταν η ποιότητα ή η ασφάλεια των υπηρεσιών που παρέχονται από τον τρίτο πάροχο υπηρεσιών ΤΠΕ σε πελάτες που είναι οντότητες οι οποίες δεν εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού ή η εμπιστευτικότητα των δεδομένων που σχετίζονται με τις εν λόγω υπηρεσίες αναμένεται ευλόγως να επηρεαστούν αρνητικά. Οι ομαδικές δοκιμές θα πρέπει επίσης να υπόκεινται σε διασφαλίσεις (κατεύθυνση από καθορισμένη χρηματοοικονομική οντότητα, βαθμονόμηση του αριθμού των συμμετεχουσών χρηματοοικονομικών οντοτήτων), ώστε να διασφαλίζεται η διενέργεια αυστηρών δοκιμών για τις εμπλεκόμενες χρηματοοικονομικές οντότητες που πληρούν τους στόχους της TLPT σύμφωνα με τον παρόντα κανονισμό.

(61) Προκειμένου να αξιοποιηθούν οι εσωτερικοί πόροι που διατίθενται σε εταιρικό επίπεδο, ο παρών κανονισμός θα πρέπει να επιτρέπει τη χρήση εσωτερικών δοκιμαστών για τους σκοπούς της διεξαγωγής TLPT, υπό την προϋπόθεση ότι υπάρχει εποπτική έγκριση, δεν υπάρχουν συγκρούσεις συμφερόντων και υπάρχει περιοδική εναλλαγή χρήσης εσωτερικών και εξωτερικών δοκιμαστών (κάθε τρεις δοκιμές), απαιτώντας παράλληλα από τον πάροχο των πληροφοριών σχετικά με τις απειλές στο πλαίσιο TLPT να είναι πάντα εξωτερικός σε σχέση με τη χρηματοοικονομική οντότητα. Η χρηματοοικονομική οντότητα θα πρέπει να εξακολουθεί να ευθύνεται πλήρως για τη διεξαγωγή TLPT. Οι βεβαιώσεις που παρέχονται από τις αρχές θα πρέπει να εξυπηρετούν αποκλειστικά τον σκοπό της αμοιβαίας αναγνώρισης και δεν θα πρέπει να αποκλείουν τυχόν επακόλουθες ενέργειες που απαιτούνται για την αντιμετώπιση των κινδύνων ΤΠΕ στους οποίους είναι εκτεθειμένη η χρηματοοικονομική οντότητα, ούτε θα πρέπει να θεωρούνται ως εποπτική έγκριση των ικανοτήτων διαχείρισης και μετριασμού των κινδύνων ΤΠΕ μιας χρηματοοικονομικής οντότητας.

(62) Για τη διασφάλιση της ορθής παρακολούθησης των κινδύνων τρίτων παρόχων ΤΠΕ στον χρηματοοικονομικό τομέα, είναι απαραίτητη η θέσπιση ενός συνόλου κανόνων βάσει αρχών, ώστε να παρέχεται καθοδήγηση στις χρηματοοικονομικές οντότητες, όταν παρακολουθούν κίνδυνο που προκύπτει στο πλαίσιο λειτουργιών που αποτελούν αντικείμενο εξωτερικής ανάθεσης σε τρίτους παρόχους υπηρεσιών ΤΠΕ, ιδίως για υπηρεσίες ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες καθώς και, γενικότερα, στο πλαίσιο όλων των εξαρτήσεων από τρίτους παρόχους ΤΠΕ.

(63) Για να αντιμετωπιστεί η πολυπλοκότητα των διάφορων πηγών κινδύνων ΤΠΕ, λαμβανομένων παράλληλα υπόψη της πληθώρας και της ποικιλομορφίας των παρόχων τεχνολογικών λύσεων που επιτρέπουν την ομαλή παροχή χρηματοοικονομικών υπηρεσιών, ο παρών κανονισμός θα πρέπει να καλύπτει ευρύ φάσμα τρίτων παρόχων υπηρεσιών ΤΠΕ, συμπεριλαμβανομένων των παρόχων υπηρεσιών υπολογιστικού νέφους, λογισμικού, υπηρεσιών ανάλυσης δεδομένων και παρόχων υπηρεσιών κέντρου δεδομένων. Ομοίως, δεδομένου ότι οι χρηματοοικονομικές οντότητες θα πρέπει να εντοπίζουν και να διαχειρίζονται αποτελεσματικά και συνεκτικά όλα τα είδη κινδύνων, μεταξύ άλλων στο πλαίσιο των υπηρεσιών ΤΠΕ που παρέχονται στο πλαίσιο ενός χρηματοοικονομικού ομίλου, θα πρέπει να διευκρινιστεί ότι επιχειρήσεις που αποτελούν μέρος χρηματοοικονομικού ομίλου και παρέχουν υπηρεσίες ΤΠΕ κυρίως στη μητρική τους επιχείρηση ή σε θυγατρικές ή υποκαταστήματα της μητρικής τους επιχείρησης, καθώς και χρηματοοικονομικές οντότητες που παρέχουν υπηρεσίες ΤΠΕ σε άλλες χρηματοοικονομικές οντότητες, θα πρέπει επίσης να θεωρούνται τρίτοι πάροχοι υπηρεσιών ΤΠΕ δυνάμει του παρόντος κανονισμού. Τέλος, δεδομένου ότι η εξελισσόμενη αγορά υπηρεσιών πληρωμών εξαρτάται όλο και περισσότερο από πολύπλοκες τεχνικές λύσεις, και λόγω των αναδυόμενων τύπων υπηρεσιών πληρωμών και λύσεων που σχετίζονται με τις πληρωμές, οι συμμετέχοντες στο οικοσύστημα υπηρεσιών πληρωμών, οι οποίοι παρέχουν δραστηριότητες επεξεργασίας πληρωμών ή λειτουργούν υποδομές πληρωμών, θα πρέπει επίσης να θεωρούνται τρίτοι πάροχοι υπηρεσιών ΤΠΕ δυνάμει του παρόντος κανονισμού, με εξαίρεση τις κεντρικές τράπεζες κατά τη λειτουργία συστημάτων πληρωμών ή διακανονισμού αξιογράφων και τις δημόσιες αρχές όταν παρέχουν υπηρεσίες που σχετίζονται με τις ΤΠΕ στο πλαίσιο της εκπλήρωσης κρατικών λειτουργιών.

(64) Οι χρηματοοικονομικές οντότητες θα πρέπει να φέρουν ανά πάσα στιγμή την πλήρη ευθύνη για τη συμμόρφωση με τις υποχρεώσεις τους που απορρέουν από τον παρόντα κανονισμό. Οι χρηματοοικονομικές οντότητες θα πρέπει να εφαρμόζουν αναλογική προσέγγιση όσον αφορά την παρακολούθηση κινδύνων που ανακύπτουν σε επίπεδο τρίτων παρόχων υπηρεσιών ΤΠΕ, λαμβανομένων δεόντως υπόψη της φύσης, της κλίμακας, της πολυπλοκότητας και της σημασίας των εξαρτήσεών τους που σχετίζονται με τις ΤΠΕ, της κρισιμότητας ή της σημασίας των υπηρεσιών, των διαδικασιών ή των λειτουργιών που υπόκεινται στις συμβατικές ρυθμίσεις και, εντέλει, βάσει προσεκτικής αξιολόγησης κάθε δυνητικού αντικτύπου στη συνέχεια και στην ποιότητα των χρηματοοικονομικών υπηρεσιών σε μεμονωμένο επίπεδο και σε επίπεδο ομίλου, ανάλογα με την περίπτωση.

(65) Για την άσκηση καθηκόντων παρακολούθησης αυτού του είδους θα πρέπει να ακολουθείται μια στρατηγική προσέγγιση ως προς τους κινδύνους τρίτων παρόχων ΤΠΕ, η οποία θα επισημοποιείται μέσω της υιοθέτησης, από το διοικητικό όργανο της χρηματοοικονομικής οντότητας, ειδικής στρατηγικής κινδύνων τρίτου παρόχου ΤΠΕ που θα βασίζεται στον διαρκή έλεγχο όλων των εξαρτήσεων από τρίτους παρόχους ΤΠΕ. Για τη βελτίωση της ευαισθητοποίησης όσον αφορά την εποπτεία των εξαρτήσεων από τρίτους παρόχους ΤΠΕ και με σκοπό την περαιτέρω στήριξη των εργασιών εντός του πλαισίου εποπτείας που θεσπίζεται με τον παρόντα κανονισμό, όλες οι χρηματοοικονομικές οντότητες θα πρέπει να υποχρεούνται να τηρούν μητρώο πληροφοριών με όλες τις συμβατικές ρυθμίσεις σχετικά με τη χρήση υπηρεσιών ΤΠΕ οι οποίες παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ. Οι αρχές χρηματοοικονομικής εποπτείας θα πρέπει να είναι σε θέση να ζητούν το πλήρες μητρώο ή συγκεκριμένα τμήματά του και, ως εκ τούτου, να λαμβάνουν βασικές πληροφορίες για την ευρύτερη κατανόηση των εξαρτήσεων των χρηματοοικονομικών οντοτήτων από τις ΤΠΕ.

(66) Μια διεξοδική ανάλυση πριν από την ανάθεση θα πρέπει να στηρίζει και να προηγείται της επίσημης σύναψης συμβατικών ρυθμίσεων, εστιάζοντας ιδίως σε στοιχεία όπως η κρισιμότητα ή η σημασία των υπηρεσιών που υποστηρίζονται από την προβλεπόμενη σύμβαση ΤΠΕ, οι αναγκαίες εποπτικές εγκρίσεις ή άλλοι όροι, ο πιθανός συνεπαγόμενος κίνδυνος συγκέντρωσης, καθώς και η εφαρμογή της δέουσας επιμέλειας κατά τη διαδικασία επιλογής και αξιολόγησης τρίτων παρόχων υπηρεσιών ΤΠΕ και η αξιολόγηση πιθανών συγκρούσεων συμφερόντων. Όσον αφορά τις συμβατικές ρυθμίσεις οι οποίες αφορούν κρίσιμες ή σημαντικές λειτουργίες, οι χρηματοοικονομικές οντότητες θα πρέπει να λαμβάνουν δεόντως υπόψη τη χρήση από τρίτους παρόχους υπηρεσιών ΤΠΕ των πλέον επικαιροποιημένων και ύψιστων προτύπων ασφάλειας πληροφοριών. Η καταγγελία των συμβατικών ρυθμίσεων θα μπορούσε να οφείλεται τουλάχιστον σε σύνολο περιστάσεων που παρουσιάζουν ελλείψεις σε επίπεδο τρίτου παρόχου υπηρεσιών ΤΠΕ, ιδίως σημαντικές παραβιάσεις νόμων ή

συμβατικών όρων, περιστάσεις που αποκαλύπτουν πιθανή μεταβολή της εκτέλεσης των καθηκόντων που προβλέπονται στις συμβατικές ρυθμίσεις, αποδεικτικά στοιχεία αδυναμιών του τρίτου παρόχου υπηρεσιών ΤΠΕ στη συνολική διαχείριση κινδύνων ΤΠΕ ή περιστάσεις που υποδεικνύουν την αδυναμία της σχετικής αρμόδιας αρχής να εποπτεύει αποτελεσματικά τη χρηματοοικονομική οντότητα.

(67) Για την αντιμετώπιση των συστημικών επιπτώσεων του κινδύνου συγκέντρωσης τρίτων παρόχων ΤΠΕ, ο παρών κανονισμός προάγει ισορροπημένη λύση μέσω της υιοθέτησης ευέλικτης και σταδιακής προσέγγισης στον εν λόγω κίνδυνο συγκέντρωσης, δεδομένου ότι η επιβολή τυχόν αυστηρών ανώτατων ορίων ή αυστηρών περιορισμών ενδέχεται να εμποδίσει τη διεξαγωγή επιχειρήσεων και να περιορίσει τη συμβατική ελευθερία. Οι χρηματοοικονομικές οντότητες θα πρέπει να αξιολογούν ενδελεχώς τις συμβατικές ρυθμίσεις τις οποίες προβλέπουν για τον προσδιορισμό της πιθανότητας εμφάνισης κινδύνου αυτού του είδους, μεταξύ άλλων μέσω εμπεριστατωμένων αναλύσεων των ρυθμίσεων υπεργολαβίας, ιδίως όταν συνάπτονται με τρίτους παρόχους υπηρεσιών ΤΠΕ που είναι εγκατεστημένοι σε τρίτη χώρα. Στο παρόν στάδιο, και για τους σκοπούς της επίτευξης δίκαιης ισορροπίας μεταξύ της επιτακτικής ανάγκης για διατήρηση της συμβατικής ελευθερίας και της ανάγκης για διασφάλιση της χρηματοοικονομικής σταθερότητας, δεν κρίνεται σκόπιμη η θέσπιση κανόνων περί αυστηρών ανώτατων ορίων και περιορισμών όσον αφορά την έκθεση σε κινδύνους τρίτων παρόχων ΤΠΕ. Εντός του πλαισίου εποπτείας, ο κύριος εποπτικός φορέας που έχει οριστεί σύμφωνα με τον παρόντα κανονισμό θα πρέπει, όσον αφορά τους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, να δίνει ιδιαίτερη προσοχή στην πλήρη κατανόηση της έκτασης των αλληλεξαρτήσεων, να ανακαλύπτει συγκεκριμένες περιπτώσεις στις οποίες ο υψηλός βαθμός συγκέντρωσης κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ στην Ένωση είναι πιθανό να ασκήσει πιέσεις στη σταθερότητα και στην ακεραιότητα του χρηματοοικονομικού συστήματος της Ένωσης και να διατηρεί διάλογο με κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, όταν εντοπίζεται ο συγκεκριμένος κίνδυνος.

(68) Για την αξιολόγηση και την παρακολούθηση σε τακτική βάση της ικανότητας τρίτου παρόχου υπηρεσιών ΤΠΕ να παρέχει με ασφάλεια υπηρεσίες σε χρηματοοικονομική οντότητα χωρίς δυσμενείς επιπτώσεις στην ψηφιακή επιχειρησιακή ανθεκτικότητά της, θα πρέπει να εναρμονιστούν διάφορα βασικά συμβατικά στοιχεία με τρίτους παρόχους υπηρεσιών ΤΠΕ. Η εναρμόνιση αυτή θα πρέπει να καλύπτει ελάχιστους τομείς που είναι ζωτικής σημασίας για την πλήρη παρακολούθηση από τη χρηματοοικονομική οντότητα των κινδύνων που θα μπορούσαν να προκύψουν από τον τρίτο πάροχο υπηρεσιών ΤΠΕ, από την άποψη της ανάγκης μιας χρηματοοικονομικής οντότητας να διασφαλίσει την ψηφιακή ανθεκτικότητά της, διότι εξαρτάται σε μεγάλο βαθμό από τη σταθερότητα, τη λειτουργικότητα, τη διαθεσιμότητα και την ασφάλεια των υπηρεσιών ΤΠΕ που λαμβάνει.

(69) Κατά την επαναδιαπραγμάτευση συμβατικών ρυθμίσεων με σκοπό την ευθυγράμμιση με τις απαιτήσεις του παρόντος κανονισμού, οι χρηματοοικονομικές οντότητες και οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ θα πρέπει να διασφαλίζουν την κάλυψη των βασικών συμβατικών διατάξεων, όπως προβλέπεται στον παρόντα κανονισμό.

(70) Ο ορισμός της «κρίσιμης ή σημαντικής λειτουργίας» που προβλέπεται στον παρόντα κανονισμό περιλαμβάνει τον ορισμό των «κρίσιμων λειτουργιών», όπως προβλέπεται στο άρθρο 2 παράγραφος 1 σημείο 35) της οδηγίας 2014/59/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([20]). Ως εκ τούτου, οι λειτουργίες που θεωρούνται κρίσιμες σύμφωνα με την οδηγία 2014/59/ΕΕ περιλαμβάνονται στον ορισμό των κρίσιμων λειτουργιών κατά την έννοια του παρόντος κανονισμού.

(71) Ανεξάρτητα από την κρισιμότητα ή τη σημασία της λειτουργίας που υποστηρίζεται από τις υπηρεσίες ΤΠΕ, οι συμβατικές ρυθμίσεις θα πρέπει να προβλέπουν ειδικότερα την πλήρη περιγραφή των λειτουργιών και των υπηρεσιών, των τοποθεσιών στις οποίες παρέχονται οι εν λόγω λειτουργίες και των τοποθεσιών στις οποίες τα δεδομένα θα υποβάλλονται σε επεξεργασία, καθώς και περιγραφή του επιπέδου υπηρεσιών. Άλλα ουσιώδη στοιχεία για να καταστεί δυνατή η παρακολούθηση των κινδύνων τρίτων μερών ΤΠΕ από μια χρηματοοικονομική οντότητα είναι: οι συμβατικές διατάξεις που καθορίζουν τον τρόπο με τον οποίο ο τρίτος πάροχος υπηρεσιών ΤΠΕ διασφαλίζει την προσβασιμότητα, τη διαθεσιμότητα, την ακεραιότητα, την ασφάλεια και την προστασία των δεδομένων προσωπικού χαρακτήρα, οι διατάξεις οι οποίες προβλέπουν τις σχετικές διασφαλίσεις που καθιστούν δυνατές την πρόσβαση, την ανάκτηση και την επιστροφή δεδομένων σε περίπτωση αφερεγγυότητας, εξυγίανσης ή διακοπής των επιχειρηματικών δραστηριοτήτων του τρίτου παρόχου υπηρεσιών ΤΠΕ, καθώς και οι διατάξεις που απαιτούν από τον τρίτο πάροχο υπηρεσιών ΤΠΕ να παρέχει συνδρομή σε περίπτωση συμβάντων ΤΠΕ σε σχέση με τις παρεχόμενες υπηρεσίες, χωρίς πρόσθετο κόστος ή με κόστος που καθορίζεται

([20]) Οδηγία 2014/59/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαΐου 2014, για τη θέσπιση πλαισίου για την ανάκαμψη και την εξυγίανση πιστωτικών ιδρυμάτων και επιχειρήσεων επενδύσεων και για την τροποποίηση της οδηγίας 82/891/ΕΟΚ του Συμβουλίου, και των οδηγιών 2001/24/ΕΚ, 2002/47/ΕΚ, 2004/25/ΕΚ, 2005/56/ΕΚ, 2007/36/ΕΚ, 2011/35/ΕΕ, 2012/30/ΕΕ και 2013/36/ΕΕ, καθώς και των κανονισμών του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (ΕΕ) αριθ. 1093/2010 και (ΕΕ) αριθ. 648/2012 (ΕΕ L 173 της 12.6.2014, σ. 190).

εκ των προτέρων· οι διατάξεις σχετικά με την υποχρέωση του τρίτου παρόχου υπηρεσιών ΤΠΕ να συνεργάζεται πλήρως με τις αρμόδιες αρχές και τις αρχές εξυγίανσης της χρηματοοικονομικής οντότητας· και οι διατάξεις σχετικά με τα δικαιώματα καταγγελίας και συναφείς ελάχιστες περιόδους προειδοποίησης για την καταγγελία των συμβατικών ρυθμίσεων, σύμφωνα με τις προσδοκίες των αρμόδιων αρχών και των αρχών εξυγίανσης.

(72) Εκτός από τις εν λόγω συμβατικές διατάξεις και προκειμένου να διασφαλιστεί ότι οι χρηματοοικονομικές οντότητες διατηρούν τον πλήρη έλεγχο όλων των εξελίξεων σε επίπεδο τρίτων μερών οι οποίες ενδέχεται να βλάψουν την ασφάλεια των ΤΠΕ τους, οι συμβάσεις για την παροχή υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες θα πρέπει επίσης να προβλέπουν τα ακόλουθα: πλήρεις περιγραφές σε επίπεδο υπηρεσιών, με ακριβείς ποσοτικούς και ποιοτικούς στόχους επιδόσεων, ώστε να καταστεί δυνατή η λήψη κατάλληλων διορθωτικών μέτρων, χωρίς αδικαιολόγητη καθυστέρηση, όταν δεν επιτυγχάνονται τα συμφωνηθέντα επίπεδα υπηρεσιών· τις σχετικές περιόδους προειδοποίησης και υποχρεώσεις αναφοράς για τον τρίτο πάροχο υπηρεσιών ΤΠΕ, σε περίπτωση εξελίξεων με δυνητικές σημαντικές επιπτώσεις στην ικανότητα του τρίτου παρόχου υπηρεσιών ΤΠΕ να παρέχει με αποτελεσματικό τρόπο τις αντίστοιχες υπηρεσίες ΤΠΕ· απαίτηση από τον τρίτο πάροχο υπηρεσιών ΤΠΕ να εφαρμόζει και να δοκιμάζει επιχειρησιακά σχέδια έκτακτης ανάγκης και να διαθέτει μέτρα, εργαλεία και πολιτικές ασφάλειας ΤΠΕ που επιτρέπουν την ασφαλή παροχή υπηρεσιών, καθώς και να συμμετέχει και να συνεργάζεται πλήρως στην TLPT που διενεργεί η χρηματοοικονομική οντότητα.

(73) Οι συμβάσεις για την παροχή υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες θα πρέπει επίσης να περιέχουν διατάξεις που διευκολύνουν την άσκηση των δικαιωμάτων πρόσβασης, επιθεώρησης και ελέγχου από τη χρηματοοικονομική οντότητα ή διορισμένο τρίτο και του δικαιώματος λήψης αντιγράφων ως μέσων καίριας σημασίας για τη συνεχή παρακολούθηση των επιδόσεων του τρίτου παρόχου υπηρεσιών ΤΠΕ από τις χρηματοοικονομικές οντότητες, σε συνδυασμό με την πλήρη συνεργασία του παρόχου υπηρεσιών κατά τη διάρκεια των επιθεωρήσεων. Ομοίως, η αρμόδια αρχή της χρηματοοικονομικής οντότητας θα πρέπει να έχει τη δυνατότητα να ασκεί, βάσει ειδοποιήσεων, τα δικαιώματα επιθεώρησης και ελέγχου του τρίτου παρόχου υπηρεσιών ΤΠΕ, με την επιφύλαξη της προστασίας εμπιστευτικών πληροφοριών.

(74) Οι εν λόγω συμβατικές ρυθμίσεις θα πρέπει επίσης να προβλέπουν εξειδικευμένες στρατηγικές εξόδου, ώστε να παρέχεται, ιδίως, η δυνατότητα καθορισμού υποχρεωτικών μεταβατικών περιόδων, κατά τη διάρκεια των οποίων οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ θα πρέπει να εξακολουθούν να παρέχουν τις σχετικές υπηρεσίες με στόχο τη μείωση του κινδύνου διαταραχών στο επίπεδο της χρηματοοικονομικής οντότητας ή την εξασφάλιση της δυνατότητας της χρηματοοικονομικής οντότητας να χρησιμοποιήσει άλλο τρίτο πάροχο υπηρεσιών ΤΠΕ ή να επιλέξει, εναλλακτικά, άλλες λύσεις εντός της επιχείρησης, ανάλογα με την πολυπλοκότητα των παρεχόμενων υπηρεσιών ΤΠΕ. Επιπλέον, οι χρηματοοικονομικές οντότητες που εμπίπτουν στο πεδίο εφαρμογής της οδηγίας 2014/59/ΕΕ θα πρέπει να διασφαλίζουν ότι οι σχετικές συμβάσεις για υπηρεσίες ΤΠΕ είναι άρτιες και πλήρως εκτελεστές σε περίπτωση εξυγίανσης των εν λόγω χρηματοοικονομικών οντοτήτων. Κατά συνέπεια, σύμφωνα με τις προσδοκίες των αρχών εξυγίανσης, οι εν λόγω χρηματοοικονομικές οντότητες θα πρέπει να διασφαλίζουν ότι οι σχετικές συμβάσεις για υπηρεσίες ΤΠΕ είναι ανθεκτικές στην εξυγίανση. Εφόσον εξακολουθούν να εκπληρώνουν τις υποχρεώσεις πληρωμής τους, οι εν λόγω χρηματοοικονομικές οντότητες θα πρέπει να διασφαλίζουν, μεταξύ άλλων απαιτήσεων, ότι οι σχετικές συμβάσεις για υπηρεσίες ΤΠΕ περιέχουν ρήτρες μη καταγγελίας, μη αναστολής και μη τροποποίησης για λόγους αναδιάρθρωσης ή εξυγίανσης.

(75) Επιπλέον, η προαιρετική χρήση τυποποιημένων συμβατικών ρητρών που έχουν αναπτύξει δημόσιες αρχές ή όργανα της Ένωσης, ιδίως η χρήση συμβατικών ρητρών που έχει αναπτύξει η Επιτροπή για τις υπηρεσίες υπολογιστικού νέφους, θα μπορούσε να εξυπηρετεί ακόμη περισσότερο τις χρηματοοικονομικές οντότητες και τους τρίτους παρόχους υπηρεσιών ΤΠΕ, με την ενίσχυση του επιπέδου ασφάλειας δικαίου όσον αφορά τη χρήση υπηρεσιών υπολογιστικού νέφους στον χρηματοοικονομικό τομέα, σε πλήρη εναρμόνιση με τις απαιτήσεις και τις προσδοκίες που προβλέπονται στη νομοθεσία της Ένωσης για τις χρηματοοικονομικές υπηρεσίες. Η ανάπτυξη τυποποιημένων συμβατικών ρητρών βασίζονται σε μέτρα που προβλέπονται ήδη στο σχέδιο δράσης του 2018 για τη χρηματοοικονομική τεχνολογία, στο πλαίσιο του οποίου ανακοινώθηκε η πρόθεση της Επιτροπής να ενθαρρύνει και να διευκολύνει την ανάπτυξη τυποποιημένων συμβατικών ρητρών για την εξωτερική ανάθεση σε πάροχο υπηρεσιών υπολογιστικού νέφους από τις χρηματοοικονομικές οντότητες, με βάση τις διατομεακές προσπάθειες των συμφεροντούχων στον τομέα του υπολογιστικού νέφους που έχουν ήδη διευκολυνθεί από την Επιτροπή με την εξασφάλιση της συμμετοχής του χρηματοοικονομικού τομέα.

(76) Με σκοπό την προώθηση της σύγκλισης και της αποτελεσματικότητας σε σχέση με τις εποπτικές προσεγγίσεις κατά την αντιμετώπιση κινδύνων τρίτων παρόχων ΤΠΕ στον χρηματοοικονομικό τομέα, καθώς και την ενίσχυση της ψηφιακής επιχειρησιακής ανθεκτικότητας των χρηματοοικονομικών οντοτήτων που βασίζονται σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ για την παροχή υπηρεσιών ΤΠΕ που υποστηρίζουν την παροχή χρηματοοικονομικών υπηρεσιών και, κατ' επέκταση, τη συμβολή στη διατήρηση της σταθερότητας του χρηματοοικονομικού συστήματος της Ένωσης και της ακεραιότητας της εσωτερικής αγοράς χρηματοοικονομικών υπηρεσιών, οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ θα πρέπει να υπόκεινται σε ενωσιακό πλαίσιο εποπτείας. Ενώ η θέσπιση του πλαισίου εποπτείας δικαιολογείται από την προστιθέμενη αξία της ανάληψης δράσης σε επίπεδο Ένωσης και λόγω του εγγενούς ρόλου και των ιδιαιτεροτήτων της

χρήσης υπηρεσιών ΤΠΕ στην παροχή χρηματοοικονομικών υπηρεσιών, θα πρέπει να υπενθυμιστεί ταυτόχρονα ότι η λύση αυτή φαίνεται κατάλληλη μόνο στο πλαίσιο του παρόντος κανονισμού που αφορά ειδικά την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα. Ωστόσο, το εν λόγω πλαίσιο εποπτείας δεν θα πρέπει να θεωρείται νέο μοντέλο ενωσιακής εποπτείας στους τομείς των χρηματοοικονομικών υπηρεσιών και δραστηριοτήτων.

(77) Το πλαίσιο εποπτείας θα πρέπει να εφαρμόζεται μόνο σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ. Ως εκ τούτου, θα πρέπει να υπάρχει ένας μηχανισμός ορισμού που θα λαμβάνει υπόψη τη διάσταση και τη φύση της εξάρτησης του χρηματοοικονομικού τομέα από τους εν λόγω τρίτους παρόχους υπηρεσιών ΤΠΕ. Ο εν λόγω μηχανισμός θα πρέπει να περιλαμβάνει ένα σύνολο ποσοτικών και ποιοτικών κριτηρίων για τον καθορισμό των παραμέτρων κρισιμότητας ως βάσης για την ένταξη στο πλαίσιο εποπτείας. Προκειμένου να διασφαλιστεί η ακρίβεια της εν λόγω αξιολόγησης, και ανεξάρτητα από την εταιρική δομή του τρίτου παρόχου υπηρεσιών ΤΠΕ, τα εν λόγω κριτήρια θα πρέπει, στην περίπτωση τρίτου παρόχου υπηρεσιών ΤΠΕ που ανήκει σε ευρύτερο όμιλο, να λαμβάνουν υπόψη ολόκληρη τη δομή του ομίλου του τρίτου παρόχου υπηρεσιών ΤΠΕ. Αφενός, οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ που δεν ορίζονται αυτομάτως δυνάμει της εφαρμογής των εν λόγω κριτηρίων θα πρέπει να έχουν τη δυνατότητα προαιρετικής συμμετοχής στο πλαίσιο εποπτείας· αφετέρου, οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ που υπόκεινται ήδη σε πλαίσια μηχανισμού εποπτείας προς υποστήριξη της εκτέλεσης των καθηκόντων του Ευρωπαϊκού Συστήματος Κεντρικών Τραπεζών με σκοπό την υποστήριξη των καθηκόντων, όπως αναφέρονται στο άρθρο 127 παράγραφος 2 ΣΛΕΕ, θα πρέπει να εξαιρούνται.

(78) Ομοίως, οι χρηματοοικονομικές οντότητες που παρέχουν υπηρεσίες ΤΠΕ σε άλλες χρηματοοικονομικές οντότητες, μολονότι ανήκουν στην κατηγορία των τρίτων παρόχων υπηρεσιών ΤΠΕ βάσει του παρόντος κανονισμού, θα πρέπει επίσης να εξαιρούνται από το πλαίσιο εποπτείας, δεδομένου ότι υπόκεινται ήδη σε εποπτικούς μηχανισμούς που θεσπίζονται από το σχετικό ενωσιακό δίκαιο για τις χρηματοοικονομικές υπηρεσίες. Κατά περίπτωση, οι αρμόδιες αρχές θα πρέπει να λαμβάνουν υπόψη, στο πλαίσιο των εποπτικών δραστηριοτήτων τους, τους κινδύνους ΤΠΕ που εγκυμονούν για τις χρηματοοικονομικές οντότητες οι χρηματοοικονομικές οντότητες που παρέχουν υπηρεσίες ΤΠΕ. Ομοίως, λόγω των υφιστάμενων μηχανισμών παρακολούθησης κινδύνων σε επίπεδο ομίλου, θα πρέπει να θεσπιστεί η ίδια εξαίρεση για τους τρίτους παρόχους υπηρεσιών ΤΠΕ που παρέχουν υπηρεσίες κυρίως στις οντότητες του δικού τους ομίλου. Οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ που παρέχουν υπηρεσίες ΤΠΕ αποκλειστικά σε ένα κράτος μέλος σε χρηματοοικονομικές οντότητες οι οποίες δραστηριοποιούνται μόνο στο εν λόγω κράτος μέλος θα πρέπει επίσης να εξαιρούνται από τον μηχανισμό ορισμού, λόγω των περιορισμένων δραστηριοτήτων τους και της έλλειψης διασυνοριακού αντικτύπου.

(79) Ο ψηφιακός μετασχηματισμός στον τομέα των χρηματοοικονομικών υπηρεσιών έχει οδηγήσει σε πρωτοφανές επίπεδο χρήσης υπηρεσιών ΤΠΕ και εξάρτησης από αυτές. Δεδομένου ότι έχει καταστεί αδιανόητο να παρέχονται χρηματοοικονομικές υπηρεσίες χωρίς τη χρήση υπηρεσιών υπολογιστικού νέφους, λύσεων λογισμικού και υπηρεσιών που σχετίζονται με δεδομένα, το χρηματοοικονομικό οικοσύστημα της Ένωσης εξαρτάται πλέον εγγενώς και από ορισμένες υπηρεσίες ΤΠΕ που παρέχονται από παρόχους υπηρεσιών ΤΠΕ. Ορισμένοι από αυτούς τους προμηθευτές, φορείς καινοτομίας στην ανάπτυξη και εφαρμογή τεχνολογιών που βασίζονται στις ΤΠΕ, διαδραματίζουν σημαντικό ρόλο στην παροχή χρηματοοικονομικών υπηρεσιών ή έχουν ενσωματωθεί στην αλυσίδα αξίας των χρηματοοικονομικών υπηρεσιών. Ως εκ τούτου, έχουν καταστεί ζωτικής σημασίας για τη σταθερότητα και την ακεραιότητα του χρηματοοικονομικού συστήματος της Ένωσης. Αυτή η ευρεία εξάρτηση από υπηρεσίες που παρέχονται από κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, σε συνδυασμό με την αλληλεξάρτηση των συστημάτων πληροφοριών διαφόρων φορέων της αγοράς, δημιουργεί άμεσο και δυνητικά σοβαρό κίνδυνο για το σύστημα χρηματοοικονομικών υπηρεσιών της Ένωσης και για τη συνέχεια της παροχής χρηματοοικονομικών υπηρεσιών σε περίπτωση που κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ επηρεαστούν από λειτουργικές διαταραχές ή μείζονα κυβερνοπεριστατικά. Τα κυβερνοπεριστατικά έχουν ιδιαίτερη ικανότητα να πολλαπλασιάζονται και να διαδίδονται σε ολόκληρο το χρηματοοικονομικό σύστημα με σημαντικά ταχύτερο ρυθμό από ό,τι άλλα είδη κινδύνου που παρακολουθούνται στον χρηματοοικονομικό τομέα και μπορούν να επεκταθούν σε διάφορους τομείς και πέραν των γεωγραφικών συνόρων. Έχουν τη δυνατότητα να εξελιχθούν σε συστημική κρίση, όπου η εμπιστοσύνη στο χρηματοοικονομικό σύστημα έχει διαβρωθεί λόγω της διαταραχής των λειτουργιών που στηρίζουν την πραγματική οικονομία, ή λόγω σημαντικών οικονομικών ζημιών, που φθάνουν σε επίπεδο κατά το οποίο το χρηματοοικονομικό σύστημα δεν είναι σε θέση να αντεπεξέλθει ή που απαιτεί την υλοποίηση αυστηρών μέτρων απορρόφησης των κραδασμών. Για να αποτραπεί η υλοποίηση αυτών των σεναρίων, πράγμα το οποίο θα έθετε σε κίνδυνο τη χρηματοοικονομική σταθερότητα και την ακεραιότητα της Ένωσης, είναι σημαντικό να εξασφαλιστεί η σύγκλιση των εποπτικών πρακτικών σχετικά με τους κινδύνους τρίτων μερών ΤΠΕ στον χρηματοοικονομικό τομέα, ιδίως μέσω νέων κανόνων που θα επιτρέπουν την ενωσιακή εποπτεία κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ.

(80) Το πλαίσιο εποπτείας εξαρτάται σε μεγάλο βαθμό από τον βαθμό συνεργασίας μεταξύ του κύριου εποπτικού φορέα και του κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ που παρέχει σε χρηματοοικονομικές οντότητες υπηρεσίες που επηρεάζουν την παροχή χρηματοοικονομικών υπηρεσιών. Η επιτυχής εποπτεία βασίζεται, μεταξύ άλλων, στην ικανότητα του κύριου εποπτικού φορέα να διενεργεί αποτελεσματικά αποστολές παρακολούθησης και επιθεωρήσεις για την αξιολόγηση των κανόνων, των δικλείδων ασφάλειας και των διαδικασιών που χρησιμοποιούνται από τους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, καθώς και για την αξιολόγηση του δυνητικού σωρευτικού αντικτύπου των δραστηριοτήτων τους στη χρηματοοικονομική σταθερότητα και την ακεραιότητα του χρηματοοικονομικού συστήματος. Ταυτόχρονα, είναι ζωτικής σημασίας οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ να ακολουθούν τις συστάσεις του κύριου εποπτικού φορέα και να αντιμετωπίζουν τους προβληματισμούς του. Δεδομένου ότι η έλλειψη συνεργασίας από κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ που παρέχει υπηρεσίες οι οποίες επηρεάζουν την παροχή χρηματοοικονομικών υπηρεσιών, όπως η άρνηση χορήγησης πρόσβασης στις εγκαταστάσεις του ή υποβολής πληροφοριών, θα στερούσε τελικά τον κύριο εποπτικό φορέα από τα βασικά εργαλεία του για την αξιολόγηση κινδύνου ΤΠΕ τρίτων και θα μπορούσε να επηρεάσει αρνητικά τη χρηματοοικονομική σταθερότητα και την ακεραιότητα του χρηματοοικονομικού συστήματος, είναι επίσης αναγκαίο να προβλεφθεί ανάλογο καθεστώς κυρώσεων.

(81) Στο πλαίσιο αυτό, η ανάγκη του κύριου εποπτικού φορέα να επιβάλει χρηματικές ποινές για να υποχρεώσει τους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ να συμμορφώνονται με τις υποχρεώσεις διαφάνειας και πρόσβασης που ορίζονται στον παρόντα κανονισμό δεν θα πρέπει να υπονομεύεται από τις δυσκολίες οι οποίες ανακύπτουν από την επιβολή των εν λόγω χρηματικών ποινών σε σχέση με κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ που είναι εγκατεστημένοι σε τρίτες χώρες. Προκειμένου να διασφαλιστεί η εκτελεστότητα των εν λόγω ποινών και να καταστεί δυνατή η ταχεία εφαρμογή των διαδικασιών που διαφυλάσσουν τα κρίσιμα δικαιώματα υπεράσπισης των τρίτων παρόχων υπηρεσιών ΤΠΕ στο πλαίσιο του μηχανισμού ορισμού και της έκδοσης συστάσεων, θα πρέπει να απαιτείται από τους εν λόγω κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, οι οποίοι παρέχουν υπηρεσίες σε χρηματοοικονομικές οντότητες υπηρεσίες που επηρεάζουν την παροχή χρηματοοικονομικών υπηρεσιών, να διατηρούν επαρκή επιχειρηματική παρουσία στην Ένωση. Λόγω της φύσης της εποπτείας και της απουσίας συγκρίσιμων ρυθμίσεων σε άλλες δικαιοδοσίες, δεν υπάρχουν κατάλληλοι εναλλακτικοί μηχανισμοί που να διασφαλίζουν αυτόν τον στόχο μέσω της αποτελεσματικής συνεργασίας με τις αρχές χρηματοοικονομικής εποπτείας σε τρίτες χώρες σε σχέση με την παρακολούθηση του αντικτύπου των ψηφιακών λειτουργικών κινδύνων που εγκυμονούν οι συστημικοί τρίτοι πάροχοι υπηρεσιών ΤΠΕ, οι οποίοι χαρακτηρίζονται κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ που είναι εγκατεστημένοι σε τρίτες χώρες. Ως εκ τούτου, προκειμένου να συνεχίσει την παροχή υπηρεσιών ΤΠΕ σε χρηματοοικονομικές οντότητες στην Ένωση, τρίτος πάροχος υπηρεσιών ΤΠΕ που είναι εγκατεστημένος σε τρίτη χώρα και έχει οριστεί ως κρίσιμος σύμφωνα με τον παρόντα κανονισμό θα πρέπει να προβεί, εντός 12 μηνών από τον εν λόγω ορισμό, σε όλες τις αναγκαίες ρυθμίσεις για να διασφαλίσει την ενσωμάτωσή του στην Ένωση, μέσω της σύστασης θυγατρικής, όπως ορίζεται σε ολόκληρο το κεκτημένο της Ένωσης, και συγκεκριμένα στην οδηγία 2013/34/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([21]).

(82) Η απαίτηση σύστασης θυγατρικής στην Ένωση δεν θα πρέπει να εμποδίζει τον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ να παρέχει υπηρεσίες ΤΠΕ και σχετική τεχνική υποστήριξη από εγκαταστάσεις και υποδομές που βρίσκονται εκτός της Ένωσης. Ο παρών κανονισμός δεν επιβάλλει υποχρέωση γεωγραφικού περιορισμού δεδομένων, καθώς δεν απαιτεί αποθήκευση ή επεξεργασία δεδομένων στην Ένωση.

(83) Οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ θα πρέπει να είναι σε θέση να παρέχουν υπηρεσίες ΤΠΕ από οπουδήποτε στον κόσμο και όχι απαραίτητα ή όχι μόνο από εγκαταστάσεις που βρίσκονται στην Ένωση. Οι δραστηριότητες εποπτείας θα πρέπει πρώτα να διεξάγονται σε εγκαταστάσεις που βρίσκονται στην Ένωση και να αλληλεπιδρούν με οντότητες που βρίσκονται στην Ένωση, συμπεριλαμβανομένων των θυγατρικών που έχουν συσταθεί από κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ σύμφωνα με τον παρόντα κανονισμό. Ωστόσο, οι εν λόγω δράσεις εντός της Ένωσης ενδέχεται να μην επαρκούν για να επιτρέψουν στον κύριο εποπτικό φορέα να εκτελέσει πλήρως και αποτελεσματικά τα καθήκοντά του δυνάμει του παρόντος κανονισμού. Ως εκ τούτου, ο κύριος εποπτικός φορέας θα πρέπει επίσης να είναι σε θέση να ασκεί τις σχετικές εποπτικές εξουσίες του σε τρίτες χώρες. Η άσκηση των εν λόγω εξουσιών σε τρίτες χώρες θα πρέπει να επιτρέπει στον κύριο εποπτικό φορέα να εξετάζει τις εγκαταστάσεις από τις οποίες όντως παρέχονται ή αποτελούν αντικείμενο διαχείρισης οι υπηρεσίες ΤΠΕ ή οι υπηρεσίες τεχνικής υποστήριξης από τον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ και θα πρέπει να επιτρέπει στον κύριο εποπτικό φορέα ολοκληρωμένη και επιχειρησιακή κατανόηση της διαχείρισης κινδύνων ΤΠΕ του κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ. Η δυνατότητα του κύριου εποπτικού φορέα, ως οργανισμού της Ένωσης, να ασκεί εξουσίες εκτός της επικράτειας της Ένωσης θα πρέπει να πλαισιώνεται δεόντως από σχετικούς όρους, ιδίως από τη συγκατάθεση του κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ. Ομοίως, οι αρμόδιες αρχές της τρίτης χώρας θα πρέπει να ενημερώνονται για την άσκηση των δραστηριοτήτων του κύριου εποπτικού φορέα στο έδαφός τους και να μην έχουν προβάλει σχετική αντίρρηση. Ωστόσο, προκειμένου να διασφαλιστεί η αποτελεσματική εφαρμογή, και με την επιφύλαξη των αντίστοιχων αρμοδιοτήτων των θεσμικών οργάνων και των κρατών μελών της Ένωσης, οι εξουσίες αυτές

([21]) Οδηγία 2013/34/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Ιουνίου 2013, σχετικά με τις ετήσιες οικονομικές καταστάσεις, τις ενοποιημένες οικονομικές καταστάσεις και συναφείς εκθέσεις επιχειρήσεων ορισμένων μορφών, την τροποποίηση της οδηγίας 2006/43/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και την κατάργηση των οδηγιών 78/660/ΕΟΚ και 83/349/ΕΟΚ του Συμβουλίου (ΕΕ L 182 της 29.6.2013, σ. 19).

είναι ανάγκη επίσης να βασίζονται πλήρως στη σύναψη ρυθμίσεων διοικητικής συνεργασίας με τις σχετικές αρχές της οικείας τρίτης χώρας. Ως εκ τούτου, ο παρών κανονισμός θα πρέπει να επιτρέπει στις ΕΕΑ να συνάπτουν ρυθμίσεις διοικητικής συνεργασίας με τις αρμόδιες αρχές τρίτων χωρών, οι οποίες δεν θα πρέπει διαφορετικά να δημιουργούν νομικές υποχρεώσεις έναντι της Ένωσης και των κρατών μελών της.

(84) Για τη διευκόλυνση της επικοινωνίας με τον κύριο εποπτικό φορέα και για τη διασφάλιση επαρκούς εκπροσώπησης, οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ που αποτελούν μέρος ομίλου θα πρέπει να ορίζουν ένα νομικό πρόσωπο ως σημείο συντονισμού τους.

(85) Το πλαίσιο εποπτείας δεν θα πρέπει να θίγει την αρμοδιότητα των κρατών μελών να πραγματοποιούν δικές τους αποστολές εποπτείας ή παρακολούθησης όσον αφορά τρίτους παρόχους υπηρεσιών ΤΠΕ οι οποίοι δεν έχουν οριστεί ως κρίσιμοι βάσει του παρόντος κανονισμού αλλά θα μπορούσαν να θεωρηθούν σημαντικοί σε εθνικό επίπεδο.

(86) Για την αξιοποίηση της πολυεπίπεδης θεσμικής αρχιτεκτονικής στον τομέα των χρηματοοικονομικών υπηρεσιών, η μεικτή επιτροπή των ΕΕΑ θα πρέπει να συνεχίσει να διασφαλίζει τον συνολικό διατομεακό συντονισμό σε σχέση με όλα τα θέματα που αφορούν τους κινδύνους ΤΠΕ, σύμφωνα με τα καθήκοντά της για την κυβερνοασφάλεια. Θα πρέπει να υποστηρίζεται από νέα υποεπιτροπή («φόρουμ εποπτείας») που εκτελεί τις προπαρασκευαστικές εργασίες τόσο για τις μεμονωμένες αποφάσεις που απευθύνονται σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, όσο και για την έκδοση συλλογικών συστάσεων, ιδίως σχετικά με τη συγκριτική αξιολόγηση των προγραμμάτων εποπτείας κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ και τον προσδιορισμό βέλτιστων πρακτικών για την αντιμετώπιση ζητημάτων κινδύνου συγκέντρωσης ΤΠΕ.

(87) Προκειμένου να διασφαλιστεί η κατάλληλη και αποτελεσματική εποπτεία των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ σε ενωσιακό επίπεδο, ο παρών κανονισμός προβλέπει ότι οποιαδήποτε από τις τρεις ΕΕΑ θα μπορούσε να οριστεί ως κύριος εποπτικός φορέας. Η ατομική ανάθεση ενός κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ σε μία από τις τρεις ΕΕΑ θα πρέπει να προκύπτει από αξιολόγηση της κυριαρχίας των χρηματοοικονομικών οντοτήτων που δραστηριοποιούνται στους χρηματοοικονομικούς τομείς για τους οποίους η ΕΕΑ έχει αρμοδιότητες. Η προσέγγιση αυτή θα πρέπει να οδηγήσει σε ισόρροπη κατανομή καθηκόντων και αρμοδιοτήτων μεταξύ των τριών ΕΕΑ, στο πλαίσιο της άσκησης των λειτουργιών εποπτείας, και θα πρέπει να αξιοποιεί με τον καλύτερο δυνατό τρόπο τους ανθρώπινους πόρους και την τεχνική εμπειρογνωσία που διαθέτει καθεμία από τις τρεις ΕΕΑ.

(88) Θα πρέπει να χορηγηθούν στους κύριους εποπτικούς φορείς οι απαραίτητες εξουσίες για τη διεξαγωγή ερευνών, τη διενέργεια επιτόπιων και εξ αποστάσεως επιθεωρήσεων στις εγκαταστάσεις και τοποθεσίες κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ και την απόκτηση πλήρων και επικαιροποιημένων πληροφοριών. Οι εν λόγω εξουσίες θα πρέπει να επιτρέπουν στον κύριο εποπτικό φορέα να αποκτήσει πραγματική εικόνα ως προς το είδος, τη διάσταση και τον αντίκτυπο των κινδύνων τρίτων παρόχων ΤΠΕ για τις χρηματοοικονομικές οντότητες και, εντέλει, για το χρηματοοικονομικό σύστημα της Ένωσης. Η ανάθεση στις ΕΕΑ του κύριου εποπτικού ρόλου συνιστά προϋπόθεση για την κατανόηση και την αντιμετώπιση της συστημικής διάστασης των κινδύνων ΤΠΕ στον χρηματοοικονομικό τομέα. Ο αντίκτυπος των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ στον χρηματοοικονομικό τομέα της Ένωσης και τα πιθανά ζητήματα που προκαλούνται από τον συνεπαγόμενο κίνδυνο συγκέντρωσης ΤΠΕ απαιτούν την υιοθέτηση συλλογικής προσέγγισης σε επίπεδο Ένωσης. Η ταυτόχρονη άσκηση πολλαπλών δικαιωμάτων ελέγχων και πρόσβασης, χωριστά από πολλές αρμόδιες αρχές, με ελάχιστο ή μηδενικό συντονισμό μεταξύ τους, θα εμπόδιζε τις χρηματοοικονομικές εποπτικές αρχές να αποκτήσουν πλήρη και ολοκληρωμένη επισκόπηση των κινδύνων τρίτων μερών ΤΠΕ στην Ένωση, ενώ παράλληλα θα δημιουργούσε πλεονασμό, επιβάρυνση και πολυπλοκότητα για τους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, εάν υπόκειντο σε πολυάριθμα αιτήματα παρακολούθησης και επιθεώρησης.

(89) Λόγω του σημαντικού αντικτύπου του ορισμού τους ως κρίσιμων, ο παρών κανονισμός θα πρέπει να διασφαλίζει ότι τα δικαιώματα των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ τηρούνται καθ' όλη τη διάρκεια εφαρμογής του πλαισίου εποπτείας. Πριν από τον ορισμό τους ως κρίσιμων, οι εν λόγω πάροχοι θα πρέπει, για παράδειγμα, να έχουν το δικαίωμα να υποβάλλουν στον κύριο εποπτικό φορέα αιτιολογημένη δήλωση που περιέχει κάθε σχετική πληροφορία για τους σκοπούς της αξιολόγησης που σχετίζεται με τον χαρακτηρισμό τους. Δεδομένου ότι ο κύριος εποπτικός φορέας θα πρέπει να εξουσιοδοτηθεί να υποβάλλει συστάσεις σχετικά με θέματα κινδύνων ΤΠΕ και κατάλληλα σχετικά διορθωτικά μέτρα, τα οποία περιλαμβάνουν την εξουσία εναντίωσης σε ορισμένες συμβατικές ρυθμίσεις που έχουν εντέλει αντίκτυπο στη σταθερότητα της χρηματοοικονομικής οντότητας ή του χρηματοοικονομικού συστήματος, οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ θα πρέπει επίσης να έχουν τη δυνατότητα να παρέχουν, πριν από την οριστικοποίηση των εν λόγω συστάσεων, εξηγήσεις σχετικά με τον αναμενόμενο αντίκτυπο των λύσεων που προβλέπονται στις συστάσεις σε πελάτες που είναι οντότητες οι οποίες δεν εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού, καθώς και να διατυπώνουν λύσεις

για τον μετριασμό των κινδύνων. Οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ που διαφωνούν με τις συστάσεις θα πρέπει να υποβάλουν αιτιολογημένη εξήγηση της πρόθεσής τους να μην εγκρίνουν τη σύσταση. Όταν η εν λόγω αιτιολογημένη εξήγηση δεν υποβάλλεται ή όταν κρίνεται ανεπαρκής, ο κύριος εποπτικός φορέας θα πρέπει να εκδίδει δημόσια ανακοίνωση στην οποία θα περιγράφεται συνοπτικά το ζήτημα της μη συμμόρφωσης.

(90) Οι αρμόδιες αρχές θα πρέπει να συμπεριλάβουν δεόντως το καθήκον της επαλήθευσης της ουσιαστικής συμμόρφωσης με τις συστάσεις που εκδίδει ο κύριος εποπτικός φορέας στα καθήκοντά τους όσον αφορά την προληπτική εποπτεία των χρηματοοικονομικών οντοτήτων. Οι αρμόδιες αρχές θα πρέπει να είναι σε θέση να απαιτούν από τις χρηματοοικονομικές οντότητες να λαμβάνουν πρόσθετα μέτρα για την αντιμετώπιση των κινδύνων που προσδιορίζονται στις συστάσεις του κύριου εποπτικού φορέα και θα πρέπει, σε εύθετο χρόνο, να εκδίδουν σχετικές κοινοποιήσεις. Όταν ο κύριος εποπτικός φορέας απευθύνει συστάσεις σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ που εποπτεύονται βάσει της οδηγίας (ΕΕ) 2022/2555 οι αρμόδιες αρχές θα πρέπει να μπορούν, σε προαιρετική βάση, και πριν από τη θέσπιση πρόσθετων μέτρων, να διαβουλεύονται με τις αρμόδιες αρχές βάσει της εν λόγω οδηγίας για την προώθηση συντονισμένης προσέγγισης όσον αφορά τους εν λόγω κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ.

(91) Η άσκηση της εποπτείας θα πρέπει να καθοδηγείται από τρεις επιχειρησιακές αρχές που αποσκοπούν στη διασφάλιση: α) στενής συνεργασίας μεταξύ των ΕΕΑ όσον αφορά τους κύριους εποπτικούς ρόλους τους, μέσω κοινού δικτύου εποπτείας (ΔΚΕ), β) συνέπειας με το πλαίσιο που θεσπίστηκε με την οδηγία (ΕΕ) 2022/2555 (μέσω προαιρετικής διαβούλευσης με οργανισμούς βάσει της εν λόγω οδηγίας για την αποφυγή επικάλυψης μέτρων τα οποία απευθύνονται σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ) και γ) επίδειξης επιμέλειας για την ελαχιστοποίηση του δυνητικού κινδύνου διαταραχής των υπηρεσιών οι οποίες παρέχονται από κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ σε πελάτες που είναι οντότητες μη εμπίπτουσες στο πεδίο εφαρμογής του παρόντος κανονισμού.

(92) Το πλαίσιο εποπτείας δεν θα πρέπει να αντικαθιστά ούτε να υποκαθιστά καθ' οιονδήποτε τρόπο και για κανένα μέρος την απαίτηση της διαχείρισης, από τις χρηματοοικονομικές οντότητες, των κινδύνων που συνεπάγεται η χρήση τρίτων παρόχων υπηρεσιών ΤΠΕ, συμπεριλαμβανομένης της υποχρέωσής τους να διατηρούν συνεχή παρακολούθηση συμβατικών ρυθμίσεων που συνάπτονται με κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ. Ομοίως, το πλαίσιο εποπτείας δεν θα πρέπει να επηρεάζει την πλήρη ευθύνη των χρηματοοικονομικών οντοτήτων όσον αφορά τη συμμόρφωσή τους με όλες τις νομικές υποχρεώσεις που περιλαμβάνονται στον παρόντα κανονισμό και στο σχετικό δίκαιο για τις χρηματοοικονομικές υπηρεσίες, καθώς και την εκπλήρωση αυτών.

(93) Για την αποφυγή επαναλήψεων και αλληλεπικαλύψεων, οι αρμόδιες αρχές θα πρέπει να αποφεύγουν τη λήψη μεμονωμένων μέτρων που αποσκοπούν στην παρακολούθηση των κινδύνων κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ και θα πρέπει, εν προκειμένω, να βασίζονται στη σχετική αξιολόγηση του κύριου εποπτικού φορέα. Όλα τα μέτρα θα πρέπει σε κάθε περίπτωση να συντονίζονται και να συμφωνούνται εκ των προτέρων με τον κύριο εποπτικό φορέα στο πλαίσιο της άσκησης των καθηκόντων του πλαισίου εποπτείας.

(94) Για την προώθηση της σύγκλισης σε διεθνές επίπεδο όσον αφορά τη χρήση βέλτιστων πρακτικών κατά την επανεξέταση και την παρακολούθηση της διαχείρισης ψηφιακών κινδύνων από τρίτους παρόχους υπηρεσιών ΤΠΕ, οι ΕΕΑ θα πρέπει να ενθαρρύνονται να συνάπτουν ρυθμίσεις συνεργασίας με τις αρμόδιες εποπτικές και ρυθμιστικές αρχές τρίτων χωρών.

(95) Για την αξιοποίηση των συγκεκριμένων αρμοδιοτήτων, των τεχνικών δεξιοτήτων και της εμπειρογνωσίας του προσωπικού που ειδικεύεται στους επιχειρησιακούς κινδύνους και κινδύνους ΤΠΕ στους κόλπους των αρμόδιων αρχών, των τριών ΕΑΑ και, σε προαιρετική βάση, των αρμόδιων αρχών δυνάμει της οδηγίας (ΕΕ) 2022/2555 ο κύριος εποπτικός φορέας θα πρέπει να αξιοποιεί τις εθνικές εποπτικές ικανότητες και γνώσεις και να συγκροτεί ειδικές εξεταστικές ομάδες για κάθε κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ, συγκεντρώνοντας διεπιστημονικές ομάδες για την υποστήριξη της προετοιμασίας και της εκτέλεσης των δραστηριοτήτων εποπτείας, συμπεριλαμβανομένων των γενικών ερευνών και επιθεωρήσεων κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ, καθώς και για οποιαδήποτε αναγκαία παρακολούθησή τους.

(96) Ενώ οι δαπάνες που προκύπτουν από τα καθήκοντα εποπτείας θα χρηματοδοτούνται πλήρως από τέλη που επιβάλλονται σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, οι ΕΕΑ είναι, ωστόσο, πιθανό να επιβαρυνθούν, πριν από την έναρξη του πλαισίου εποπτείας, με δαπάνες για την εφαρμογή ειδικών συστημάτων ΤΠΕ που υποστηρίζουν την επικείμενη εποπτεία, δεδομένου ότι θα πρέπει να αναπτυχθούν και να εφαρμοστούν εκ των προτέρων ειδικά συστήματα ΤΠΕ. Ως εκ τούτου, ο παρών κανονισμός προβλέπει ένα μοντέλο υβριδικής χρηματοδότησης, βάσει του οποίου το πλαίσιο εποπτείας θα χρηματοδοτείται πλήρως από τέλη, ενώ η ανάπτυξη των συστημάτων ΤΠΕ των ΕΕΑ θα χρηματοδοτείται από συνεισφορές της Ένωσης και των εθνικών αρμόδιων αρχών.

(97) Οι αρμόδιες αρχές θα πρέπει να διαθέτουν όλες τις απαιτούμενες εξουσίες εποπτείας, έρευνας και επιβολής κυρώσεων που είναι απαραίτητες για τη διασφάλιση της ορθής άσκησης των καθηκόντων τους δυνάμει του παρόντος κανονισμού. Θα πρέπει, καταρχήν, να δημοσιεύουν ανακοινώσεις σχετικά με τις διοικητικές κυρώσεις που επιβάλλουν. Δεδομένου ότι οι χρηματοοικονομικές οντότητες και οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ μπορούν να είναι εγκατεστημένοι σε διαφορετικά κράτη μέλη και να τελούν υπό την εποπτεία διαφορετικών αρμόδιων αρχών, η εφαρμογή του παρόντος κανονισμού θα πρέπει να διευκολύνεται, αφενός, από τη στενή συνεργασία μεταξύ των σχετικών αρμόδιων αρχών, συμπεριλαμβανομένης της ΕΚΤ όσον αφορά συγκεκριμένα καθήκοντα που της ανατίθενται βάσει του κανονισμού (ΕΕ) αριθ. 1024/2013 του Συμβουλίου, και, αφετέρου, από τη διαβούλευση με τις ΕΕΑ μέσω της αμοιβαίας ανταλλαγής πληροφοριών και της παροχής συνδρομής στο πλαίσιο των σχετικών εποπτικών δραστηριοτήτων.

(98) Για τον περαιτέρω ποσοτικό και ποιοτικό προσδιορισμό των κριτηρίων για τον ορισμό τρίτων παρόχων υπηρεσιών ΤΠΕ ως κρίσιμων και για την εναρμόνιση των τελών εποπτείας, θα πρέπει να ανατεθεί στην Επιτροπή η εξουσία να εκδίδει πράξεις, σύμφωνα με το άρθρο 290 ΣΛΕΕ για τη συμπλήρωση του παρόντος κανονισμού, προσδιορίζοντας περαιτέρω τις συστημικές επιπτώσεις που θα μπορούσε να έχει η αθέτηση υποχρεώσεων ή η διακοπή λειτουργίας τρίτου παρόχου υπηρεσιών ΤΠΕ στις χρηματοοικονομικές οντότητες στις οποίες παρέχει υπηρεσίες ΤΠΕ, τον αριθμό των παγκόσμιων συστημικώς σημαντικών ιδρυμάτων (G-SII) ή άλλων συστημικώς σημαντικών ιδρυμάτων (O-SII) που βασίζονται στον αντίστοιχο τρίτο πάροχο υπηρεσιών ΤΠΕ, τον αριθμό των τρίτων παρόχων υπηρεσιών ΤΠΕ που δραστηριοποιούνται σε συγκεκριμένη αγορά, το κόστος μετάβασης δεδομένων και φόρτου εργασίας ΤΠΕ σε άλλον τρίτο πάροχο υπηρεσιών ΤΠΕ, καθώς και το ύψος των τελών εποπτείας και τον τρόπο με τον οποίο πρέπει να καταβάλλονται. Είναι ιδιαίτερα σημαντικό η Επιτροπή να διεξάγει, κατά τις προπαρασκευαστικές της εργασίες, τις κατάλληλες διαβουλεύσεις, μεταξύ άλλων σε επίπεδο εμπειρογνωμόνων, οι οποίες να πραγματοποιούνται σύμφωνα με τις αρχές που ορίζονται στη διοργανική συμφωνία της 13ης Απριλίου 2016 για τη βελτίωση του νομοθετικού έργου ([22]). Πιο συγκεκριμένα, προκειμένου να διασφαλιστεί η ίση συμμετοχή στην προετοιμασία των κατ' εξουσιοδότηση πράξεων, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο θα πρέπει να λαμβάνουν όλα τα έγγραφα κατά τον ίδιο χρόνο με τους εμπειρογνώμονες των κρατών μελών, και οι εμπειρογνώμονές τους θα πρέπει να έχουν συστηματικά πρόσβαση στις συνεδριάσεις των ομάδων εμπειρογνωμόνων της Επιτροπής που ασχολούνται με την προετοιμασία κατ' εξουσιοδότηση πράξεων.

(99) Η συνεκτική εναρμόνιση των απαιτήσεων που καθορίζονται στον παρόντα κανονισμό θα πρέπει να διασφαλίζεται με ρυθμιστικά τεχνικά πρότυπα. Σύμφωνα με τους ρόλους τους ως φορείς που διαθέτουν υψηλό επίπεδο εμπειρογνωσίας, οι ΕΑΑ θα πρέπει να αναπτύσσουν ρυθμιστικά τεχνικά πρότυπα που δεν συνεπάγονται επιλογές πολιτικής και τα οποία πρέπει να υποβάλλονται στην Επιτροπή. Θα πρέπει να αναπτυχθούν ρυθμιστικά τεχνικά πρότυπα στους τομείς της διαχείρισης κινδύνων ΤΠΕ, της αναφοράς μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ, των δοκιμών, καθώς και σε σχέση με βασικές απαιτήσεις για την ορθή παρακολούθηση των κινδύνων τρίτων παρόχων ΤΠΕ. Η Επιτροπή και οι ΕΕΑ θα πρέπει να διασφαλίζουν ότι τα εν λόγω πρότυπα και απαιτήσεις μπορούν να εφαρμόζονται από όλες τις χρηματοοικονομικές οντότητες κατά τρόπο ανάλογο προς το μέγεθος και το συνολικό προφίλ κινδύνου τους και τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών τους. Θα πρέπει επίσης να ανατεθεί στην Επιτροπή η εξουσία να εγκρίνει τα εν λόγω ρυθμιστικά τεχνικά πρότυπα μέσω κατ' εξουσιοδότηση πράξεων δυνάμει του άρθρου 290 ΣΛΕΕ και σύμφωνα με τα άρθρα 10 έως 14 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010.

(100) Προκειμένου να διευκολυνθεί η συγκρισιμότητα των αναφορών μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ και μειζόνων λειτουργικών συμβάντων ή συμβάντων ασφάλειας που σχετίζονται με πληρωμές, καθώς και να διασφαλιστεί η διαφάνεια όσον αφορά τις συμβατικές ρυθμίσεις για τη χρήση των υπηρεσιών ΤΠΕ που παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ, οι ΕΕΑ θα πρέπει να αναπτύσσουν σχέδια εκτελεστικών τεχνικών προτύπων για την κατάρτιση τυποποιημένων υποδειγμάτων, εντύπων και διαδικασιών, ώστε οι χρηματοοικονομικές οντότητες να είναι σε θέση να αναφέρουν μείζον συμβάν που σχετίζεται με τις ΤΠΕ και μείζον λειτουργικό συμβάν ή συμβάν ασφάλειας που σχετίζεται με πληρωμές, καθώς και τυποποιημένων υποδειγμάτων για το μητρώο πληροφοριών. Κατά την ανάπτυξη των εν λόγω προτύπων, οι ΕΕΑ θα πρέπει να λαμβάνουν υπόψη το μέγεθος και το συνολικό προφίλ κινδύνου της χρηματοοικονομικής οντότητας και τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών της. Θα πρέπει επίσης να ανατεθεί στην Επιτροπή η εξουσία να εγκρίνει τα εν λόγω εκτελεστικά τεχνικά πρότυπα μέσω εκτελεστικών πράξεων δυνάμει του άρθρου 291 ΣΛΕΕ και του άρθρου 15 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010.

([22]) ΕΕ L 123 της 12.5.2016, σ. 1.

(101) Δεδομένου ότι έχουν ήδη καθοριστεί περαιτέρω απαιτήσεις μέσω κατ' εξουσιοδότηση και εκτελεστικών πράξεων βάσει ρυθμιστικών και εκτελεστικών τεχνικών προτύπων που περιλαμβάνονται στους κανονισμούς (ΕΚ) αριθ. 1060/2009 ([23]), (ΕΕ) αριθ. 648/2012 ([24]), (ΕΕ) αριθ. 600/2014 ([25]) και (ΕΕ) αριθ. 909/2014 ([26]) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, είναι σκόπιμο να ανατεθεί στις ΕΕΑ η εντολή, είτε μεμονωμένα είτε από κοινού μέσω της μεικτής επιτροπής, να υποβάλλουν ρυθμιστικά και εκτελεστικά τεχνικά πρότυπα στην Επιτροπή για την έκδοση κατ' εξουσιοδότηση και εκτελεστικών πράξεων με τις οποίες θα μεταφέρονται και θα επικαιροποιούνται οι υφιστάμενοι κανόνες διαχείρισης κινδύνων ΤΠΕ.

(102) Δεδομένου ότι ο παρών κανονισμός, σε συνδυασμό με την οδηγία (ΕΕ) 2022/2556 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([27]), συνεπάγεται την ενοποίηση των διατάξεων διαχείρισης κινδύνων ΤΠΕ που περιλαμβάνονται σε μεγάλο αριθμό κανονισμών και οδηγιών του κεκτημένου της Ένωσης στον τομέα των χρηματοοικονομικών υπηρεσιών, συμπεριλαμβανομένων των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014 και (ΕΕ) αριθ. 909/2014 και του κανονισμού (ΕΕ) 2016/1011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([28]), και για τους σκοπούς της διασφάλισης πλήρους διαφάνειας, οι εν λόγω κανονισμοί θα πρέπει να τροποποιηθούν ώστε να αποσαφηνιστεί ότι οι εφαρμοστέες διατάξεις που σχετίζονται με τους κινδύνους ΤΠΕ καθορίζονται στον παρόντα κανονισμό.

(103) Κατά συνέπεια, το πεδίο εφαρμογής των σχετικών άρθρων που αφορούν τον λειτουργικό κίνδυνο, βάσει των οποίων ασκήθηκαν οι εξουσιοδοτήσεις που προβλέπονται στους κανονισμούς (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 για την ανάθεση της εντολής έκδοσης κατ' εξουσιοδότηση και εκτελεστικών πράξεων, θα πρέπει να περιοριστεί ενόψει της μεταφοράς στον παρόντα κανονισμό όλων των διατάξεων που καλύπτουν τις πτυχές της ψηφιακής επιχειρησιακής ανθεκτικότητας και αποτελούν σήμερα μέρος των εν λόγω κανονισμών.

(104) Ο δυνητικός συστημικός κίνδυνος στον κυβερνοχώρο που συνδέεται με τη χρήση υποδομών ΤΠΕ οι οποίες καθιστούν δυνατή τη λειτουργία των συστημάτων πληρωμών και την παροχή δραστηριοτήτων επεξεργασίας πληρωμών θα πρέπει να αντιμετωπιστεί δεόντως σε επίπεδο Ένωσης μέσω εναρμονισμένων κανόνων ψηφιακής ανθεκτικότητας. Για τον σκοπό αυτό, η Επιτροπή θα πρέπει να αξιολογήσει ταχέως την ανάγκη επανεξέτασης του πεδίου εφαρμογής του παρόντος κανονισμού, ευθυγραμμίζοντας παράλληλα την εν λόγω επανεξέταση με το αποτέλεσμα της συνολικής επανεξέτασης που προβλέπεται στην οδηγία (ΕΕ) 2015/2366. Πολυάριθμες επιθέσεις μεγάλης κλίμακας κατά την τελευταία δεκαετία καταδεικνύουν τον τρόπο με τον οποίο τα συστήματα πληρωμών έχουν εκτεθεί σε κυβερνοαπειλές. Τα συστήματα πληρωμών και οι δραστηριότητες επεξεργασίας πληρωμών, που βρίσκονται στο επίκεντρο της αλυσίδας υπηρεσιών πληρωμών και παρουσιάζουν ισχυρές διασυνδέσεις με το συνολικό χρηματοοικονομικό σύστημα, απέκτησαν κρίσιμη σημασία για τη λειτουργία των χρηματοοικονομικών αγορών της Ένωσης. Οι κυβερνοεπιθέσεις σε τέτοια συστήματα μπορούν να προκαλέσουν σοβαρές επιχειρησιακές διαταραχές με άμεσες επιπτώσεις σε βασικές οικονομικές λειτουργίες, όπως η διευκόλυνση των πληρωμών, και έμμεσες επιπτώσεις στις σχετικές οικονομικές διαδικασίες. Έως ότου εφαρμοστούν εναρμονισμένο καθεστώς και η εποπτεία των φορέων εκμετάλλευσης συστημάτων πληρωμών και των οντοτήτων επεξεργασίας σε επίπεδο Ένωσης, τα κράτη μέλη μπορούν, με σκοπό την εφαρμογή παρόμοιων πρακτικών της αγοράς, να αντλούν έμπνευση από τις απαιτήσεις ψηφιακής επιχειρησιακής ανθεκτικότητας που ορίζονται στον παρόντα κανονισμό, κατά την εφαρμογή των κανόνων στους διαχειριστές συστημάτων πληρωμών και τις οντότητες επεξεργασίας που αποτελούν αντικείμενο εποπτείας υπό τη δικαιοδοσία τους.

([23]) Κανονισμός (ΕΚ) αριθ. 1060/2009 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 16ης Σεπτεμβρίου 2009, για τους οργανισμούς αξιολόγησης πιστοληπτικής ικανότητας (ΕΕ L 302 της 17.11.2009, σ. 1).

([24]) Κανονισμός (ΕΕ) αριθ. 648/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 4ης Ιουλίου 2012, για τα εξωχρηματιστηριακά παράγωγα, τους κεντρικούς αντισυμβαλλομένους και τα αρχεία καταγραφής συναλλαγών (ΕΕ L 201 της 27.7.2012, σ. 1).

([25]) Κανονισμός (ΕΕ) αριθ. 600/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαΐου 2014, για τις αγορές χρηματοπιστωτικών μέσων και για την τροποποίηση του κανονισμού (ΕΕ) αριθ. 648/2012 (ΕΕ L 173 της 12.6.2014, σ. 84).

([26]) Κανονισμός (ΕΕ) αριθ. 909/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Ιουλίου 2014, σχετικά με τη βελτίωση του διακανονισμού αξιογράφων στην Ευρωπαϊκή Ένωση και τα κεντρικά αποθετήρια τίτλων και για την τροποποίηση των οδηγιών 98/26/ΕΚ και 2014/65/ΕΕ και του κανονισμού (ΕΕ) αριθ. 236/2012 (ΕΕ L 257 της 28.8.2014, σ. 1).

([27]) Οδηγία (ΕΕ) 2022/2556 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, για την τροποποίηση των οδηγιών 2009/65/ΕΚ, 2009/138/ΕΚ, 2011/61/ΕΕ, 2013/36/ΕΕ, 2014/59/ΕΕ, 2014/65/ΕΕ, (ΕΕ) 2015/2366 και (ΕΕ) 2016/2341 όσον αφορά την ψηφιακή επιχειρησιακή ανθεκτικότητα για τον χρηματοοικονομικό τομέα (βλέπε σελίδα 153 της παρούσας Επίσημης Εφημερίδας).

([28]) Κανονισμός (ΕΕ) 2016/1011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 8ης Ιουνίου 2016, σχετικά με τους δείκτες που χρησιμοποιούνται ως δείκτες αναφοράς σε χρηματοπιστωτικά μέσα και χρηματοπιστωτικές συμβάσεις ή για τη μέτρηση της απόδοσης επενδυτικών κεφαλαίων, και για την τροποποίηση των οδηγιών 2008/48/ΕΚ και 2014/17/ΕΕ και του κανονισμού (ΕΕ) αριθ. 596/2014 (ΕΕ L 171 της 29.6.2016, σ. 1).

(105) Δεδομένου ότι ο στόχος του παρόντος κανονισμού, και συγκεκριμένα η διασφάλιση υψηλού επιπέδου ψηφιακής επιχειρησιακής ανθεκτικότητας για ρυθμιζόμενες χρηματοοικονομικές οντότητες, δεν μπορεί να επιτευχθεί επαρκώς από τα κράτη μέλη, διότι προϋποθέτει εναρμόνιση ποικίλων διαφορετικών κανόνων του ενωσιακού και εθνικού δικαίου, αλλά, λόγω της κλίμακας και των επιπτώσεών του, μπορεί να επιτευχθεί καλύτερα σε επίπεδο Ένωσης, η Ένωση δύναται να λάβει μέτρα σύμφωνα με την αρχή της επικουρικότητας, όπως διατυπώνεται στο άρθρο 5 της Συνθήκης για την Ευρωπαϊκή Ένωση. Σύμφωνα με την αρχή της αναλογικότητας, όπως διατυπώνεται στο εν λόγω άρθρο, ο παρών κανονισμός δεν βαίνει πέραν των αναγκαίων ορίων για την επίτευξη του επιδιωκόμενου στόχου.

(106) Ζητήθηκε, σύμφωνα με το άρθρο 42 παράγραφος 1 του κανονισμού (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([29]), η γνώμη του Ευρωπαίου Επόπτη Προστασίας Δεδομένων, που γνωμοδότησε στις 10 Μαΐου 2021 ([30]),

ΕΞΕΔΩΣΑΝ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

ΚΕΦΑΛΑΙΟ I

Γενικές διατάξεις

Άρθρο 1

Αντικείμενο

1. Προκειμένου να επιτευχθεί υψηλό κοινό επίπεδο ψηφιακής επιχειρησιακής ανθεκτικότητας, ο παρών κανονισμός καθορίζει ενιαίες απαιτήσεις σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών, τα οποία υποστηρίζουν τις επιχειρηματικές διαδικασίες των χρηματοοικονομικών οντοτήτων ως εξής:

α) απαιτήσεις που ισχύουν για τις χρηματοοικονομικές οντότητες όσον αφορά τα εξής:

i) διαχείριση κινδύνων των τεχνολογιών των πληροφοριών και των επικοινωνιών (ΤΠΕ),

ii) αναφορά μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ και κοινοποίηση, σε προαιρετική βάση, σημαντικών κυβερνοαπειλών στις αρμόδιες αρχές,

iii) αναφορά μειζόνων λειτουργικών συμβάντων ή συμβάντων ασφάλειας που σχετίζονται με πληρωμές στις αρμόδιες αρχές από τις χρηματοοικονομικές οντότητες που αναφέρονται στο άρθρο 2 παράγραφος 1 στοιχεία α)έως δ),

iv) δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας,

v) ανταλλαγή πληροφοριών και στοιχείων σχετικά με κυβερνοαπειλές και ευπάθειες,

vi) μέτρα για τη χρηστή διαχείριση των κινδύνων τρίτων παρόχων ΤΠΕ,

β) απαιτήσεις σε σχέση με τις συμβατικές ρυθμίσεις που συνάπτονται μεταξύ τρίτων παρόχων υπηρεσιών ΤΠΕ και χρηματοοικονομικών οντοτήτων,

γ) κανόνες για τον καθορισμό και τη λειτουργία του πλαισίου εποπτείας για κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ κατά την παροχή υπηρεσιών σε χρηματοοικονομικές οντότητες,

δ) κανόνες για τη συνεργασία μεταξύ των αρμόδιων αρχών και κανόνες για την εποπτεία και την επιβολή του νόμου από τις αρμόδιες αρχές σε σχέση με όλα τα ζητήματα που καλύπτονται από τον παρόντα κανονισμό.

2. Όσον αφορά τις χρηματοοικονομικές οντότητες που προσδιορίζονται ως βασικές ή σημαντικές οντότητες σύμφωνα με τους εθνικούς κανόνες που μεταφέρουν το άρθρο 3 της οδηγίας (ΕΕ) 2022/2555 στο εθνικό δίκαιο, ο παρών κανονισμός θεωρείται τομεακή νομική πράξη της Ένωσης για τους σκοπούς του άρθρου 4 της εν λόγω οδηγίας.

3. Ο παρών κανονισμός δεν θίγει την ευθύνη των κρατών μελών όσον αφορά βασικές λειτουργίες του κράτους σχετικά με τη δημόσια ασφάλεια, την άμυνα και την εθνική ασφάλεια σύμφωνα με το δίκαιο της Ένωσης.

([29]) Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2018, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ (ΕΕ L 295 της 21.11.2018, σ. 39).

([30]) ΕΕ C 229 της 15.6.2021, σ. 16.

Άρθρο 2

Πεδίο εφαρμογής

1. Με την επιφύλαξη των παραγράφων 3 και 4, ο παρών κανονισμός εφαρμόζεται στις ακόλουθες οντότητες:

α) πιστωτικά ιδρύματα,

β) ιδρύματα πληρωμών, συμπεριλαμβανομένων των ιδρυμάτων πληρωμών που εξαιρούνται σύμφωνα με την οδηγία (ΕΕ) 2015/2366,

γ) παρόχους υπηρεσιών πληροφοριών λογαριασμού,

δ) ιδρύματα ηλεκτρονικού χρήματος, συμπεριλαμβανομένων των ιδρυμάτων ηλεκτρονικού χρήματος που εξαιρούνται σύμφωνα με την οδηγία 2009/110/ΕΚ,

ε) επιχειρήσεις επενδύσεων,

στ) παρόχους υπηρεσιών κρυπτοστοιχείων που έχουν λάβει άδεια βάσει κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τις αγορές κρυπτοστοιχείων και την τροποποίηση των κανονισμών (ΕΕ) αριθ. 1093/2010 και (ΕΕ) αριθ. 1095/2010 και των οδηγιών 2013/36/ΕΕ and (ΕΕ) 2019/1937 («κανονισμός σχετικά με τις αγορές κρυπτοστοιχείων») και τους εκδότες ψηφιακών μαρκών με εγγύηση περιουσιακών στοιχείων,

ζ) κεντρικά αποθετήρια τίτλων,

η) κεντρικούς αντισυμβαλλομένους,

θ) τόπους διαπραγμάτευσης,

ι) αρχεία καταγραφής συναλλαγών,

ια) διαχειριστές οργανισμών εναλλακτικών επενδύσεων,

ιβ) εταιρείες διαχείρισης,

ιγ) παρόχους υπηρεσιών αναφοράς δεδομένων,

ιδ) ασφαλιστικές και αντασφαλιστικές επιχειρήσεις,

ιε) ασφαλιστικούς διαμεσολαβητές, αντασφαλιστικούς διαμεσολαβητές και ασφαλιστικούς διαμεσολαβητές που ασκούν ως δευτερεύουσα δραστηριότητα την ασφαλιστική διαμεσολάβηση,

ιστ) ιδρύματα επαγγελματικών συνταξιοδοτικών παροχών,

ιζ) οργανισμούς αξιολόγησης πιστοληπτικής ικανότητας,

ιη) διαχειριστές δεικτών αναφοράς κρίσιμης σημασίας,

ιθ) παρόχους υπηρεσιών συμμετοχικής χρηματοδότησης,

κ) αρχεία καταγραφής τιτλοποιήσεων,

κα) τρίτους παρόχους υπηρεσιών ΤΠΕ.

2. Για τους σκοπούς του παρόντος κανονισμού, οι οντότητες που αναφέρονται στην παράγραφο 1 στοιχεία α) έως κ) αναφέρονται συλλογικά ως «χρηματοοικονομικές οντότητες».

3. Ο παρών κανονισμός δεν εφαρμόζεται σε:

α) διαχειριστές οργανισμών εναλλακτικών επενδύσεων, όπως αναφέρονται στο άρθρο 3 παράγραφος 2 της οδηγίας 2011/61/ΕΕ,

β) ασφαλιστικές και αντασφαλιστικές επιχειρήσεις, όπως αναφέρονται στο άρθρο 4 της οδηγίας 2009/138/ΕΚ,

γ) ιδρύματα επαγγελματικών συνταξιοδοτικών παροχών που διαχειρίζονται συνταξιοδοτικά συστήματα τα οποία συνολικά δεν έχουν περισσότερα από 15 μέλη,

δ) φυσικά ή νομικά πρόσωπα που εξαιρούνται σύμφωνα με τα άρθρα 2 και 3 της οδηγίας 2014/65/ΕΕ,

ε) ασφαλιστικούς διαμεσολαβητές, αντασφαλιστικούς διαμεσολαβητές και ασφαλιστικούς διαμεσολαβητές που ασκούν ως δευτερεύουσα δραστηριότητα την ασφαλιστική διαμεσολάβηση που είναι πολύ μικρές επιχειρήσεις ή μικρές ή μεσαίες επιχειρήσεις,

στ) γραφεία ταχυδρομικών επιταγών, όπως αναφέρονται στο άρθρο 2 παράγραφος 5 σημείο 3) της οδηγίας 2013/36/ΕΕ.

4. Τα κράτη μέλη μπορούν να εξαιρούν από το πεδίο εφαρμογής του παρόντος κανονισμού τις οντότητες που αναφέρονται στο άρθρο 2 παράγραφος 5 σημεία 4) έως 23) της οδηγίας 2013/36/ΕΕ και οι οποίες είναι εγκατεστημένες στην αντίστοιχη επικράτειά τους. Όταν ένα κράτος μέλος κάνει χρήση της δυνατότητας αυτής, ενημερώνει σχετικά την Επιτροπή, καθώς και για κάθε μεταγενέστερη τροποποίησή της. Η Επιτροπή δημοσιοποιεί τις πληροφορίες αυτές στον ιστότοπό της ή σε άλλα εύκολα προσβάσιμα μέσα.

Άρθρο 3

Ορισμοί

Για τους σκοπούς του παρόντος κανονισμού, ισχύουν οι ακόλουθοι ορισμοί:

1) «ψηφιακή επιχειρησιακή ανθεκτικότητα»: η ικανότητα μιας χρηματοοικονομικής οντότητας να διαμορφώνει, να εξασφαλίζει και να επανεξετάζει την επιχειρησιακή ακεραιότητα και αξιοπιστία της, διασφαλίζοντας, άμεσα ή έμμεσα μέσω της χρήσης υπηρεσιών που προσφέρονται από τρίτους παρόχους υπηρεσιών ΤΠΕ, το πλήρες φάσμα των ικανοτήτων ΤΠΕ που απαιτούνται, ώστε να ανταποκρίνεται στην ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιεί η χρηματοοικονομική οντότητα και τα οποία υποστηρίζουν τη συνεχή παροχή χρηματοοικονομικών υπηρεσιών και την ποιότητά τους, μεταξύ άλλων καθ' όλη τη διάρκεια διαταραχών,

2) «σύστημα δικτύου και πληροφοριών»: σύστημα δικτύου και πληροφοριών, όπως ορίζεται στο άρθρο 6 σημείο 1) της οδηγίας (ΕΕ) 2022/2555

3) «παρωχημένο σύστημα ΤΠΕ»: σύστημα ΤΠΕ που έχει φτάσει στο τέλος του κύκλου ζωής του (τέλος κύκλου ζωής), το οποίο δεν είναι κατάλληλο για αναβαθμίσεις ή επιδιορθώσεις, για τεχνολογικούς ή εμπορικούς λόγους, ή δεν υποστηρίζεται πλέον από τον προμηθευτή του ή από τρίτο πάροχο υπηρεσιών ΤΠΕ, αλλά εξακολουθεί να χρησιμοποιείται και υποστηρίζει τις λειτουργίες της χρηματοοικονομικής οντότητας,

4) «ασφάλεια συστημάτων δικτύου και πληροφοριών»: η ασφάλεια των συστημάτων δικτύου και πληροφοριών, όπως ορίζεται στο άρθρο 6 σημείο 2) της οδηγίας (ΕΕ) 2022/2555

5) «κίνδυνος ΤΠΕ»: κάθε ευλόγως προσδιορίσιμη περίσταση σε σχέση με τη χρήση συστημάτων δικτύου και πληροφοριών η οποία, εάν επέλθει, ενδέχεται να θέσει σε κίνδυνο την ασφάλεια των συστημάτων δικτύου και πληροφοριών, κάθε εργαλείου ή διαδικασίας που εξαρτάται από την τεχνολογία, λειτουργιών και διαδικασιών ή της παροχής υπηρεσιών, προκαλώντας δυσμενείς επιπτώσεις στο ψηφιακό ή υλικό περιβάλλον,

6) «πληροφοριακός πόρος»: συλλογή πληροφοριών, ενσώματων ή άυλων, που αξίζουν να προστατευτούν,

7) «πόρος ΤΠΕ»: πόρος λογισμικού ή υλισμικού στα συστήματα δικτύου και πληροφοριών που χρησιμοποιεί η χρηματοοικονομική οντότητα,

8) «συμβάν που σχετίζεται με τις ΤΠΕ»: μεμονωμένο συμβάν ή σειρά συνδεδεμένων γεγονότων που δεν έχει προγραμματιστεί από τη χρηματοοικονομική οντότητα και θέτει σε κίνδυνο την ασφάλεια των συστημάτων δικτύου και πληροφοριών, και έχει δυσμενείς επιπτώσεις στη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα ή την εμπιστευτικότητα των δεδομένων, ή στις υπηρεσίες που παρέχονται από τη χρηματοοικονομική οντότητα,

9) «λειτουργικό συμβάν ή συμβάν ασφάλειας που σχετίζεται με πληρωμές»: μεμονωμένο συμβάν ή σειρά συνδεδεμένων συμβάντων που δεν έχει προγραμματιστεί από τις χρηματοοικονομικές οντότητες που αναφέρονται στο άρθρο 2 παράγραφος 1 στοιχεία α) έως δ), είτε σχετίζεται με τις ΤΠΕ είτε όχι, το οποίο έχει δυσμενείς επιπτώσεις στη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα ή την εμπιστευτικότητα των δεδομένων που σχετίζονται με πληρωμές δεδομένων ή στις παρεχόμενες από τη χρηματοοικονομική οντότητα υπηρεσίες που σχετίζονται με πληρωμές,

10) «μείζον συμβάν που σχετίζεται με τις ΤΠΕ»: συμβάν που σχετίζεται με τις ΤΠΕ και το οποίο έχει εξαιρετικά δυσμενείς επιπτώσεις στα συστήματα δικτύου και πληροφοριών που υποστηρίζουν κρίσιμες λειτουργίες της χρηματοοικονομικής οντότητας,

11) «μείζον λειτουργικό συμβάν ή συμβάν ασφάλειας που σχετίζεται με πληρωμές»: λειτουργικό συμβάν ή συμβάν ασφάλειας που σχετίζεται με πληρωμές και το οποίο έχει εξαιρετικά δυσμενείς επιπτώσεις στις παρεχόμενες υπηρεσίες που σχετίζονται με πληρωμές,

12) «κυβερνοαπειλή»: κυβερνοαπειλή, όπως ορίζεται στο άρθρο 2 σημείο 8) του κανονισμού (ΕΕ) 2019/881,

13) «σημαντική κυβερνοαπειλή»: κυβερνοαπειλή της οποίας τα τεχνικά χαρακτηριστικά δείχνουν ότι θα μπορούσε να οδηγήσει σε μείζον συμβάν που σχετίζεται με τις ΤΠΕ ή σε μείζον λειτουργικό συμβάν ή συμβάν ασφάλειας που σχετίζεται με πληρωμές,

14) «κυβερνοεπίθεση»: κακόβουλο συμβάν που σχετίζεται με τις ΤΠΕ και προκαλείται μέσω απόπειρας καταστροφής, έκθεσης, μεταβολής, απενεργοποίησης, υποκλοπής ή απόκτησης μη εξουσιοδοτημένης πρόσβασης ή μη εξουσιοδοτημένης χρήσης πόρου, η οποία τελείται από οποιονδήποτε παράγοντα απειλής,

15) «πληροφορίες για απειλές»: πληροφορίες που έχουν συγκεντρωθεί, μετατραπεί, αναλυθεί, ερμηνευθεί ή εμπλουτιστεί με σκοπό την παροχή του απαραίτητου πλαισίου λήψης αποφάσεων και επιτρέπουν τη σχετική και επαρκή κατανόηση για τον μετριασμό των επιπτώσεων ενός συμβάντος που σχετίζεται με τις ΤΠΕ ή μιας κυβερνοαπειλής, συμπεριλαμβανομένων των τεχνικών λεπτομερειών μιας κυβερνοεπίθεσης, των προσώπων που ευθύνονται για την επίθεση και του τρόπου λειτουργίας και των κινήτρων τους,

16) «ευπάθεια»: αδυναμία, ευαισθησία ή ελάττωμα πόρου, συστήματος, διαδικασίας ή ελέγχου που μπορεί να αποτελέσει αντικείμενο εκμετάλλευσης,

17) «δοκιμές παρείσδυσης βάσει απειλών (TLPT)»: πλαίσιο μίμησης των τακτικών, των τεχνικών και των διαδικασιών που χρησιμοποιούν πραγματικοί παράγοντες απειλής που θεωρείται ως γνήσια κυβερνοαπειλή, το οποίο παρέχει ελεγχόμενη, κατά παραγγελία και βάσει στοιχείων (κόκκινη ομάδα) δοκιμή των κρίσιμων συστημάτων παραγωγής της χρηματοοικονομικής οντότητας,

18) «κίνδυνος τρίτων παρόχων ΤΠΕ»: κίνδυνος ΤΠΕ που μπορεί να ανακύψει για χρηματοοικονομική οντότητα σε σχέση με τη χρήση υπηρεσιών ΤΠΕ που παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ ή υπεργολάβους των παρόχων αυτών, μεταξύ άλλων μέσω ρυθμίσεων εξωτερικής ανάθεσης,

19) «τρίτος πάροχος υπηρεσιών ΤΠΕ»: επιχείρηση που παρέχει υπηρεσίες ΤΠΕ,

20) «ενδοομιλικός πάροχος υπηρεσιών ΤΠΕ»: επιχείρηση που αποτελεί μέρος χρηματοοικονομικού ομίλου και παρέχει κυρίως υπηρεσίες ΤΠΕ σε χρηματοοικονομικές οντότητες του ίδιου ομίλου ή σε χρηματοοικονομικές οντότητες που ανήκουν στο ίδιο θεσμικό σύστημα προστασίας, συμπεριλαμβανομένων των μητρικών επιχειρήσεων, των θυγατρικών και των υποκαταστημάτων τους ή άλλων οντοτήτων που τελούν υπό κοινή ιδιοκτησία ή έλεγχο,

21) «υπηρεσίες ΤΠΕ»: ψηφιακές υπηρεσίες και υπηρεσίες δεδομένων που παρέχονται μέσω συστημάτων ΤΠΕ σε έναν ή περισσότερους εσωτερικούς ή εξωτερικούς χρήστες σε συνεχή βάση, συμπεριλαμβανομένων του υλισμικού ως υπηρεσίας και υπηρεσιών υλισμικού που περιλαμβάνουν την παροχή τεχνικής υποστήριξης μέσω ενημερώσεων λογισμικού ή υλικολογισμικού από τον πάροχο υλισμικού, εξαιρουμένων των παραδοσιακών αναλογικών τηλεφωνικών υπηρεσιών,

22) «κρίσιμη ή σημαντική λειτουργία»: λειτουργία η διαταραχή της οποίας θα έβλαπτε ουσιωδώς τις οικονομικές επιδόσεις χρηματοοικονομικής οντότητας ή την ορθότητα ή τη συνέχεια των υπηρεσιών και δραστηριοτήτων της ή της οποίας η ασυνεχής, πλημμελής ή αποτυχημένη εκτέλεση θα έβλαπτε ουσιωδώς τη συνεχή συμμόρφωση μιας χρηματοοικονομικής οντότητας με τους όρους και τις υποχρεώσεις της άδειας λειτουργίας της ή με τις λοιπές υποχρεώσεις τις οποίες υπέχει βάσει του ισχύοντος δικαίου για τις χρηματοοικονομικές υπηρεσίες,

23) «κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ»: τρίτος πάροχος υπηρεσιών ο οποίος έχει οριστεί ως κρίσιμος σύμφωνα με το άρθρο 31,

24) «τρίτος πάροχος υπηρεσιών ΤΠΕ εγκατεστημένος σε τρίτη χώρα»: τρίτος πάροχος υπηρεσιών ΤΠΕ ο οποίος είναι νομικό πρόσωπο εγκατεστημένο σε τρίτη χώρα που έχει συνάψει συμβατικές ρυθμίσεις με χρηματοοικονομική οντότητα για την παροχή υπηρεσιών ΤΠΕ,

25) «θυγατρική»: θυγατρική επιχείρηση κατά την έννοια του άρθρου 2 σημείο 10) και του άρθρου 22 της οδηγίας 2013/34/ΕΕ,

26) «όμιλος»: όμιλος κατά την έννοια του άρθρου 2 σημείο 11) της οδηγίας 2013/34/ΕΕ,

27) «μητρική επιχείρηση»: μητρική επιχείρηση κατά την έννοια του άρθρου 2 σημείο 9) και του άρθρου 22 της οδηγίας 2013/34/ΕΕ,

28) «υπεργολάβος ΤΠΕ εγκατεστημένος σε τρίτη χώρα»: υπεργολάβος ΤΠΕ ο οποίος είναι νομικό πρόσωπο εγκατεστημένο σε τρίτη χώρα που έχει συνάψει συμβατικές ρυθμίσεις με τρίτο πάροχο υπηρεσιών ΤΠΕ ή με τρίτο πάροχο υπηρεσιών ΤΠΕ εγκατεστημένο σε τρίτη χώρα,

29) «κίνδυνος συγκέντρωσης ΤΠΕ»: έκθεση σε μεμονωμένους ή πολλαπλούς σχετιζόμενους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, η οποία δημιουργεί έναν βαθμό εξάρτησης από τους εν λόγω παρόχους, έτσι ώστε η μη διαθεσιμότητα, η αθέτηση υποχρεώσεων ή άλλου είδους αδυναμία του εν λόγω παρόχου να ενδέχεται να θέσει σε κίνδυνο την ικανότητα μιας χρηματοοικονομικής οντότητας να παρέχει κρίσιμες ή σημαντικές λειτουργίες ή να της προκαλέσει άλλες μορφές δυσμενών επιπτώσεων, συμπεριλαμβανομένων μεγάλων ζημιών, ή να θέσει σε κίνδυνο τη χρηματοοικονομική σταθερότητα της Ένωσης στο σύνολό της,

30) «διοικητικό όργανο»: διοικητικό όργανο, όπως ορίζεται στο άρθρο 4 παράγραφος 1 σημείο 36) της οδηγίας 2014/65/ΕΕ, στο άρθρο 3 παράγραφος 1 σημείο 7) της οδηγίας 2013/36/ΕΕ, στο άρθρο 2 παράγραφος 1 στοιχείο ιθ) της οδηγίας 2009/65/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([31]), στο άρθρο 2 παράγραφος 1 σημείο 45) του κανονισμού (ΕΕ) αριθ. 909/2014, στο άρθρο 3 παράγραφος 1 σημείο 20) του κανονισμού (ΕΕ) 2016/1011 και στις σχετικές διατάξεις του κανονισμού σχετικά με τις αγορές κρυπτοστοιχείων ή τα ισοδύναμα πρόσωπα που διευθύνουν πράγματι την οντότητα ή ασκούν βασικά καθήκοντα σύμφωνα με τη σχετική ενωσιακή ή εθνική νομοθεσία,

31) «πιστωτικό ίδρυμα»: πιστωτικό ίδρυμα όπως ορίζεται στο άρθρο 4 παράγραφος 1 σημείο 1) του κανονισμού (ΕΕ) αριθ. 575/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([32]),

32) «ίδρυμα που εξαιρείται βάσει της οδηγίας 2013/36/ΕΕ»: οντότητα όπως αναφέρεται στο άρθρο 2 παράγραφος 5 σημεία 4) έως 23) της οδηγίας 2013/36/ΕΕ,

33) «επιχείρηση επενδύσεων»: επιχείρηση επενδύσεων όπως ορίζεται στο άρθρο 4 παράγραφος 1 σημείο 1) της οδηγίας 2014/65/ΕΕ,

34) «μικρή και μη διασυνδεδεμένη επιχείρηση επενδύσεων»: επιχείρηση επενδύσεων που πληροί τους όρους που ορίζονται στο άρθρο 12 παράγραφος 1 του κανονισμού (ΕΕ) 2019/2033 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([33]),

35) «ίδρυμα πληρωμών»: ίδρυμα πληρωμών όπως ορίζεται στο άρθρο 4 σημείο 4) της οδηγίας (ΕΕ) 2015/2366,

36) «ίδρυμα πληρωμών που εξαιρείται βάσει της οδηγίας (ΕΕ) 2015/2366»: ίδρυμα πληρωμών που εξαιρείται βάσει του άρθρου 32 παράγραφος 1 της οδηγίας (ΕΕ) 2015/2366,

37) «πάροχος υπηρεσιών πληροφοριών λογαριασμού»: πάροχος υπηρεσιών πληροφοριών λογαριασμού όπως αναφέρεται στο άρθρο 33 παράγραφος 1 της οδηγίας (ΕΕ) 2015/2366,

38) «ίδρυμα ηλεκτρονικού χρήματος»: ίδρυμα ηλεκτρονικού χρήματος όπως ορίζεται στο άρθρο 2 σημείο 1) της οδηγίας 2009/110/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου,

39) «ίδρυμα ηλεκτρονικού χρήματος που εξαιρείται βάσει της οδηγίας 2009/110/ΕΚ»: ίδρυμα ηλεκτρονικού χρήματος που δικαιούται απαλλαγής, όπως αναφέρεται στο άρθρο 9 παράγραφος 1 της οδηγίας 2009/110/ΕΚ,

40) «κεντρικός αντισυμβαλλόμενος»: κεντρικός αντισυμβαλλόμενος όπως ορίζεται στο άρθρο 2 σημείο 1) του κανονισμού (ΕΕ) αριθ. 648/2012,

41) «αρχείο καταγραφής συναλλαγών»: αρχείο καταγραφής συναλλαγών όπως ορίζεται στο άρθρο 2 σημείο 2) του κανονισμού (ΕΕ) αριθ. 648/2012,

42) «κεντρικό αποθετήριο τίτλων»: κεντρικό αποθετήριο τίτλων όπως ορίζεται στο άρθρο 2 παράγραφος 1 σημείο 1) του κανονισμού (ΕΕ) αριθ. 909/2014,

43) «τόπος διαπραγμάτευσης»: τόπος διαπραγμάτευσης όπως ορίζεται στο άρθρο 4 παράγραφος 1 σημείο 24) της οδηγίας 2014/65/ΕΕ,

44) «διαχειριστής οργανισμών εναλλακτικών επενδύσεων»: διαχειριστής οργανισμών εναλλακτικών επενδύσεων όπως ορίζεται στο άρθρο 4 παράγραφος 1 στοιχείο β) της οδηγίας 2011/61/ΕΕ,

45) «εταιρεία διαχείρισης»: εταιρεία διαχείρισης όπως ορίζεται στο άρθρο 2 παράγραφος 1 στοιχείο β) της οδηγίας 2009/65/ΕΚ,

46) «πάροχος υπηρεσιών αναφοράς δεδομένων»: πάροχος υπηρεσιών αναφοράς δεδομένων κατά την έννοια του κανονισμού (ΕΕ) αριθ. 600/2014, όπως αναφέρεται στο άρθρο 2 παράγραφος 1 σημεία 34) έως 36),

47) «ασφαλιστική επιχείρηση»: ασφαλιστική επιχείρηση όπως ορίζεται στο άρθρο 13 σημείο 1) της οδηγίας 2009/138/ΕΚ,

48) «αντασφαλιστική επιχείρηση»: αντασφαλιστική επιχείρηση όπως ορίζεται στο άρθρο 13 σημείο 4) της οδηγίας 2009/138/ΕΚ,

([31]) Οδηγία 2009/65/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Ιουλίου 2009, για τον συντονισμό των νομοθετικών, κανονιστικών και διοικητικών διατάξεων σχετικά με ορισμένους οργανισμούς συλλογικών επενδύσεων σε κινητές αξίες (ΟΣΕΚΑ) (ΕΕ L 302 της 17.11.2009, σ. 32).

([32]) Κανονισμός (ΕΕ) αριθ. 575/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Ιουνίου 2013, σχετικά με τις απαιτήσεις προληπτικής εποπτείας για πιστωτικά ιδρύματα και την τροποποίηση του κανονισμού (ΕΕ) αριθ. 648/2012 (ΕΕ L 176 της 27.6.2013, σ. 1).

([33]) Κανονισμός (ΕΕ) 2019/2033 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Νοεμβρίου 2019, σχετικά με τις απαιτήσεις προληπτικής εποπτείας επιχειρήσεων επενδύσεων και την τροποποίηση των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 575/2013, (ΕΕ) αριθ. 600/2014 και (ΕΕ) αριθ. 806/2014 (ΕΕ L 314 της 5.12.2019, σ. 1).

49) «ασφαλιστικός διαμεσολαβητής»: ασφαλιστικός διαμεσολαβητής όπως ορίζεται στο άρθρο 2 παράγραφος 1 σημείο 3) της οδηγίας (ΕΕ) 2016/97 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([34]),

50) «ασφαλιστικός διαμεσολαβητής που ασκεί ως δευτερεύουσα δραστηριότητα την ασφαλιστική διαμεσολάβηση»: ασφαλιστικός διαμεσολαβητής που ασκεί ως δευτερεύουσα δραστηριότητα την ασφαλιστική διαμεσολάβηση, όπως ορίζεται στο άρθρο 2 παράγραφος 1 σημείο 4) της οδηγίας (ΕΕ) 2016/97,

51) «αντασφαλιστικός διαμεσολαβητής»: αντασφαλιστικός διαμεσολαβητής όπως ορίζεται στο άρθρο 2 παράγραφος 1 σημείο 5) της οδηγίας (ΕΕ) 2016/97,

52) «ίδρυμα επαγγελματικών συνταξιοδοτικών παροχών»: ίδρυμα επαγγελματικών συνταξιοδοτικών παροχών όπως ορίζεται στο άρθρο 6 σημείο 1) της οδηγίας (ΕΕ) 2016/2341,

53) «μικρό ίδρυμα επαγγελματικών συνταξιοδοτικών παροχών»: ίδρυμα επαγγελματικών συνταξιοδοτικών παροχών που διαχειρίζεται συνταξιοδοτικά συστήματα τα οποία έχουν συνολικά λιγότερα από 100 μέλη,

54) «οργανισμός αξιολόγησης πιστοληπτικής ικανότητας»: οργανισμός αξιολόγησης πιστοληπτικής ικανότητας όπως ορίζεται στο άρθρο 3 παράγραφος 1 στοιχείο β) του κανονισμού (ΕΚ) αριθ. 1060/2009,

55) «πάροχος υπηρεσιών κρυπτοστοιχείων»: πάροχος υπηρεσιών κρυπτοστοιχείων όπως ορίζεται στη σχετική διάταξη του κανονισμού σχετικά με τις αγορές κρυπτοστοιχείων,

56) «εκδότης ψηφιακών μαρκών με εγγύηση περιουσιακών στοιχείων»: εκδότης ψηφιακών μαρκών με εγγύηση περιουσιακών στοιχείων όπως ορίζεται στη σχετική διάταξη του κανονισμού σχετικά με τις αγορές κρυπτοστοιχείων,

57) «διαχειριστής δεικτών αναφοράς κρίσιμης σημασίας»: διαχειριστής δεικτών αναφοράς κρίσιμης σημασίας όπως ορίζεται στο άρθρο 3 παράγραφος 1 σημείο 25) του κανονισμού (ΕΕ) 2016/1011,

58) «πάροχος υπηρεσιών συμμετοχικής χρηματοδότησης»: πάροχος υπηρεσιών συμμετοχικής χρηματοδότησης όπως ορίζεται στο άρθρο 2 παράγραφος 1 στοιχείο ε) του κανονισμού (ΕΕ) 2020/1503 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([35]),

59) «αρχείο καταγραφής τιτλοποιήσεων»: αρχείο καταγραφής τιτλοποιήσεων όπως ορίζεται στο άρθρο 2 σημείο 23) του κανονισμού (ΕΕ) 2017/2402 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([36]),

60) «πολύ μικρή επιχείρηση»: χρηματοοικονομική οντότητα, εκτός από τόπο διαπραγμάτευσης, κεντρικό αντισυμβαλλόμενο, αρχείο καταγραφής συναλλαγών ή κεντρικό αποθετήριο τίτλων, η οποία απασχολεί λιγότερα από 10 άτομα και έχει ετήσιο κύκλο εργασιών και/ή ετήσιο σύνολο ισολογισμού που δεν υπερβαίνει τα 2 εκατομμύρια EUR,

61) «κύριος εποπτικός φορέας»: η Ευρωπαϊκή Εποπτική Αρχή που διορίζεται σύμφωνα με το άρθρο 31 παράγραφος 1 στοιχείο β) του παρόντος κανονισμού,

62) «μεικτή επιτροπή»: η επιτροπή που αναφέρεται στο άρθρο 54 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010,

63) «μικρή επιχείρηση»: χρηματοοικονομική οντότητα που απασχολεί 10 ή περισσότερα άτομα, αλλά λιγότερα από 50 άτομα, και της οποίας ο ετήσιος κύκλος εργασιών και/ή το σύνολο του ετήσιου ισολογισμού υπερβαίνει τα 2 εκατομμύρια EUR, αλλά δεν υπερβαίνει τα 10 εκατομμύρια EUR,

64) «μεσαία επιχείρηση»: χρηματοοικονομική οντότητα που δεν είναι μικρή επιχείρηση και απασχολεί λιγότερα από 250 άτομα και της οποίας ο ετήσιος κύκλος εργασιών δεν υπερβαίνει τα 50 εκατομμύρια EUR και/ή το σύνολο του ετήσιου ισολογισμού δεν υπερβαίνει τα 43 εκατομμύρια EUR,

65) «δημόσια αρχή»: κάθε κυβερνητικός ή άλλος φορέας δημόσιας διοίκησης, συμπεριλαμβανομένων των εθνικών κεντρικών τραπεζών.

([34]) Οδηγία (ΕΕ) 2016/97 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Ιανουαρίου 2016, σχετικά με τη διανομή ασφαλιστικών προϊόντων (ΕΕ L 26 της 2.2.2016, σ. 19).

([35]) Κανονισμός (ΕΕ) 2020/1503 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Οκτωβρίου 2020, σχετικά με τους Ευρωπαίους παρόχους υπηρεσιών συμμετοχικής χρηματοδότησης για επιχειρήσεις και την τροποποίηση του κανονισμού (ΕΕ) 2017/1129 και της οδηγίας (ΕΕ) 2019/1937 (ΕΕ L 347 της 20.10.2020, σ. 1).

([36]) Κανονισμός (ΕΕ) 2017/2402 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Δεκεμβρίου 2017, σχετικά με τη θέσπιση γενικού πλαισίου για την τιτλοποίηση και σχετικά με τη δημιουργία ειδικού πλαισίου για απλή, διαφανή και τυποποιημένη τιτλοποίηση και σχετικά με την τροποποίηση των οδηγιών 2009/65/ΕΚ, 2009/138/ΕΚ και 2011/61/ΕΕ και των κανονισμών (ΕΚ) αριθ. 1060/2009 και (ΕΕ) αριθ. 648/2012 (ΕΕ L 347 της 28.12.2017, σ. 35).

Άρθρο 4

Αρχή της αναλογικότητας

1. Οι χρηματοοικονομικές οντότητες εφαρμόζουν τους κανόνες που θεσπίζονται στο κεφάλαιο ΙΙ, σύμφωνα με την αρχή της αναλογικότητας, λαμβάνοντας υπόψη το μέγεθος, το συνολικό προφίλ κινδύνου, τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, δραστηριοτήτων και λειτουργιών τους.

2. Επιπλέον, η εφαρμογή από τις χρηματοοικονομικές οντότητες των κεφαλαίων ΙΙΙ και IV και του κεφαλαίου V τμήμα Ι είναι αναλογική προς το μέγεθός τους και το συνολικό προφίλ κινδύνου τους, καθώς και προς τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών τους, όπως προβλέπεται ειδικά στους σχετικούς κανόνες των εν λόγω κεφαλαίων.

3. Οι αρμόδιες αρχές εξετάζουν το ενδεχόμενο εφαρμογής της αρχής της αναλογικότητας από τις χρηματοοικονομικές οντότητες κατά την επανεξέταση της συνέπειας του πλαισίου διαχείρισης κινδύνων ΤΠΕ βάσει των εκθέσεων που υποβάλλονται κατόπιν αιτήματος των αρμόδιων αρχών σύμφωνα με το άρθρο 6 παράγραφος 5 και το άρθρο 16 παράγραφος 2.

ΚΕΦΑΛΑΙΟ ΙΙ

Διαχείριση κινδύνων ΤΠΕ

Τμήμα Ι

Άρθρο 5

Διακυβέρνηση και οργάνωση

1. Οι χρηματοοικονομικές οντότητες εφαρμόζουν πλαίσιο εσωτερικής διακυβέρνησης και ελέγχου το οποίο διασφαλίζει την αποτελεσματική και συνετή διαχείριση των κινδύνων ΤΠΕ, σύμφωνα με το άρθρο 6 παράγραφος 4, με σκοπό την επίτευξη υψηλού επιπέδου ψηφιακής επιχειρησιακής ανθεκτικότητας.

2. Το διοικητικό όργανο της χρηματοοικονομικής οντότητας καθορίζει, εγκρίνει, εποπτεύει και είναι υπεύθυνο για την εφαρμογή όλων των ρυθμίσεων σχετικά με το πλαίσιο διαχείρισης κινδύνων ΤΠΕ που προβλέπεται στο άρθρο 6 παράγραφος 1.

Για τους σκοπούς του πρώτου εδαφίου, το διοικητικό όργανο:

α) φέρει την τελική ευθύνη για τη διαχείριση κινδύνων ΤΠΕ της χρηματοοικονομικής οντότητας,

β) εφαρμόζει πολιτικές που στοχεύουν στη διασφάλιση της διατήρησης υψηλών προτύπων διαθεσιμότητας, γνησιότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων,

γ) καθορίζει σαφείς ρόλους και αρμοδιότητες για όλες τις λειτουργίες που σχετίζονται με τις ΤΠΕ και θεσπίζει κατάλληλες ρυθμίσεις διακυβέρνησης για τη διασφάλιση αποτελεσματικής και έγκαιρης επικοινωνίας, συνεργασίας και συντονισμού μεταξύ των εν λόγω λειτουργιών,

δ) φέρει τη συνολική ευθύνη για τον καθορισμό και την έγκριση της στρατηγικής ψηφιακής επιχειρησιακής ανθεκτικότητας, όπως αναφέρεται στο άρθρο 6 παράγραφος 8, συμπεριλαμβανομένου του καθορισμού του κατάλληλου επιπέδου ανοχής των κινδύνων ΤΠΕ της χρηματοοικονομικής οντότητας, όπως αναφέρεται στο άρθρο 6 παράγραφος 8 στοιχείο β),

ε) εγκρίνει, εποπτεύει και επανεξετάζει περιοδικά την εφαρμογή της πολιτικής επιχειρησιακής συνέχειας των ΤΠΕ και των σχεδίων αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ, που αναφέρονται, αντίστοιχα, στο άρθρο 11 παράγραφοι 1 και 3, τα οποία μπορούν να εγκριθούν ως ειδική συγκεκριμένη πολιτική που αποτελεί αναπόσπαστο μέρος της συνολικής πολιτικής επιχειρησιακής συνέχειας και του σχεδίου αντιμετώπισης και ανάκαμψης της λειτουργίας της χρηματοοικονομικής οντότητας,

στ) εγκρίνει και επανεξετάζει περιοδικά τα προγράμματα εσωτερικού ελέγχου ΤΠΕ και τους ελέγχους ΤΠΕ της χρηματοοικονομικής οντότητας, καθώς και τις σημαντικές μεταβολές τους,

ζ) διαθέτει τον κατάλληλο προϋπολογισμό και τον επανεξετάζει τακτικά, ώστε να καλύπτονται οι ανάγκες ψηφιακής επιχειρησιακής ανθεκτικότητας της χρηματοοικονομικής οντότητας όσον αφορά όλα τα είδη πόρων, μεταξύ των οποίων τα σχετικά προγράμματα ευαισθητοποίησης σε θέματα ασφάλειας των ΤΠΕ και η κατάρτιση για την ψηφιακή επιχειρησιακή ανθεκτικότητα που αναφέρονται στο άρθρο 13 παράγραφος 6, και τις δεξιότητες ΤΠΕ για όλους,

η) εγκρίνει και επανεξετάζει τακτικά την πολιτική της χρηματοοικονομικής οντότητας σχετικά με τις ρυθμίσεις που αφορούν τη χρήση των υπηρεσιών ΤΠΕ οι οποίες παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ,

θ) θέτει σε εφαρμογή σε εταιρικό επίπεδο διαύλους αναφοράς που θα του επιτρέπουν να ενημερώνεται δεόντως σχετικά με τα ακόλουθα:

i) ρυθμίσεις που συνάπτονται με τρίτους παρόχους υπηρεσιών ΤΠΕ σχετικά με τη χρήση υπηρεσιών ΤΠΕ,

ii) οποιεσδήποτε σχετικές προγραμματισμένες ουσιώδεις αλλαγές όσον αφορά τους τρίτους παρόχους υπηρεσιών ΤΠΕ,

iii) τον δυνητικό αντίκτυπο των εν λόγω αλλαγών στις κρίσιμες ή σημαντικές λειτουργίες που υπόκεινται στις εν λόγω ρυθμίσεις, συμπεριλαμβανομένης σύνοψης ανάλυσης κινδύνου για την αξιολόγηση των επιπτώσεων των εν λόγω αλλαγών, και τουλάχιστον τα μείζονα συμβάντα που σχετίζονται με τις ΤΠΕ και τις επιπτώσεις τους, καθώς και σχετικά με τα μέτρα αντιμετώπισης και ανάκαμψης και τα διορθωτικά μέτρα.

3. Οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, καθορίζουν ρόλο για την παρακολούθηση των ρυθμίσεων που συνάπτονται με τρίτους παρόχους υπηρεσιών ΤΠΕ όσον αφορά τη χρήση των υπηρεσιών ΤΠΕ ή ορίζουν ένα ανώτερο διοικητικό στέλεχος ως αρμόδιο για την εποπτεία της έκθεσης σε σχετικό κίνδυνο και της συναφούς τεκμηρίωσης.

4. Τα μέλη του διοικητικού οργάνου της χρηματοοικονομικής οντότητας εξελίσσουν ενεργά και επαρκώς τις γνώσεις και τις δεξιότητές τους, ώστε να κατανοούν και να αξιολογούν τους κινδύνους ΤΠΕ και τις επιπτώσεις τους στις δραστηριότητες της χρηματοοικονομικής οντότητας, μεταξύ άλλων παρακολουθώντας ειδική κατάρτιση σε τακτική βάση, ανάλογη προς τους κινδύνους ΤΠΕ που τελούν υπό διαχείριση.

ΤΜΉΜΑ ΙΙ

Άρθρο 6

Πλαίσιο διαχείρισης κινδύνων ΤΠΕ

1. Οι χρηματοοικονομικές οντότητες διαθέτουν ισχυρό, ολοκληρωμένο και άρτια τεκμηριωμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ στο πλαίσιο του συνολικού τους συστήματος διαχείρισης κινδύνων, που τους επιτρέπει να αντιμετωπίζουν τους κινδύνους ΤΠΕ με γρήγορο, αποτελεσματικό και εμπεριστατωμένο τρόπο και να διασφαλίζουν υψηλό επίπεδο ψηφιακής επιχειρησιακής ανθεκτικότητας.

2. Το πλαίσιο διαχείρισης κινδύνων ΤΠΕ περιλαμβάνει τουλάχιστον στρατηγικές, πολιτικές, διαδικασίες, πρωτόκολλα και εργαλεία ΤΠΕ που απαιτούνται για τη δέουσα και επαρκή προστασία όλων των πληροφοριακών πόρων και πόρων ΤΠΕ, συμπεριλαμβανομένου του λογισμικού, του υλισμικού, των διακομιστών, καθώς και για την προστασία όλων των σχετικών υλικών συνιστωσών και υποδομών, όπως εγκαταστάσεων, κέντρων δεδομένων και ευαίσθητων οριοθετημένων χώρων, ώστε να διασφαλίζεται ότι όλοι αυτοί οι πληροφοριακοί πόροι και πόροι ΤΠΕ προστατεύονται επαρκώς από κινδύνους, συμπεριλαμβανομένων τυχόν βλάβης και μη εξουσιοδοτημένης πρόσβασης ή χρήσης.

3. Σύμφωνα με το πλαίσιο διαχείρισης κινδύνων ΤΠΕ, οι χρηματοοικονομικές οντότητες ελαχιστοποιούν τις επιπτώσεις των κινδύνων ΤΠΕ με την ανάπτυξη κατάλληλων στρατηγικών, πολιτικών, διαδικασιών, πρωτοκόλλων ΤΠΕ και εργαλείων. Παρέχουν πλήρεις και επικαιροποιημένες πληροφορίες σχετικά με τους κινδύνους ΤΠΕ και σχετικά με το πλαίσιό τους για τη διαχείριση κινδύνων ΤΠΕ στις αρμόδιες αρχές κατόπιν αιτήματός τους.

4. Οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, εκχωρούν την ευθύνη για τη διαχείριση και την εποπτεία των κινδύνων ΤΠΕ σε μια λειτουργία ελέγχου και διασφαλίζουν σε επαρκές επίπεδο την ανεξαρτησία της εν λόγω λειτουργίας ελέγχου, προκειμένου να αποφεύγεται η σύγκρουση συμφερόντων. Οι χρηματοοικονομικές οντότητες διασφαλίζουν τον κατάλληλο διαχωρισμό και την κατάλληλη ανεξαρτησία των λειτουργιών διαχείρισης κινδύνων ΤΠΕ, των λειτουργιών ελέγχου και των λειτουργιών εσωτερικής επιθεώρησης, σύμφωνα με το μοντέλο των τριών γραμμών άμυνας ή ένα εσωτερικό μοντέλο διαχείρισης κινδύνων και ελέγχου.

5. Το πλαίσιο διαχείρισης κινδύνων ΤΠΕ τεκμηριώνεται και επανεξετάζεται τουλάχιστον μία φορά ετησίως, ή περιοδικά όσον αφορά τις πολύ μικρές επιχειρήσεις, καθώς και κατά την επέλευση μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ, και σύμφωνα με εποπτικές οδηγίες ή συμπεράσματα που προκύπτουν από σχετικές δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας ή διαδικασίες ελέγχου. Το πλαίσιο βελτιώνεται διαρκώς με βάση τα διδάγματα που αντλούνται από την εφαρμογή και την παρακολούθηση. Έκθεση σχετικά με την επανεξέταση του πλαισίου διαχείρισης κινδύνων ΤΠΕ υποβάλλεται στην αρμόδια αρχή κατόπιν αιτήματός της.

6. Το πλαίσιο διαχείρισης κινδύνων ΤΠΕ των χρηματοοικονομικών οντοτήτων, πλην των πολύ μικρών επιχειρήσεων, υπόκειται σε εσωτερική επιθεώρηση από ελεγκτές σε τακτική βάση, σύμφωνα με το πρόγραμμα ελέγχου των χρηματοοικονομικών οντοτήτων. Οι εν λόγω ελεγκτές διαθέτουν επαρκείς γνώσεις, δεξιότητες και εμπειρογνωσία όσον αφορά τους κινδύνους ΤΠΕ, καθώς και κατάλληλη ανεξαρτησία. Η συχνότητα και η εστίαση των ελέγχων ΤΠΕ είναι ανάλογες προς τους κινδύνους ΤΠΕ που αντιμετωπίζει η χρηματοοικονομική οντότητα.

7. Με βάση τα συμπεράσματα της επανεξέτασης εσωτερικής επιθεώρησης, οι χρηματοοικονομικές οντότητες θεσπίζουν επίσημη διαδικασία παρακολούθησης, συμπεριλαμβανομένων κανόνων για την έγκαιρη επαλήθευση και αποκατάσταση κρίσιμων ευρημάτων ελέγχου ΤΠΕ.

8. Το πλαίσιο διαχείρισης κινδύνων ΤΠΕ περιλαμβάνει στρατηγική επιχειρησιακής ψηφιακής ανθεκτικότητας για τον καθορισμό του τρόπου εφαρμογής του πλαισίου. Για τον σκοπό αυτόν, η στρατηγική επιχειρησιακής ψηφιακής ανθεκτικότητας περιλαμβάνει τις μεθόδους αντιμετώπισης κινδύνων ΤΠΕ και επίτευξης συγκεκριμένων στόχων ΤΠΕ, ως εξής:

α) επεξηγώντας τον τρόπο με τον οποίο το πλαίσιο διαχείρισης κινδύνων ΤΠΕ υποστηρίζει την επιχειρηματική στρατηγική και τους στόχους της χρηματοοικονομικής οντότητας,

β) θεσπίζοντας το επίπεδο ανοχής κινδύνου για τους κινδύνους ΤΠΕ, σύμφωνα με τη διάθεση ανάληψης κινδύνων της χρηματοοικονομικής οντότητας, και αναλύοντας την ανοχή στις επιπτώσεις για τις διαταραχές των ΤΠΕ,

γ) καθορίζοντας σαφείς στόχους ασφάλειας των πληροφοριών, συμπεριλαμβανομένων των βασικών δεικτών επιδόσεων και των βασικών μετρήσεων κινδύνου,

δ) επεξηγώντας την αρχιτεκτονική αναφοράς των ΤΠΕ και τυχόν αλλαγές που απαιτούνται για την επίτευξη συγκεκριμένων επιχειρηματικών στόχων,

ε) περιγράφοντας τους διάφορους μηχανισμούς που εφαρμόζονται για τον εντοπισμό των συμβάντων που σχετίζονται με τις ΤΠΕ, την αποτροπή των επιπτώσεών τους και την παροχή προστασίας από αυτές,

στ) τεκμηριώνοντας την τρέχουσα κατάσταση όσον αφορά την ψηφιακή επιχειρησιακή ανθεκτικότητα με βάση τον αριθμό των αναφερόμενων μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ και την αποτελεσματικότητα των προληπτικών μέτρων,

ζ) εφαρμόζοντας δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας, σύμφωνα με το κεφάλαιο IV του παρόντος κανονισμού,

η) περιγράφοντας μια στρατηγική επικοινωνίας σε περίπτωση συμβάντων που σχετίζονται με τις ΤΠΕ, η γνωστοποίηση των οποίων απαιτείται σύμφωνα με το άρθρο 14.

9. Οι χρηματοοικονομικές οντότητες μπορούν, στο πλαίσιο της στρατηγικής ψηφιακής επιχειρησιακής ανθεκτικότητας που αναφέρεται στην παράγραφο 8, να καθορίσουν μια ολιστική στρατηγική πολλαπλών προμηθευτών ΤΠΕ, σε επίπεδο ομίλου ή οντότητας, η οποία αναδεικνύει βασικές εξαρτήσεις από τρίτους παρόχους υπηρεσιών ΤΠΕ και επεξηγεί το σκεπτικό στο οποίο βασίζεται ο συνδυασμός προμηθειών από τρίτους παρόχους υπηρεσιών ΤΠΕ.

10. Οι χρηματοοικονομικές οντότητες δύνανται, σύμφωνα με το ενωσιακό και το εθνικό τομεακό δίκαιο, να αναθέσουν τα καθήκοντα επαλήθευσης της συμμόρφωσης με τις απαιτήσεις διαχείρισης κινδύνων ΤΠΕ σε ενδοομιλικές ή εξωτερικές επιχειρήσεις. Σε περίπτωση τέτοιας εξωτερικής ανάθεσης, η χρηματοοικονομική οντότητα παραμένει εξολοκλήρου υπεύθυνη για την επαλήθευση της συμμόρφωσης με τις απαιτήσεις διαχείρισης κινδύνων ΤΠΕ.

Άρθρο 7

Συστήματα, πρωτόκολλα και εργαλεία ΤΠΕ

Για την αντιμετώπιση και τη διαχείριση των κινδύνων ΤΠΕ, οι χρηματοοικονομικές οντότητες χρησιμοποιούν και διατηρούν επικαιροποιημένα συστήματα, πρωτόκολλα και εργαλεία ΤΠΕ, τα οποία:

α) είναι ανάλογα προς το μέγεθος των λειτουργιών που υποστηρίζουν τη διεξαγωγή των δραστηριοτήτων τους, σύμφωνα με την αρχή της αναλογικότητας που αναφέρεται στο άρθρο 4,

β) είναι αξιόπιστα,

γ) διαθέτουν επαρκή χωρητικότητα ώστε να επεξεργάζονται με ακρίβεια τα δεδομένα που είναι αναγκαία για την εκτέλεση δραστηριοτήτων και την έγκαιρη παροχή υπηρεσιών, και να εξυπηρετούν μεγάλο όγκο εντολών, μηνυμάτων ή συναλλαγών, όπως απαιτείται, μεταξύ άλλων σε περίπτωση υιοθέτησης νέας τεχνολογίας,

δ) είναι τεχνολογικά ανθεκτικά, ώστε να αντιμετωπίζουν επαρκώς τις πρόσθετες ανάγκες επεξεργασίας πληροφοριών, όπως απαιτείται υπό ακραίες συνθήκες της αγοράς ή άλλες αντίξοες καταστάσεις.

Άρθρο 8

Προσδιορισμός

1. Στο πλαίσιο διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στο άρθρο 6 παράγραφος 1, οι χρηματοοικονομικές οντότητες προσδιορίζουν, ταξινομούν και τεκμηριώνουν επαρκώς όλες τις επιχειρηματικές λειτουργίες, τους ρόλους και τις αρμοδιότητες που υποστηρίζονται από ΤΠΕ, τους πληροφοριακούς πόρους και τους πόρους ΤΠΕ που υποστηρίζουν τις εν λόγω λειτουργίες, καθώς και τους ρόλους και τις εξαρτήσεις τους σε σχέση με τους κινδύνους ΤΠΕ. Οι χρηματοοικονομικές οντότητες επανεξετάζουν, όταν κρίνεται αναγκαίο, και τουλάχιστον σε ετήσια βάση, την επάρκεια αυτής της ταξινόμησης και τυχόν συναφούς τεκμηρίωσης.

2. Οι χρηματοοικονομικές οντότητες προσδιορίζουν σε διαρκή βάση όλες τις πηγές κινδύνων ΤΠΕ, ιδίως την έκθεση σε κίνδυνο από και προς άλλες χρηματοοικονομικές οντότητες, και αξιολογούν τις κυβερνοαπειλές και τις ευπάθειες των ΤΠΕ που αφορούν τις οικείες επιχειρηματικές λειτουργίες που υποστηρίζονται από ΤΠΕ, τους πληροφοριακούς πόρους και τους πόρους ΤΠΕ. Οι χρηματοοικονομικές οντότητες επανεξετάζουν τακτικά, και τουλάχιστον σε ετήσια βάση, τα σενάρια κινδύνου που τις επηρεάζουν.

3. Οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, προβαίνουν σε αξιολόγηση κινδύνων έπειτα από κάθε σημαντική αλλαγή της υποδομής των συστημάτων δικτύου και πληροφοριών, των διαδικασιών ή των διεργασιών που επηρεάζουν τις οικείες επιχειρηματικές λειτουργίες που υποστηρίζονται από ΤΠΕ, τους πληροφοριακούς πόρους ή τους πόρους ΤΠΕ.

4. Οι χρηματοοικονομικές οντότητες προσδιορίζουν όλους τους πληροφοριακούς πόρους και τους πόρους ΤΠΕ, συμπεριλαμβανομένων εκείνων που βρίσκονται σε απομακρυσμένες τοποθεσίες, τους πόρους δικτύου και τον εξοπλισμό υλισμικού, και καταγράφουν όσους θεωρούνται κρίσιμοι. Καταγράφουν τις παραμέτρους των πληροφοριακών πόρων και των πόρων ΤΠΕ, καθώς και τις συνδέσεις και τις αλληλεξαρτήσεις μεταξύ των διαφόρων πληροφοριακών πόρων και πόρων ΤΠΕ.

5. Οι χρηματοοικονομικές οντότητες προσδιορίζουν και τεκμηριώνουν όλες τις διαδικασίες που εξαρτώνται από τρίτους παρόχους υπηρεσιών ΤΠΕ και προσδιορίζουν τις διασυνδέσεις με τρίτους παρόχους υπηρεσιών ΤΠΕ οι οποίοι παρέχουν υπηρεσίες που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες.

6. Για τους σκοπούς των παραγράφων 1, 4 και 5, οι χρηματοοικονομικές οντότητες τηρούν τους σχετικούς καταλόγους και τους ενημερώνουν περιοδικά και κάθε φορά που επέρχεται οποιαδήποτε σημαντική αλλαγή όπως αναφέρεται στην παράγραφο 3.

7. Οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, διενεργούν τακτικά, και τουλάχιστον σε ετήσια βάση, ειδική αξιολόγηση κινδύνων ΤΠΕ σε όλα τα παρωχημένα συστήματα ΤΠΕ και οπωσδήποτε πριν και μετά τη σύνδεση τεχνολογιών, εφαρμογών ή συστημάτων.

Άρθρο 9

Προστασία και πρόληψη

1. Για τους σκοπούς της διασφάλισης επαρκούς επιπέδου προστασίας συστημάτων ΤΠΕ και με στόχο την οργάνωση μέτρων αντιμετώπισης, οι χρηματοοικονομικές οντότητες παρακολουθούν και ελέγχουν σε διαρκή βάση την ασφάλεια και τη λειτουργία των συστημάτων και εργαλείων ΤΠΕ και ελαχιστοποιούν τις επιπτώσεις των σχετικών κινδύνων ΤΠΕ στα συστήματα ΤΠΕ με την ανάπτυξη κατάλληλων εργαλείων, πολιτικών και διαδικασιών για την ασφάλεια των ΤΠΕ.

2. Οι χρηματοοικονομικές οντότητες σχεδιάζουν, αποκτούν και εφαρμόζουν πολιτικές, διαδικασίες, πρωτόκολλα και εργαλεία ασφάλειας ΤΠΕ που έχουν ως στόχο τη διασφάλιση της ανθεκτικότητας, της συνέχειας και της διαθεσιμότητας των συστημάτων ΤΠΕ, ιδίως όσων υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες, και τη διατήρηση υψηλών προτύπων διαθεσιμότητας, γνησιότητας, ακεραιότητας και εμπιστευτικότητας δεδομένων, ανεξάρτητα από το αν βρίσκονται σε κατάσταση αποθήκευσης, χρήσης ή διαβίβασης.

3. Για την επίτευξη των στόχων που αναφέρονται στην παράγραφο 2, οι χρηματοοικονομικές οντότητες χρησιμοποιούν λύσεις και διαδικασίες ΤΠΕ που είναι κατάλληλες σύμφωνα με το άρθρο 4. Οι εν λόγω λύσεις και διαδικασίες ΤΠΕ:

α) εγγυώνται την ασφάλεια των μέσων διαβίβασης δεδομένων,

β) ελαχιστοποιούν τον κίνδυνο αλλοίωσης ή απώλειας δεδομένων, μη εξουσιοδοτημένης πρόσβασης και τεχνικών σφαλμάτων που ενδέχεται να παρεμποδίσουν την επιχειρηματική δραστηριότητα,

γ) προλαμβάνουν την έλλειψη διαθεσιμότητας, την υποβάθμιση της γνησιότητας και της ακεραιότητας, τις παραβιάσεις της εμπιστευτικότητας και την απώλεια δεδομένων,

δ) διασφαλίζουν ότι τα δεδομένα προστατεύονται από κινδύνους που προκύπτουν από τη διαχείριση των δεδομένων, συμπεριλαμβανομένων της πλημμελούς διοίκησης, των κινδύνων που σχετίζονται με την επεξεργασία και του ανθρώπινου σφάλματος.

4. Στο πλαίσιο της διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στο άρθρο 6 παράγραφος 1, οι χρηματοοικονομικές οντότητες:

α) καταρτίζουν και τεκμηριώνουν πολιτική ασφάλειας των πληροφοριών που καθορίζει κανόνες για την προστασία της διαθεσιμότητας, της γνησιότητας, της ακεραιότητας και της εμπιστευτικότητας των δεδομένων, των πληροφοριακών πόρων και των πόρων ΤΠΕ, συμπεριλαμβανομένων εκείνων των πελατών τους, κατά περίπτωση,

β) ακολουθώντας μια προσέγγιση βάσει κινδύνων, θεσπίζουν δομή ορθής διαχείρισης δικτύων και υποδομών, χρησιμοποιώντας κατάλληλες τεχνικές, μεθόδους και πρωτόκολλα, που μπορούν να περιλαμβάνουν την εφαρμογή αυτοματοποιημένων μηχανισμών για την απομόνωση των πληροφοριακών πόρων που επηρεάζονται σε περίπτωση κυβερνοεπιθέσεων,

γ) εφαρμόζουν πολιτικές που περιορίζουν την υλική ή λογική πρόσβαση σε πληροφοριακούς πόρους και πόρους ΤΠΕ στην πρόσβαση που είναι απολύτως αναγκαία για τις νόμιμες και εγκεκριμένες λειτουργίες και δραστηριότητες και θεσπίζουν, για τον σκοπό αυτόν, ένα σύνολο πολιτικών, διαδικασιών και δικλείδων ασφάλειας που αφορούν τα δικαιώματα πρόσβασης και διασφαλίζουν την ορθή διαχείρισή τους,

δ) εφαρμόζουν πολιτικές και πρωτόκολλα για ισχυρούς μηχανισμούς αυθεντικοποίησης, με βάση σχετικά πρότυπα και ειδικά συστήματα ελέγχου, και προστατευτικά μέτρα κρυπτογραφικών κλειδιών με τα οποία κρυπτογραφούνται δεδομένα, βάσει αποτελεσμάτων εγκεκριμένων διαδικασιών κατηγοριοποίησης δεδομένων και αξιολόγησης κινδύνων ΤΠΕ,

ε) εφαρμόζουν τεκμηριωμένες πολιτικές, διαδικασίες και δικλείδες ασφάλειας για τη διαχείριση αλλαγών στις ΤΠΕ, συμπεριλαμβανομένων αλλαγών σε λογισμικό, υλισμικό, στοιχεία, συστήματα ή παράμετροι ασφάλειας υλικολογισμικού, που βασίζονται σε μια προσέγγιση αξιολόγησης κινδύνου και αποτελούν αναπόσπαστο μέρος της συνολικής διαδικασίας διαχείρισης αλλαγών της χρηματοοικονομικής οντότητας, ώστε να διασφαλιστεί ότι όλες οι αλλαγές στα συστήματα ΤΠΕ καταγράφονται, δοκιμάζονται, αξιολογούνται, εγκρίνονται, εφαρμόζονται και επαληθεύονται με ελεγχόμενο τρόπο,

στ) διαθέτουν κατάλληλες και ολοκληρωμένες τεκμηριωμένες πολιτικές σχετικά με τις ενημερώσεις κώδικα και τις επικαιροποιήσεις.

Για τους σκοπούς του πρώτου εδαφίου στοιχείο β), οι χρηματοοικονομικές οντότητες σχεδιάζουν την υποδομή σύνδεσης δικτύου κατά τρόπο ώστε να μπορεί να διακοπεί ή να κατατμηθεί στιγμιαία, προκειμένου να ελαχιστοποιείται και να αποτρέπεται η μετάδοση, ιδίως όσον αφορά τις διασυνδεδεμένες χρηματοοικονομικές διαδικασίες.

Για τους σκοπούς του πρώτου εδαφίου στοιχείο ε), η διαδικασία διαχείρισης αλλαγών ΤΠΕ εγκρίνεται από κατάλληλες ιεραρχικές δομές και διαθέτει ειδικά πρωτόκολλα.

Άρθρο 10

Εντοπισμός

1. Οι χρηματοοικονομικές οντότητες διαθέτουν μηχανισμούς για τον άμεσο εντοπισμό ασυνήθιστων δραστηριοτήτων, σύμφωνα με το άρθρο 17, συμπεριλαμβανομένων ζητημάτων που αφορούν τις επιδόσεις του δικτύου ΤΠΕ και συμβάντων που σχετίζονται με τις ΤΠΕ, καθώς και για τον προσδιορισμό των δυνητικά σημαντικών μοναδικών σημείων αποτυχίας.

Όλοι οι μηχανισμοί εντοπισμού που αναφέρονται στο πρώτο εδάφιο υποβάλλονται τακτικά σε δοκιμές σύμφωνα με το άρθρο 25.

2. Οι μηχανισμοί εντοπισμού που αναφέρονται στην παράγραφο 1 επιτρέπουν την ενεργοποίηση πολυεπίπεδων δικλείδων ασφάλειας, καθορίζουν όρια προειδοποίησης και κριτήρια για την ενεργοποίηση και έναρξη διαδικασιών αντιμετώπισης συμβάντων που σχετίζονται με τις ΤΠΕ, συμπεριλαμβανομένων αυτόματων μηχανισμών προειδοποίησης για το προσωπικό που είναι αρμόδιο για την αντιμετώπιση συμβάντων που σχετίζονται με τις ΤΠΕ.

3. Οι χρηματοοικονομικές οντότητες διαθέτουν επαρκείς πόρους και ικανότητες, ώστε να παρακολουθούν τη δραστηριότητα των χρηστών, την εμφάνιση ασυνήθιστων δραστηριοτήτων ΤΠΕ και συμβάντων που σχετίζονται με τις ΤΠΕ, ιδίως όσον αφορά κυβερνοεπιθέσεις.

4. Οι πάροχοι υπηρεσιών αναφοράς δεδομένων διαθέτουν, επιπλέον, συστήματα τα οποία μπορούν να ελέγχουν αποτελεσματικά αν οι αναφορές συναλλαγών είναι πλήρεις, να εντοπίζουν παραλείψεις και εμφανή σφάλματα και να ζητούν την εκ νέου διαβίβαση των εν λόγω αναφορών.

Άρθρο 11

Αντιμετώπιση και ανάκαμψη

1. Στο πλαίσιο διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στο άρθρο 6 παράγραφος 1 και βάσει των απαιτήσεων προσδιορισμού που προβλέπονται στο άρθρο 8, οι χρηματοοικονομικές οντότητες θέτουν σε εφαρμογή ολοκληρωμένη πολιτική επιχειρησιακής συνέχειας των ΤΠΕ, η οποία μπορεί να εγκριθεί ως ειδική και συγκεκριμένη πολιτική, που συνιστά αναπόσπαστο μέρος της συνολικής πολιτικής επιχειρησιακής συνέχειας της χρηματοοικονομικής οντότητας.

2. Οι χρηματοοικονομικές οντότητες εφαρμόζουν την πολιτική επιχειρησιακής συνέχειας των ΤΠΕ μέσω ειδικών, κατάλληλων και τεκμηριωμένων ρυθμίσεων, σχεδίων, διαδικασιών και μηχανισμών, με στόχο:

α) τη διασφάλιση της συνέχειας των κρίσιμων ή σημαντικών λειτουργιών της χρηματοοικονομικής οντότητας,

β) την ταχεία, κατάλληλη και αποτελεσματική αντιμετώπιση και επίλυση όλων των συμβάντων που σχετίζονται με τις ΤΠΕ, κατά τρόπο ώστε να περιορίζεται η βλάβη και να δίνεται προτεραιότητα στην επανεκκίνηση των δραστηριοτήτων και στις ενέργειες αποκατάστασης,

γ) την ενεργοποίηση, χωρίς καθυστέρηση, ειδικών σχεδίων που παρέχουν τη δυνατότητα εφαρμογής μέτρων, διαδικασιών και τεχνολογιών περιορισμού που αρμόζουν σε κάθε τύπο συμβάντος που σχετίζεται με τις ΤΠΕ και αποτρέπουν περαιτέρω βλάβες, καθώς και ειδικά προσαρμοσμένων διαδικασιών αντιμετώπισης και ανάκαμψης, οι οποίες θεσπίζονται σύμφωνα με το άρθρο 12,

δ) την προκαταρκτική εκτίμηση επιπτώσεων, βλαβών και ζημιών,

ε) τον καθορισμό δράσεων επικοινωνίας και διαχείρισης κρίσεων, οι οποίες διασφαλίζουν τη διαβίβαση επικαιροποιημένων πληροφοριών σε όλα τα μέλη του αρμόδιου εσωτερικού προσωπικού και τους εξωτερικούς συμφεροντούχους, σύμφωνα με το άρθρο 14, και αναφέρονται στις αρμόδιες αρχές σύμφωνα με το άρθρο 19.

3. Στο πλαίσιο της διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στο άρθρο 6 παράγραφος 1, οι χρηματοοικονομικές οντότητες εφαρμόζουν σχετικά σχέδια αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ, τα οποία υπόκεινται, στην περίπτωση των χρηματοοικονομικών οντοτήτων πλην των πολύ μικρών επιχειρήσεων, σε ανεξάρτητη επανεξέταση εσωτερικής επιθεώρησης.

4. Οι χρηματοοικονομικές οντότητες θεσπίζουν, διατηρούν και υποβάλλουν περιοδικά σε δοκιμή κατάλληλα σχέδια επιχειρησιακής συνέχειας των ΤΠΕ, ιδίως όσον αφορά κρίσιμες ή σημαντικές λειτουργίες που αποτελούν αντικείμενο εξωτερικής ανάθεσης ή υπεργολαβίας μέσω ρυθμίσεων με τρίτους παρόχους υπηρεσιών ΤΠΕ.

5. Στο πλαίσιο της συνολικής πολιτικής επιχειρησιακής συνέχειας, οι χρηματοοικονομικές οντότητες διενεργούν ανάλυση επιχειρηματικών επιπτώσεων (ΑΕΕ) της έκθεσής τους σε σοβαρές διαταραχές της επιχειρηματικής δραστηριότητας. Στο πλαίσιο της ΑΕΕ, οι χρηματοοικονομικές οντότητες αξιολογούν τις πιθανές επιπτώσεις σοβαρών διαταραχών της επιχειρηματικής δραστηριότητας μέσω ποσοτικών και ποιοτικών κριτηρίων, χρησιμοποιώντας εσωτερικά και εξωτερικά δεδομένα και ανάλυση σεναρίων, κατά περίπτωση. Η ΑΕΕ εξετάζει την κρισιμότητα των προσδιορισμένων και χαρτογραφημένων επιχειρηματικών λειτουργιών, των διαδικασιών υποστήριξης, των εξαρτήσεων από τρίτους και των πληροφοριακών πόρων, καθώς και των αλληλεξαρτήσεών τους. Οι χρηματοοικονομικές οντότητες διασφαλίζουν ότι οι πόροι ΤΠΕ και οι υπηρεσίες ΤΠΕ σχεδιάζονται και χρησιμοποιούνται σε πλήρη ευθυγράμμιση με την ΑΕΕ, ιδίως όσον αφορά την επαρκή διασφάλιση της εφεδρείας όλων των κρίσιμων στοιχείων.

6. Στο πλαίσιο της ολοκληρωμένης διαχείρισης κινδύνων ΤΠΕ, οι χρηματοοικονομικές οντότητες:

α) δοκιμάζουν τα σχέδια επιχειρησιακής συνέχειας των ΤΠΕ και τα σχέδια αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ σε σχέση με τα συστήματα ΤΠΕ που υποστηρίζουν όλες τις λειτουργίες τουλάχιστον σε ετήσια βάση, καθώς και σε περίπτωση τυχόν ουσιαστικών αλλαγών στα συστήματα ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες,

β) υποβάλλουν σε δοκιμή τα σχέδια επικοινωνίας σε καταστάσεις κρίσης που καταρτίζονται σύμφωνα με το άρθρο 14.

Για τους σκοπούς του πρώτου εδαφίου στοιχείο α), οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, περιλαμβάνουν στα σχέδια δοκιμών σενάρια κυβερνοεπιθέσεων και μετάβασης μεταξύ της κύριας υποδομής ΤΠΕ και της εφεδρικής χωρητικότητας, αντίγραφα ασφαλείας και εφεδρικές εγκαταστάσεις που απαιτούνται για την εκπλήρωση των υποχρεώσεων που προβλέπονται στο άρθρο 12.

Οι χρηματοοικονομικές οντότητες επανεξετάζουν ανά τακτά χρονικά διαστήματα τα σχέδια επιχειρησιακής συνέχειας των ΤΠΕ και αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ, λαμβάνοντας υπόψη τα αποτελέσματα των δοκιμών που διενεργούνται σύμφωνα με το πρώτο εδάφιο και τις συστάσεις που προκύπτουν από ελέγχους ή εποπτικές αξιολογήσεις.

7. Οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, διαθέτουν λειτουργία διαχείρισης κρίσεων, η οποία, σε περίπτωση ενεργοποίησης των σχεδίων επιχειρησιακής συνέχειας των ΤΠΕ ή των σχεδίων αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ, καθορίζει, μεταξύ άλλων, σαφείς διαδικασίες για τη διαχείριση της εσωτερικής και εξωτερικής επικοινωνίας σε καταστάσεις κρίσης σύμφωνα με το άρθρο 14.

8. Οι χρηματοοικονομικές οντότητες τηρούν εύκολα προσβάσιμα αρχεία δραστηριοτήτων προ και κατά τη διάρκεια γεγονότων διαταραχής, όταν ενεργοποιούνται τα σχέδια επιχειρησιακής συνέχειας των ΤΠΕ και τα σχέδια αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ.

9. Τα κεντρικά αποθετήρια τίτλων παρέχουν στις αρμόδιες αρχές αντίγραφα των αποτελεσμάτων των δοκιμών επιχειρησιακής συνέχειας των ΤΠΕ ή παρόμοιων δραστηριοτήτων.

10. Οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, υποβάλλουν στις αρμόδιες αρχές, κατόπιν αιτήματός τους, εκτίμηση των συγκεντρωτικών ετήσιων δαπανών και ζημιών, οι οποίες προκαλούνται από μείζονα συμβάντα που σχετίζονται με τις ΤΠΕ.

11. Σύμφωνα με το άρθρο 16 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010, οι ΕΕΑ, μέσω της μεικτής επιτροπής, καταρτίζουν έως τις 17 Ιουλίου 2024 κοινές κατευθυντήριες γραμμές για την εκτίμηση των συγκεντρωτικών ετήσιων δαπανών και ζημιών που αναφέρονται στην παράγραφο 10.

Άρθρο 12

Πολιτικές και διαδικασίες δημιουργίας εφεδρικών συστημάτων, διαδικασίες και μέθοδοι αποκατάστασης και ανάκτησης

1. Για τους σκοπούς της διασφάλισης της αποκατάστασης των συστημάτων και δεδομένων ΤΠΕ με ελάχιστο χρόνο διακοπής, με περιορισμό της διαταραχής και της ζημίας, στο πλαίσιο της οικείας διαχείρισης κινδύνων ΤΠΕ, οι χρηματοοικονομικές οντότητες καταρτίζουν και τεκμηριώνουν:

α) πολιτικές και διαδικασίες δημιουργίας εφεδρικών συστημάτων στις οποίες προσδιορίζεται το εύρος των δεδομένων που υπόκεινται σε εφεδρικά συστήματα και η ελάχιστη συχνότητα δημιουργίας αντιγράφων ασφαλείας, βάσει της κρισιμότητας των πληροφοριών ή του επιπέδου εμπιστευτικότητας των δεδομένων,

β) διαδικασίες και μεθόδους αποκατάστασης και ανάκτησης.

2. Οι χρηματοοικονομικές οντότητες δημιουργούν εφεδρικά συστήματα που μπορούν να ενεργοποιηθούν σύμφωνα με τις πολιτικές και τις διαδικασίες δημιουργίας εφεδρικών συστημάτων, καθώς και τις διαδικασίες και τις μεθόδους αποκατάστασης και ανάκτησης. Η ενεργοποίηση εφεδρικών συστημάτων δεν θέτει σε κίνδυνο την ασφάλεια των συστημάτων δικτύου και πληροφοριών ή τη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα και την εμπιστευτικότητα των δεδομένων. Διενεργούνται περιοδικά δοκιμές των διαδικασιών δημιουργίας εφεδρικών συστημάτων και των διαδικασιών και μεθόδων αποκατάστασης και ανάκτησης.

3. Κατά την αποκατάσταση εφεδρικών δεδομένων με τη χρήση ιδίων συστημάτων, οι χρηματοοικονομικές οντότητες χρησιμοποιούν συστήματα ΤΠΕ που διαχωρίζονται φυσικά και λογικά από το σύστημα ΤΠΕ πηγής. Τα συστήματα ΤΠΕ προστατεύονται με ασφάλεια από κάθε μη εξουσιοδοτημένη πρόσβαση ή διαφθορά ΤΠΕ και επιτρέπουν την έγκαιρη αποκατάσταση των υπηρεσιών που χρησιμοποιούν τα εφεδρικά δεδομένα και συστήματα, ανάλογα με τις ανάγκες.

Για τους κεντρικούς αντισυμβαλλομένους, τα σχέδια αποκατάστασης επιτρέπουν την αποκατάσταση όλων των συναλλαγών κατά τον χρόνο της διαταραχής, ώστε ο κεντρικός αντισυμβαλλόμενος να είναι σε θέση να εξακολουθήσει να λειτουργεί με ασφάλεια και να ολοκληρώσει τον διακανονισμό κατά την προγραμματισμένη ημερομηνία.

Οι πάροχοι υπηρεσιών αναφοράς δεδομένων διατηρούν, επιπλέον, επαρκείς πόρους και διαθέτουν εφεδρικές εγκαταστάσεις και εγκαταστάσεις αποκατάστασης, προκειμένου να προσφέρουν και να διατηρούν τις υπηρεσίες τους ανά πάσα στιγμή.

4. Οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, διατηρούν εφεδρικές χωρητικότητες ΤΠΕ εξοπλισμένες με επαρκείς πόρους, ικανότητες και λειτουργίες για την κάλυψη των επιχειρηματικών αναγκών. Οι πολύ μικρές επιχειρήσεις αξιολογούν την ανάγκη διατήρησης αυτών των εφεδρικών χωρητικοτήτων ΤΠΕ με βάση το προφίλ κινδύνου τους.

5. Τα κεντρικά αποθετήρια τίτλων διατηρούν τουλάχιστον έναν δευτερεύοντα τόπο επεξεργασίας με επαρκείς πόρους, ικανότητες, λειτουργίες και στελέχωση για την κάλυψη των επιχειρηματικών αναγκών.

Ο δευτερεύων τόπος επεξεργασίας:

α) βρίσκεται σε γεωγραφική απόσταση από τον κύριο τόπο επεξεργασίας, ώστε να διασφαλίζεται ότι έχει διαφορετικό προφίλ κινδύνου και ώστε να μην είναι εφικτό να πληγεί από το ίδιο γεγονός που έχει επηρεάσει τον κύριο τόπο,

β) έχει την ικανότητα να διασφαλίζει την αδιάλειπτη λειτουργία κρίσιμων ή σημαντικών υπηρεσιών κατά πανομοιότυπο τρόπο με τον κύριο τόπο ή να παρέχει το απαιτούμενο επίπεδο υπηρεσιών ώστε να διασφαλίζεται ότι η χρηματοοικονομική οντότητα εκτελεί τις κρίσιμες δραστηριότητές της στο πλαίσιο των στόχων αποκατάστασης,

γ) είναι άμεσα προσβάσιμος από το προσωπικό της χρηματοοικονομικής οντότητας, ώστε να διασφαλίζεται η αδιάλειπτη λειτουργία κρίσιμων ή σημαντικών λειτουργιών σε περίπτωση που ο κύριος τόπος επεξεργασίας δεν είναι διαθέσιμος.

6. Κατά τον καθορισμό των στόχων ως προς τον χρόνο και το σημείο αποκατάστασης για κάθε λειτουργία, οι χρηματοοικονομικές οντότητες λαμβάνουν υπόψη αν πρόκειται για κρίσιμη ή σημαντική λειτουργία και τον δυνητικό συνολικό αντίκτυπο στην αποδοτικότητα της αγοράς. Οι εν λόγω στόχοι ως προς τον χρόνο διασφαλίζουν ότι, σε ακραία σενάρια, πληρούνται τα συμφωνημένα επίπεδα εξυπηρέτησης.

7. Κατά την αποκατάσταση λειτουργίας μετά από συμβάν που σχετίζεται με τις ΤΠΕ, οι χρηματοοικονομικές οντότητες διενεργούν τους απαραίτητους ελέγχους, συμπεριλαμβανομένων οποιωνδήποτε πολλαπλών ελέγχων και συμφωνιών, προκειμένου να διασφαλίσουν ότι η ακεραιότητα των δεδομένων διατηρείται στο ανώτατο επίπεδο. Οι έλεγχοι αυτοί διενεργούνται επίσης κατά την ανακατασκευή δεδομένων από εξωτερικούς συμφεροντούχους, ώστε να διασφαλίζεται η συνεκτικότητα όλων των δεδομένων μεταξύ των συστημάτων.

Άρθρο 13

Εκπαίδευση και εξέλιξη

1. Οι χρηματοοικονομικές οντότητες διαθέτουν ικανότητες και προσωπικό για τη συλλογή πληροφοριών σχετικά με τις ευπάθειες και τις κυβερνοαπειλές, τα συμβάντα που σχετίζονται με τις ΤΠΕ, ιδίως όσον αφορά τις κυβερνοεπιθέσεις, και για την ανάλυση των πιθανών επιπτώσεών τους στην ψηφιακή επιχειρησιακή τους ανθεκτικότητα.

2. Οι χρηματοοικονομικές οντότητες προβαίνουν σε επανεξετάσεις κατόπιν συμβάντων που σχετίζονται με τις ΤΠΕ, αφότου μείζον συμβάν που σχετίζεται με τις ΤΠΕ διαταράσσει τις βασικές τους δραστηριότητες, αναλύοντας τα αίτια της διαταραχής και προσδιορίζοντας τις βελτιώσεις που απαιτούνται στις λειτουργίες των ΤΠΕ ή στο πλαίσιο της πολιτικής επιχειρησιακής συνέχειας των ΤΠΕ, όπως αναφέρεται στο άρθρο 11.

Οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, κοινοποιούν στις αρμόδιες αρχές, κατόπιν αιτήματος, τις αλλαγές που εφαρμόστηκαν μετά τις επανεξετάσεις κατόπιν συμβάντων που σχετίζονται με τις ΤΠΕ, όπως αναφέρεται στο πρώτο εδάφιο.

Οι επανεξετάσεις κατόπιν συμβάντων που σχετίζονται με τις ΤΠΕ, που αναφέρονται στο πρώτο εδάφιο, εξακριβώνουν αν τηρήθηκαν οι καθιερωμένες διαδικασίες και αν τα μέτρα που έχουν ληφθεί ήταν αποτελεσματικά, μεταξύ άλλων σε σχέση με τα εξής:

α) την ταχύτητα αντίδρασης σε ειδοποιήσεις ασφάλειας και προσδιορισμού των επιπτώσεων και της σοβαρότητας των συμβάντων που σχετίζονται με τις ΤΠΕ,

β) την ποιότητα και την ταχύτητα διενέργειας εγκληματολογικής ανάλυσης, εφόσον κρίνεται σκόπιμο,

γ) την αποτελεσματικότητα της παραπομπής του συμβάντος στο κατάλληλο επίπεδο εντός της χρηματοοικονομικής οντότητας,

δ) την αποτελεσματικότητα της εσωτερικής και εξωτερικής επικοινωνίας.

3. Τα διδάγματα που αντλούνται τόσο από τις δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας που πραγματοποιούνται σύμφωνα με τα άρθρα 26 και 27 όσο και από πραγματικά συμβάντα που σχετίζονται με τις ΤΠΕ, ιδίως κυβερνοεπιθέσεις, μαζί με τις προκλήσεις που αντιμετωπίστηκαν κατά την ενεργοποίηση σχεδίων επιχειρησιακής συνέχειας των ΤΠΕ και σχεδίων αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ, σε συνδυασμό με τις σχετικές πληροφορίες που ανταλλάσσονται με αντισυμβαλλομένους και αξιολογούνται κατά τη διάρκεια εποπτικών ελέγχων, ενσωματώνονται δεόντως, σε διαρκή βάση, στη διαδικασία αξιολόγησης κινδύνων ΤΠΕ. Τα εν λόγω ευρήματα αποτελούν τη βάση για τη δέουσα επανεξέταση των συναφών συνιστωσών του πλαισίου διαχείρισης κινδύνων ΤΠΕ, όπως αναφέρεται στο άρθρο 6 παράγραφος 1.

4. Οι χρηματοοικονομικές οντότητες παρακολουθούν την αποτελεσματικότητα της εφαρμογής της στρατηγικής τους για την ψηφιακή επιχειρησιακή ανθεκτικότητα που καθορίζεται στο άρθρο 6 παράγραφος 8. Χαρτογραφούν την εξέλιξη των κινδύνων ΤΠΕ με την πάροδο του χρόνου, αναλύουν τη συχνότητα, τα είδη, το μέγεθος και την εξέλιξη των συμβάντων που σχετίζονται με τις ΤΠΕ, ιδίως όσον αφορά τις κυβερνοεπιθέσεις και τις πρακτικές που ακολουθούν, με σκοπό να κατανοήσουν το επίπεδο έκθεσης σε κινδύνους ΤΠΕ, ιδίως όσον αφορά κρίσιμες ή σημαντικές λειτουργίες, και να ενισχύσουν τα επίπεδα ωριμότητας και ετοιμότητας της χρηματοοικονομικής οντότητας στον κυβερνοχώρο.

5. Τα ανώτερα στελέχη ΤΠΕ υποβάλλουν στο διοικητικό όργανο έκθεση, τουλάχιστον σε ετήσια βάση, σχετικά με τα ευρήματα που αναφέρονται στην παράγραφο 3 και διατυπώνουν συστάσεις.

6. Οι χρηματοοικονομικές οντότητες αναπτύσσουν προγράμματα ευαισθητοποίησης σε θέματα ασφάλειας των ΤΠΕ και προγράμματα κατάρτισης για την ψηφιακή επιχειρησιακή ανθεκτικότητα ως υποχρεωτικές ενότητες των προγραμμάτων κατάρτισης του προσωπικού τους. Τα εν λόγω προγράμματα και καταρτίσεις ισχύουν για όλους τους υπαλλήλους και τα ανώτερα διοικητικά στελέχη και έχουν επίπεδο πολυπλοκότητας ανάλογο προς το αντικείμενο των καθηκόντων τους. Κατά περίπτωση, οι χρηματοοικονομικές οντότητες περιλαμβάνουν επίσης τρίτους παρόχους υπηρεσιών ΤΠΕ στα σχετικά προγράμματα κατάρτισής τους σύμφωνα με το άρθρο 30 παράγραφος 2 στοιχείο θ).

7. Οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, παρακολουθούν τις σχετικές τεχνολογικές εξελίξεις σε διαρκή βάση, με σκοπό επίσης την κατανόηση των πιθανών επιπτώσεων της ανάπτυξης νέων τεχνολογιών αυτού του είδους στις απαιτήσεις ασφάλειας των ΤΠΕ και στην ψηφιακή επιχειρησιακή ανθεκτικότητα. Ενημερώνονται για τις πρόσφατες διαδικασίες διαχείρισης κινδύνων ΤΠΕ, ώστε να καταπολεμούνται αποτελεσματικά οι τρέχουσες ή νέες μορφές κυβερνοεπιθέσεων.

Άρθρο 14

Επικοινωνία

1. Στο πλαίσιο της διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στο άρθρο 6 παράγραφος 1, οι χρηματοοικονομικές οντότητες διαθέτουν σχέδια επικοινωνίας σε καταστάσεις κρίσης που καθιστούν δυνατή την υπεύθυνη γνωστοποίηση, τουλάχιστον, μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ ή ευπαθειών σε πελάτες και αντισυμβαλλομένους, καθώς και στο κοινό, ανάλογα με την περίπτωση.

2. Στο πλαίσιο της διαχείρισης κινδύνων ΤΠΕ, οι χρηματοοικονομικές οντότητες εφαρμόζουν πολιτικές επικοινωνίας που απευθύνονται στο εσωτερικό προσωπικό και σε εξωτερικούς συμφεροντούχους. Στις πολιτικές επικοινωνίας για το προσωπικό λαμβάνεται υπόψη η ανάγκη διαχωρισμού μεταξύ, αφενός, του προσωπικού που συμμετέχει στη διαχείριση κινδύνων ΤΠΕ, ιδίως του προσωπικού που είναι υπεύθυνο για την αντιμετώπιση και την ανάκαμψη, και, αφετέρου, του προσωπικού που πρέπει να ενημερωθεί.

3. Η αρμοδιότητα της εφαρμογής της στρατηγικής επικοινωνίας για συμβάντα που σχετίζονται με τις ΤΠΕ και της εκτέλεσης των καθηκόντων προς το κοινό και τα μέσα ενημέρωσης ανατίθεται τουλάχιστον σε ένα πρόσωπο της χρηματοοικονομικής οντότητας.

Άρθρο 15

Περαιτέρω εναρμόνιση των εργαλείων, μεθόδων, διαδικασιών και πολιτικών διαχείρισης κινδύνων ΤΠΕ

Οι ΕΕΑ, μέσω της μεικτής επιτροπής, σε συνεννόηση με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), καταρτίζουν κοινά σχέδια ρυθμιστικών τεχνικών προτύπων, προκειμένου:

α) να προσδιορίσουν περαιτέρω στοιχεία που πρέπει να συμπεριλαμβάνονται στις πολιτικές, τις διαδικασίες, τα πρωτόκολλα και τα εργαλεία ασφάλειας των ΤΠΕ που αναφέρονται στο άρθρο 9 παράγραφος 2, ώστε να διασφαλίζεται η ασφάλεια των δικτύων, να παρέχεται η δυνατότητα επαρκών διασφαλίσεων έναντι εισβολών και κατάχρησης δεδομένων, να διατηρούνται η διαθεσιμότητα, η γνησιότητα, η ακεραιότητα και η εμπιστευτικότητα των δεδομένων, συμπεριλαμβανομένων των τεχνικών κρυπτογράφησης, και να εξασφαλίζεται η ακριβής και έγκαιρη διαβίβαση δεδομένων χωρίς σημαντικές διαταραχές και αδικαιολόγητες καθυστερήσεις,

β) να αναπτύξουν περαιτέρω συνιστώσες των δικλείδων ασφάλειας για τη διαχείριση δικαιωμάτων πρόσβασης, που αναφέρονται στο άρθρο 9 παράγραφος 4 στοιχείο γ), και της σχετικής πολιτικής ανθρώπινων πόρων που ορίζει τα δικαιώματα πρόσβασης, τις διαδικασίες για τη χορήγηση και την ανάκληση δικαιωμάτων, την παρακολούθηση ασυνήθιστων δραστηριοτήτων σε σχέση με τους κινδύνους ΤΠΕ μέσω κατάλληλων δεικτών, συμπεριλαμβανομένων των πρακτικών χρήσης του δικτύου, των ωρών, της δραστηριότητας ΤΠ και των μη αναγνωρίσιμων συσκευών,

γ) να αναπτύξουν περαιτέρω τους μηχανισμούς που προσδιορίζονται στο άρθρο 10 παράγραφος 1, παρέχοντας τη δυνατότητα έγκαιρου εντοπισμού ασυνήθιστων δραστηριοτήτων, και τα κριτήρια που καθορίζονται στο άρθρο 10 παράγραφος 2 ενεργοποιώντας διαδικασίες εντοπισμού και αντιμετώπισης συμβάντων που σχετίζονται με τις ΤΠΕ,

δ) να προσδιορίσουν περαιτέρω τις συνιστώσες της πολιτικής επιχειρησιακής συνέχειας των ΤΠΕ που αναφέρεται στο άρθρο 11 παράγραφος 1,

ε) να προσδιορίσουν περαιτέρω τις δοκιμές των σχεδίων επιχειρησιακής συνέχειας των ΤΠΕ που αναφέρονται στο άρθρο 11 παράγραφος 6, με σκοπό να διασφαλίζεται ότι κατά τις εν λόγω δοκιμές λαμβάνονται δεόντως υπόψη σενάρια στα οποία η ποιότητα της παροχής κρίσιμης ή σημαντικής λειτουργίας επιδεινώνεται σε μη αποδεκτό επίπεδο ή αποτυγχάνει, καθώς και ότι εξετάζονται δεόντως οι πιθανές επιπτώσεις της αφερεγγυότητας ή άλλης αθέτησης υποχρεώσεων οποιουδήποτε σχετικού τρίτου παρόχου υπηρεσιών ΤΠΕ και, κατά περίπτωση, οι πολιτικοί κίνδυνοι στις αντίστοιχες δικαιοδοσίες των παρόχων,

στ) να προσδιορίσουν περαιτέρω τις συνιστώσες των σχεδίων αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ που αναφέρονται στο άρθρο 11 παράγραφος 3,

ζ) να προσδιορίσουν περαιτέρω το περιεχόμενο και τη μορφή της έκθεσης σχετικά με την επανεξέταση του πλαισίου διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στο άρθρο 6 παράγραφος 5.

Κατά την κατάρτιση των εν λόγω σχεδίων ρυθμιστικών τεχνικών προτύπων, οι ΕΕΑ λαμβάνουν υπόψη το μέγεθος και το συνολικό προφίλ κινδύνου της χρηματοοικονομικής οντότητας, καθώς και τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών της, λαμβάνοντας δεόντως υπόψη τυχόν ειδικά χαρακτηριστικά που προκύπτουν από τη διακριτή φύση των δραστηριοτήτων σε διάφορους τομείς χρηματοοικονομικών υπηρεσιών.

Οι ΕΕΑ υποβάλλουν τα εν λόγω σχέδια ρυθμιστικών τεχνικών προτύπων στην Επιτροπή έως τις 17 Ιανουαρίου 2024.

Ανατίθεται στην Επιτροπή η εξουσία να συμπληρώνει τον παρόντα κανονισμό εκδίδοντας τα ρυθμιστικά τεχνικά πρότυπα που αναφέρονται στο πρώτο εδάφιο, σύμφωνα με τα άρθρα 10 έως 14 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010.

Άρθρο 16

Απλουστευμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ

1. Τα άρθρα 5 έως 15 του παρόντος κανονισμού δεν εφαρμόζονται σε μικρές και μη διασυνδεδεμένες επιχειρήσεις επενδύσεων, ιδρύματα πληρωμών που εξαιρούνται δυνάμει της οδηγίας (ΕΕ) 2015/2366· ιδρύματα που εξαιρούνται δυνάμει της οδηγίας 2013/36/ΕΕ για τα οποία τα κράτη μέλη έχουν αποφασίσει να μην εφαρμόσουν την επιλογή που αναφέρεται στο άρθρο 2 παράγραφος 4 του παρόντος κανονισμού· ιδρύματα ηλεκτρονικού χρήματος που εξαιρούνται δυνάμει της οδηγίας 2009/110/ΕΚ· και μικρά ιδρύματα επαγγελματικών συνταξιοδοτικών παροχών.

Με την επιφύλαξη του πρώτου εδαφίου, οι οντότητες που απαριθμούνται στο πρώτο εδάφιο:

α) θεσπίζουν και διατηρούν ένα άρτιο και τεκμηριωμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ, το οποίο περιγράφει λεπτομερώς τους μηχανισμούς και τα μέτρα που αποσκοπούν στην ταχεία, αποτελεσματική και ολοκληρωμένη διαχείριση των κινδύνων ΤΠΕ, μεταξύ άλλων για την προστασία των σχετικών υλικών συνιστωσών και υποδομών,

β) παρακολουθούν συνεχώς την ασφάλεια και τη λειτουργία όλων των συστημάτων ΤΠΕ,

γ) ελαχιστοποιούν τον αντίκτυπο των κινδύνων ΤΠΕ μέσω της χρήσης ορθών, ανθεκτικών και επικαιροποιημένων συστημάτων, πρωτοκόλλων και εργαλείων ΤΠΕ, τα οποία είναι κατάλληλα για την υποστήριξη της εκτέλεσης των δραστηριοτήτων τους και της παροχής υπηρεσιών και προστατεύουν επαρκώς τη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα και την εμπιστευτικότητα των δεδομένων στα συστήματα δικτύου και πληροφοριών,

δ) επιτρέπουν τον άμεσο εντοπισμό και την ανίχνευση πηγών κινδύνων και ανωμαλιών ΤΠΕ στα δικτυακά και πληροφοριακά συστήματα και τον άμεσο χειρισμό συμβάντων ΤΠΕ,

ε) εντοπίζουν βασικές εξαρτήσεις από τρίτους παρόχους υπηρεσιών ΤΠΕ,

στ) διασφαλίζουν τη συνέχεια κρίσιμων ή σημαντικών λειτουργιών, μέσω σχεδίων επιχειρησιακής συνέχειας και μέτρων αντιμετώπισης και ανάκαμψης, τα οποία περιλαμβάνουν, τουλάχιστον, μέτρα υποστήριξης και αποκατάστασης,

ζ) δοκιμάζουν, σε τακτική βάση, τα σχέδια και τα μέτρα που αναφέρονται στο στοιχείο στ), καθώς και την αποτελεσματικότητα των ελέγχων που υλοποιούνται σύμφωνα με τα στοιχεία α) και γ),

η) εφαρμόζουν, κατά περίπτωση, τα σχετικά επιχειρησιακά συμπεράσματα που προκύπτουν από τις δοκιμές οι οποίες αναφέρονται στο στοιχείο ζ) και από την ανάλυση κατόπιν συμβάντος στη διαδικασία αξιολόγησης κινδύνων ΤΠΕ και καταρτίζουν, σύμφωνα με τις ανάγκες και το προφίλ κινδύνου ΤΠΕ, προγράμματα ευαισθητοποίησης σε θέματα ασφάλειας των ΤΠΕ και προγράμματα κατάρτισης για την ψηφιακή επιχειρησιακή ανθεκτικότητα για το προσωπικό και τη διοίκηση στον τομέα της ασφάλειας ΤΠΕ.

2. Το πλαίσιο διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στην παράγραφο 1 δεύτερο εδάφιο στοιχείο α) τεκμηριώνεται και επανεξετάζεται περιοδικά και σε περίπτωση εκδήλωσης μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ σύμφωνα με τις εποπτικές οδηγίες. Το πλαίσιο βελτιώνεται διαρκώς με βάση τα διδάγματα που αντλούνται από την εφαρμογή και την παρακολούθηση. Έκθεση σχετικά με την επανεξέταση του πλαισίου διαχείρισης κινδύνων ΤΠΕ υποβάλλεται στην αρμόδια αρχή κατόπιν αιτήματός της.

3. Οι ΕΕΑ, μέσω της μεικτής επιτροπής, σε συνεννόηση με τον ENISA, καταρτίζουν κοινά σχέδια ρυθμιστικών τεχνικών προτύπων προκειμένου:

α) να προσδιορίσουν περαιτέρω τα στοιχεία που πρέπει να περιλαμβάνονται στο πλαίσιο διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στην παράγραφο 1 δεύτερο εδάφιο στοιχείο α),

β) να προσδιορίσουν περαιτέρω τα στοιχεία σε σχέση με τα συστήματα, τα πρωτόκολλα και τα εργαλεία για την ελαχιστοποίηση του αντικτύπου των κινδύνων ΤΠΕ που αναφέρεται στην παράγραφο 1 δεύτερο εδάφιο στοιχείο γ), με σκοπό τη διαφύλαξη της ασφάλειας των δικτύων, την παροχή επαρκών διασφαλίσεων έναντι εισβολών και κατάχρησης δεδομένων και τη διατήρηση της διαθεσιμότητας, της γνησιότητας, της ακεραιότητας και της εμπιστευτικότητας των δεδομένων,

γ) να προσδιορίσουν περαιτέρω τις συνιστώσες των σχεδίων επιχειρησιακής συνέχειας των ΤΠΕ που αναφέρονται στο άρθρο 1 δεύτερο εδάφιο στοιχείο στ),

δ) να προσδιορίσουν περαιτέρω τους κανόνες σχετικά με τη δοκιμή των σχεδίων επιχειρησιακής συνέχειας και να διασφαλίσουν την αποτελεσματικότητα των ελέγχων που αναφέρονται στην παράγραφο 1 δεύτερο εδάφιο στοιχείο ζ) και να διασφαλιστεί ότι οι εν λόγω δοκιμές λαμβάνουν δεόντως υπόψη σενάρια στα οποία η ποιότητα της παροχής μιας κρίσιμης ή σημαντικής λειτουργίας επιδεινώνεται σε μη αποδεκτό επίπεδο ή αποτυγχάνει,

ε) να προσδιορίσουν περαιτέρω το περιεχόμενο και τη μορφή της ετήσιας έκθεσης σχετικά με την επανεξέταση του πλαισίου διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στην παράγραφο 2.

Κατά την κατάρτιση των εν λόγω σχεδίων ρυθμιστικών τεχνικών προτύπων, οι ΕΕΑ λαμβάνουν υπόψη το μέγεθος και το συνολικό προφίλ κινδύνου της χρηματοοικονομικής οντότητας και τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών της.

Οι ΕΕΑ υποβάλλουν τα εν λόγω σχέδια ρυθμιστικών τεχνικών προτύπων στην Επιτροπή έως τις 17 Ιανουαρίου 2024.

Ανατίθεται στην Επιτροπή η εξουσία να συμπληρώνει τον παρόντα κανονισμό εκδίδοντας τα ρυθμιστικά τεχνικά πρότυπα που αναφέρονται στο πρώτο εδάφιο, σύμφωνα με τα άρθρα 10 έως 14 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010.

ΚΕΦΑΛΑΙΟ III

Διαχείριση, ταξινόμηση και αναφορά συμβάντων που σχετίζονται με τις ΤΠΕ

Άρθρο 17

Διαδικασία διαχείρισης συμβάντων που σχετίζονται με τις ΤΠΕ

1. Οι χρηματοοικονομικές οντότητες ορίζουν, θεσπίζουν και εφαρμόζουν διαδικασία διαχείρισης συμβάντων που σχετίζονται με τις ΤΠΕ, με σκοπό τον εντοπισμό, τη διαχείριση και την κοινοποίηση συμβάντων που σχετίζονται με τις ΤΠΕ.

2. Οι χρηματοοικονομικές οντότητες καταγράφουν όλα τα συμβάντα που σχετίζονται με τις ΤΠΕ και τις σημαντικές κυβερνοαπειλές. Οι χρηματοοικονομικές οντότητες θεσπίζουν κατάλληλες διεργασίες και διαδικασίες για τη διασφάλιση συνεπούς και ολοκληρωμένου ελέγχου, χειρισμού και παρακολούθησης συμβάντων που σχετίζονται με τις ΤΠΕ, ώστε να εξασφαλιστεί ότι τα βαθύτερα αίτια προσδιορίζονται, τεκμηριώνονται και αντιμετωπίζονται προκειμένου να προληφθεί η εκδήλωση τέτοιων συμβάντων.

3. Η διαδικασία διαχείρισης συμβάντων που σχετίζονται με τις ΤΠΕ που αναφέρεται στην παράγραφο 1:

α) θέτει σε εφαρμογή δείκτες έγκαιρης προειδοποίησης,

β) καθιερώνει διαδικασίες για τον προσδιορισμό, την ανίχνευση, την καταγραφή, την κατηγοριοποίηση και την ταξινόμηση συμβάντων που σχετίζονται με τις ΤΠΕ ανάλογα με την προτεραιότητα και τη σοβαρότητά τους, και την κρισιμότητα των υπηρεσιών που επηρεάζονται, σύμφωνα με τα κριτήρια που καθορίζονται στο άρθρο 18 παράγραφος 1,

γ) αναθέτει ρόλους και αρμοδιότητες που πρέπει να ενεργοποιηθούν για διάφορα είδη και σενάρια συμβάντων που σχετίζονται με τις ΤΠΕ,

δ) καθορίζει σχέδια για την επικοινωνία με το προσωπικό, τους εκτός οντότητας συμφεροντούχους και τα μέσα ενημέρωσης, σύμφωνα με το άρθρο 14, και για την κοινοποίηση σε πελάτες, για εσωτερικές διαδικασίες παραπομπής συμβάντων στο κατάλληλο επίπεδο, συμπεριλαμβανομένων καταγγελιών πελατών που αφορούν τις ΤΠΕ, καθώς και για την παροχή πληροφοριών σε χρηματοοικονομικές οντότητες που ενεργούν ως αντισυμβαλλόμενοι, ανάλογα με την περίπτωση,

ε) διασφαλίζει ότι τουλάχιστον τα μείζονα συμβάντα που σχετίζονται με τις ΤΠΕ αναφέρονται στα αρμόδια ανώτερα διοικητικά στελέχη και ότι το διοικητικό όργανο τηρείται ενήμερο τουλάχιστον για τα μείζονα συμβάντα που σχετίζονται με τις ΤΠΕ, επεξηγώντας τις επιπτώσεις, την αντιμετώπιση και τις πρόσθετες δικλείδες ασφάλειας που πρέπει να καθοριστούν ως αποτέλεσμα τέτοιων συμβάντων που σχετίζονται με τις ΤΠΕ,

στ) καθιερώνει διαδικασίες αντιμετώπισης συμβάντων που σχετίζονται με τις ΤΠΕ για να μετριαστούν οι επιπτώσεις και να διασφαλιστεί ότι οι υπηρεσίες καθίστανται εγκαίρως λειτουργικές και ασφαλείς.

Άρθρο 18

Ταξινόμηση συμβάντων που σχετίζονται με τις ΤΠΕ και κυβερνοαπειλών

1. Οι χρηματοοικονομικές οντότητες ταξινομούν τα συμβάντα που σχετίζονται με τις ΤΠΕ και προσδιορίζουν τις επιπτώσεις τους με βάση τα ακόλουθα κριτήρια:

α) τον αριθμό και/ή τη συνάφεια των επηρεαζόμενων πελατών ή χρηματοοικονομικών αντισυμβαλλομένων και, κατά περίπτωση, το ύψος ή τον αριθμό των συναλλαγών που επηρεάζονται από τη διαταραχή που προκλήθηκε από το συμβάν που σχετίζεται με τις ΤΠΕ, και κατά πόσο το εν λόγω συμβάν έχει επιπτώσεις στη φήμη,

β) τη διάρκεια του συμβάντος που σχετίζεται με τις ΤΠΕ, συμπεριλαμβανομένου του χρόνου διακοπής της υπηρεσίας,

γ) τη γεωγραφική εξάπλωση των περιοχών που επηρεάζονται από το συμβάν που σχετίζεται με τις ΤΠΕ, ιδίως εάν επηρεάζει περισσότερα από δύο κράτη μέλη,

δ) τις απώλειες δεδομένων που συνεπάγεται το συμβάν που σχετίζεται με τις ΤΠΕ, όσον αφορά τη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα ή την εμπιστευτικότητα των δεδομένων,

ε) την κρισιμότητα των επηρεαζόμενων υπηρεσιών, συμπεριλαμβανομένων των συναλλαγών και των δραστηριοτήτων της χρηματοοικονομικής οντότητας,

στ) τις οικονομικές επιπτώσεις, ιδίως τις άμεσες και έμμεσες δαπάνες και απώλειες, του συμβάντος που σχετίζεται με τις ΤΠΕ σε απόλυτους και σχετικούς όρους.

2. Οι χρηματοοικονομικές οντότητες ταξινομούν τις κυβερνοαπειλές ως σημαντικές με βάση την κρισιμότητα των υπηρεσιών που διατρέχουν κίνδυνο, συμπεριλαμβανομένων των συναλλαγών και των δραστηριοτήτων της χρηματοοικονομικής οντότητας, του αριθμού και/ή της συνάφειας των στοχευόμενων πελατών ή χρηματοοικονομικών αντισυμβαλλομένων και της γεωγραφικής εξάπλωσης των περιοχών που διατρέχουν κίνδυνο.

3. Οι ΕΕΑ, μέσω της μεικτής επιτροπής των ΕΕΑ και σε συνεννόηση με την ΕΚΤ και τον ENISA, καταρτίζουν κοινά σχέδια ρυθμιστικών τεχνικών προτύπων, προκειμένου να προσδιορίσουν περαιτέρω τα εξής:

α) τα κριτήρια που καθορίζονται στην παράγραφο 1, συμπεριλαμβανομένων κατώτατων ορίων σημαντικότητας για τον προσδιορισμό μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ ή, κατά περίπτωση, μειζόνων λειτουργικών συμβάντων ή συμβάντων ασφάλειας που σχετίζονται με πληρωμές, τα οποία υπόκεινται στην υποχρέωση αναφοράς που προβλέπεται στο άρθρο 19 παράγραφος 1,

β) τα κριτήρια που πρέπει να εφαρμόζουν οι αρμόδιες αρχές για την αξιολόγηση της συνάφειας μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ ή, κατά περίπτωση, μειζόνων λειτουργικών συμβάντων ή συμβάντων ασφάλειας που σχετίζονται με πληρωμές στις σχετικές αρμόδιες αρχές σε άλλα κράτη μέλη, καθώς και τα στοιχεία των αναφορών μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ ή, κατά περίπτωση, μειζόνων λειτουργικών συμβάντων ή συμβάντων ασφάλειας που σχετίζονται με πληρωμές, τα οποία πρέπει να κοινοποιούνται σε άλλες αρμόδιες αρχές σύμφωνα με το άρθρο 19 παράγραφοι 6 και 7,

γ) τα κριτήρια που καθορίζονται στην παράγραφο 2 του παρόντος άρθρου, συμπεριλαμβανομένων των κατώτατων ορίων υψηλής σημαντικότητας για τον προσδιορισμό σημαντικών κυβερνοαπειλών.

4. Κατά την κατάρτιση των κοινών σχεδίων ρυθμιστικών τεχνικών προτύπων που αναφέρονται στην παράγραφο 3 του παρόντος άρθρου, οι ΕΕΑ λαμβάνουν υπόψη τα κριτήρια που καθορίζονται στο άρθρο 4 παράγραφος 2 καθώς και τα διεθνή πρότυπα, τις κατευθυντήριες γραμμές και τις προδιαγραφές που αναπτύσσει και δημοσιεύει ο ENISA, συμπεριλαμβανομένων, κατά περίπτωση, των προδιαγραφών που ισχύουν για άλλους οικονομικούς τομείς. Για τους σκοπούς της εφαρμογής των κριτηρίων που καθορίζονται στο άρθρο 4 παράγραφος 2, οι ΕΕΑ λαμβάνουν δεόντως υπόψη την ανάγκη οι πολύ μικρές και οι μικρές και μεσαίες επιχειρήσεις να κινητοποιήσουν επαρκείς πόρους και ικανότητες για να διασφαλίσουν την ταχεία διαχείριση συμβάντων που σχετίζονται με τις ΤΠΕ.

Οι ΕΕΑ υποβάλλουν τα εν λόγω κοινά σχέδια ρυθμιστικών τεχνικών προτύπων στην Επιτροπή έως τις 17 Ιανουαρίου 2024.

Ανατίθεται στην Επιτροπή η εξουσία να συμπληρώνει τον παρόντα κανονισμό εκδίδοντας τα ρυθμιστικά τεχνικά πρότυπα που αναφέρονται στην παράγραφο 3, σύμφωνα με τα άρθρα 10 έως 14 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010.

Άρθρο 19

Αναφορά μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ και προαιρετική κοινοποίηση σημαντικών κυβερνοαπειλών

1. Οι χρηματοοικονομικές οντότητες αναφέρουν στην αρμόδια αρχή μείζονα συμβάντα που σχετίζονται με τις ΤΠΕ, όπως ορίζεται στο άρθρο 46, σύμφωνα με την παράγραφο 4 του παρόντος άρθρου.

Όταν μια χρηματοοικονομική οντότητα υπόκειται σε εποπτεία από περισσότερες από μία εθνικές αρμόδιες αρχές, οι οποίες αναφέρονται στο άρθρο 46, τα κράτη μέλη ορίζουν ενιαία αρμόδια αρχή ως τη σχετική αρμόδια αρχή που είναι υπεύθυνη για την εκτέλεση των λειτουργιών και των καθηκόντων που προβλέπονται στο παρόν άρθρο.

Τα πιστωτικά ιδρύματα που ταξινομούνται ως σημαντικά, σύμφωνα με το άρθρο 6 παράγραφος 4 του κανονισμού (ΕΕ) αριθ. 1024/2013, αναφέρουν μείζονα συμβάντα που σχετίζονται με τις ΤΠΕ στη σχετική εθνική αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 4 της οδηγίας 2013/36/ΕΕ, η οποία διαβιβάζει αμέσως την εν λόγω αναφορά στην ΕΚΤ.

Για τους σκοπούς του πρώτου εδαφίου, οι χρηματοοικονομικές οντότητες, αφού συλλέξουν και αναλύσουν όλες τις σχετικές πληροφορίες, καταρτίζουν την αρχική κοινοποίηση και τις αναφορές που προβλέπονται στην παράγραφο 4 του παρόντος άρθρου, χρησιμοποιώντας τα υποδείγματα που αναφέρονται στο άρθρο 20, και τις υποβάλλουν στην αρμόδια αρχή. Σε περίπτωση που μια τεχνική αδυναμία εμποδίζει την υποβολή της αρχικής κοινοποίησης με τη χρήση του υποδείγματος, οι χρηματοοικονομικές οντότητες ενημερώνουν σχετικά την αρμόδια αρχή με εναλλακτικά μέσα.

Η αρχική κοινοποίηση και οι αναφορές που προβλέπονται στην παράγραφο 4 περιλαμβάνουν όλες τις απαραίτητες πληροφορίες προκειμένου η αρμόδια αρχή να είναι σε θέση να προσδιορίσει τη σημασία του μείζονος συμβάντος που σχετίζεται με τις ΤΠΕ και να προβεί σε εκτίμηση των πιθανών διασυνοριακών επιπτώσεων.

Με την επιφύλαξη των αναφορών σύμφωνα με το πρώτο εδάφιο από τη χρηματοοικονομική οντότητα στη σχετική αρμόδια αρχή, τα κράτη μέλη μπορούν επιπλέον να ορίζουν ότι ορισμένες ή όλες οι χρηματοοικονομικές οντότητες παρέχουν επίσης την αρχική κοινοποίηση και κάθε αναφορά που προβλέπεται στην παράγραφο 4 του παρόντος άρθρου, χρησιμοποιώντας τα υποδείγματα που αναφέρονται στο άρθρο 20, στις αρμόδιες αρχές ή στις ομάδες αντιμετώπισης συμβάντων ασφάλειας σε υπολογιστές (CSIRT) που έχουν οριστεί ή συσταθεί σύμφωνα με την οδηγία (ΕΕ) 2022/2555

2. Οι χρηματοοικονομικές οντότητες μπορούν, σε προαιρετική βάση, να κοινοποιούν σημαντικές κυβερνοαπειλές στη σχετική αρμόδια αρχή όταν θεωρούν ότι η απειλή είναι σημαντική για το χρηματοοικονομικό σύστημα, τους χρήστες υπηρεσιών ή τους πελάτες. Η σχετική αρμόδια αρχή μπορεί να παρέχει τις πληροφορίες αυτές σε άλλες σχετικές αρχές που αναφέρονται στην παράγραφο 6.

Τα πιστωτικά ιδρύματα που ταξινομούνται ως σημαντικά, σύμφωνα με το άρθρο 6 παράγραφος 4 του κανονισμού (ΕΕ) αριθ. 1024/2013, μπορούν, σε προαιρετική βάση, να κοινοποιούν σημαντικές κυβερνοαπειλές στη σχετική εθνική αρμόδια αρχή, η οποία έχει οριστεί σύμφωνα με το άρθρο 4 της οδηγίας 2013/36/ΕΕ, και η οποία διαβιβάζει αμέσως την κοινοποίηση στην ΕΚΤ.

Τα κράτη μέλη μπορούν να ορίζουν ότι οι χρηματοοικονομικές οντότητες που κοινοποιούν σε προαιρετική βάση σύμφωνα με το πρώτο εδάφιο μπορούν επίσης να διαβιβάζουν την εν λόγω κοινοποίηση στις CSIRT που ορίζονται ή συστήνονται σύμφωνα με ην οδηγία (ΕΕ) 2022/2555

3. Κατά την εκδήλωση μείζονος συμβάντος, το οποίο σχετίζεται με τις ΤΠΕ και έχει επιπτώσεις στα οικονομικά συμφέροντα των πελατών, οι χρηματοοικονομικές οντότητες ενημερώνουν, χωρίς αδικαιολόγητη καθυστέρηση, αφού λάβουν γνώση του συμβάντος, τους πελάτες όσον αφορά το μείζον συμβάν που σχετίζεται με τις ΤΠΕ και σχετικά με τα μέτρα που έχουν ληφθεί για τον περιορισμό των δυσμενών επιπτώσεων του εν λόγω συμβάντος.

Σε περίπτωση σημαντικής κυβερνοαπειλής, οι χρηματοοικονομικές οντότητες ενημερώνουν, κατά περίπτωση, τους πελάτες τους που ενδέχεται να επηρεαστούν σχετικά με τυχόν κατάλληλα μέτρα προστασίας τα οποία ενδέχεται να εξετάσουν οι τελευταίοι.

4. Οι χρηματοοικονομικές οντότητες, εντός των προθεσμιών που καθορίζονται σύμφωνα με το άρθρο 20 πρώτο εδάφιο στοιχείο α) σημείο ii), υποβάλλουν τα ακόλουθα στη σχετική αρμόδια αρχή:

α) αρχική κοινοποίηση,

β) ενδιάμεση αναφορά μετά την αρχική κοινοποίηση που αναφέρεται στο στοιχείο α), αμέσως μόλις μεταβληθεί σημαντικά η κατάσταση του αρχικού συμβάντος ή μεταβληθεί ο χειρισμός του μείζονος συμβάντος που σχετίζεται με τις ΤΠΕ βάσει νέων διαθέσιμων πληροφοριών, ακολουθούμενη, κατά περίπτωση, από επικαιροποιημένες κοινοποιήσεις κάθε φορά που είναι διαθέσιμη σχετική επικαιροποίηση της κατάστασης, καθώς και κατόπιν συγκεκριμένου αιτήματος της αρμόδιας αρχής,

γ) τελική αναφορά, όταν ολοκληρωθεί η ανάλυση των βαθύτερων αιτίων, ανεξάρτητα από το αν έχουν ήδη εφαρμοστεί μέτρα μετριασμού, και όταν είναι διαθέσιμα τα στοιχεία των πραγματικών επιπτώσεων προς αντικατάσταση των εκτιμήσεων.

5. Οι χρηματοοικονομικές οντότητες μπορούν να αναθέτουν, σύμφωνα με το ενωσιακό και εθνικό τομεακό δίκαιο, τις υποχρεώσεις αναφοράς που προβλέπονται στο παρόν άρθρο σε τρίτο πάροχο υπηρεσιών. Σε περίπτωση τέτοιας εξωτερικής ανάθεσης, η χρηματοοικονομική οντότητα παραμένει εξολοκλήρου υπεύθυνη για την εκπλήρωση των απαιτήσεων αναφοράς συμβάντων.

6. Μετά την παραλαβή της αρχικής κοινοποίησης και κάθε αναφοράς που προβλέπεται στην παράγραφο 4, η αρμόδια αρχή παρέχει εγκαίρως λεπτομερή στοιχεία για το μείζον συμβάν που σχετίζεται με τις ΤΠΕ στους ακόλουθους αποδέκτες με βάση, κατά περίπτωση, τις αντίστοιχες αρμοδιότητές τους:

α) στην ΕΑΤ, στην ΕΑΚΑΑ ή στην ΕΑΑΕΣ,

β) στην ΕΚΤ, στην περίπτωση των χρηματοοικονομικών οντοτήτων που αναφέρονται στο άρθρο 2 παράγραφος 1 στοιχεία α), β) και δ),

γ) στις αρμόδιες αρχές, στα ενιαία σημεία επαφής ή στις CSIRT που έχουν οριστεί ή συσταθεί, σύμφωνα με την οδηγία (ΕΕ) 2022/2555

δ) στις αρχές εξυγίανσης, όπως αναφέρονται στο άρθρο 3 της οδηγίας 2014/59/ΕΕ, και στο Ενιαίο Συμβούλιο Εξυγίανσης (ΕΣΕ) όσον αφορά τις οντότητες που αναφέρονται στο άρθρο 7 παράγραφος 2 του κανονισμού (ΕΕ) αριθ. 806/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([37]), και όσον αφορά τις οντότητες και τους ομίλους που αναφέρονται στο άρθρο 7 παράγραφος 4 στοιχείο β) και στο άρθρο 7 παράγραφος 5 του κανονισμού (ΕΕ) αριθ. 806/2014, εάν οι λεπτομέρειες αυτές αφορούν συμβάντα που ενέχουν κίνδυνο για τη διασφάλιση κρίσιμων λειτουργιών κατά την έννοια του άρθρου 2 παράγραφος 1 σημείο 35) της οδηγίας 2014/59/ΕΕ, και

ε) σε άλλες αρμόδιες δημόσιες αρχές βάσει του εθνικού δικαίου.

7. Μετά την παραλαβή των πληροφοριών σύμφωνα με την παράγραφο 6, η ΕΑΤ, η ΕΑΚΑΑ ή η ΕΑΑΕΣ και η ΕΚΤ, σε συνεννόηση με τον ENISA και σε συνεργασία με τη σχετική αρμόδια αρχή, αξιολογούν αν το μείζον συμβάν που σχετίζεται με τις ΤΠΕ έχει ενδιαφέρον για τις αρμόδιες αρχές σε άλλα κράτη μέλη. Μετά την εν λόγω αξιολόγηση, η ΕΑΤ, η ΕΑΚΑΑ ή η ΕΑΑΕΣ ενημερώνουν σχετικά, το συντομότερο δυνατόν, τις σχετικές αρμόδιες αρχές άλλων κρατών μελών. Η ΕΚΤ ενημερώνει τα μέλη του Ευρωπαϊκού Συστήματος Κεντρικών Τραπεζών για θέματα που σχετίζονται με το σύστημα πληρωμών. Βάσει της εν λόγω ενημέρωσης, οι αρμόδιες αρχές λαμβάνουν, κατά περίπτωση, όλα τα αναγκαία μέτρα για την προστασία της άμεσης σταθερότητας του χρηματοοικονομικού συστήματος.

([37]) Κανονισμός (ΕΕ) αριθ. 806/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Ιουλίου 2014, περί θεσπίσεως ενιαίων κανόνων και διαδικασίας για την εξυγίανση πιστωτικών ιδρυμάτων και ορισμένων επιχειρήσεων επενδύσεων στο πλαίσιο ενός Ενιαίου Μηχανισμού Εξυγίανσης και ενός Ενιαίου Ταμείου Εξυγίανσης και τροποποιήσεως του κανονισμού (ΕΕ) αριθ. 1093/2010 (ΕΕ L 225 της 30.7.2014, σ. 1).

8. Η κοινοποίηση που πρέπει να γίνει από την ΕΑΚΑΑ σύμφωνα με την παράγραφο 7 του παρόντος άρθρου δεν θίγει την ευθύνη της αρμόδιας αρχής να διαβιβάζει επειγόντως τις λεπτομέρειες του μείζονος συμβάντος που σχετίζεται με τις ΤΠΕ στη σχετική αρχή του κράτους μέλους υποδοχής, όταν ένα κεντρικό αποθετήριο τίτλων ασκεί σημαντική διασυνοριακή δραστηριότητα στο κράτος μέλος υποδοχής, το μείζον συμβάν που σχετίζεται με τις ΤΠΕ είναι πιθανό να έχει σοβαρές επιπτώσεις στις χρηματοοικονομικές αγορές του κράτους μέλους υποδοχής και όταν υπάρχουν ρυθμίσεις συνεργασίας μεταξύ των αρμόδιων αρχών σχετικά με την εποπτεία των χρηματοοικονομικών οντοτήτων.

Άρθρο 20

Εναρμόνιση του περιεχομένου και των υποδειγμάτων των αναφορών

Οι ΕΕΑ, μέσω της μεικτής επιτροπής και σε συνεννόηση με τον ENISA και την ΕΚΤ, καταρτίζουν:

α) κοινά σχέδια ρυθμιστικών τεχνικών προτύπων προκειμένου:

i) καθορίζουν το περιεχόμενο των αναφορών για μείζονα συμβάντα που σχετίζονται με τις ΤΠΕ, ώστε να αντικατοπτρίζει τα κριτήρια του άρθρου 18 παράγραφος 1 και να ενσωματώνει περαιτέρω στοιχεία, όπως λεπτομέρειες για τον προσδιορισμό της συνάφειας της υποβολής εκθέσεων για άλλα κράτη μέλη και του αν πρόκειται ή όχι για μείζον λειτουργικό συμβάν ή συμβάν ασφάλειας που σχετίζεται με πληρωμές,

ii) καθορίζουν τις προθεσμίες για την αρχική κοινοποίηση και για κάθε αναφορά που προβλέπεται στο άρθρο 19 παράγραφος 4,

iii) καθορίζουν το περιεχόμενο της κοινοποίησης για σημαντικές κυβερνοαπειλές.

Κατά την κατάρτιση των εν λόγω σχεδίων ρυθμιστικών τεχνικών προτύπων, οι ΕΕΑ λαμβάνουν υπόψη το μέγεθος και το συνολικό προφίλ κινδύνου της χρηματοοικονομικής οντότητας, και τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών της, και ιδίως προκειμένου να διασφαλιστεί ότι, για τους σκοπούς του σημείου ii) του στοιχείου α) του παρόντος εδαφίου, διαφορετικές προθεσμίες μπορούν να αντικατοπτρίζουν, κατά περίπτωση, τις ιδιαιτερότητες των χρηματοοικονομικών τομέων, με την επιφύλαξη της διατήρησης συνεκτικής προσέγγισης για την αναφορά συμβάντων που σχετίζονται με τις ΤΠΕ σύμφωνα με τον παρόντα κανονισμό και την οδηγία (ΕΕ) 2022/2555 Οι ΕΕΑ παρέχουν, κατά περίπτωση, αιτιολόγηση όταν αποκλίνουν από τις προσεγγίσεις που υιοθετούνται στο πλαίσιο της εν λόγω οδηγίας,

β) κοινά σχέδια εκτελεστικών τεχνικών προτύπων με σκοπό τη δημιουργία τυποποιημένων εντύπων, υποδειγμάτων και διαδικασιών για την αναφορά μείζονος συμβάντος που σχετίζεται με τις ΤΠΕ και την κοινοποίηση σημαντικής κυβερνοαπειλής από τις χρηματοοικονομικές οντότητες.

Οι ΕΕΑ υποβάλλουν στην Επιτροπή τα κοινά σχέδια ρυθμιστικών τεχνικών προτύπων που αναφέρονται στο πρώτο εδάφιο στοιχείο α) και τα κοινά σχέδια εκτελεστικών τεχνικών προτύπων που αναφέρονται στο πρώτο εδάφιο στοιχείο β) στην Επιτροπή έως τις 17 Ιουλίου 2024.

Ανατίθεται στην Επιτροπή η εξουσία να συμπληρώνει τον παρόντα κανονισμό εκδίδοντας τα κοινά ρυθμιστικά τεχνικά πρότυπα που αναφέρονται στο πρώτο εδάφιο στοιχείο α), σύμφωνα με τα άρθρα 10 έως 14 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010.

Ανατίθεται στην Επιτροπή η εξουσία να εγκρίνει τα κοινά εκτελεστικά τεχνικά πρότυπα που αναφέρονται στο πρώτο εδάφιο στοιχείο β), σύμφωνα με το άρθρο 15 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010.

Άρθρο 21

Κεντρική διαχείριση της αναφοράς μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ

1. Οι ΕΕΑ, μέσω της μεικτής επιτροπής και σε συνεννόηση με την ΕΚΤ και τον ENISA, καταρτίζουν κοινή έκθεση στην οποία αξιολογείται η σκοπιμότητα περαιτέρω συγκέντρωσης της αναφοράς συμβάντων μέσω της δημιουργίας ενός ενιαίου κόμβου της ΕΕ για την αναφορά μείζονος συμβάντος που σχετίζεται με τις ΤΠΕ από τις χρηματοοικονομικές οντότητες. Στην κοινή έκθεση εξετάζονται πιθανοί τρόποι για τη διευκόλυνση της ροής των αναφορών συμβάντων που σχετίζονται με τις ΤΠΕ, τη μείωση των σχετικών δαπανών και τη στήριξη θεματικών αναλύσεων με στόχο την ενίσχυση της εποπτικής σύγκλισης.

2. Στην κοινή έκθεση που αναφέρεται στην παράγραφο 1 περιλαμβάνονται τουλάχιστον τα εξής στοιχεία:

α) προϋποθέσεις για τη δημιουργία ενιαίου κόμβου της ΕΕ,

β) οφέλη, περιορισμοί και κίνδυνοι, συμπεριλαμβανομένων των κινδύνων που συνδέονται με την υψηλή συγκέντρωση ευαίσθητων πληροφοριών,

γ) η αναγκαία ικανότητα για τη διασφάλιση της διαλειτουργικότητας όσον αφορά άλλα σχετικά συστήματα αναφοράς,

δ) στοιχεία λειτουργικής διαχείρισης,

ε) όροι συμμετοχής,

στ) τεχνικές ρυθμίσεις για την πρόσβαση των χρηματοοικονομικών οντοτήτων και των εθνικών αρμόδιων αρχών στον ενιαίο κόμβο της ΕΕ,

ζ) προκαταρκτική αξιολόγηση του οικονομικού κόστους που προκύπτει από τη σύσταση της επιχειρησιακής πλατφόρμας για την υποστήριξη του ενιαίου κόμβου της ΕΕ, συμπεριλαμβανομένης της απαιτούμενης εμπειρογνωσίας.

3. Οι ΕΕΑ υποβάλλουν στο Ευρωπαϊκό Κοινοβούλιο, στο Συμβούλιο και στην Επιτροπή την έκθεση που αναφέρεται στην παράγραφο 1 έως τις 17 Ιανουαρίου 2025.

Άρθρο 22

Εποπτικές παρατηρήσεις

1. Με την επιφύλαξη της τεχνικής συμβολής, των συμβουλών ή των διορθωτικών μέτρων και της επακόλουθης συνέχειας που μπορεί να δοθεί, κατά περίπτωση, σύμφωνα με το εθνικό δίκαιο, από τις CSIRT δυνάμει της οδηγίας (ΕΕ) 2022/2555 η αρμόδια αρχή, μόλις λάβει την αρχική κοινοποίηση και κάθε αναφορά, όπως προβλέπεται στο άρθρο 19 παράγραφος 4, επιβεβαιώνει την παραλαβή και μπορεί, όπου είναι εφικτό, να παρέχει εγκαίρως σχετικές και αναλογικές παρατηρήσεις ή κατευθυντήριες γραμμές υψηλού επιπέδου στη χρηματοοικονομική οντότητα, ιδίως καθιστώντας διαθέσιμες τυχόν σχετικές ανωνυμοποιημένες πληροφορίες και στοιχεία σχετικά με παρόμοιες απειλές, και μπορεί να συζητά τα διορθωτικά μέτρα που εφαρμόζονται στο επίπεδο της χρηματοοικονομικής οντότητας και τους τρόπους ελαχιστοποίησης και μετριασμού των δυσμενών επιπτώσεων σε ολόκληρο τον χρηματοοικονομικό τομέα. Με την επιφύλαξη των εποπτικών παρατηρήσεων που λαμβάνονται, οι χρηματοοικονομικές οντότητες παραμένουν πλήρως υπεύθυνες για τον χειρισμό και για τις συνέπειες των συμβάντων που σχετίζονται με τις ΤΠΕ και αναφέρονται σύμφωνα με το άρθρο 19 παράγραφος 1.

2. Οι ΕΕΑ, μέσω της μεικτής επιτροπής, αναφέρουν ετησίως σε ανωνυμοποιημένη και συγκεντρωτική βάση τα μείζονα συμβάντα που σχετίζονται με τις ΤΠΕ, των οποίων τα λεπτομερή στοιχεία παρέχονται από τις αρμόδιες αρχές σύμφωνα με το άρθρο 19 παράγραφος 6, εκθέτοντας τουλάχιστον τον αριθμό των μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ, τη φύση τους, τις επιπτώσεις τους στις λειτουργίες των χρηματοοικονομικών οντοτήτων ή των πελατών, τα διορθωτικά μέτρα που λήφθηκαν και τις δαπάνες που πραγματοποιήθηκαν.

Οι ΕΕΑ εκδίδουν προειδοποιήσεις και παράγουν στατιστικά στοιχεία υψηλού επιπέδου προς υποστήριξη των αξιολογήσεων των απειλών και των ευπαθειών για τις ΤΠΕ.

Άρθρο 23

Λειτουργικά συμβάντα ή συμβάντα ασφάλειας που σχετίζονται με πληρωμές, τα οποία αφορούν πιστωτικά ιδρύματα, ιδρύματα πληρωμών, παρόχους υπηρεσιών πληροφοριών λογαριασμού και ιδρύματα ηλεκτρονικού χρήματος

Οι απαιτήσεις που ορίζονται στο παρόν κεφάλαιο ισχύουν επίσης για λειτουργικά συμβάντα ή συμβάντα ασφάλειας που σχετίζονται με πληρωμές και για μείζονα λειτουργικά συμβάντα ή συμβάντα ασφάλειας που σχετίζονται με πληρωμές, όταν αφορούν πιστωτικά ιδρύματα, ιδρύματα πληρωμών, παρόχους υπηρεσιών πληροφοριών λογαριασμού και ιδρύματα ηλεκτρονικού χρήματος.

ΚΕΦΑΛΑΙΟ IV

Δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας

Άρθρο 24

Γενικές απαιτήσεις για τη διενέργεια δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας

1. Για τους σκοπούς της αξιολόγησης της ετοιμότητας όσον αφορά τον χειρισμό συμβάντων που σχετίζονται με τις ΤΠΕ, του εντοπισμού αδυναμιών, ελλείψεων και κενών στην ψηφιακή επιχειρησιακή ανθεκτικότητα, καθώς και της άμεσης εφαρμογής διορθωτικών μέτρων, οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, λαμβάνοντας υπόψη τα κριτήρια του άρθρου 4 παράγραφος 2, θεσπίζουν, διατηρούν και επανεξετάζουν ένα άρτιο και ολοκληρωμένο πρόγραμμα δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας ως αναπόσπαστο μέρος του πλαισίου διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στο άρθρο 6.

2. Το πρόγραμμα δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας περιλαμβάνει σειρά αξιολογήσεων, δοκιμών, μεθοδολογιών, πρακτικών και εργαλείων που πρέπει να εφαρμόζονται σύμφωνα με τα άρθρα 25 και 26.

3. Κατά τη διεξαγωγή του προγράμματος δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας που αναφέρεται στην παράγραφο 1 του παρόντος άρθρου, οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, ακολουθούν προσέγγιση βάσει κινδύνου, λαμβάνοντας υπόψη τα κριτήρια που ορίζονται στο άρθρο 4 παράγραφος 2, συνεκτιμώντας δεόντως το εξελισσόμενο τοπίο του κινδύνου ΤΠΕ, τυχόν ειδικούς κινδύνους στους οποίους εκτίθεται ή ενδέχεται να εκτεθεί η συγκεκριμένη χρηματοοικονομική οντότητα, την κρισιμότητα των πληροφοριακών πόρων και των παρεχόμενων υπηρεσιών, καθώς και κάθε άλλο παράγοντα τον οποίο κρίνει κατάλληλο η χρηματοοικονομική οντότητα.

4. Οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, διασφαλίζουν ότι οι δοκιμές πραγματοποιούνται από ανεξάρτητους φορείς, εσωτερικούς ή εξωτερικούς. Όταν διενεργούνται δοκιμές από εσωτερικό δοκιμαστή, οι χρηματοοικονομικές οντότητες διαθέτουν επαρκείς πόρους και διασφαλίζουν την αποφυγή συγκρούσεων συμφερόντων καθ' όλη τη διάρκεια των φάσεων σχεδιασμού και εκτέλεσης της δοκιμής.

5. Οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, θεσπίζουν διαδικασίες και πολιτικές για την ιεράρχηση, την ταξινόμηση και την επίλυση όλων των ζητημάτων που ανακύπτουν κατά τη διενέργεια των δοκιμών, και καθιερώνουν εσωτερικές μεθοδολογίες επικύρωσης, ώστε να εξακριβώνεται ότι αντιμετωπίζονται πλήρως όλες οι αδυναμίες, οι ελλείψεις ή τα κενά που έχουν διαπιστωθεί.

6. Οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, διασφαλίζουν τουλάχιστον ετησίως ότι διενεργούνται κατάλληλες δοκιμές σε όλα τα συστήματα και εφαρμογές ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες.

Άρθρο 25

Δοκιμές των εργαλείων και συστημάτων ΤΠΕ

1. Το πρόγραμμα δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας που αναφέρεται στο άρθρο 24 προβλέπει**,** σύμφωνα με τα κριτήρια του άρθρου 4 παράγραφος 2, τη διενέργεια κατάλληλων δοκιμών, όπως αξιολογήσεις και έλεγχοι ευπαθειών, αναλύσεις ανοικτού κώδικα, αξιολογήσεις ασφάλειας δικτύου, αναλύσεις ελλείψεων, επισκοπήσεις υλικής ασφάλειας, ερωτηματολόγια και λύσεις λογισμικού σάρωσης, επανεξετάσεις πηγαίου κώδικα εφόσον είναι εφικτό, δοκιμές βάσει σεναρίων, δοκιμές συμβατότητας, δοκιμές επιδόσεων, διατερματικές δοκιμές και δοκιμές παρείσδυσης.

2. Τα κεντρικά αποθετήρια τίτλων και οι κεντρικοί αντισυμβαλλόμενοι διενεργούν αξιολογήσεις ευπαθειών πριν από την υλοποίηση ή αναδιάταξη νέων ή υφιστάμενων εφαρμογών και στοιχείων υποδομής και υπηρεσιών ΤΠΕ που υποστηρίζουν τις κρίσιμες ή σημαντικές λειτουργίες της χρηματοοικονομικής οντότητα.

3. Οι πολύ μικρές επιχειρήσεις διενεργούν τις δοκιμές που αναφέρονται στην παράγραφο 1 συνδυάζοντας μια προσέγγιση βάσει κινδύνου με στρατηγικό σχεδιασμό των δοκιμών ΤΠΕ, λαμβάνοντας δεόντως υπόψη την ανάγκη διατήρησης ισορροπημένης προσέγγισης μεταξύ της κλίμακας των πόρων και του χρόνου που πρέπει να διατεθεί στις δοκιμές ΤΠΕ σύμφωνα με το παρόν άρθρο, αφενός, και του επείγοντος χαρακτήρα, του είδους του κινδύνου, της κρισιμότητας των πληροφοριακών πόρων και των παρεχόμενων υπηρεσιών, καθώς και κάθε άλλο σχετικό παράγοντα, συμπεριλαμβανομένης της ικανότητας της χρηματοοικονομικής οντότητας να αναλαμβάνει υπολογιζόμενους κινδύνους, αφετέρου.

Άρθρο 26

Προηγμένες δοκιμές εργαλείων, συστημάτων και διαδικασιών ΤΠΕ με βάση τις δοκιμές διείσδυσης βάσει απειλών (TLPT)

1. Οι χρηματοοικονομικές οντότητες, πλην των οντοτήτων που αναφέρονται στο άρθρο 16 παράγραφος 1 πρώτο εδάφιο και των πολύ μικρών επιχειρήσεων, οι οποίες προσδιορίζονται σύμφωνα με την παράγραφο 8 τρίτο εδάφιο του παρόντος άρθρου, διενεργούν τουλάχιστον ανά τριετία προηγμένες δοκιμές μέσω TLPT. Με βάση το προφίλ κινδύνου της χρηματοοικονομικής οντότητας και λαμβάνοντας υπόψη τις επιχειρησιακές συνθήκες, η αρμόδια αρχή μπορεί, εφόσον απαιτείται, να ζητήσει από τη χρηματοοικονομική οντότητα να μειώσει ή να αυξήσει τη συχνότητα αυτή.

2. Κάθε δοκιμή παρείσδυσης βάσει απειλών καλύπτει μερικές ή όλες τις κρίσιμες ή σημαντικές λειτουργίες μιας χρηματοοικονομικής οντότητας και διενεργείται σε συστήματα παραγωγής που υποστηρίζουν τις εν λόγω λειτουργίες.

Οι χρηματοοικονομικές οντότητες προσδιορίζουν όλα τα σχετικά υποκείμενα συστήματα, διαδικασίες και τεχνολογίες ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες και υπηρεσίες ΤΠΕ, συμπεριλαμβανομένων όσων υποστηρίζουν τις κρίσιμες ή σημαντικές λειτουργίες που έχουν αποτελέσει αντικείμενο εξωτερικής ανάθεσης ή υπεργολαβίας σε τρίτους παρόχους υπηρεσιών ΤΠΕ.

Οι χρηματοοικονομικές οντότητες αξιολογούν ποιες κρίσιμες ή σημαντικές λειτουργίες είναι ανάγκη να καλύπτονται από τις TLPT. Το αποτέλεσμα της αξιολόγησης αυτής καθορίζει το ακριβές πεδίο των TLPT και επικυρώνεται από τις αρμόδιες αρχές.

3. Όταν στο πεδίο των TLPT περιλαμβάνονται τρίτοι πάροχοι υπηρεσιών ΤΠΕ, η χρηματοοικονομική οντότητα λαμβάνει τα αναγκαία μέτρα και διασφαλίσεις για να εξασφαλίσει τη συμμετοχή των εν λόγω τρίτων παρόχων υπηρεσιών ΤΠΕ στις TLPT και διατηρεί ανά πάσα στιγμή την πλήρη ευθύνη για τη διασφάλιση της συμμόρφωσης με τον παρόντα κανονισμό.

4. Με την επιφύλαξη της παραγράφου 2 πρώτο και δεύτερο εδάφιο, όταν η συμμετοχή τρίτου παρόχου υπηρεσιών ΤΠΕ στις TLPT, που αναφέρεται στην παράγραφο 3, αναμένεται ευλόγως να έχει αρνητικό αντίκτυπο στην ποιότητα ή στην ασφάλεια των υπηρεσιών που παρέχονται από τον τρίτο πάροχο υπηρεσιών ΤΠΕ σε πελάτες που είναι οντότητες μη εμπίπτουσες στο πεδίο εφαρμογής του παρόντος κανονισμού, ή στην εμπιστευτικότητα των δεδομένων που σχετίζονται με τις εν λόγω υπηρεσίες, η χρηματοοικονομική οντότητα και ο τρίτος πάροχος υπηρεσιών ΤΠΕ μπορούν να συμφωνήσουν εγγράφως ότι ο τρίτος πάροχος υπηρεσιών ΤΠΕ συνάπτει απευθείας συμβατικές ρυθμίσεις με εξωτερικό δοκιμαστή, για τον σκοπό της διεξαγωγής, υπό τη διεύθυνση μιας ορισθείσας χρηματοοικονομικής οντότητας, ομαδικών TLPT όπου συμμετέχουν διάφορες χρηματοοικονομικές οντότητες (ομαδικές δοκιμές) στις οποίες ο τρίτος πάροχος υπηρεσιών ΤΠΕ παρέχει υπηρεσίες ΤΠΕ.

Οι εν λόγω ομαδικές δοκιμές καλύπτουν το σχετικό φάσμα υπηρεσιών ΤΠΕ που υποστηρίζουν τις κρίσιμες ή σημαντικές λειτουργίες που ανατίθενται στον αντίστοιχο τρίτο πάροχο υπηρεσιών ΤΠΕ από τις χρηματοοικονομικές οντότητες. Οι ομαδικές δοκιμές θεωρούνται TLPT που διενεργούνται από τις χρηματοοικονομικές οντότητες που συμμετέχουν στις ομαδικές δοκιμές.

Ο αριθμός των χρηματοοικονομικών οντοτήτων που συμμετέχουν στις ομαδικές δοκιμές βαθμονομείται δεόντως, λαμβανομένων υπόψη της πολυπλοκότητας και των τύπων των σχετικών υπηρεσιών.

5. Οι χρηματοοικονομικές οντότητες, σε συνεργασία με τρίτους παρόχους υπηρεσιών ΤΠΕ και άλλα εμπλεκόμενα μέρη, συμπεριλαμβανομένων δοκιμαστών αλλά εξαιρουμένων των αρμόδιων αρχών, εφαρμόζουν αποτελεσματικούς ελέγχους διαχείρισης κινδύνων με σκοπό τη μείωση των κινδύνων όσον αφορά τις πιθανές επιπτώσεις στα δεδομένα, την πρόκληση ζημίας στα περιουσιακά στοιχεία και τη διαταραχή κρίσιμων ή σημαντικών λειτουργιών, υπηρεσιών ή δραστηριοτήτων της ίδιας της χρηματοοικονομικής οντότητας, των αντισυμβαλλομένων της ή του χρηματοοικονομικού τομέα.

6. Με την ολοκλήρωση της δοκιμής, αφού συμφωνηθούν οι εκθέσεις και τα σχέδια αποκατάστασης, η χρηματοοικονομική οντότητα και, κατά περίπτωση, οι εξωτερικοί δοκιμαστές παρέχουν, στην αρχή που έχει οριστεί σύμφωνα με την παράγραφο 9 ή 10, περίληψη των σχετικών ευρημάτων, των σχεδίων αποκατάστασης και της τεκμηρίωσης που αποδεικνύει ότι η TLPT διενεργήθηκε σύμφωνα με τις απαιτήσεις.

7. Οι αρχές παρέχουν σε χρηματοοικονομικές οντότητες βεβαίωση που επιβεβαιώνει ότι η δοκιμή διενεργήθηκε σύμφωνα με τις απαιτήσεις και τα στοιχεία της τεκμηρίωσης, προκειμένου να καταστεί δυνατή η αμοιβαία αναγνώριση των δοκιμών παρείσδυσης βάσει απειλών μεταξύ των αρμόδιων αρχών. Η χρηματοοικονομική οντότητα κοινοποιεί στη σχετική αρμόδια αρχή τη βεβαίωση, την περίληψη των σχετικών ευρημάτων και τα σχέδια αποκατάστασης.

Με την επιφύλαξη της βεβαίωσης αυτής, οι χρηματοοικονομικές οντότητες παραμένουν ανά πάσα στιγμή πλήρως υπεύθυνες για τις επιπτώσεις των δοκιμών που αναφέρονται στην παράγραφο 4.

8. Οι χρηματοοικονομικές οντότητες συνάπτουν συμβάσεις με δοκιμαστές για τους σκοπούς της ανάληψης TLPT σύμφωνα με το άρθρο 27. Όταν οι χρηματοοικονομικές οντότητες χρησιμοποιούν εσωτερικούς δοκιμαστές για τους σκοπούς της ανάληψης TLPT, συνάπτουν σύμβαση με εξωτερικούς δοκιμαστές ανά τρεις δοκιμές.

Τα πιστωτικά ιδρύματα τα οποία χαρακτηρίζονται ως σημαντικά σύμφωνα με το άρθρο 6 παράγραφος 4 του κανονισμού (ΕΕ) αριθ. 1024/2013 χρησιμοποιούν μόνο εξωτερικούς δοκιμαστές σύμφωνα με το άρθρο 27 παράγραφος 1 στοιχεία α) έως ε).

Οι αρμόδιες αρχές προσδιορίζουν τις χρηματοοικονομικές οντότητες που υποχρεούνται να διενεργούν TLPT, λαμβάνοντας υπόψη τα κριτήρια που ορίζονται στο άρθρο 4 παράγραφος 2, αξιολογώντας τα ακόλουθα:

α) παράγοντες που σχετίζονται με τις επιπτώσεις, ιδίως όσον αφορά τον βαθμό στον οποίο οι παρεχόμενες υπηρεσίες και δραστηριότητες που αναλαμβάνει η χρηματοοικονομική οντότητα επηρεάζουν τον χρηματοοικονομικό τομέα,

β) πιθανούς προβληματισμούς σχετικά με τη χρηματοοικονομική σταθερότητα, συμπεριλαμβανομένου του συστημικού χαρακτήρα της χρηματοοικονομικής οντότητας σε ενωσιακό ή εθνικό επίπεδο, κατά περίπτωση,

γ) το ειδικό προφίλ κινδύνου ΤΠΕ, το επίπεδο ωριμότητας ΤΠΕ της χρηματοοικονομικής οντότητας ή τα σχετικά τεχνολογικά χαρακτηριστικά.

9. Τα κράτη μέλη μπορούν να ορίσουν μία ενιαία δημόσια αρχή στον χρηματοοικονομικό τομέα ως υπεύθυνη για θέματα σχετικά με τις TLPT στον χρηματοοικονομικό τομέα σε εθνικό επίπεδο και της αναθέτουν όλες τις αρμοδιότητες και τα καθήκοντα για τον σκοπό αυτό.

10. Ελλείψει ορισμού σύμφωνα με την παράγραφο 9 του παρόντος άρθρου, και με την επιφύλαξη της εξουσίας προσδιορισμού των χρηματοοικονομικών οντοτήτων που απαιτούνται για την εκτέλεση TLPT, μια αρμόδια αρχή μπορεί να αναθέσει την άσκηση ορισμένων ή όλων των καθηκόντων που αναφέρονται στο παρόν άρθρο και στο άρθρο 27 σε άλλη εθνική αρχή του χρηματοοικονομικού τομέα.

11. Οι ΕΕΑ, σε συμφωνία με την ΕΚΤ, καταρτίζουν κοινά σχέδια ρυθμιστικών τεχνικών προτύπων σύμφωνα με το πλαίσιο TIBER-EU, προκειμένου να προσδιορίσουν περαιτέρω:

α) τα κριτήρια που χρησιμοποιούνται για την εφαρμογή της παραγράφου 8 δεύτερο εδάφιο,

β) τις απαιτήσεις και τα πρότυπα που διέπουν τη χρήση εσωτερικών δοκιμαστών,

γ) τις απαιτήσεις σχετικά με:

   i) το πεδίο των TLPT που αναφέρεται στην παράγραφο 2,

   ii) τη μεθοδολογία των δοκιμών και την προσέγγιση που πρέπει να ακολουθείται σε κάθε συγκεκριμένο στάδιο της διαδικασίας δοκιμής,

   iii) τα αποτελέσματα, τα στάδια ολοκλήρωσης και αποκατάστασης στο πλαίσιο της δοκιμής,

δ) το είδος της εποπτικής και άλλης σχετικής συνεργασίας που απαιτούνται για την εφαρμογή TLPT και για τη διευκόλυνση της αμοιβαίας αναγνώρισης των εν λόγω δοκιμών, στο πλαίσιο των χρηματοοικονομικών οντοτήτων που δραστηριοποιούνται σε περισσότερα από ένα κράτη μέλη, ώστε να παρέχεται η δυνατότητα κατάλληλου επιπέδου εποπτικής συμμετοχής, καθώς και η δυνατότητα ευέλικτης εφαρμογής για την κάλυψη των ιδιαίτερων χαρακτηριστικών επιμέρους χρηματοοικονομικών τομέων ή τοπικών χρηματοοικονομικών αγορών.

Κατά την κατάρτιση των εν λόγω σχεδίων ρυθμιστικών τεχνικών προτύπων, οι ΕΕΑ λαμβάνουν δεόντως υπόψη κάθε ειδικό χαρακτηριστικό που προκύπτει από τη διακριτή φύση των δραστηριοτήτων σε διάφορους τομείς χρηματοοικονομικών υπηρεσιών.

Οι ΕΕΑ υποβάλλουν τα εν λόγω σχέδια ρυθμιστικών τεχνικών προτύπων στην Επιτροπή έως τις 17 Ιουλίου 2024.

Ανατίθεται στην Επιτροπή η εξουσία να συμπληρώνει τον παρόντα κανονισμό εκδίδοντας τα ρυθμιστικά τεχνικά πρότυπα που αναφέρονται στο πρώτο εδάφιο, σύμφωνα με τα άρθρα 10 έως 14 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010.

Άρθρο 27

Απαιτήσεις για δοκιμαστές για τη διενέργεια TLPT

1. Οι χρηματοοικονομικές οντότητες, για τη διενέργεια TLPT, χρησιμοποιούν μόνο δοκιμαστές οι οποίοι:

α) είναι απολύτως κατάλληλοι και έγκριτοι,

β) διαθέτουν τεχνικές και οργανωτικές ικανότητες και επιδεικνύουν ειδική εμπειρογνωσία σε θέματα πληροφοριών για απειλές, δοκιμών παρείσδυσης και δοκιμών κόκκινης ομάδας,

γ) έχουν πιστοποίηση από οργανισμό διαπίστευσης κράτους μέλους ή τηρούν επίσημους κώδικες ή πλαίσια δεοντολογίας,

δ) παρέχουν ανεξάρτητη διαβεβαίωση ή έκθεση ελέγχου όσον αφορά την ορθή διαχείριση των κινδύνων που σχετίζονται με τη διενέργεια TLPT, συμπεριλαμβανομένων της δέουσας προστασίας των εμπιστευτικών πληροφοριών της χρηματοοικονομικής οντότητας και της αντιμετώπισης των επιχειρηματικών κινδύνων της χρηματοοικονομικής οντότητας,

ε) καλύπτονται δεόντως και πλήρως από σχετική ασφάλιση επαγγελματικής ευθύνης, μεταξύ άλλων έναντι κινδύνων παραπτωμάτων και αμέλειας.

2. Όταν χρησιμοποιούν εσωτερικούς δοκιμαστές, οι χρηματοοικονομικές οντότητες διασφαλίζουν ότι, πέραν των απαιτήσεων στην παράγραφο 1, πληρούνται και οι ακόλουθες προϋποθέσεις:

α) η χρήση αυτή έχει εγκριθεί από τη σχετική αρμόδια αρχή ή από την ενιαία δημόσια αρχή που έχει οριστεί σύμφωνα με το άρθρο 26 παράγραφοι 9 και 10,

β) η σχετική αρμόδια αρχή έχει επαληθεύσει ότι η χρηματοοικονομική οντότητα διαθέτει επαρκείς ειδικούς πόρους και έχει διασφαλίσει την αποφυγή συγκρούσεων συμφερόντων καθ' όλη τη διάρκεια των φάσεων σχεδιασμού και εκτέλεσης της δοκιμής και

γ) ο πάροχος πληροφοριών για απειλές είναι εξωτερικός σε σχέση με τη χρηματοοικονομική οντότητα.

3. Οι χρηματοοικονομικές οντότητες διασφαλίζουν ότι οι συμβάσεις που συνάπτονται με εξωτερικούς δοκιμαστές προϋποθέτουν την ορθή διαχείριση των αποτελεσμάτων των TLPT και ότι οποιαδήποτε σχετική επεξεργασία δεδομένων, συμπεριλαμβανομένων τυχόν παραγωγής, αποθήκευσης, συγκέντρωσης, σχεδίου, αναφοράς, επικοινωνίας ή καταστροφής, δεν προκαλεί κινδύνους για τη χρηματοοικονομική οντότητα.

ΚΕΦΑΛΑΙΟ V

Διαχείριση κινδύνου τρίτων παρόχων ΤΠΕ

Τμήμα I

Βασικές αρχές για τη χρηστή διαχείριση κινδύνου τρίτων παρόχων ΤΠΕ

Άρθρο 28

Γενικές αρχές

1. Οι χρηματοοικονομικές οντότητες διαχειρίζονται τον κίνδυνο τρίτων παρόχων ΤΠΕ ως αναπόσπαστο στοιχείο των κινδύνων ΤΠΕ εντός του πλαισίου τους διαχείρισης κινδύνων ΤΠΕ όπως αναφέρεται στο άρθρο 6 παράγραφος 1 και σύμφωνα με τις ακόλουθες αρχές:

α) οι χρηματοοικονομικές οντότητες που έχουν θεσπίσει συμβατικές ρυθμίσεις για τη χρήση των υπηρεσιών ΤΠΕ με σκοπό τη διεξαγωγή των επιχειρηματικών τους δραστηριοτήτων εξακολουθούν σε κάθε περίπτωση να είναι πλήρως υπεύθυνες για την τήρηση και την εκπλήρωση όλων των υποχρεώσεων που απορρέουν από τον παρόντα κανονισμό και το ισχύον δίκαιο για τις χρηματοοικονομικές υπηρεσίες,

β) η διαχείριση κινδύνου τρίτων παρόχων ΤΠΕ από τις χρηματοοικονομικές οντότητες εφαρμόζεται βάσει της αρχής της αναλογικότητας, λαμβάνοντας υπόψη:

i) τη φύση, την κλίμακα, την πολυπλοκότητα και τη σημασία των εξαρτήσεων που σχετίζονται με τις ΤΠΕ,

ii) τους κινδύνους που απορρέουν από συμβατικές ρυθμίσεις για τη χρήση υπηρεσιών ΤΠΕ, οι οποίες έχουν συναφθεί με τρίτους παρόχους υπηρεσιών ΤΠΕ, λαμβάνοντας υπόψη την κρισιμότητα ή τη σημασία της αντίστοιχης υπηρεσίας, διαδικασίας ή λειτουργίας, και τις πιθανές επιπτώσεις στη συνέχεια και τη διαθεσιμότητα των χρηματοοικονομικών υπηρεσιών και δραστηριοτήτων, τόσο σε μεμονωμένο επίπεδο όσο και σε επίπεδο ομίλου.

2. Στο πλαίσιο της διαχείρισης κινδύνου ΤΠΕ, οι χρηματοοικονομικές οντότητες, εκτός των οντοτήτων που αναφέρονται στο άρθρο 16 παράγραφος 1 πρώτο εδάφιο και εκτός των πολύ μικρών επιχειρήσεων, εγκρίνουν και επανεξετάζουν τακτικά τη στρατηγική για τους κινδύνους τρίτων παρόχων ΤΠΕ, λαμβάνοντας υπόψη τη στρατηγική πολλαπλών προμηθευτών που αναφέρεται στο άρθρο 6 παράγραφος 9, κατά περίπτωση. Η στρατηγική για τη διαχείριση κινδύνου τρίτων παρόχων ΤΠΕ περιλαμβάνει πολιτική για τη χρήση υπηρεσιών ΤΠΕ που υποστηρίζουν κριτικές ή σημαντικές λειτουργίες, οι οποίες παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ και εφαρμόζεται σε μεμονωμένη βάση και, ανάλογα με την περίπτωση, σε υποενοποιημένη και ενοποιημένη βάση. Το διοικητικό όργανο, βάσει αξιολόγησης του συνολικού προφίλ κινδύνου της χρηματοοικονομικής οντότητας και της κλίμακας και της πολυπλοκότητας των επιχειρηματικών υπηρεσιών, επανεξετάζει τακτικά τους κινδύνους που εντοπίζονται σε σχέση με συμβατικές ρυθμίσεις σχετικά με τη χρήση υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες.

3. Στο πλαίσιο της διαχείρισης κινδύνου ΤΠΕ, οι χρηματοοικονομικές οντότητες τηρούν και επικαιροποιούν σε επίπεδο οντότητας και σε υποενοποιημένο και ενοποιημένο επίπεδο, μητρώο πληροφοριών όσον αφορά το σύνολο των συμβατικών ρυθμίσεων σχετικά με τη χρήση υπηρεσιών ΤΠΕ που παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ.

Οι συμβατικές ρυθμίσεις που αναφέρονται στο πρώτο εδάφιο τεκμηριώνονται κατάλληλα, με διαχωρισμό των ρυθμίσεων που καλύπτουν υπηρεσίες ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες από τις υπόλοιπες ρυθμίσεις.

Οι χρηματοοικονομικές οντότητες αναφέρουν στις αρμόδιες αρχές, τουλάχιστον ετησίως, τον αριθμό των νέων συμβατικών ρυθμίσεων για τη χρήση υπηρεσιών ΤΠΕ, τις κατηγορίες τρίτων παρόχων υπηρεσιών ΤΠΕ, το είδος των συμβατικών ρυθμίσεων και τις παρεχόμενες υπηρεσίες και λειτουργίες ΤΠΕ.

Οι χρηματοοικονομικές οντότητες θέτουν στη διάθεση της αρμόδιας αρχής, κατόπιν αιτήματός της, το πλήρες μητρώο πληροφοριών ή, εφόσον ζητείται, συγκεκριμένα τμήματα αυτού, καθώς και κάθε πληροφορία που κρίνεται απαραίτητη για την αποτελεσματική εποπτεία της χρηματοοικονομικής οντότητας.

Οι χρηματοοικονομικές οντότητες ενημερώνουν εγκαίρως την αρμόδια αρχή για οποιαδήποτε προγραμματισμένη συμβατική ρύθμιση σχετικά με τη χρήση υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες, καθώς και για τη χρονική στιγμή κατά την οποία καθίσταται κρίσιμη ή σημαντική μια λειτουργία.

4. Πριν από τη σύναψη συμβατικής ρύθμισης σχετικά με τη χρήση υπηρεσιών ΤΠΕ, οι χρηματοοικονομικές οντότητες:

α) αξιολογούν αν η συμβατική ρύθμιση καλύπτει τη χρήση υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμη ή σημαντική λειτουργία,

β) αξιολογούν αν πληρούνται οι όροι εποπτείας της σύμβασης,

γ) προσδιορίζουν και αξιολογούν όλους τους συναφείς κινδύνους σε σχέση με τη συμβατική ρύθμιση, συμπεριλαμβανομένης της πιθανότητας συμβολής της εν λόγω συμβατικής ρύθμισης στην ενίσχυση του κινδύνου συγκέντρωσης ΤΠΕ, όπως αναφέρεται στο άρθρο 29,

δ) αναλαμβάνουν κάθε δέουσα επιμέλεια των υποψήφιων τρίτων παρόχων υπηρεσιών ΤΠΕ και διασφαλίζουν καθ' όλη τη διαδικασία επιλογής και αξιολόγησης ότι ο τρίτος πάροχος υπηρεσιών ΤΠΕ είναι κατάλληλος,

ε) προσδιορίζουν και αξιολογούν συγκρούσεις συμφερόντων που μπορεί να προκαλέσει η συμβατική ρύθμιση.

5. Οι χρηματοοικονομικές οντότητες μπορούν να συνάπτουν συμβατικές ρυθμίσεις μόνο με τρίτους παρόχους υπηρεσιών ΤΠΕ που συμμορφώνονται με κατάλληλα πρότυπα ασφάλειας των πληροφοριών. Όταν οι εν λόγω συμβατικές ρυθμίσεις αφορούν κρίσιμες ή σημαντικές λειτουργίες, οι χρηματοοικονομικές οντότητες, πριν από τη σύναψη των ρυθμίσεων, λαμβάνουν δεόντως υπόψη τη χρήση, από τρίτους παρόχους υπηρεσιών ΤΠΕ, των πλέον επικαιροποιημένων και ύψιστης ποιότητας προτύπων ασφάλειας πληροφοριών.

6. Κατά την άσκηση των δικαιωμάτων πρόσβασης, επιθεώρησης και ελέγχου έναντι του τρίτου παρόχου υπηρεσιών ΤΠΕ, οι χρηματοοικονομικές οντότητες προκαθορίζουν, σύμφωνα με την προσέγγιση βάσει κινδύνων, τη συχνότητα των ελέγχων και των επιθεωρήσεων, καθώς και τους τομείς που πρέπει να ελέγχονται μέσω της τήρησης κοινώς αποδεκτών προτύπων ελέγχου σύμφωνα με τυχόν εποπτικές οδηγίες σχετικά με τη χρήση και την ενσωμάτωση προτύπων ελέγχου αυτού του είδους.

Όταν οι συμβατικές ρυθμίσεις που συνάπτονται με τρίτους παρόχους υπηρεσιών ΤΠΕ σχετικά με τη χρήση υπηρεσιών ΤΠΕ συνεπάγονται υψηλή τεχνική πολυπλοκότητα, η χρηματοοικονομική οντότητα εξακριβώνει αν οι ελεγκτές, είτε πρόκειται για εσωτερικούς ή εξωτερικούς είτε για ομάδα ελεγκτών, διαθέτουν τις κατάλληλες δεξιότητες και γνώσεις για την αποτελεσματική διενέργεια των σχετικών ελέγχων και αξιολογήσεων.

7. Οι χρηματοοικονομικές οντότητες διασφαλίζουν ότι οι συμβατικές ρυθμίσεις σχετικά με τη χρήση υπηρεσιών ΤΠΕ μπορούν να καταγγέλλονται όταν συντρέχει οποιαδήποτε από τις παρακάτω συνθήκες:

α) σημαντική παραβίαση των εφαρμοστέων νομοθετικών, κανονιστικών διατάξεων ή συμβατικών όρων από τον τρίτο πάροχο υπηρεσιών ΤΠΕ,

β) συνθήκες που προσδιορίζονται καθ' όλη τη διάρκεια παρακολούθησης των κινδύνων τρίτων παρόχων ΤΠΕ και οι οποίες θεωρούνται ικανές να μεταβάλουν την εκτέλεση των λειτουργιών που παρέχονται μέσω της συμβατικής ρύθμισης, συμπεριλαμβανομένων σημαντικών μεταβολών που επηρεάζουν τη ρύθμιση ή την κατάσταση του τρίτου παρόχου υπηρεσιών ΤΠΕ,

γ) αποδεδειγμένες αδυναμίες του τρίτου παρόχου υπηρεσιών ΤΠΕ που αφορούν τη συνολική διαχείριση κινδύνου ΤΠΕ από μέρους του και ειδικότερα στον τρόπο με τον οποίο εγγυάται τη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα και την εμπιστευτικότητα εμπιστευτικών, προσωπικών ή άλλως ευαίσθητων δεδομένων ή μη προσωπικών δεδομένων,

δ) όταν η αρμόδια αρχή δεν μπορεί πλέον να εποπτεύει αποτελεσματικά τη χρηματοοικονομική οντότητα συνεπεία των συνθηκών της αντίστοιχης συμβατικής ρύθμισης ή των περιστάσεων που σχετίζονται με αυτήν.

8. Για τις υπηρεσίες ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες, οι χρηματοοικονομικές οντότητες θέτουν σε εφαρμογή στρατηγικές εξόδου. Οι στρατηγικές εξόδου λαμβάνουν υπόψη τους κινδύνους που ενδέχεται να ανακύψουν στο επίπεδο των τρίτων παρόχων υπηρεσιών ΤΠΕ, ιδίως όσον αφορά την πιθανότητα αθέτησης υποχρεώσεων εκ μέρους τους, την υποβάθμιση της ποιότητας των παρεχόμενων υπηρεσιών ΤΠΕ, τυχόν διαταραχή της δραστηριότητας λόγω ακατάλληλης ή μη παροχής υπηρεσιών ΤΠΕ ή οποιονδήποτε σημαντικό κίνδυνο που ανακύπτει σε σχέση με την ενδεδειγμένη και συνεχή ανάπτυξη της αντίστοιχης υπηρεσίας ΤΠΕ ή την καταγγελία συμβατικών ρυθμίσεων με τρίτους παρόχους υπηρεσιών ΤΠΕ υπό οποιαδήποτε από τις περιστάσεις οι οποίες προβλέπονται στην παράγραφο 7.

Οι χρηματοοικονομικές οντότητες διασφαλίζουν ότι είναι σε θέση να αποχωρήσουν από συμβατικές ρυθμίσεις:

α) χωρίς διαταραχή των επιχειρηματικών τους δραστηριοτήτων,

β) χωρίς περιορισμό της συμμόρφωσης με τις κανονιστικές απαιτήσεις,

γ) χωρίς αυτό να αποβαίνει εις βάρος της συνέχειας και της ποιότητας των υπηρεσιών που παρέχονται σε πελάτες.

Τα σχέδια εξόδου είναι πλήρη, τεκμηριωμένα και, σύμφωνα με τα κριτήρια που ορίζονται στο άρθρο 4 παράγραφος 2, υποβάλλονται σε επαρκείς δοκιμές και επανεξετάζονται περιοδικά.

Οι χρηματοοικονομικές οντότητες προσδιορίζουν εναλλακτικές λύσεις και καταρτίζουν μεταβατικά σχέδια που τους παρέχουν τη δυνατότητα να αφαιρέσουν τις συμβατικές υπηρεσίες ΤΠΕ και τα σχετικά δεδομένα από τον τρίτο πάροχο υπηρεσιών ΤΠΕ και να τα μεταφέρουν με ασφαλή και ολοκληρωμένο τρόπο σε εναλλακτικούς παρόχους ή να τα ενσωματώνουν εκ νέου εντός της επιχείρησης.

Οι χρηματοοικονομικές οντότητες θέτουν σε εφαρμογή ενδεδειγμένα μέτρα έκτακτης ανάγκης για τη διατήρηση της επιχειρησιακής συνέχειας, εφόσον συντρέχουν οι συνθήκες που αναφέρονται στο πρώτο εδάφιο.

9. Οι ΕΕΑ καταρτίζουν, μέσω της μεικτής επιτροπής, σχέδια εκτελεστικών τεχνικών προτύπων για τη δημιουργία των τυποποιημένων υποδειγμάτων για τους σκοπούς του μητρώου πληροφοριών που αναφέρεται στην παράγραφο 3, συμπεριλαμβανομένων των πληροφοριών που είναι κοινές σε όλες τις συμβατικές ρυθμίσεις σχετικά με τη χρήση υπηρεσιών ΤΠΕ. Οι ΕΕΑ υποβάλλουν τα εν λόγω σχέδια εκτελεστικών τεχνικών προτύπων στην Επιτροπή έως τις 17 Ιανουαρίου 2024.

Ανατίθεται στην Επιτροπή η εξουσία να εκδίδει τα εκτελεστικά τεχνικά πρότυπα που αναφέρονται στο πρώτο εδάφιο, σύμφωνα με το άρθρο 15 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010.

10. Οι ΕΕΑ, μέσω της μεικτής επιτροπής, καταρτίζουν σχέδια ρυθμιστικών τεχνικών προτύπων για τον περαιτέρω προσδιορισμό των λεπτομερειών του περιεχομένου της πολιτικής που αναφέρεται στην παράγραφο 2 σε σχέση με τις συμβατικές ρυθμίσεις σχετικά με τη χρήση υπηρεσιών ΤΠΕ οι οποίες υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες που παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ.

Κατά την κατάρτιση των εν λόγω σχεδίων ρυθμιστικών τεχνικών προτύπων, οι ΕΕΑ λαμβάνουν υπόψη το μέγεθος και το συνολικό προφίλ κινδύνου της χρηματοοικονομικής οντότητας, και τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών της. Οι ΕΕΑ υποβάλλουν τα εν λόγω σχέδια εκτελεστικών τεχνικών προτύπων στην Επιτροπή έως τις 17 Ιανουαρίου 2024.

Ανατίθεται στην Επιτροπή η εξουσία να συμπληρώνει τον παρόντα κανονισμό εκδίδοντας τα ρυθμιστικά τεχνικά πρότυπα που αναφέρονται στο πρώτο εδάφιο, σύμφωνα με τα άρθρα 10 έως 14 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010.

Άρθρο 29

Προκαταρκτική αξιολόγηση κινδύνου συγκέντρωσης ΤΠΕ

1. Κατά τον προσδιορισμό και την αξιολόγηση των κινδύνων που αναφέρονται στο άρθρο 28 παράγραφος 4 στοιχείο γ), οι χρηματοοικονομικές οντότητες λαμβάνουν επίσης υπόψη αν η προβλεπόμενη σύναψη συμβατικής ρύθμισης σε σχέση με υπηρεσίες ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες μπορεί να έχει οποιοδήποτε από τα ακόλουθα αποτελέσματα:

α) εργολαβική ανάθεση σε τρίτο πάροχο υπηρεσιών ΤΠΕ που δεν μπορεί να αντικατασταθεί εύκολα ή

β) εφαρμογή πολλαπλών συμβατικών ρυθμίσεων σχετικά με την παροχή υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες με τον ίδιο τρίτο πάροχο υπηρεσιών ΤΠΕ ή με στενά συνδεδεμένους τρίτους παρόχους υπηρεσιών ΤΠΕ.

Οι χρηματοοικονομικές οντότητες σταθμίζουν τα οφέλη και το κόστος εναλλακτικών λύσεων, όπως η χρήση διαφορετικών τρίτων παρόχων υπηρεσιών ΤΠΕ, λαμβάνοντας υπόψη αν και με ποιον τρόπο οι προτεινόμενες λύσεις ανταποκρίνονται στις επιχειρηματικές ανάγκες και τους στόχους που καθορίζονται στην οικεία στρατηγική ψηφιακής ανθεκτικότητας.

2. Όταν οι συμβατικές ρυθμίσεις σχετικά με τη χρήση υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες περιλαμβάνουν την πιθανότητα ένας τρίτος πάροχος υπηρεσιών ΤΠΕ να αναθέσει περαιτέρω με υπεργολαβία υπηρεσίες ΤΠΕ που υποστηρίζουν κρίσιμη ή σημαντική λειτουργία σε άλλους τρίτους παρόχους υπηρεσιών ΤΠΕ, οι χρηματοοικονομικές οντότητες σταθμίζουν τα οφέλη και τους κινδύνους που ενδέχεται να προκύψουν σε σχέση με την εν λόγω πιθανή υπεργολαβία, ιδίως σε περίπτωση υπεργολάβου ΤΠΕ εγκατεστημένου σε τρίτη χώρα.

Όταν οι συμβατικές ρυθμίσεις αφορούν υπηρεσίες ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες, οι χρηματοοικονομικές οντότητες λαμβάνουν δεόντως υπόψη τις διατάξεις της νομοθεσίας περί αφερεγγυότητας που θα ίσχυαν σε περίπτωση πτώχευσης του τρίτου παρόχου υπηρεσιών ΤΠΕ, καθώς και κάθε περιορισμό που ενδέχεται να ανακύψει σε σχέση με την επείγουσα ανάκτηση των δεδομένων της χρηματοοικονομικής οντότητας.

Όταν συνάπτονται συμβατικές ρυθμίσεις σχετικά με τη χρήση υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες με τρίτο πάροχο υπηρεσιών ΤΠΕ εγκατεστημένο σε τρίτη χώρα, οι χρηματοοικονομικές οντότητες, πέραν των εκτιμήσεων που αναφέρονται στο δεύτερο εδάφιο, εξετάζουν επίσης τη συμμόρφωση με τους κανόνες της Ένωσης για την προστασία των δεδομένων και την αποτελεσματική επιβολή του δικαίου στην εν λόγω τρίτη χώρα.

Όταν οι συμβατικές ρυθμίσεις σχετικά με τη χρήση υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες προβλέπουν υπεργολαβική ανάθεση, οι χρηματοοικονομικές οντότητες αξιολογούν αν και με ποιον τρόπο μπορούν οι δυνητικά μεγάλες και πολύπλοκες αλυσίδες υπεργολαβικής ανάθεσης να επηρεάσουν την ικανότητά τους να παρακολουθούν πλήρως τις λειτουργίες που αποτελούν αντικείμενο ανάθεσης, καθώς και την ικανότητα της αρμόδιας αρχής να εποπτεύει αποτελεσματικά τη χρηματοοικονομική οντότητα στο πλαίσιο αυτό.

Άρθρο 30

Βασικές συμβατικές διατάξεις

1. Τα δικαιώματα και οι υποχρεώσεις της χρηματοοικονομικής οντότητας και του τρίτου παρόχου υπηρεσιών ΤΠΕ επιμερίζονται με σαφήνεια και καθορίζονται εγγράφως. Η πλήρης σύμβαση περιλαμβάνει τις συμφωνίες επιπέδου εξυπηρέτησης και τεκμηριώνεται με έγγραφο το οποίο τίθεται στη διάθεση των συμβαλλομένων σε έντυπη μορφή, ή με έγγραφο σε άλλο τηλεφορτώσιμο, σταθερό και προσβάσιμο μορφότυπο.

2. Οι συμβατικές ρυθμίσεις σχετικά με τη χρήση υπηρεσιών ΤΠΕ περιλαμβάνουν τουλάχιστον τα ακόλουθα στοιχεία:

α) σαφή και πλήρη περιγραφή όλων των λειτουργιών και υπηρεσιών ΤΠΕ που πρέπει να παρέχονται από τον τρίτο πάροχο υπηρεσιών ΤΠΕ, με αναφορά στη δυνατότητα ή μη υπεργολαβικής ανάθεσης υπηρεσίας ΤΠΕ που υποστηρίζει κρίσιμη ή σημαντική λειτουργία, ή σημαντικών μερών της, και, εάν αυτή επιτρέπεται, αναφορά των όρων που διέπουν την υπεργολαβική ανάθεση,

β) τις τοποθεσίες, δηλαδή τις περιοχές και τις χώρες στις οποίες πρέπει να παρέχονται οι λειτουργίες και υπηρεσίες ΤΠΕ που αποτελούν αντικείμενο ανάθεσης ή υπεργολαβίας και στις οποίες θα πραγματοποιείται η επεξεργασία δεδομένων, συμπεριλαμβανομένου του χώρου αποθήκευσης, και την απαίτηση ενημέρωσης της χρηματοοικονομικής οντότητας από τον τρίτο πάροχο υπηρεσιών ΤΠΕ εκ των προτέρων, σε περίπτωση που προτίθεται να αλλάξει τις τοποθεσίες αυτές,

γ) διατάξεις σχετικά με τη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα και την εμπιστευτικότητα όσον αφορά την προστασία δεδομένων, συμπεριλαμβανομένων των δεδομένων προσωπικού χαρακτήρα,

δ) διατάξεις σχετικά με τη διασφάλιση της πρόσβασης, της ανάκτησης και της επιστροφής σε εύκολα προσβάσιμη μορφή δεδομένων προσωπικού και μη προσωπικού χαρακτήρα, τα οποία επεξεργάζεται η χρηματοοικονομική οντότητα σε περίπτωση αφερεγγυότητας, εξυγίανσης, διακοπής των επιχειρηματικών δραστηριοτήτων του τρίτου παρόχου υπηρεσιών ΤΠΕ, ή σε περίπτωση καταγγελίας των συμβατικών ρυθμίσεων,

ε) περιγραφές των επιπέδων εξυπηρέτησης, συμπεριλαμβανομένων των επικαιροποιήσεων και των αναθεωρήσεών τους,

στ) την υποχρέωση του τρίτου παρόχου υπηρεσιών ΤΠΕ να παρέχει συνδρομή στη χρηματοοικονομική οντότητα χωρίς πρόσθετο κόστος ή με κόστος που καθορίζεται εκ των προτέρων, σε περίπτωση συμβάντος ΤΠΕ το οποίο σχετίζεται με την υπηρεσία ΤΠΕ που παρέχεται στη χρηματοοικονομική οντότητα,

ζ) την υποχρέωση του τρίτου παρόχου υπηρεσιών ΤΠΕ να συνεργάζεται πλήρως με τις αρμόδιες αρχές και τις αρχές εξυγίανσης της χρηματοοικονομικής οντότητας, συμπεριλαμβανομένων των προσώπων που διορίζονται από αυτές,

η) δικαιώματα καταγγελίας και συναφή ελάχιστη περίοδο προειδοποίησης για την καταγγελία των συμβατικών ρυθμίσεων, σύμφωνα με τις προσδοκίες των αρμόδιων αρχών και των αρχών εξυγίανσης,

θ) τους όρους συμμετοχής τρίτων παρόχων υπηρεσιών ΤΠΕ στα προγράμματα ευαισθητοποίησης για την ασφάλεια ΤΠΕ των χρηματοοικονομικών οντοτήτων και στην κατάρτιση για την ψηφιακή επιχειρησιακή ανθεκτικότητα σύμφωνα με το άρθρο 13 παράγραφος 6.

3. Οι συμβατικές ρυθμίσεις σχετικά με τη χρήση υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες περιλαμβάνουν, επιπλέον των στοιχείων που αναφέρονται στην παράγραφο 2, τουλάχιστον τα ακόλουθα:

α) πλήρεις περιγραφές των επιπέδων εξυπηρέτησης, συμπεριλαμβανομένων των επικαιροποιήσεων και των αναθεωρήσεών τους με ακριβείς ποσοτικούς και ποιοτικούς στόχους επιδόσεων εντός των συμφωνημένων επιπέδων εξυπηρέτησης, ώστε να παρέχεται η δυνατότητα αποτελεσματικής παρακολούθησης από τη χρηματοοικονομική οντότητα των υπηρεσιών ΤΠΕ και να επιτρέπεται η λήψη κατάλληλων διορθωτικών μέτρων, χωρίς αδικαιολόγητη καθυστέρηση, όταν δεν πληρούνται τα συμφωνημένα επίπεδα εξυπηρέτησης,

β) προθεσμίες προειδοποίησης και υποχρεώσεις υποβολής εκθέσεων εκ μέρους του τρίτου παρόχου υπηρεσιών ΤΠΕ προς τη χρηματοοικονομική οντότητα, συμπεριλαμβανομένης της κοινοποίησης οποιασδήποτε εξέλιξης η οποία θα μπορούσε να έχει σημαντικές επιπτώσεις στην ικανότητα του τρίτου παρόχου υπηρεσιών ΤΠΕ όσον αφορά την αποτελεσματική παροχή υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες σύμφωνα με τα συμφωνημένα επίπεδα εξυπηρέτησης,

γ) απαιτήσεις για τον τρίτο πάροχο υπηρεσιών ΤΠΕ να θέτει σε εφαρμογή και να υποβάλλει σε δοκιμή επιχειρησιακά σχέδια έκτακτης ανάγκης και να εφαρμόζει μέτρα, εργαλεία και πολιτικές ασφάλειας των ΤΠΕ που παρέχουν κατάλληλο επίπεδο ασφάλειας για την παροχή υπηρεσιών από τη χρηματοοικονομική οντότητα σύμφωνα με το ρυθμιστικό της πλαίσιο,

δ) την υποχρέωση του τρίτου παρόχου υπηρεσιών ΤΠΕ να συμμετέχει και να συνεργάζεται πλήρως στις TLPT της χρηματοοικονομικής οντότητας, όπως αναφέρεται στα άρθρα 26 και 27,

ε) το δικαίωμα παρακολούθησης, σε διαρκή βάση, των επιδόσεων του τρίτου παρόχου υπηρεσιών ΤΠΕ, το οποίο συνεπάγεται τα ακόλουθα:

i) απεριόριστα δικαιώματα πρόσβασης, επιθεώρησης και ελέγχου από τη χρηματοοικονομική οντότητα ή διορισμένο τρίτο φορέα, και από την αρμόδια αρχή, και το δικαίωμα λήψης αντιγράφων της σχετικής τεκμηρίωσης επιτόπου εάν είναι κρίσιμα για τις δραστηριότητες του τρίτου παρόχου υπηρεσιών ΤΠΕ, η αποτελεσματική άσκηση των οποίων δεν εμποδίζεται ούτε περιορίζεται από άλλες συμβατικές ρυθμίσεις ή την εφαρμογή πολιτικών,

ii) το δικαίωμα συμφωνίας περί εναλλακτικών επιπέδων βεβαιότητας, όταν θίγονται τα δικαιώματα άλλων πελατών,

iii) την υποχρέωση του τρίτου παρόχου υπηρεσιών ΤΠΕ για πλήρη συνεργασία κατά τις επιτόπιες επιθεωρήσεις και τους ελέγχους που διενεργούνται από τις αρμόδιες αρχές, τον κύριο εποπτικό φορέα, τη χρηματοοικονομική οντότητα ή διορισμένο τρίτο φορέα και

iv) την υποχρέωση παροχής λεπτομερειών σχετικά με το εύρος, τις ακολουθητέες διαδικασίες και τη συχνότητα διενέργειας των εν λόγω επιθεωρήσεων και ελέγχων,

στ) στρατηγικές εξόδου, ιδίως όσον αφορά τον καθορισμό υποχρεωτικής επαρκούς μεταβατικής περιόδου:

i) κατά τη διάρκεια της οποίας ο τρίτος πάροχος υπηρεσιών ΤΠΕ θα συνεχίσει να παρέχει τις αντίστοιχες λειτουργίες ή υπηρεσίες ΤΠΕ, με σκοπό τη μείωση του κινδύνου διαταραχής στη χρηματοοικονομική οντότητα ή τη διασφάλιση της αποτελεσματικής εξυγίανσης και αναδιάρθρωσής της,

(ii) η οποία παρέχει στη χρηματοοικονομική οντότητα τη δυνατότητα μετάβασης σε άλλον τρίτο πάροχο υπηρεσιών ΤΠΕ ή τη δυνατότητα επιλογής άλλων λύσεων εντός της επιχείρησης, ανάλογα με την πολυπλοκότητα της παρεχόμενης υπηρεσίας.

Κατά παρέκκλιση από το στοιχείο ε), ο τρίτος πάροχος υπηρεσιών ΤΠΕ και η χρηματοοικονομική οντότητα που αποτελεί πολύ μικρή επιχείρηση μπορούν να συμφωνήσουν ότι τα δικαιώματα πρόσβασης, επιθεώρησης και ελέγχου της χρηματοοικονομικής οντότητας μπορούν να ανατεθούν σε ανεξάρτητο τρίτο μέρος, το οποίο ορίζεται από τον τρίτο πάροχο υπηρεσιών ΤΠΕ, και ότι η χρηματοοικονομική οντότητα είναι σε θέση να ζητήσει από το τρίτο μέρος ανά πάσα στιγμή πληροφορίες και διαβεβαιώσεις σχετικά με τις επιδόσεις του τρίτου παρόχου υπηρεσιών ΤΠΕ.

4. Κατά τη διαπραγμάτευση των συμβατικών ρυθμίσεων, οι χρηματοοικονομικές οντότητες και οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ λαμβάνουν υπόψη τη χρήση τυποποιημένων συμβατικών ρητρών που έχουν καταρτισθεί από τις αρμόδιες αρχές για συγκεκριμένες υπηρεσίες.

5. Οι ΕΕΑ καταρτίζουν, μέσω της μεικτής επιτροπής, σχέδια ρυθμιστικών τεχνικών προτύπων για τον περαιτέρω προσδιορισμό των στοιχείων της παραγράφου 2 στοιχείο α) τα οποία πρέπει να καθορίζει και να αξιολογεί η χρηματοοικονομική οντότητα κατά την υπεργολαβική ανάθεση υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες.

Κατά την κατάρτιση των εν λόγω σχεδίων ρυθμιστικών τεχνικών προτύπων, οι ΕΕΑ λαμβάνουν υπόψη το μέγεθος και το συνολικό προφίλ κινδύνου της χρηματοοικονομικής οντότητας και τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών της.

Οι ΕΕΑ υποβάλλουν τα εν λόγω σχέδια ρυθμιστικών τεχνικών προτύπων στην Επιτροπή έως τις 17 Ιουλίου 2024.

Ανατίθεται στην Επιτροπή η εξουσία να συμπληρώνει τον παρόντα κανονισμό εκδίδοντας τα ρυθμιστικά τεχνικά πρότυπα που αναφέρονται στο πρώτο εδάφιο, σύμφωνα με τα άρθρα 10 έως 14 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010.

ΤΜΗΜΑ ΙΙ

Πλαίσιο εποπτείας κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ

Άρθρο 31

Ορισμός κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ

1. Οι ΕΕΑ, μέσω της μεικτής επιτροπής και κατόπιν σύστασης του φόρουμ εποπτείας που συγκροτείται βάσει του άρθρου 32 παράγραφος 1:

α) ορίζουν τους τρίτους παρόχους υπηρεσιών ΤΠΕ που είναι κρίσιμοι για τις χρηματοοικονομικές οντότητες, κατόπιν αξιολόγησης κατά την οποία λαμβάνονται υπόψη τα κριτήρια που καθορίζονται στην παράγραφο 2,

β) ορίζουν ως κύριο εποπτικό φορέα για κάθε κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ την ΕΕΑ η οποία είναι υπεύθυνη, σύμφωνα με τους κανονισμούς (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 ή (ΕΕ) αριθ. 1095/2010, για τις χρηματοοικονομικές οντότητες που έχουν από κοινού το μεγαλύτερο μερίδιο των συνολικών περιουσιακών στοιχείων επί της αξίας των συνολικών περιουσιακών στοιχείων όλων των χρηματοοικονομικών οντοτήτων που χρησιμοποιούν τις υπηρεσίες του σχετικού κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ, όπως αποδεικνύεται από το άθροισμα των επιμέρους ισολογισμών των εν λόγω χρηματοοικονομικών οντοτήτων.

2. Ο ορισμός που αναφέρεται στην παράγραφο 1 στοιχείο α) βασίζεται σε όλα τα ακόλουθα κριτήρια σε σχέση με τις υπηρεσίες ΤΠΕ που παρέχονται από τρίτο πάροχο υπηρεσιών ΤΠΕ:

α) τις συστημικές επιπτώσεις στη σταθερότητα, τη συνέχεια ή την ποιότητα της παροχής χρηματοοικονομικών υπηρεσιών σε περίπτωση που ο σχετικός τρίτος πάροχος υπηρεσιών ΤΠΕ αντιμετωπίσει λειτουργική ανεπάρκεια μεγάλης κλίμακας κατά την παροχή των υπηρεσιών του, λαμβάνοντας υπόψη τον αριθμό των χρηματοοικονομικών οντοτήτων και τη συνολική αξία των περιουσιακών στοιχείων των χρηματοοικονομικών οντοτήτων στις οποίες ο οικείος τρίτος πάροχος υπηρεσιών ΤΠΕ παρέχει τις υπηρεσίες του,

β) τον συστημικό χαρακτήρα ή τη σημασία των χρηματοοικονομικών οντοτήτων οι οποίες βασίζονται στον οικείο τρίτο πάροχο υπηρεσιών ΤΠΕ, που αξιολογείται σύμφωνα με τις ακόλουθες παραμέτρους:

i) τον αριθμό των παγκόσμιων συστημικώς σημαντικών ιδρυμάτων (G-SII) ή άλλων συστημικώς σημαντικών ιδρυμάτων (O-SII) που βασίζονται στον αντίστοιχο τρίτο πάροχο υπηρεσιών ΤΠΕ,

ii) την αλληλεξάρτηση μεταξύ των G-SII ή των O-SII που αναφέρονται στο σημείο i) και άλλων χρηματοοικονομικών οντοτήτων, συμπεριλαμβανομένων των καταστάσεων στις οποίες τα G-SII ή τα O-SII παρέχουν υπηρεσίες χρηματοοικονομικών υποδομών σε άλλες χρηματοοικονομικές οντότητες,

γ) την εξάρτηση των χρηματοοικονομικών οντοτήτων από τις υπηρεσίες που παρέχονται από τον σχετικό τρίτο πάροχο υπηρεσιών ΤΠΕ σε σχέση με κρίσιμες ή σημαντικές λειτουργίες χρηματοοικονομικών οντοτήτων στις οποίες συμμετέχει τελικά ο ίδιος τρίτος πάροχος υπηρεσιών ΤΠΕ, ανεξάρτητα από το αν οι χρηματοοικονομικές οντότητες στηρίζονται στις υπηρεσίες αυτές άμεσα ή έμμεσα, μέσω ρυθμίσεων υπεργολαβίας,

δ) τη δυνατότητα υποκατάστασης του τρίτου παρόχου υπηρεσιών ΤΠΕ, λαμβάνοντας υπόψη τις ακόλουθες παραμέτρους:

i) την έλλειψη πραγματικών εναλλακτικών επιλογών, έστω και εν μέρει, λόγω του περιορισμένου αριθμού τρίτων παρόχων υπηρεσιών ΤΠΕ που δραστηριοποιούνται σε συγκεκριμένη αγορά, ή του μεριδίου αγοράς του σχετικού τρίτου παρόχου υπηρεσιών ΤΠΕ ή της τεχνικής πολυπλοκότητας ή του εξειδικευμένου χαρακτήρα που απαιτείται, μεταξύ άλλων σε σχέση με τυχόν αποκλειστική τεχνολογία, ή των συγκεκριμένων χαρακτηριστικών της οργάνωσης ή της δραστηριότητας του τρίτου παρόχου υπηρεσιών ΤΠΕ,

ii) δυσκολίες σε σχέση με τη μερική ή συνολική μεταφορά των σχετικών δεδομένων και του φόρτου εργασίας από τον οικείο τρίτο πάροχο υπηρεσιών ΤΠΕ σε άλλον τρίτο πάροχο υπηρεσιών ΤΠΕ, είτε λόγω του σημαντικού οικονομικού κόστους, του χρόνου ή άλλου πόρου που μπορεί να συνεπάγεται η διαδικασία μεταφοράς είτε λόγω αυξημένων κινδύνων ΤΠΕ ή άλλων λειτουργικών κινδύνων στους οποίους ενδέχεται να εκτεθεί η χρηματοοικονομική οντότητα λόγω της μεταφοράς αυτής.

3. Όταν ο τρίτος πάροχος υπηρεσιών ΤΠΕ ανήκει σε όμιλο, τα κριτήρια που αναφέρονται στην παράγραφο 2 λαμβάνονται υπόψη σε σχέση με τις υπηρεσίες ΤΠΕ που παρέχονται από τον όμιλο στο σύνολό του.

4. Οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ που αποτελούν μέρος ομίλου ορίζουν ένα νομικό πρόσωπο ως σημείο συντονισμού για τη διασφάλιση επαρκούς εκπροσώπησης και επικοινωνίας με τον κύριο εποπτικό φορέα.

5. Ο κύριος εποπτικός φορέας κοινοποιεί στον τρίτο πάροχο υπηρεσιών ΤΠΕ το αποτέλεσμα της αξιολόγησης που οδηγεί στον ορισμό που αναφέρεται στην παράγραφο 1 στοιχείο α). Εντός 6 εβδομάδων από την ημερομηνία της κοινοποίησης, ο τρίτος πάροχος υπηρεσιών ΤΠΕ μπορεί να υποβάλει στον κύριο εποπτικό φορέα αιτιολογημένη δήλωση με κάθε σχετική πληροφορία για τους σκοπούς της αξιολόγησης. Ο κύριος εποπτικός φορέας εξετάζει την αιτιολογημένη δήλωση και μπορεί να ζητήσει την υποβολή πρόσθετων πληροφοριών εντός 30 ημερολογιακών ημερών από την παραλαβή της εν λόγω δήλωσης.

Μετά τον ορισμό τρίτου παρόχου υπηρεσιών ΤΠΕ ως κρίσιμου, οι ΕΕΑ, μέσω της μεικτής επιτροπής, κοινοποιούν στον τρίτο πάροχο υπηρεσιών ΤΠΕ τον εν λόγω ορισμό και την ημερομηνία έναρξης από την οποία θα υπόκεινται ουσιαστικά σε δραστηριότητες εποπτείας. Η εν λόγω ημερομηνία έναρξης δεν υπερβαίνει τον ένα μήνα μετά την κοινοποίηση. Ο τρίτος πάροχος υπηρεσιών ΤΠΕ κοινοποιεί στις χρηματοοικονομικές οντότητες στις οποίες παρέχει υπηρεσίες τον χαρακτηρισμό τους ως κρίσιμων.

6. Ανατίθεται στην Επιτροπή η εξουσία να εκδώσει κατ' εξουσιοδότηση πράξη, σύμφωνα με το άρθρο 57, για τη συμπλήρωση του παρόντος κανονισμού, προσδιορίζοντας περαιτέρω τα κριτήρια που προβλέπονται στην παράγραφο 2 του παρόντος άρθρου έως τις 17 Ιουλίου 2024.

7. Ο ορισμός που αναφέρεται στην παράγραφο 1 στοιχείο α) δεν χρησιμοποιείται έως ότου η Επιτροπή εκδώσει κατ' εξουσιοδότηση πράξη σύμφωνα με την παράγραφο 6.

8. Ο ορισμός που αναφέρεται στην παράγραφο 1 στοιχείο α) δεν εφαρμόζεται στα ακόλουθα:

i) χρηματοοικονομικές οντότητες που παρέχουν υπηρεσίες ΤΠΕ σε άλλες χρηματοοικονομικές οντότητες,

ii) τρίτους παρόχους υπηρεσιών ΤΠΕ που υπόκεινται σε πλαίσια εποπτείας, τα οποία έχουν θεσπιστεί με σκοπό την υποστήριξη των καθηκόντων που αναφέρονται στο άρθρο 127 παράγραφος 2 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης,

iii) ενδοομιλικούς παρόχους υπηρεσιών ΤΠΕ,

iv) τρίτους παρόχους υπηρεσιών ΤΠΕ που παρέχουν υπηρεσίες ΤΠΕ αποκλειστικά σε ένα κράτος μέλος σε χρηματοοικονομικές οντότητες που δραστηριοποιούνται μόνο στο εν λόγω κράτος μέλος.

9. Οι ΕΕΑ, μέσω της μεικτής επιτροπής, καταρτίζουν, δημοσιεύουν και επικαιροποιούν ετησίως τον κατάλογο των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ σε επίπεδο Ένωσης.

10. Για τους σκοπούς της παραγράφου 1 στοιχείο α), οι αρμόδιες αρχές διαβιβάζουν, σε ετήσια και συγκεντρωτική βάση, τις εκθέσεις που αναφέρονται στο άρθρο 28 παράγραφος 3 τρίτο εδάφιο στο φόρουμ εποπτείας, το οποίο συγκροτείται σύμφωνα με το άρθρο 32. Το φόρουμ εποπτείας αξιολογεί τις εξαρτήσεις των τρίτων παρόχων ΤΠΕ από χρηματοοικονομικές οντότητες βάσει των πληροφοριών που λαμβάνει από τις αρμόδιες αρχές.

11. Οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ που δεν περιλαμβάνονται στον κατάλογο που αναφέρεται στην παράγραφο 9 μπορούν να ζητήσουν να οριστούν ως κρίσιμοι σύμφωνα με την παράγραφο 1 στοιχείο α).

Για τους σκοπούς του πρώτου εδαφίου, ο τρίτος πάροχος υπηρεσιών ΤΠΕ υποβάλλει αιτιολογημένη αίτηση στην ΕΑΤ, την ΕΑΚΑΑ ή την ΕΑΑΕΣ, οι οποίες αποφασίζουν, μέσω της μεικτής επιτροπής, αν ο εν λόγω τρίτος πάροχος υπηρεσιών ΤΠΕ θα οριστεί ως κρίσιμος σύμφωνα με την παράγραφο 1 στοιχείο α).

Η απόφαση που αναφέρεται στο δεύτερο εδάφιο εκδίδεται και κοινοποιείται στον τρίτο πάροχο υπηρεσιών ΤΠΕ εντός 6 μηνών από την παραλαβή της αίτησης.

12. Οι χρηματοοικονομικές οντότητες χρησιμοποιούν τις υπηρεσίες τρίτου παρόχου υπηρεσιών ΤΠΕ που είναι εγκατεστημένος σε τρίτη χώρα και έχει οριστεί ως κρίσιμος, σύμφωνα με την παράγραφο 1 στοιχείο α) μόνο εφόσον ο εν λόγω πάροχος έχει εγκαταστήσει θυγατρική στην Ένωση εντός των 12 μηνών μετά τον ορισμό.

13. Ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ που αναφέρεται στην παράγραφο 12 κοινοποιεί στον κύριο εποπτικό φορέα τυχόν αλλαγές στη δομή της διοίκησης της θυγατρικής που είναι εγκατεστημένη στην Ένωση.

Άρθρο 32

Δομή του πλαισίου εποπτείας

1. Η μεικτή επιτροπή συγκροτεί, σύμφωνα με το άρθρο 57 παράγραφος 1 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010, το φόρουμ εποπτείας ως υποεπιτροπή για τους σκοπούς της υποστήριξης των εργασιών της μεικτής επιτροπής και του κύριου εποπτικού φορέα που αναφέρεται στο άρθρο 31 παράγραφος 1 στοιχείο β) όσον αφορά τους κινδύνους τρίτων παρόχων ΤΠΕ σε όλους τους χρηματοοικονομικούς τομείς. Το φόρουμ εποπτείας καταρτίζει τα σχέδια κοινών θέσεων και τα σχέδια κοινών πράξεων της μεικτής επιτροπής στο πεδίο αυτό.

Το φόρουμ εποπτείας συζητά τακτικά τις σχετικές εξελίξεις όσον αφορά τους κινδύνους και τις ευπάθειες των ΤΠΕ και προωθεί την υιοθέτηση συνεκτικής προσέγγισης για την παρακολούθηση των κινδύνων τρίτων παρόχων ΤΠΕ στο επίπεδο της Ένωσης.

2. Το φόρουμ εποπτείας προβαίνει ετησίως σε συλλογική αξιολόγηση των αποτελεσμάτων και των ευρημάτων των εποπτικών δραστηριοτήτων που διεξάγονται για όλους τους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ και προωθεί μέτρα συντονισμού με σκοπό την αύξηση της ψηφιακής επιχειρησιακής ανθεκτικότητας των χρηματοοικονομικών οντοτήτων, την προώθηση βέλτιστων πρακτικών αντιμετώπισης του κινδύνου συγκέντρωσης ΤΠΕ και τη διερεύνηση μέσων μετριασμού σε περιπτώσεις διατομεακής μεταφοράς κινδύνων.

3. Το φόρουμ εποπτείας υποβάλλει γενικούς δείκτες αναφοράς για κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ προς έγκριση από τη μεικτή επιτροπή ως κοινές θέσεις των ΕΕΑ, σύμφωνα με το άρθρο 56 παράγραφος 1 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010.

4. Το φόρουμ εποπτείας απαρτίζεται από:

α) τους προέδρους των ΕΕΑ,

β) έναν υψηλόβαθμο εκπρόσωπο από κάθε κράτος μέλος, προερχόμενο από το εν ενεργεία προσωπικό της σχετικής αρμόδιας αρχής που αναφέρεται στο άρθρο 46,

γ) τους εκτελεστικούς διευθυντές κάθε ΕΕΑ και έναν εκπρόσωπο από την Επιτροπή, το ΕΣΣΚ, την ΕΚΤ και τον ENISA ως παρατηρητές,

δ) κατά περίπτωση, έναν επιπλέον εκπρόσωπο αρμόδιας αρχής που αναφέρεται στο άρθρο 46 από κάθε κράτος μέλος ως παρατηρητή,

ε) κατά περίπτωση, έναν εκπρόσωπο των αρμόδιων αρχών που ορίζονται ή συστήνονται σύμφωνα με την οδηγία (ΕΕ) 2022/2555 αρμόδιο για την εποπτεία βασικής ή σημαντικής οντότητας που υπόκειται στις διατάξεις της εν λόγω οδηγίας, και η οποία έχει οριστεί ως κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ, ως παρατηρητής.

Το φόρουμ εποπτείας μπορεί, κατά περίπτωση, να ζητεί τη γνώμη ανεξάρτητων εμπειρογνωμόνων που διορίζονται σύμφωνα με την παράγραφο 6.

5. Κάθε κράτος μέλος ορίζει τη σχετική αρμόδια αρχή της οποίας το μέλος του προσωπικού είναι ο υψηλόβαθμος εκπρόσωπος που αναφέρεται στην παράγραφο 4 πρώτο εδάφιο στοιχείο β), και ενημερώνει σχετικά τον κύριο εποπτικό φορέα.

Οι ΕΕΑ δημοσιεύουν στον ιστότοπό τους τον κατάλογο των υψηλόβαθμων εκπροσώπων προερχόμενων από το εν ενεργεία προσωπικό της σχετικής αρμόδιας αρχής που ορίζονται από τα κράτη μέλη.

6. Το φόρουμ εποπτείας ορίζει τους αναφερόμενους στην παράγραφο 4 δεύτερο εδάφιο ανεξάρτητους εμπειρογνώμονες από ομάδα εμπειρογνωμόνων που επιλέγονται με δημόσια και διαφανή διαδικασία υποβολής αιτήσεων.

Οι ανεξάρτητοι εμπειρογνώμονες διορίζονται με βάση την εμπειρογνωσία τους σε θέματα χρηματοοικονομικής σταθερότητας, ψηφιακής επιχειρησιακής ανθεκτικότητας και ασφάλειας. Ενεργούν ανεξάρτητα και αντικειμενικά αποκλειστικά προς το συμφέρον της Ένωσης συνολικά και ούτε ζητούν ούτε δέχονται οδηγίες από θεσμικά όργανα ή οργανισμούς της Ένωσης, από οποιαδήποτε κυβέρνηση κράτους μέλους ή από οποιονδήποτε άλλον δημόσιο ή ιδιωτικό φορέα.

7. Σύμφωνα με το άρθρο 16 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010, οι ΕΕΑ έως τις 17 Ιουλίου 2024 εκδίδουν, για τους σκοπούς του παρόντος τμήματος, κατευθυντήριες γραμμές σχετικά με τη συνεργασία μεταξύ των ΕΕΑ και των αρμόδιων αρχών οι οποίες καλύπτουν τις λεπτομερείς διαδικασίες και προϋποθέσεις για την κατανομή και την εκτέλεση των καθηκόντων μεταξύ των αρμόδιων αρχών και των ΕΕΑ, καθώς και τις λεπτομέρειες σχετικά με την ανταλλαγή των πληροφοριών οι οποίες είναι απαραίτητες για τις αρμόδιες αρχές, προκειμένου να διασφαλιστεί ότι δίνεται συνέχεια στις συστάσεις που απευθύνονται σύμφωνα με το άρθρο 35 παράγραφος 1 στοιχείο δ) σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ.

8. Οι απαιτήσεις που ορίζονται στο παρόν τμήμα δεν θίγουν την εφαρμογή της οδηγίας (ΕΕ) 2022/2555 και άλλων κανόνων της Ένωσης για την εποπτεία που εφαρμόζεται σε παρόχους υπηρεσιών υπολογιστικού νέφους.

9. Οι ΕΕΑ, μέσω της μεικτής επιτροπής και βάσει των προπαρασκευαστικών εργασιών που διεξάγονται από το φόρουμ εποπτείας, υποβάλλουν ετησίως στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο και την Επιτροπή έκθεση σχετικά με την εφαρμογή του παρόντος τμήματος.

Άρθρο 33

Καθήκοντα του κύριου εποπτικού φορέα

1. Ο κύριος εποπτικός φορέας, ο οποίος διορίζεται σύμφωνα με το άρθρο 31 παράγραφος 1 στοιχείο β), ασκεί την εποπτεία των τρίτων παρόχων υπηρεσιών ΤΠΕ που του έχουν ανατεθεί, και είναι, για τους σκοπούς όλων των θεμάτων που σχετίζονται με την εποπτεία, το κύριο σημείο επαφής για τους εν λόγω κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ.

2. Για τους σκοπούς της παραγράφου 1, ο κύριος εποπτικός φορέας αξιολογεί αν κάθε κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ διαθέτει εμπεριστατωμένους, ορθούς και αποτελεσματικούς κανόνες, διαδικασίες, μηχανισμούς και ρυθμίσεις για τη διαχείριση του κινδύνου ΤΠΕ στον οποίο ενδέχεται να εκθέτει τις χρηματοοικονομικές οντότητες.

Η αξιολόγηση που αναφέρεται στο πρώτο εδάφιο επικεντρώνεται κυρίως στις υπηρεσίες ΤΠΕ που παρέχονται από τον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ και υποστηρίζουν τις κρίσιμες ή σημαντικές λειτουργίες των χρηματοοικονομικών οντοτήτων. Όταν είναι αναγκαίο για την αντιμετώπιση όλων των σχετικών κινδύνων, η εν λόγω αξιολόγηση επεκτείνεται σε υπηρεσίες ΤΠΕ που υποστηρίζουν λειτουργίες πέραν των κρίσιμων ή σημαντικών.

3. Η αξιολόγηση που αναφέρεται στην παράγραφο 2 καλύπτει:

α) απαιτήσεις ΤΠΕ για τη διασφάλιση, ιδίως, της ασφάλειας, της διαθεσιμότητας, της συνέχειας, της επεκτασιμότητας και της ποιότητας των υπηρεσιών που παρέχει ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ σε χρηματοοικονομικές οντότητες, καθώς και την ικανότητα να διατηρεί ανά πάσα στιγμή υψηλά πρότυπα διαθεσιμότητας, γνησιότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων,

β) την υλική ασφάλεια που συμβάλλει στη διασφάλιση της ασφάλειας των ΤΠΕ, συμπεριλαμβανομένης της ασφάλειας των χώρων, των εγκαταστάσεων, των κέντρων δεδομένων,

γ) τις διαδικασίες διαχείρισης κινδύνων, συμπεριλαμβανομένων των πολιτικών για τη διαχείριση κινδύνων ΤΠΕ και της πολιτικής επιχειρησιακής συνέχειας των ΤΠΕ και των σχεδίων αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ,

δ) τις ρυθμίσεις διακυβέρνησης, συμπεριλαμβανομένης της οργανωτικής δομής με σαφείς, διαφανείς και συνεκτικούς κανόνες για τα όρια αρμοδιότητας και λογοδοσίας που καθιστούν δυνατή την αποτελεσματική διαχείριση κινδύνων ΤΠΕ,

ε) τον προσδιορισμό, την παρακολούθηση και την έγκαιρη αναφορά σημαντικών συμβάντων που σχετίζονται με τις ΤΠΕ στις χρηματοοικονομικές οντότητες, τη διαχείριση και την επίλυση των συμβάντων αυτών, ιδίως κυβερνοεπιθέσεων,

στ) τους μηχανισμούς φορητότητας δεδομένων, φορητότητας εφαρμογών και διαλειτουργικότητας, οι οποίοι διασφαλίζουν την αποτελεσματική άσκηση δικαιωμάτων καταγγελίας από τις χρηματοοικονομικές οντότητες,

ζ) τη δοκιμή συστημάτων, υποδομών και δικλείδων ασφάλειας ΤΠΕ,

η) τους ελέγχους ΤΠΕ,

θ) τη χρήση σχετικών εθνικών και διεθνών προτύπων που ισχύουν για την παροχή των υπηρεσιών ΤΠΕ στις χρηματοοικονομικές οντότητες.

4. Με βάση την αξιολόγηση που αναφέρεται στην παράγραφο 2 και σε συντονισμό με το δίκτυο κοινής εποπτείας (ΔΚΕ) που αναφέρεται στο άρθρο 34 παράγραφος 1, ο κύριος εποπτικός φορέας εγκρίνει σαφές, λεπτομερές και τεκμηριωμένο εξατομικευμένο σχέδιο εποπτείας στο οποίο περιγράφονται οι ετήσιοι στόχοι εποπτείας και οι κύριες δράσεις εποπτείας που σχεδιάζονται για κάθε κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ. Το σχέδιο αυτό κοινοποιείται ετησίως στον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ.

Πριν από την έγκριση του σχεδίου εποπτείας, ο κύριος εποπτικός φορέας κοινοποιεί το προσχέδιο εποπτείας στον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ.

Μετά την παραλαβή του προσχεδίου εποπτείας, ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ μπορεί να υποβάλει αιτιολογημένη δήλωση εντός 15 ημερολογιακών ημερών, αποδεικνύοντας τον αναμενόμενο αντίκτυπο στους πελάτες που είναι οντότητες οι οποίες δεν εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού και, κατά περίπτωση, διατυπώνοντας λύσεις για τον μετριασμό των κινδύνων.

5. Μόλις εγκριθούν τα ετήσια σχέδια εποπτείας που αναφέρονται στην παράγραφο 4 και κοινοποιηθούν στους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, οι αρμόδιες αρχές δύνανται να λάβουν μέτρα για τους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ μόνο κατόπιν συμφωνίας με τον κύριο εποπτικό φορέα.

Άρθρο 34

Επιχειρησιακός συντονισμός μεταξύ κύριων εποπτικών φορέων

1. Για να εξασφαλιστεί συνεπής προσέγγιση των δραστηριοτήτων εποπτείας και με σκοπό να καταστούν δυνατές συντονισμένες στρατηγικές γενικής εποπτείας και συνεκτικές επιχειρησιακές προσεγγίσεις και μεθοδολογίες εργασίας, οι τρεις κύριοι εποπτικοί φορείς, οι οποίοι διορίζονται σύμφωνα με το άρθρο 31 παράγραφος 1 στοιχείο β), συγκροτούν ΔΚΕ, ώστε να συντονίζονται μεταξύ τους κατά τα προπαρασκευαστικά στάδια και να συντονίζουν τη διεξαγωγή των δραστηριοτήτων εποπτείας επί των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ τους οποίους επιβλέπουν αντίστοιχα, καθώς και σχετικά με κάθε τρόπο δράσης που ενδέχεται να απαιτείται σύμφωνα με το άρθρο 42.

2. Για τους σκοπούς της παραγράφου 1, οι κύριοι εποπτικοί φορείς καταρτίζουν κοινό πρωτόκολλο εποπτείας στο οποίο καθορίζονται οι λεπτομερείς διαδικασίες που πρέπει να ακολουθούνται για τη διεξαγωγή του καθημερινού συντονισμού και για τη διασφάλιση ταχειών ανταλλαγών και αντιδράσεων. Το πρωτόκολλο αναθεωρείται περιοδικά ώστε να αντικατοπτρίζει τις επιχειρησιακές ανάγκες, ιδίως την εξέλιξη των πρακτικών ρυθμίσεων εποπτείας.

3. Οι κύριοι εποπτικοί φορείς μπορούν, σε ad hoc βάση, να καλούν την ΕΚΤ και τον ENISA να παρέχουν τεχνικές συμβουλές, να ανταλλάσσουν πρακτικές εμπειρίες ή να συμμετέχουν σε ειδικές συντονιστικές συνεδριάσεις του ΔΚΕ.

Άρθρο 35

Εξουσίες του κύριου εποπτικού φορέα

1. Για τους σκοπούς της εκτέλεσης των καθηκόντων που προβλέπονται στο παρόν τμήμα, ο κύριος εποπτικός φορέας διαθέτει τις ακόλουθες εξουσίες όσον αφορά τους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ:

α) να ζητεί όλες τις σχετικές πληροφορίες και τα έγγραφα τεκμηρίωσης σύμφωνα με το άρθρο 37,

β) να διενεργεί γενικές έρευνες και επιθεωρήσεις σύμφωνα με τα άρθρα 38 και 39, αντίστοιχα,

γ) να ζητεί την υποβολή εκθέσεων μετά την ολοκλήρωση των εποπτικών δραστηριοτήτων, στις οποίες προσδιορίζονται οι ενέργειες που υλοποίησαν ή τα διορθωτικά μέτρα που έλαβαν οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ όσον αφορά τις συστάσεις που αναφέρονται στο στοιχείο δ) της παρούσας παραγράφου,

δ) να διατυπώνει συστάσεις για τους τομείς που αναφέρονται στο άρθρο 33 παράγραφος 3, ιδίως όσον αφορά τα ακόλουθα:

i) τη χρήση συγκεκριμένων απαιτήσεων ή διαδικασιών ασφάλειας και ποιότητας ΤΠΕ, ιδίως όσον αφορά τη σταδιακή υλοποίηση ενημερώσεων κώδικα, επικαιροποιήσεων, κρυπτογράφησης και άλλων μέτρων ασφάλειας τα οποία ο κύριος εποπτικός φορέας θεωρεί συναφή για τη διασφάλιση της ασφάλειας των υπηρεσιών ΤΠΕ που παρέχονται στις χρηματοοικονομικές οντότητες,

ii) τη χρήση όρων και προϋποθέσεων, συμπεριλαμβανομένης της τεχνικής εφαρμογής τους, σύμφωνα με τις οποίες οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ παρέχουν υπηρεσίες ΤΠΕ σε χρηματοοικονομικές οντότητες, τις οποίες ο κύριος εποπτικός φορέας θεωρεί συναφείς για την αποτροπή της δημιουργίας μοναδικών σημείων αποτυχίας, ή την ενίσχυσή τους, ή για την ελαχιστοποίηση των πιθανών συστημικών επιπτώσεων στον χρηματοοικονομικό τομέα της Ένωσης σε περίπτωση κινδύνου συγκέντρωσης ΤΠΕ,

iii) κάθε προγραμματισμένη υπεργολαβία, όταν ο κύριος εποπτικός φορέας θεωρεί ότι η περαιτέρω υπεργολαβία, συμπεριλαμβανομένων των ρυθμίσεων υπεργολαβικής ανάθεσης τις οποίες οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ προγραμματίζουν να συνάψουν με άλλους τρίτους παρόχους υπηρεσιών ΤΠΕ ή με υπεργολάβους ΤΠΕ εγκατεστημένους σε τρίτη χώρα, ενδέχεται να ενεργοποιήσει κινδύνους όσον αφορά την παροχή υπηρεσιών από τη χρηματοοικονομική οντότητα ή κινδύνους για τη χρηματοοικονομική σταθερότητα, βάσει της εξέτασης των πληροφοριών που συλλέγονται σύμφωνα με τα άρθρα 37 και 38,

iv) την αποτροπή σύναψης περαιτέρω ρύθμισης υπεργολαβίας, εφόσον πληρούνται οι ακόλουθες σωρευτικές προϋποθέσεις:

— ο προβλεπόμενος υπεργολάβος είναι τρίτος πάροχος υπηρεσιών ΤΠΕ ή υπεργολάβος ΤΠΕ εγκατεστημένος σε τρίτη χώρα,

— η υπεργολαβία αφορά κρίσιμη ή σημαντική λειτουργία της χρηματοοικονομικής οντότητας και

— ο κύριος εποπτικός φορέας θεωρεί ότι η χρήση της εν λόγω υπεργολαβίας ενέχει σαφή και σοβαρό κίνδυνο για τη χρηματοοικονομική σταθερότητα της Ένωσης ή για τις χρηματοοικονομικές οντότητες, συμπεριλαμβανομένης της ικανότητας των χρηματοοικονομικών οντοτήτων να συμμορφώνονται με τις εποπτικές απαιτήσεις.

Για τους σκοπούς του σημείου iv) του παρόντος στοιχείου, οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ, χρησιμοποιώντας το υπόδειγμα που προβλέπεται στο άρθρο 41 παράγραφος 1 στοιχείο β), διαβιβάζουν τις πληροφορίες σχετικά με την υπεργολαβία στον κύριο εποπτικό φορέα.

2. Κατά την άσκηση των εξουσιών που αναφέρονται στο παρόν άρθρο, ο κύριος εποπτικός φορέας:

α) διασφαλίζει τον τακτικό συντονισμό εντός του ΔΚΕ και, ειδικότερα, επιδιώκει συνεκτικές προσεγγίσεις, κατά περίπτωση, όσον αφορά την εποπτεία κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ,

β) λαμβάνει δεόντως υπόψη το πλαίσιο που θεσπίζεται με την οδηγία (ΕΕ) 2022/2555 και, όπου κρίνεται αναγκαίο, διαβουλεύεται με τις σχετικές αρμόδιες αρχές που ορίζονται ή συστήνονται σύμφωνα με την εν λόγω οδηγία, προκειμένου να αποφευχθεί η επικάλυψη τεχνικών και οργανωτικών μέτρων που ενδέχεται να εφαρμόζονται σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ σύμφωνα με την εν λόγω οδηγία,

γ) επιδιώκει να ελαχιστοποιήσει, στο μέτρο του δυνατού, τον κίνδυνο διαταραχής των υπηρεσιών που παρέχονται από κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ σε πελάτες που είναι οντότητες οι οποίες δεν εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού.

3. Ο κύριος εποπτικός φορέας ζητεί τη γνώμη του φόρουμ εποπτείας πριν από την άσκηση των εξουσιών που αναφέρονται στην παράγραφο 1.

Πριν από τη διατύπωση συστάσεων σύμφωνα με την παράγραφο 1 στοιχείο δ), ο κύριος εποπτικός φορέας δίνει στον τρίτο πάροχο υπηρεσιών ΤΠΕ την ευκαιρία να παράσχει, εντός 30 ημερολογιακών ημερών, σχετικές πληροφορίες που αποδεικνύουν τον αναμενόμενο αντίκτυπο στους πελάτες που είναι οντότητες οι οποίες δεν εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού, διατυπώνοντας, κατά περίπτωση, λύσεις για τον μετριασμό των κινδύνων.

4. Ο κύριος εποπτικός φορέας ενημερώνει το ΔΚΕ για το αποτέλεσμα της άσκησης των εξουσιών που αναφέρονται στην παράγραφο 1 στοιχεία α) και β). Ο κύριος εποπτικός φορέας διαβιβάζει, χωρίς αδικαιολόγητη καθυστέρηση, τις εκθέσεις που αναφέρονται στην παράγραφο 1 στοιχείο γ), στο ΔΚΕ και στις αρμόδιες αρχές των χρηματοοικονομικών οντοτήτων που χρησιμοποιούν τις υπηρεσίες ΤΠΕ του εν λόγω κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ.

5. Οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ συνεργάζονται καλόπιστα με τον κύριο εποπτικό φορέα και του παρέχουν τη συνδρομή τους κατά την εκπλήρωση των καθηκόντων του.

6. Σε περίπτωση ολικής ή μερικής μη συμμόρφωσης με τα μέτρα που απαιτείται να ληφθούν σύμφωνα με την εκτέλεση των εξουσιών δυνάμει της παραγράφου 1 στοιχεία α), β) και γ), και μετά την εκπνοή περιόδου τουλάχιστον 30 ημερολογιακών ημερών από την ημερομηνία κατά την οποία ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ έλαβε κοινοποίηση των αντίστοιχων μέτρων, ο κύριος εποπτικός φορέας εκδίδει απόφαση με την οποία επιβάλλει περιοδική χρηματική ποινή για να υποχρεώσει τον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ να συμμορφωθεί με τα εν λόγω μέτρα.

7. Η περιοδική χρηματική ποινή που αναφέρεται στην παράγραφο 6 επιβάλλεται σε ημερήσια βάση έως ότου επιτευχθεί συμμόρφωση και για μέγιστο διάστημα έξι μηνών από την κοινοποίηση της απόφασης επιβολής περιοδικής χρηματικής ποινής στον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ.

8. Το ύψος της περιοδικής χρηματικής ποινής, το οποίο υπολογίζεται από την ημερομηνία που ορίζεται στην απόφαση επιβολής της περιοδικής χρηματικής ποινής, ανέρχεται έως το 1 % του μέσου ημερήσιου κύκλου εργασιών που πραγματοποίησε παγκοσμίως ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ κατά την προηγούμενη χρήση. Κατά τον καθορισμό του ποσού της χρηματικής ποινής, ο κύριος εποπτικός φορέας λαμβάνει υπόψη τα ακόλουθα κριτήρια όσον αφορά τη μη συμμόρφωση με τα μέτρα που αναφέρονται στην παράγραφο 6:

α) τη βαρύτητα και τη διάρκεια της μη συμμόρφωσης,

β) αν η μη συμμόρφωση τελέστηκε εκ προθέσεως ή εξ αμελείας,

γ) το επίπεδο συνεργασίας του τρίτου παρόχου υπηρεσιών ΤΠΕ με τον κύριο εποπτικό φορέα.

Για τους σκοπούς του πρώτου εδαφίου, προκειμένου να διασφαλιστεί συνεκτική προσέγγιση, ο κύριος εποπτικός φορέας προβαίνει σε διαβούλευση στο πλαίσιο του ΔΚΕ.

9. Οι χρηματικές ποινές έχουν διοικητικό χαρακτήρα και είναι εκτελεστές. Η εκτέλεση διέπεται από τους κανόνες της πολιτικής δικονομίας που ισχύουν στο κράτος μέλος στο οποίο πραγματοποιούνται οι επιθεωρήσεις και η πρόσβαση. Τα δικαστήρια του οικείου κράτους μέλους είναι αρμόδια για καταγγελίες που αφορούν την παράτυπη διενέργεια της εκτέλεσης. Τα ποσά των χρηματικών ποινών διοχετεύονται στον γενικό προϋπολογισμό της Ευρωπαϊκής Ένωσης.

10. Ο κύριος εποπτικός φορέας δημοσιοποιεί κάθε περιοδική χρηματική ποινή που έχει επιβληθεί, εκτός εάν η εν λόγω δημοσιοποίηση θέτει σε σοβαρό κίνδυνο τις χρηματοοικονομικές αγορές ή προκαλεί δυσανάλογη ζημία στα εμπλεκόμενα μέρη.

11. Πριν από την επιβολή περιοδικής χρηματικής ποινής σύμφωνα με την παράγραφο 6, ο κύριος εποπτικός φορέας παρέχει στους εκπροσώπους του κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ που υπόκειται στην πειθαρχική διαδικασία, τη δυνατότητα να εκθέσουν την άποψή τους σχετικά με τα ευρήματα και στηρίζει τις αποφάσεις του μόνο σε ευρήματα για τα οποία είχε την ευκαιρία να διατυπώσει παρατηρήσεις ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ που υπόκειται στην πειθαρχική διαδικασία.

Κατά τη διεξαγωγή της διαδικασίας διασφαλίζονται πλήρως τα δικαιώματα υπεράσπισης των προσώπων που υπόκεινται σε πειθαρχικές διαδικασίες. Ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ που υπόκειται στην εν λόγω διαδικασία έχει δικαίωμα πρόσβασης στον φάκελο, με την επιφύλαξη του έννομου συμφέροντος άλλων προσώπων για την προστασία του επιχειρηματικού απορρήτου τους. Το δικαίωμα πρόσβασης στον φάκελο δεν καλύπτει τις εμπιστευτικές πληροφορίες ή τα προπαρασκευαστικά έγγραφα εσωτερικής χρήσης του κύριου εποπτικού φορέα.

Άρθρο 36

Άσκηση των εξουσιών του κύριου εποπτικού φορέα εκτός της Ένωσης

1. Όταν οι στόχοι εποπτείας δεν μπορούν να επιτευχθούν μέσω αλληλεπίδρασης με τη θυγατρική που έχει συσταθεί για τους σκοπούς του άρθρου 31 παράγραφος 12 ή μέσω άσκησης δραστηριοτήτων εποπτείας σε εγκαταστάσεις που βρίσκονται στην Ένωση, ο κύριος εποπτικός φορέας μπορεί να ασκεί τις εξουσίες που αναφέρονται στις ακόλουθες διατάξεις σε κάθε χώρο που βρίσκεται σε τρίτη χώρα και ανήκει ή χρησιμοποιείται με οποιονδήποτε τρόπο, με σκοπό την παροχή υπηρεσιών σε χρηματοοικονομικές οντότητες της Ένωσης, από κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ, σε σχέση με τις οικείες επιχειρηματικές δραστηριότητες, τις λειτουργίες ή τις υπηρεσίες, μεταξύ άλλων, τυχόν διοικητικές, τις επιχειρήσεις ή τα επιχειρησιακά γραφεία, τις εγκαταστάσεις, τις εκτάσεις, τα κτίρια ή άλλα ακίνητα:

α) στο άρθρο 35 παράγραφος 1 στοιχείο α) και

β) στο άρθρο 35 παράγραφος 1 στοιχείο β), σύμφωνα με το άρθρο 38 παράγραφος 2 στοιχεία α), β) και δ), και στο άρθρο 39 παράγραφος 1 και στο άρθρο 39 παράγραφος 2 στοιχείο α).

Οι εξουσίες που αναφέρονται στο πρώτο εδάφιο μπορούν να ασκούνται υπό όλες τις ακόλουθες προϋποθέσεις:

i) η διενέργεια επιθεώρησης σε τρίτη χώρα κρίνεται αναγκαία από τον κύριο εποπτικό φορέα, ώστε να είναι σε θέση να εκτελεί πλήρως και αποτελεσματικά τα καθήκοντά του δυνάμει του παρόντος κανονισμού,

ii) η επιθεώρηση σε τρίτη χώρα σχετίζεται άμεσα με την παροχή υπηρεσιών ΤΠΕ σε χρηματοοικονομικές οντότητες στην Ένωση,

iii) ο εν λόγω κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ συναινεί στη διενέργεια επιθεώρησης σε τρίτη χώρα και

iv) η αρμόδια αρχή της οικείας τρίτης χώρας έχει ενημερωθεί επίσημα από τον κύριο εποπτικό φορέα και δεν εγείρει αντιρρήσεις.

2. Με την επιφύλαξη των αντίστοιχων αρμοδιοτήτων των θεσμικών οργάνων της Ένωσης και των κρατών μελών, για τους σκοπούς της παραγράφου 1, η ΕΑΤ, η ΕΑΚΑΑ ή η ΕΑΑΕΣ, συνάπτουν συμφωνίες διοικητικής συνεργασίας με την αρμόδια αρχή της τρίτης χώρας, προκειμένου να καταστεί δυνατή η ομαλή διεξαγωγή των επιθεωρήσεων στη συγκεκριμένη τρίτη χώρα από τον κύριο εποπτικό φορέα και την ομάδα του που έχει οριστεί για την αποστολή στην εν λόγω τρίτη χώρα. Οι εν λόγω ρυθμίσεις συνεργασίας δεν δημιουργούν νομικές υποχρεώσεις έναντι της Ένωσης και των κρατών μελών της ούτε εμποδίζουν τα κράτη μέλη και τις αρμόδιες αρχές τους να συνάπτουν διμερείς ή πολυμερείς ρυθμίσεις με τις εν λόγω τρίτες χώρες και τις οικείες αρχές τους.

Οι εν λόγω ρυθμίσεις συνεργασίας προσδιορίζουν τουλάχιστον τα ακόλουθα στοιχεία:

α) τις διαδικασίες για τον συντονισμό των δραστηριοτήτων εποπτείας που διεξάγονται δυνάμει του παρόντος κανονισμού και κάθε ανάλογη παρακολούθηση των κινδύνων τρίτων μερών ΤΠΕ στον χρηματοοικονομικό τομέα που ασκείται από τη σχετική αρχή της οικείας τρίτης χώρας, συμπεριλαμβανομένων λεπτομερειών για τη διαβίβαση της συμφωνίας της τρίτης χώρας, ώστε να καταστεί δυνατή η διεξαγωγή, από τον κύριο εποπτικό φορέα και την ορισθείσα ομάδα του, γενικών ερευνών και επιτόπιων επιθεωρήσεων, όπως αναφέρεται στην παράγραφο 1 πρώτο εδάφιο, στην επικράτεια υπό τη δικαιοδοσία της,

β) τον μηχανισμό για τη διαβίβαση κάθε σχετικής πληροφορίας μεταξύ της ΕΑΤ, της ΕΑΚΑΑ ή της ΕΑΑΕΣ και της σχετικής αρχής της συγκεκριμένης τρίτης χώρας, ιδίως σε σχέση με τις πληροφορίες που μπορεί να ζητήσει ο κύριος εποπτικός φορέας σύμφωνα με το άρθρο 37,

γ) τους μηχανισμούς για την άμεση κοινοποίηση από την αρμόδια αρχή της οικείας τρίτης χώρας στην ΕΑΤ, την ΕΑΚΑΑ ή την ΕΑΑΕΣ των περιπτώσεων κατά τις οποίες ένας τρίτος πάροχος υπηρεσιών ΤΠΕ που είναι εγκατεστημένος σε τρίτη χώρα και έχει οριστεί ως κρίσιμος σύμφωνα με το άρθρο 31 παράγραφος 1 στοιχείο α), θεωρείται ότι έχει παραβιάσει τις απαιτήσεις τις οποίες υποχρεούται να τηρεί σύμφωνα με το εφαρμοστέο δίκαιο της συγκεκριμένης τρίτης χώρας κατά την παροχή υπηρεσιών σε χρηματοοικονομικά ιδρύματα στην εν λόγω τρίτη χώρα, καθώς και τα διορθωτικά μέτρα και τις κυρώσεις που επιβλήθηκαν,

δ) την τακτική διαβίβαση επικαιροποιήσεων σχετικά με τις ρυθμιστικές ή εποπτικές εξελίξεις όσον αφορά την παρακολούθηση των κινδύνων τρίτων μερών ΤΠΕ για χρηματοοικονομικά ιδρύματα στη συγκεκριμένη τρίτη χώρα,

ε) τις λεπτομέρειες που επιτρέπουν, εφόσον απαιτείται, τη συμμετοχή ενός εκπροσώπου της αρμόδιας αρχής της τρίτης χώρας στις επιθεωρήσεις που διενεργούνται από τον κύριο εποπτικό φορέα και την ορισθείσα ομάδα.

3. Όταν ο κύριος εποπτικός φορέας δεν είναι σε θέση να διεξάγει εποπτικές δραστηριότητες, που αναφέρονται στις παραγράφους 1 και 2, ο κύριος εποπτικός φορέας:

α) ασκεί τις εξουσίες της δυνάμει του άρθρου 35 με βάση όλα τα πραγματικά περιστατικά και τα έγγραφα που έχει στη διάθεσή του,

β) τεκμηριώνει και εξηγεί κάθε συνέπεια της αδυναμίας του να διεξαγάγει τις προβλεπόμενες δραστηριότητες εποπτείας που αναφέρονται στο παρόν άρθρο.

Οι πιθανές συνέπειες που αναφέρονται στο στοιχείο β) του παρόντος εδαφίου λαμβάνονται υπόψη στις συστάσεις του κύριου εποπτικού φορέα που εκδίδονται σύμφωνα με το άρθρο 35 παράγραφος 1 στοιχείο δ).

Άρθρο 37

Αίτηση παροχής πληροφοριών

1. Ο κύριος εποπτικός φορέας δύναται να ζητήσει από τον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ, με απλό αίτημα ή με απόφαση, να παράσχει όλες τις απαραίτητες πληροφορίες ώστε ο κύριος εποπτικός φορέας να είναι σε θέση να εκτελέσει τα καθήκοντά του σύμφωνα με τον παρόντα κανονισμό, συμπεριλαμβανομένων όλων των σχετικών επιχειρηματικών ή επιχειρησιακών εγγράφων, των συμβολαίων, των εγγράφων τεκμηρίωσης πολιτικών, των εκθέσεων ελέγχου της ασφάλειας ΤΠΕ, των αναφορών συμβάντων που σχετίζονται με τις ΤΠΕ, καθώς και κάθε πληροφορία σε σχέση με συμβαλλόμενα μέρη στα οποία ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ έχει αναθέσει εξωτερικά επιχειρησιακές λειτουργίες ή δραστηριότητες.

2. Κατά τη διαβίβαση απλού αιτήματος παροχής πληροφοριών δυνάμει της παραγράφου 1, ο κύριος εποπτικός φορέας:

α) παραπέμπει στο παρόν άρθρο ως νομική βάση του αιτήματος,

β) αναφέρει τον σκοπό του αιτήματος,

γ) προσδιορίζει τις πληροφορίες που ζητούνται,

δ) τάσσει προθεσμία εντός της οποίας πρέπει να παρασχεθούν οι πληροφορίες,

ε) ενημερώνει τον εκπρόσωπο του κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ από τον οποίο ζητούνται οι πληροφορίες ότι δεν υφίσταται υποχρέωση παροχής πληροφοριών, αλλά ότι στην περίπτωση εκούσιας απάντησης στο αίτημα οι παρεχόμενες πληροφορίες δεν πρέπει να είναι ανακριβείς ή παραπλανητικές.

3. Κατά την υποβολή, κατόπιν αποφάσεως, αιτήματος παροχής πληροφοριών σύμφωνα με την παράγραφο 1, ο κύριος εποπτικός φορέας:

α) παραπέμπει στο παρόν άρθρο ως νομική βάση του αιτήματος,

β) αναφέρει τον σκοπό του αιτήματος,

γ) προσδιορίζει τις πληροφορίες που ζητούνται,

δ) τάσσει προθεσμία εντός της οποίας πρέπει να παρασχεθούν οι πληροφορίες,

ε) επισημαίνει τις περιοδικές χρηματικές ποινές που προβλέπονται στο άρθρο 35 παράγραφος 6 στην περίπτωση ελλιπούς παροχής των απαιτούμενων πληροφοριών ή όταν οι πληροφορίες αυτές δεν παρέχονται εντός της προθεσμίας που αναφέρεται στο στοιχείο δ) του παρόντος εδαφίου,

στ) επισημαίνει το δικαίωμα άσκησης προσφυγής κατά της απόφασης στο συμβούλιο προσφυγών των ΕΕΑ και του δικαιώματος υποβολής αίτησης επανεξέτασης της απόφασης από το Δικαστήριο της Ευρωπαϊκής Ένωσης (Δικαστήριο) σύμφωνα με τα άρθρα 60 και 61 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010.

4. Οι εκπρόσωποι των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ παρέχουν τις ζητούμενες πληροφορίες. Οι πληροφορίες μπορούν να παρέχονται από δεόντως εξουσιοδοτημένους δικηγόρους εξ ονόματος των πελατών τους. Ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ εξακολουθεί να ευθύνεται πλήρως για την παροχή ελλιπών, ανακριβών ή παραπλανητικών πληροφοριών.

5. Ο κύριος εποπτικός φορέας διαβιβάζει αμελλητί αντίγραφο της απόφασης για την παροχή πληροφοριών στις αρμόδιες αρχές των χρηματοοικονομικών οντοτήτων που χρησιμοποιούν τις υπηρεσίες των σχετικών κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ και στο ΔΚΕ.

Άρθρο 38

Γενικές έρευνες

1. Για την εκτέλεση των καθηκόντων του σύμφωνα με τον παρόντα κανονισμό, ο κύριος εποπτικός φορέας, επικουρούμενος από την κοινή εξεταστική ομάδα που αναφέρεται στο άρθρο 40 παράγραφος 1, μπορεί, εφόσον απαιτείται, να διεξαγάγει τις απαραίτητες έρευνες σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ:

2. Ο κύριος εποπτικός φορέας έχει την εξουσία:

α) να εξετάζει αρχεία, δεδομένα, διαδικασίες και κάθε άλλο συναφές υλικό για την εκτέλεση των καθηκόντων του, ανεξάρτητα από το μέσο στο οποίο αποθηκεύονται,

β) να λαμβάνει ή να αποκτά θεωρημένα αντίγραφα ή αποσπάσματα από τα εν λόγω αρχεία, τα δεδομένα, τις τεκμηριωμένες διαδικασίες και κάθε άλλο υλικό,

γ) να καλεί εκπροσώπους του κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ για προφορικές ή γραπτές εξηγήσεις σχετικά με γεγονότα ή έγγραφα που αφορούν το αντικείμενο και τον σκοπό της έρευνας και να καταγράφει τις απαντήσεις,

δ) να εξετάζει κάθε άλλο φυσικό ή νομικό πρόσωπο που συναινεί να ερωτηθεί με σκοπό τη συγκέντρωση πληροφοριών σχετικά με το αντικείμενο της έρευνας,

ε) να ζητεί αρχεία τηλεφωνικών κλήσεων και διαβίβασης δεδομένων.

3. Οι υπάλληλοι και άλλα πρόσωπα που εξουσιοδοτούνται από τον κύριο εποπτικό φορέα για τους σκοπούς της έρευνας, κατά τα οριζόμενα στην παράγραφο 1, ασκούν τις εξουσίες τους επιδεικνύοντας έγγραφη εξουσιοδότηση που ορίζει το αντικείμενο και τον σκοπό της έρευνας.

Στην εν λόγω εξουσιοδότηση επισημαίνονται επίσης οι περιοδικές χρηματικές ποινές που προβλέπονται στο άρθρο 35 παράγραφος 6, όταν τα απαιτούμενα αρχεία, τα δεδομένα, οι τεκμηριωμένες διαδικασίες ή οποιοδήποτε άλλο υλικό, ή οι απαντήσεις σε ερωτήσεις που υποβάλλονται σε εκπροσώπους του τρίτου παρόχου υπηρεσιών ΤΠΕ, δεν παρέχονται ή παρουσιάζουν ελλείψεις.

4. Οι εκπρόσωποι των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ υποχρεούνται να αποδέχονται τις έρευνες βάσει απόφασης του κύριου εποπτικού φορέα. Η απόφαση προσδιορίζει το αντικείμενο και τον σκοπό της έρευνας, τις περιοδικές χρηματικές ποινές που προβλέπονται στο άρθρο 35 παράγραφος 6, τα ένδικα μέσα που διατίθενται δυνάμει των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010, καθώς και το δικαίωμα επανεξέτασης της απόφασης από το Δικαστήριο.

5. Πριν από την έναρξη της έρευνας, ο κύριος εποπτικός φορέας ενημερώνει εγκαίρως την αρμόδια αρχή της χρηματοοικονομικής οντότητας που χρησιμοποιεί τις υπηρεσίες ΤΠΕ του εν λόγω κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ σχετικά με την έρευνα και την ταυτότητα των εξουσιοδοτημένων προσώπων.

Ο κύριος εποπτικός φορέας κοινοποιεί στο ΔΚΕ όλες τις πληροφορίες που μεταβιβάζονται σύμφωνα με το πρώτο εδάφιο.

Άρθρο 39

Επιθεωρήσεις

1. Για την εκπλήρωση των καθηκόντων του σύμφωνα με τον παρόντα κανονισμό, ο κύριος εποπτικός φορέας, επικουρούμενος από τις κοινές εξεταστικές ομάδες που αναφέρονται στο άρθρο 40 παράγραφος 1, μπορεί να εισέλθει και να διενεργήσει όλες τις απαραίτητες επιτόπιες επιθεωρήσεις σε κάθε επιχειρηματικό χώρο, έκταση ή ιδιοκτησία των τρίτων παρόχων υπηρεσιών ΤΠΕ, όπως κεντρικά γραφεία, επιχειρησιακά κέντρα, δευτερεύοντες χώροι, καθώς και να διενεργεί επιθεωρήσεις εξ αποστάσεως.

Για τους σκοπούς της άσκησης των εξουσιών που αναφέρονται στο πρώτο εδάφιο, ο κύριος εποπτικός φορέας συμβουλεύεται το ΔΚΕ.

2. Οι υπάλληλοι και τα λοιπά άτομα που έχουν εξουσιοδοτηθεί από τον κύριο εποπτικό φορέα για τη διενέργεια επιτόπιας επιθεώρησης έχουν την εξουσία:

α) να εισέρχονται σε αυτούς τους επαγγελματικούς χώρους, εκτάσεις ή ακίνητα και

β) να σφραγίζουν κάθε τέτοιο επαγγελματικό χώρο, βιβλία ή έγγραφα κατά την περίοδο και στον βαθμό που απαιτούνται για την επιθεώρηση.

Οι υπάλληλοι και τα λοιπά άτομα που έχουν εξουσιοδοτηθεί από τον κύριο εποπτικό φορέα ασκούν τις εξουσίες τους επιδεικνύοντας έγγραφη εξουσιοδότηση που ορίζει το αντικείμενο και τον σκοπό της επιθεώρησης και τις περιοδικές χρηματικές ποινές που προβλέπονται στο άρθρο 35 παράγραφος 6, σε περίπτωση που οι εκπρόσωποι των εν λόγω κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ δεν αποδέχονται την επιθεώρηση.

3. Πριν από την έναρξη της επιθεώρησης, ο κύριος εποπτικός φορέας ενημερώνει εγκαίρως τις αρμόδιες αρχές των χρηματοοικονομικών οντοτήτων που χρησιμοποιούν τον εν λόγω τρίτο πάροχο υπηρεσιών ΤΠΕ.

4. Οι επιθεωρήσεις καλύπτουν το πλήρες φάσμα των σχετικών συστημάτων, δικτύων, συσκευών, πληροφοριών και δεδομένων ΤΠΕ που χρησιμοποιούνται ή συμβάλλουν στην παροχή υπηρεσιών ΤΠΕ προς χρηματοοικονομικές οντότητες.

5. Πριν από κάθε προγραμματισμένη επιτόπια επιθεώρηση, ο κύριος εποπτικός φορέας ειδοποιεί ευλόγως τους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, εκτός εάν η ειδοποίηση αυτή δεν είναι δυνατή λόγω καταστάσεων έκτακτης ανάγκης ή κρίσης, ή εάν δημιουργεί κατάσταση κατά την οποία η επιθεώρηση ή ο έλεγχος δεν συνιστούν πλέον αποτελεσματική ενέργεια.

6. Ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ αποδέχεται τις επιτόπιες επιθεωρήσεις που έχουν διαταχθεί με απόφαση του κύριου εποπτικού φορέα. Η απόφαση προσδιορίζει το αντικείμενο και τον σκοπό της επιθεώρησης, καθορίζει την ημερομηνία έναρξης της επιθεώρησης και αναφέρει τις περιοδικές χρηματικές ποινές που προβλέπονται στο άρθρο 35 παράγραφος 6, τα ένδικα βοηθήματα που είναι διαθέσιμα βάσει των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010, καθώς και το δικαίωμα επανεξέτασης της απόφασης από το Δικαστήριο.

7. Όταν οι υπάλληλοι και άλλα πρόσωπα που εξουσιοδοτούνται από τον κύριο εποπτικό φορέα διαπιστώσουν ότι ένας κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ προβάλει αντίρρηση για τη διεξαγωγή επιθεώρησης που έχει διαταχθεί σύμφωνα με το παρόν άρθρο, ο κύριος εποπτικός φορέας ενημερώνει τον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ σχετικά με τις συνέπειες της αντίρρησης, συμπεριλαμβανομένης της δυνατότητας των αρμόδιων αρχών των σχετικών χρηματοοικονομικών οντοτήτων να απαιτήσουν από τις χρηματοοικονομικές οντότητες να καταγγείλουν τις συμβατικές ρυθμίσεις που έχουν συναφθεί με τον εν λόγω κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ.

Άρθρο 40

Εν εξελίξει εποπτεία

1. Κατά τη διεξαγωγή εποπτικών δραστηριοτήτων, ιδίως γενικών ερευνών ή επιθεωρήσεων, ο κύριος εποπτικός φορέας επικουρείται από την κοινή εξεταστική ομάδα που έχει συγκροτηθεί για κάθε κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ.

2. Η κοινή εξεταστική ομάδα που αναφέρεται στην παράγραφο 1 απαρτίζεται από μέλη του προσωπικού:

α) των ΕΕΑ,

β) των σχετικών αρμόδιων αρχών που εποπτεύουν τις χρηματοοικονομικές οντότητες στις οποίες παρέχει υπηρεσίες ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ,

γ) της εθνικής αρμόδιας αρχής που αναφέρεται στο άρθρο 32 παράγραφος 4 στοιχείο ε), σε προαιρετική βάση,

δ) μίας εθνικής αρμόδιας αρχής από το κράτος μέλος στο οποίο είναι εγκατεστημένος ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ, σε προαιρετική βάση.

Τα μέλη της κοινής εξεταστικής ομάδας διαθέτουν εμπειρογνωσία όσον αφορά θέματα ΤΠΕ και τον λειτουργικό κίνδυνο. Η κοινή εξεταστική ομάδα εκτελεί τις εργασίες της υπό τον συντονισμό ενός μέλους του προσωπικού που ορίζεται κύριος εποπτικός φορέας (στο εξής: συντονιστής κύριου εποπτικού φορέα).

3. Εντός 3 μηνών από την ολοκλήρωση μιας έρευνας ή επιθεώρησης, ο κύριος εποπτικός φορέας, κατόπιν διαβούλευσης με το φόρουμ εποπτείας, εγκρίνει συστάσεις τις οποίες πρέπει να απευθύνει στον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ σύμφωνα με τις εξουσίες που αναφέρονται στο άρθρο 35.

4. Οι συστάσεις που αναφέρονται στην παράγραφο 3 κοινοποιούνται αμέσως στον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ και στις αρμόδιες αρχές των χρηματοοικονομικών οντοτήτων στις οποίες παρέχει υπηρεσίες ΤΠΕ.

Για την εκπλήρωση των δραστηριοτήτων εποπτείας, ο κύριος εποπτικός φορέας μπορεί να λαμβάνει υπόψη τυχόν σχετικές πιστοποιήσεις τρίτων και εσωτερικές ή εξωτερικές εκθέσεις ελέγχου τρίτων παρόχων ΤΠΕ, τις οποίες θέτει στη διάθεσή του ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ.

Άρθρο 41

Εναρμόνιση με τους όρους που καθιστούν δυνατή την άσκηση δραστηριοτήτων εποπτείας

1. Οι ΕΕΑ, μέσω της μεικτής επιτροπής, καταρτίζουν σχέδια ρυθμιστικών τεχνικών προτύπων με σκοπό να προσδιορίσουν:

α) τις πληροφορίες που πρέπει να παρέχει ο τρίτος πάροχος υπηρεσιών ΤΠΕ στην αίτηση για προαιρετικό αίτημα ορισμού ως κρίσιμος βάσει του άρθρου 31 παράγραφος 11,

β) το περιεχόμενο, τη δομή και τη μορφή των πληροφοριών που πρέπει να υποβάλλονται, να γνωστοποιούνται ή να αναφέρονται από τους τρίτους παρόχους υπηρεσιών ΤΠΕ σύμφωνα με το άρθρο 35 παράγραφος 1, συμπεριλαμβανομένου του υποδείγματος για την παροχή πληροφοριών σχετικά με τις ρυθμίσεις υπεργολαβίας,

γ) τα κριτήρια για τον καθορισμό της σύνθεσης της κοινής εξεταστικής ομάδας, διασφαλίζοντας την ισόρροπη συμμετοχή των μελών του προσωπικού των ΕΕΑ και των σχετικών αρμόδιων αρχών, τον ορισμό τους, τα καθήκοντά τους και τις ρυθμίσεις εργασίας τους,

δ) τις λεπτομέρειες της αξιολόγησης των αρμόδιων αρχών όσον αφορά τα μέτρα που έλαβε ο τρίτος πάροχος υπηρεσιών ΤΠΕ βάσει των συστάσεων του κύριου εποπτικού φορέα σύμφωνα με το άρθρο 42 παράγραφος 3.

2. Οι ΕΕΑ υποβάλλουν τα εν λόγω σχέδια ρυθμιστικών τεχνικών προτύπων στην Επιτροπή έως τις 17 Ιουλίου 2024.

Ανατίθεται στην Επιτροπή η εξουσία να συμπληρώνει τον παρόντα κανονισμό εκδίδοντας τα ρυθμιστικά τεχνικά πρότυπα που αναφέρονται στην παράγραφο 1, σύμφωνα με τη διαδικασία που ορίζεται στα άρθρα 10 έως 14 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010.

Άρθρο 42

Συνέχεια που δίνεται από τις αρμόδιες αρχές

1. Εντός 60 ημερολογιακών ημερών από την παραλαβή των συστάσεων που εκδίδει ο κύριος εποπτικός φορέας σύμφωνα με το άρθρο 35 παράγραφος 1 στοιχείο δ), οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ είτε ενημερώνουν τον κύριο εποπτικό φορέα για την πρόθεσή τους να ακολουθήσουν τις συστάσεις είτε παρέχουν αιτιολογημένη εξήγηση για τη μη τήρηση των εν λόγω συστάσεων. Ο κύριος εποπτικός φορέας διαβιβάζει αμέσως τις πληροφορίες αυτές στις αρμόδιες αρχές των σχετικών χρηματοοικονομικών οντοτήτων.

2. Ο κύριος εποπτικός φορέας δημοσιοποιεί το γεγονός ότι ένας κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ δεν ενημερώνει τον κύριο εποπτικό φορέα σύμφωνα με την παράγραφο 1 ή ότι η εξήγηση που παρέχεται από τον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ δεν κρίνεται επαρκής. Οι πληροφορίες που δημοσιεύονται αποκαλύπτουν την ταυτότητα του κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ, καθώς και πληροφορίες σχετικά με το είδος και τη φύση της μη συμμόρφωσης. Οι πληροφορίες αυτές περιορίζονται σε ό,τι είναι σημαντικό και αναλογικό για τη διασφάλιση της ευαισθητοποίησης του κοινού, εκτός εάν η δημοσιοποίηση αυτή θα προκαλούσε δυσανάλογη ζημία στα εμπλεκόμενα μέρη ή θα μπορούσε να θέσει σε σοβαρό κίνδυνο την εύρυθμη λειτουργία και την ακεραιότητα των χρηματοοικονομικών αγορών ή τη σταθερότητα ολόκληρου ή μέρους του χρηματοοικονομικού συστήματος της Ένωσης.

Ο κύριος εποπτικός φορέας ενημερώνει τον τρίτο πάροχο υπηρεσιών ΤΠΕ σχετικά με την εν λόγω δημοσιοποίηση.

3. Οι αρμόδιες αρχές ενημερώνουν τις σχετικές χρηματοοικονομικές οντότητες για τους κινδύνους που προσδιορίζονται στις συστάσεις που απευθύνονται σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ σύμφωνα με το άρθρο 35 παράγραφος 1 στοιχείο δ).

Κατά τη διαχείριση του κινδύνου τρίτων μερών ΤΠΕ, οι χρηματοοικονομικές οντότητες λαμβάνουν υπόψη τους κινδύνους που αναφέρονται στο πρώτο εδάφιο.

4. Όταν μια αρμόδια αρχή κρίνει ότι μια χρηματοοικονομική οντότητα δεν λαμβάνει υπόψη ή δεν αντιμετωπίζει επαρκώς στο πλαίσιο της διαχείρισης του κινδύνου τρίτων μερών ΤΠΕ τους συγκεκριμένους κινδύνους που προσδιορίζονται στις συστάσεις, κοινοποιεί στη χρηματοοικονομική οντότητα την πιθανότητα να ληφθεί απόφαση, εντός 60 ημερολογιακών ημερών από την παραλαβή της εν λόγω κοινοποίησης, σύμφωνα με την παράγραφο 6, ελλείψει κατάλληλων συμβατικών ρυθμίσεων με στόχο την αντιμετώπιση των εν λόγω κινδύνων.

5. Μετά την παραλαβή των αναφορών που προβλέπονται στο άρθρο 35 παράγραφος 1 στοιχείο γ) και πριν από τη λήψη της απόφασης όπως αναφέρεται στην παράγραφο 6 του παρόντος άρθρου, οι αρμόδιες αρχές μπορούν, σε προαιρετική βάση, να διαβουλεύονται με τις αρμόδιες αρχές οι οποίες έχουν οριστεί ή συσταθεί σύμφωνα με την οδηγία (ΕΕ) 2022/2555 και είναι υπεύθυνες για την εποπτεία μιας βασικής ή σημαντικής οντότητας που υπόκειται στις διατάξεις της εν λόγω οδηγίας και η οποία έχει οριστεί ως κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ.

6. Οι αρμόδιες αρχές δύνανται, ως μέτρο έσχατης ανάγκης, μετά την κοινοποίηση και, κατά περίπτωση, τη διαβούλευση κατά τα οριζόμενα στις παραγράφους 4 και 5 του παρόντος άρθρου, σύμφωνα με το άρθρο 50, να λάβουν απόφαση με την οποία απαιτούν από τις χρηματοοικονομικές οντότητες να αναστείλουν προσωρινά, εν μέρει ή πλήρως, τη χρήση ή την ανάπτυξη μιας υπηρεσίας που παρέχεται από τον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ, έως ότου αντιμετωπιστούν οι κίνδυνοι που προσδιορίζονται στις συστάσεις που απευθύνονται σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ. Εάν κρίνεται σκόπιμο, μπορούν να ζητήσουν από τις χρηματοοικονομικές οντότητες να προβούν σε μερική ή ολική καταγγελία των σχετικών ρυθμίσεων που έχουν συναφθεί με τους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ.

7. Όταν ένας κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ αρνείται να εγκρίνει συστάσεις βασιζόμενος σε αποκλίνουσα προσέγγιση από εκείνη που συνιστά ο κύριος εποπτικός φορέας, και η εν λόγω αποκλίνουσα προσέγγιση μπορεί να επηρεάσει αρνητικά μεγάλο αριθμό χρηματοοικονομικών οντοτήτων ή σημαντικό μέρος του χρηματοοικονομικό τομέα, και οι μεμονωμένες προειδοποιήσεις που εκδίδονται από αρμόδιες αρχές δεν έχουν οδηγήσει σε συνεπείς προσεγγίσεις για τον μετριασμό του δυνητικού κινδύνου για τη χρηματοοικονομική σταθερότητα, ο κύριος εποπτικός φορέας μπορεί, κατόπιν διαβούλευσης με το φόρουμ εποπτείας, να εκδίδει μη δεσμευτικές και μη δημόσιες γνώμες προς τις αρμόδιες αρχές, προκειμένου να προωθήσει συνεπή και συγκλίνοντα εποπτικά μέτρα παρακολούθησης, κατά περίπτωση.

8. Μετά την παραλαβή των εκθέσεων που αναφέρονται στο άρθρο 35 παράγραφος 1 στοιχείο γ), οι αρμόδιες αρχές, κατά τη λήψη απόφασης που προβλέπεται στην παράγραφο 6 του παρόντος άρθρου, λαμβάνουν υπόψη το είδος και το μέγεθος του κινδύνου που δεν αντιμετωπίστηκε από τον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ, καθώς και τη σοβαρότητα της μη συμμόρφωσης, λαμβάνοντας υπόψη τα ακόλουθα κριτήρια:

α) τη βαρύτητα και τη διάρκεια της μη συμμόρφωσης,

β) αν η μη συμμόρφωση αποκάλυψε σοβαρές αδυναμίες στις διαδικασίες, τα συστήματα διαχείρισης, τη διαχείριση κινδύνων και τις εσωτερικές δικλείδες ασφάλειας του κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ,

γ) αν η μη συμμόρφωση διευκόλυνε, προκάλεσε ή ευθύνεται με άλλον τρόπο για την τέλεση οικονομικού εγκλήματος,

δ) αν η μη συμμόρφωση οφείλεται σε πρόθεση ή σε αμέλεια,

ε) αν η αναστολή ή η καταγγελία των συμβατικών ρυθμίσεων ενέχει κίνδυνο για τη συνέχεια των επιχειρηματικών δραστηριοτήτων της χρηματοοικονομικής οντότητας, παρά τις προσπάθειες της χρηματοοικονομικής οντότητας να αποφευχθεί η διαταραχή στην παροχή των υπηρεσιών της,

στ) κατά περίπτωση, τη γνώμη των αρμόδιων αρχών που έχουν οριστεί ή συσταθεί σύμφωνα με την οδηγία (ΕΕ) 2022/2555 ως υπεύθυνες για την εποπτεία μιας βασικής ή σημαντικής οντότητας που υπόκειται στις διατάξεις της εν λόγω οδηγίας και η οποία έχει οριστεί ως κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ, η οποία ζητείται σε προαιρετική βάση σύμφωνα με την παράγραφο 5 του παρόντος άρθρου.

Οι αρμόδιες αρχές παρέχουν στις χρηματοοικονομικές οντότητες το αναγκαίο χρονικό διάστημα, ώστε να μπορέσουν να προσαρμόσουν τις συμβατικές ρυθμίσεις με κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, προκειμένου να αποφευχθούν οι αρνητικές επιπτώσεις στην ψηφιακή επιχειρησιακή ανθεκτικότητά τους και να μπορέσουν να αναπτύξουν στρατηγικές εξόδου και σχέδια μετάβασης όπως αναφέρονται στο άρθρο 28.

9. Η απόφαση που αναφέρεται στην παράγραφο 6 του παρόντος άρθρου κοινοποιείται στα μέλη του φόρουμ εποπτείας που αναφέρεται στο άρθρο 32 παράγραφος 4 στοιχεία α), β) και γ) και στο ΔΚΕ.

Οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ που επηρεάζονται από τις αποφάσεις της παραγράφου 6 συνεργάζονται πλήρως με τις θιγόμενες χρηματοοικονομικές οντότητες, ιδίως στο πλαίσιο της διαδικασίας αναστολής ή καταγγελίας των συμβατικών τους ρυθμίσεων.

10. Οι αρμόδιες αρχές ενημερώνουν τακτικά τον κύριο εποπτικό φορέα σχετικά με τις προσεγγίσεις και τα μέτρα που λαμβάνονται κατά την εκτέλεση των εποπτικών καθηκόντων τους σε σχέση με τις χρηματοοικονομικές οντότητες, καθώς και σε σχέση με τις συμβατικές ρυθμίσεις που έχουν συνάψει, σε περίπτωση που οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ δεν έχουν εγκρίνει εν μέρει ή πλήρως τις συστάσεις που τους απηύθυνε ο κύριος εποπτικός φορέας.

11. Ο κύριος εποπτικός φορέας μπορεί, κατόπιν αιτήματος, να παράσχει περαιτέρω διευκρινίσεις σχετικά με τις εκδοθείσες συστάσεις για να καθοδηγήσει τις αρμόδιες αρχές σχετικά με τα μέτρα παρακολούθησης.

Άρθρο 43

Εποπτικά τέλη

1. Ο κύριος εποπτικός φορέας χρεώνει, σύμφωνα με την κατ' εξουσιοδότηση πράξη που αναφέρεται στην παράγραφο 2 του παρόντος άρθρου, κρίσιμες αμοιβές τρίτων παρόχων υπηρεσιών ΤΠΕ που καλύπτουν πλήρως τις αναγκαίες δαπάνες του κύριου εποπτικού φορέα σε σχέση με την εκτέλεση των καθηκόντων εποπτείας σύμφωνα με τον παρόντα κανονισμό, συμπεριλαμβανομένης της επιστροφής τυχόν δαπανών που ενδέχεται να προκύψουν ως αποτέλεσμα των εργασιών της κοινής εξεταστικής ομάδας που αναφέρεται στο άρθρο 40, καθώς και των δαπανών για συμβουλές που παρέχονται από τους ανεξάρτητους εμπειρογνώμονες, όπως αναφέρεται στο άρθρο 32 δεύτερο εδάφιο παράγραφος 4, σε σχέση με θέματα που εμπίπτουν στην αρμοδιότητα των δραστηριοτήτων άμεσης εποπτείας.

Το ύψος των τελών που χρεώνονται σε κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ καλύπτει όλες τις δαπάνες που προκύπτουν ως αποτέλεσμα της εκτέλεσης των καθηκόντων που προβλέπονται στην παρούσα ενότητα και είναι ανάλογο προς τον κύκλο εργασιών του.

2. Ανατίθεται στην Επιτροπή η εξουσία να εκδώσει κατ' εξουσιοδότηση πράξη, σύμφωνα με το άρθρο 57, για τη συμπλήρωση του παρόντος κανονισμού με τον προσδιορισμό του ύψους των τελών και του τρόπου καταβολής τους έως τις 17 Ιουλίου 2024.

Άρθρο 44

Διεθνής συνεργασία

1. Με την επιφύλαξη του άρθρου 36, η ΕΑΤ, η ΕΑΚΑΑ και η ΕΑΑΕΣ δύνανται, σύμφωνα με το άρθρο 33 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1095/2010 και (ΕΕ) αριθ. 1094/2010, αντίστοιχα, να συνάπτουν διοικητικές ρυθμίσεις με κανονιστικές και εποπτικές αρχές τρίτων χωρών, με σκοπό την προώθηση της διεθνούς συνεργασίας όσον αφορά τους κινδύνους τρίτων παρόχων ΤΠΕ σε διάφορους χρηματοοικονομικούς τομείς, ιδίως με την ανάπτυξη βέλτιστων πρακτικών για την επανεξέταση των πρακτικών και των ελέγχων διαχείρισης κινδύνων ΤΠΕ, των μέτρων μετριασμού και της αντιμετώπισης συμβάντων.

2. Οι ΕΕΑ, μέσω της μεικτής επιτροπής, υποβάλλουν ανά πενταετία στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο και την Επιτροπή κοινή εμπιστευτική έκθεση, στην οποία συνοψίζονται τα ευρήματα των σχετικών συζητήσεων που διεξάγονται με τις αρχές τρίτων χωρών που αναφέρονται στην παράγραφο 1, εστιάζοντας στην εξέλιξη των κινδύνων τρίτων παρόχων ΤΠΕ και στις συνέπειες που έχει για τη χρηματοοικονομική σταθερότητα, την ακεραιότητα της αγοράς, την προστασία των επενδυτών ή τη λειτουργία της εσωτερικής αγοράς.

ΚΕΦΑΛΑΙΟ VI

Ρυθμίσεις ανταλλαγής πληροφοριών

Άρθρο 45

Ρυθμίσεις ανταλλαγής πληροφοριών όσον αφορά στοιχεία και πληροφορίες για κυβερνοαπειλές

1. Οι χρηματοοικονομικές οντότητες μπορούν να ανταλλάσσουν μεταξύ τους στοιχεία και πληροφορίες για κυβερνοαπειλές, συμπεριλαμβανομένων των δεικτών έκθεσης σε κίνδυνο, τακτικών, τεχνικών και διαδικασιών, ειδοποιήσεων κυβερνοασφάλειας και εργαλείων παραμετροποίησης, στον βαθμό που η εν λόγω ανταλλαγή στοιχείων και πληροφοριών:

α) έχει ως στόχο την ενίσχυση της ψηφιακής επιχειρησιακής ανθεκτικότητας των χρηματοοικονομικών οντοτήτων, ιδίως μέσω της ευαισθητοποίησης σχετικά με τις κυβερνοαπειλές, του περιορισμού ή της παρεμπόδισης της ικανότητας διάδοσης των κυβερνοαπειλών, της υποστήριξης των αμυντικών ικανοτήτων, των τεχνικών ανίχνευσης απειλών, των στρατηγικών μετριασμού ή των σταδίων αντιμετώπισης και ανάκαμψης,

β) πραγματοποιείται στο πλαίσιο αξιόπιστων κοινοτήτων χρηματοοικονομικών οντοτήτων,

γ) υλοποιείται μέσω ρυθμίσεων ανταλλαγής πληροφοριών που προστατεύουν τον δυνητικά ευαίσθητο χαρακτήρα των ανταλλασσόμενων πληροφοριών, και οι οποίες διέπονται από κανόνες δεοντολογίας, τηρουμένων πλήρως του επιχειρηματικού απορρήτου, της προστασίας των δεδομένων προσωπικού χαρακτήρα σύμφωνα με τον κανονισμό (ΕΕ) 2016/679 και των κατευθυντήριων γραμμών για την πολιτική ανταγωνισμού.

2. Για τους σκοπούς της παραγράφου 1 στοιχείο γ), οι ρυθμίσεις ανταλλαγής πληροφοριών καθορίζουν τους όρους συμμετοχής και, ανάλογα με την περίπτωση, τις λεπτομέρειες σχετικά με την εξασφάλιση της συμμετοχής των δημόσιων αρχών και την ιδιότητα με την οποία μπορούν να συνδέονται με τις ρυθμίσεις ανταλλαγής πληροφοριών, σχετικά με τη συμμετοχή των τρίτων παρόχων υπηρεσιών ΤΠΕ, καθώς και σχετικά με τα επιχειρησιακά στοιχεία, συμπεριλαμβανομένης της χρήσης ειδικών πλατφορμών ΤΠ.

3. Οι χρηματοοικονομικές οντότητες κοινοποιούν στις αρμόδιες αρχές τη συμμετοχή τους στις ρυθμίσεις ανταλλαγής πληροφοριών που αναφέρονται στην παράγραφο 1, κατά την επικύρωση της συμμετοχής τους ως μελών ή, κατά περίπτωση, της παύσης της συμμετοχής τους ως μελών, αμέσως μετά την έναρξη ισχύος της.

ΚΕΦΑΛΑΙΟ VII

Αρμόδιες αρχές

Άρθρο 46

Αρμόδιες αρχές

Με την επιφύλαξη των διατάξεων σχετικά με το πλαίσιο εποπτείας κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ που αναφέρονται στο κεφάλαιο V τμήμα II του παρόντος κανονισμού, η συμμόρφωση με τον παρόντα κανονισμό διασφαλίζεται από τις κατωτέρω αρμόδιες αρχές σύμφωνα με τις εξουσίες που τους έχουν χορηγηθεί βάσει των αντίστοιχων νομικών πράξεων:

α) για πιστωτικά ιδρύματα και για ιδρύματα που εξαιρούνται δυνάμει της οδηγίας 2013/36/ΕΕ, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 4 της εν λόγω οδηγίας, και για πιστωτικά ιδρύματα που χαρακτηρίζονται ως σημαντικά σύμφωνα με το άρθρο 6 παράγραφος 4 του κανονισμού (ΕΕ) αριθ. 1024/2013, την ΕΚΤ σύμφωνα με τις εξουσίες και τα καθήκοντα που ανατίθενται με τον εν λόγω κανονισμό,

β) για ιδρύματα πληρωμών, συμπεριλαμβανομένων των ιδρυμάτων πληρωμών που εξαιρούνται δυνάμει της οδηγίας (ΕΕ) 2015/2366, για ιδρύματα ηλεκτρονικού χρήματος, συμπεριλαμβανομένων εκείνων που εξαιρούνται δυνάμει της οδηγίας 2009/110/ΕΚ, και για παρόχους υπηρεσιών πληροφοριών λογαριασμού, όπως αναφέρονται στο άρθρο 33 παράγραφος 1 της οδηγίας (ΕΕ) 2015/2366, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 22 της οδηγίας (ΕΕ) 2015/2366,

γ) για επιχειρήσεις επενδύσεων, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 4 της οδηγίας (ΕΕ) 2019/2034 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([38]),

δ) για παρόχους υπηρεσιών κρυπτοστοιχείων που έχουν λάβει άδεια βάσει του του κανονισμού σχετικά με τις αγορές κρυπτοστοιχείων και για εκδότες ψηφιακών μαρκών με εγγύηση περιουσιακών στοιχείων, την αρμόδια αρχή που ορίζεται σύμφωνα με τη σχετική διάταξη του εν λόγω κανονισμού,

ε) για κεντρικά αποθετήρια τίτλων, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 11 του κανονισμού (ΕΕ) αριθ. 909/2014,

στ) για κεντρικούς αντισυμβαλλομένους, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 22 του κανονισμού (ΕΕ) αριθ. 648/2012,

ζ) για τόπους διαπραγμάτευσης και παρόχους υπηρεσιών αναφοράς δεδομένων, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 67 της οδηγίας 2014/65/ΕΕ και την αρμόδια αρχή όπως ορίζεται στο άρθρο 2 παράγραφος 1 σημείο 18) του κανονισμού (ΕΕ) αριθ. 600/2014,

η) για αρχεία καταγραφής συναλλαγών, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 22 του κανονισμού (ΕΕ) αριθ. 648/2012,

θ) για διαχειριστές οργανισμών εναλλακτικών επενδύσεων, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 44 της οδηγίας 2011/61/ΕΕ,

ι) για εταιρείες διαχείρισης, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 97 της οδηγίας 2009/65/ΕΚ,

ια) για ασφαλιστικές και αντασφαλιστικές επιχειρήσεις, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 30 της οδηγίας 2009/138/ΕΚ,

ιβ) για ασφαλιστικούς διαμεσολαβητές, αντασφαλιστικούς διαμεσολαβητές και ασφαλιστικούς διαμεσολαβητές που ασκούν ως δευτερεύουσα δραστηριότητα την ασφαλιστική διαμεσολάβηση, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 12 της οδηγίας (ΕΕ) 2016/97,

ιγ) για ιδρύματα επαγγελματικών συνταξιοδοτικών παροχών, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 47 της οδηγίας (ΕΕ) 2016/2341,

ιδ) για οργανισμούς αξιολόγησης πιστοληπτικής ικανότητας, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 21 του κανονισμού (ΕΚ) αριθ. 1060/2009,

ιε) για διαχειριστές δεικτών αναφοράς κρίσιμης σημασίας, την αρμόδια αρχή που ορίζεται σύμφωνα με τα άρθρα 40 και 41 του κανονισμού (ΕΕ) 2016/1011,

([38]) Οδηγία (ΕΕ) 2019/2034 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Νοεμβρίου 2019, σχετικά με την προληπτική εποπτεία επιχειρήσεων επενδύσεων και την τροποποίηση των οδηγιών 2002/87/ΕΚ, 2009/65/ΕΚ, 2011/61/ΕΕ, 2013/36/ΕΕ, 2014/59/ΕΕ και 2014/65/ΕΕ (ΕΕ L 314 της 5.12.2019, σ. 64).

ιστ) για παρόχους υπηρεσιών συμμετοχικής χρηματοδότησης, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 29 του κανονισμού (ΕΕ) 2020/1503,

ιζ) για αρχεία καταγραφής τιτλοποιήσεων, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 10 και το άρθρο 14 παράγραφος 1 του κανονισμού (ΕΕ) 2017/2402.

Άρθρο 47

Συνεργασία με δομές και αρχές που έχουν συγκροτηθεί βάσει της οδηγίας (ΕΕ) 2022/2555

1. Για την ενίσχυση της συνεργασίας και τη διευκόλυνση των ανταλλαγών εποπτικών πληροφοριών μεταξύ των αρμόδιων αρχών, που ορίζονται σύμφωνα με τον παρόντα κανονισμό, και της ομάδας συνεργασίας, που έχει συγκροτηθεί σύμφωνα με το άρθρο 14 της οδηγίας (ΕΕ) 2022/2555 οι ΕΕΑ και οι αρμόδιες αρχές μπορούν να συμμετέχουν στις δραστηριότητες της ομάδας συνεργασίας για θέματα που αφορούν τις εποπτικές δραστηριότητές τους σε σχέση με χρηματοοικονομικές οντότητες. Οι ΕΕΑ και οι αρμόδιες αρχές μπορούν να ζητήσουν να κληθούν να συμμετάσχουν στις δραστηριότητες της ομάδας συνεργασίας για θέματα που αφορούν βασικές ή σημαντικές οντότητες που υπόκεινται στις διατάξεις της οδηγίας (ΕΕ) 2022/2555 οι οποίες έχουν επίσης οριστεί ως κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ σύμφωνα με το άρθρο 31 του παρόντος κανονισμού.

2. Κατά περίπτωση, οι αρμόδιες αρχές μπορούν να συμβουλεύονται και να ανταλλάσσουν πληροφορίες με τα ενιαία σημεία επαφής και τις CSIRT που έχουν οριστεί ή συσταθεί σύμφωνα με την οδηγία (ΕΕ) 2022/2555

3. Κατά περίπτωση, οι αρμόδιες αρχές μπορούν να ζητούν κάθε σχετική τεχνική συμβουλή και βοήθεια από τις αρμόδιες αρχές που ορίζονται ή συστήνονται σύμφωνα με την οδηγία (ΕΕ) 2022/2555 και να θεσπίζουν ρυθμίσεις συνεργασίας για τη δημιουργία αποτελεσματικών μηχανισμών συντονισμού ταχείας απόκρισης.

4. Οι ρυθμίσεις που αναφέρονται στην παράγραφο 3 του παρόντος άρθρου μπορούν, μεταξύ άλλων, να προσδιορίζουν τις διαδικασίες για τον συντονισμό των δραστηριοτήτων εποπτείας, αντίστοιχα, σε σχέση με τις βασικές ή σημαντικές οντότητες που υπόκεινται στις διατάξεις της οδηγίας (ΕΕ) 2022/2555 οι οποίοι έχουν οριστεί ως κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ σύμφωνα με το άρθρο 31 του παρόντος κανονισμού, μεταξύ άλλων για τη διεξαγωγή, σύμφωνα με το εθνικό δίκαιο, ερευνών και επιτόπιων επιθεωρήσεων, καθώς και για μηχανισμούς ανταλλαγής πληροφοριών μεταξύ των αρμόδιων αρχών δυνάμει του παρόντος κανονισμού και των αρμόδιων αρχών που ορίζονται ή συστήνονται σύμφωνα με την εν λόγω οδηγία, συμπεριλαμβανομένης της πρόσβασης σε πληροφορίες που ζητούν οι τελευταίες αυτές αρχές.

Άρθρο 48

Συνεργασία μεταξύ αρχών

1. Οι αρμόδιες αρχές συνεργάζονται στενά μεταξύ τους και, κατά περίπτωση, με τον κύριο εποπτικό φορέα.

2. Οι αρμόδιες αρχές και ο κύριος εποπτικός φορέας ανταλλάσσουν εγκαίρως όλες τις σχετικές πληροφορίες που αφορούν κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ και είναι απαραίτητες για την εκτέλεση των αντίστοιχων καθηκόντων τους δυνάμει του παρόντος κανονισμού, ιδίως σε σχέση με προσδιορισμένους κινδύνους, προσεγγίσεις και μέτρα που λαμβάνονται στο πλαίσιο των εποπτικών καθηκόντων του κύριου εποπτικού φορέα.

Άρθρο 49

Ασκήσεις, επικοινωνία και συνεργασία μεταξύ των χρηματοοικονομικών τομέων

1. Οι ΕΕΑ, μέσω της μεικτής επιτροπής και σε συνεργασία με τις αρμόδιες αρχές, τις αρχές εξυγίανσης που αναφέρονται στο άρθρο 3 της οδηγίας 2014/59/ΕΕ, την ΕΚΤ, το Ενιαίο Συμβούλιο Εξυγίανσης όσον αφορά πληροφορίες σχετικά με οντότητες που εμπίπτουν στο πεδίο εφαρμογής του κανονισμού (ΕΕ) αριθ. 806/2014, το ΕΣΣΚ και τον ENISA, κατά περίπτωση, μπορούν να θεσπίσουν μηχανισμούς ώστε να είναι δυνατή η ανταλλαγή αποτελεσματικών πρακτικών μεταξύ των χρηματοοικονομικών τομέων για την ενίσχυση της επίγνωσης των καταστάσεων και τον εντοπισμό κοινών ευπαθειών στον κυβερνοχώρο και κινδύνων μεταξύ των τομέων.

Μπορούν να αναπτύξουν ασκήσεις διαχείρισης κρίσεων και έκτακτης ανάγκης που περιλαμβάνουν σενάρια κυβερνοεπιθέσεων, με σκοπό την ανάπτυξη διαύλων επικοινωνίας και τη σταδιακή εξασφάλιση της δυνατότητας αποτελεσματικής συντονισμένης απόκρισης σε επίπεδο ΕΕ, σε περίπτωση μείζονος διασυνοριακού συμβάντος που σχετίζεται με τις ΤΠΕ ή σχετικής απειλής με συστημικές επιπτώσεις στον χρηματοοικονομικό τομέα της Ένωσης συνολικά.

Στο πλαίσιο των ασκήσεων αυτών παρέχεται, κατά περίπτωση, η δυνατότητα ελέγχου των εξαρτήσεων του χρηματοοικονομικού τομέα από άλλους οικονομικούς τομείς.

2. Οι αρμόδιες αρχές, οι ΕΕΑ και η ΕΚΤ συνεργάζονται στενά μεταξύ τους και ανταλλάσσουν πληροφορίες στο πλαίσιο της εκτέλεσης των καθηκόντων τους, σύμφωνα με τα άρθρα 47 έως 54. Συντονίζουν στενά την εποπτεία τους ώστε να εντοπίζουν και να διορθώνουν παραβιάσεις του παρόντος κανονισμού, να αναπτύσσουν και να προωθούν βέλτιστες πρακτικές, να διευκολύνουν τη συνεργασία, να προάγουν τη συνεπή ερμηνεία και να παρέχουν αξιολογήσεις σε περισσότερες από μία περιοχές δικαιοδοσίας σε περίπτωση διαφωνίας.

Άρθρο 50

Διοικητικές κυρώσεις και διορθωτικά μέτρα

1. Οι αρμόδιες αρχές διαθέτουν όλες τις εξουσίες εποπτείας, έρευνας και επιβολής κυρώσεων που απαιτούνται για την εκπλήρωση των καθηκόντων τους σύμφωνα με τον παρόντα κανονισμό.

2. Οι εξουσίες που αναφέρονται στην παράγραφο 1 περιλαμβάνουν τουλάχιστον τις ακόλουθες εξουσίες:

α) πρόσβαση σε οποιοδήποτε έγγραφο ή δεδομένο που τηρείται σε οποιαδήποτε μορφή, το οποίο η αρμόδια αρχή θεωρεί ότι μπορεί να είναι συναφές για την εκτέλεση των καθηκόντων τους, και να λαμβάνουν αντίγραφό του,

β) διενέργεια επιτόπιων ελέγχων ή ερευνών, που περιλαμβάνουν, μεταξύ άλλων:

   i) πρόσκληση εκπροσώπων των χρηματοοικονομικών υπηρεσιών για προφορικές ή γραπτές εξηγήσεις σχετικά με γεγονότα ή έγγραφα που αφορούν το αντικείμενο και τον σκοπό της έρευνας και καταγραφή των απαντήσεων,

   ii) εξέταση κάθε άλλου φυσικού ή νομικού προσώπου που συναινεί να ερωτηθεί με σκοπό τη συγκέντρωση πληροφοριών σχετικά με το αντικείμενο της έρευνας,

γ) αίτηση λήψης διορθωτικών μέτρων για παραβιάσεις των απαιτήσεων του παρόντος κανονισμού.

3. Με την επιφύλαξη του δικαιώματος των κρατών μελών να επιβάλλουν ποινικές κυρώσεις σύμφωνα με το άρθρο 52, τα κράτη μέλη θεσπίζουν κανόνες για τη θέσπιση κατάλληλων διοικητικών κυρώσεων και διορθωτικών μέτρων σε περιπτώσεις παραβίασης του παρόντος κανονισμού και διασφαλίζουν την αποτελεσματική εφαρμογή τους.

Ο χαρακτήρας των εν λόγω κυρώσεων και μέτρων είναι αποτελεσματικός, αναλογικός και αποτρεπτικός.

4. Τα κράτη μέλη αναθέτουν στις αρμόδιες αρχές την εξουσία να εφαρμόζουν τουλάχιστον τις ακόλουθες διοικητικές κυρώσεις ή διορθωτικά μέτρα σε περιπτώσεις παραβίασης του παρόντος κανονισμού:

α) να εκδίδουν εντολή βάσει της οποίας το φυσικό ή νομικό πρόσωπο υποχρεούται να παύσει τη συμπεριφορά που παραβιάζει τον παρόντα κανονισμό και να μην την επαναλάβει,

β) να απαιτούν την προσωρινή ή οριστική παύση κάθε πρακτικής ή συμπεριφοράς που η αρμόδια αρχή θεωρεί ότι αντιβαίνει στις διατάξεις του παρόντος κανονισμού και να προλαμβάνουν την επανάληψη της εν λόγω πρακτικής ή συμπεριφοράς,

γ) να εγκρίνουν κάθε είδους μέτρα, μεταξύ άλλων χρηματικής φύσης, ώστε να διασφαλίζεται ότι οι χρηματοοικονομικές οντότητες εξακολουθούν να συμμορφώνονται με τις νομικές απαιτήσεις,

δ) να ζητούν, στον βαθμό που επιτρέπεται από το εθνικό δίκαιο, τα υφιστάμενα αρχεία κίνησης δεδομένων που τηρούνται από πάροχο τηλεπικοινωνιακών υπηρεσιών, όταν υπάρχει εύλογη υπόνοια παραβίασης του παρόντος κανονισμού και όταν τα εν λόγω αρχεία μπορεί να είναι συναφή για τη διερεύνηση περιπτώσεων παραβίασης του παρόντος κανονισμού, και

ε) να εκδίδουν δημόσιες ανακοινώσεις, συμπεριλαμβανομένων των δημόσιων δηλώσεων, στις οποίες αναφέρεται το υπαίτιο φυσικό ή νομικό πρόσωπο και η φύση της παραβίασης.

5. Σε περίπτωση που η παράγραφος 2 στοιχείο γ) και η παράγραφος 4 εφαρμόζονται σε νομικά πρόσωπα, τα κράτη μέλη αναθέτουν στις αρμόδιες αρχές την εξουσία επιβολής των διοικητικών κυρώσεων και των διορθωτικών μέτρων, με την επιφύλαξη των προϋποθέσεων που προβλέπονται στο εθνικό δίκαιο, σε μέλη του διοικητικού οργάνου, καθώς και σε οποιοδήποτε άλλο φυσικό πρόσωπο το οποίο θεωρείται υπαίτιο για την παραβίαση δυνάμει του εθνικού δικαίου.

6. Τα κράτη μέλη διασφαλίζουν ότι οποιαδήποτε απόφαση επιβολής διοικητικών κυρώσεων ή διορθωτικών μέτρων που προβλέπεται από την παράγραφο 2 στοιχείο γ) αιτιολογείται δεόντως και υπόκειται σε δικαίωμα προσφυγής.

Άρθρο 51

Άσκηση της εξουσίας επιβολής διοικητικών κυρώσεων και διορθωτικών μέτρων

1. Οι αρμόδιες αρχές ασκούν την εξουσία επιβολής των διοικητικών κυρώσεων και των διορθωτικών μέτρων του άρθρου 50 σύμφωνα με το εκάστοτε εθνικό νομικό πλαίσιο, ανάλογα με την περίπτωση, ως εξής:

α) άμεσα,

β) σε συνεργασία με άλλες αρχές,

γ) υπό την ευθύνη τους με ανάθεση καθηκόντων σε άλλες αρχές ή

δ) κατόπιν αίτησης στις αρμόδιες δικαστικές αρχές.

2. Οι αρμόδιες αρχές, όταν καθορίζουν το είδος και το επίπεδο διοικητικών κυρώσεων ή διορθωτικών μέτρων που πρέπει να επιβληθούν δυνάμει του άρθρου 50, λαμβάνουν υπόψη αν η παραβίαση τελέστηκε εκ προθέσεως ή εξ αμελείας, καθώς και όλες τις άλλες σχετικές περιστάσεις, μεταξύ των οποίων τα ακόλουθα, κατά περίπτωση:

α) τη σημαντικότητα, τη βαρύτητα και τη διάρκεια της παραβίασης,

β) τον βαθμό υπαιτιότητας του φυσικού ή νομικού προσώπου που ευθύνεται για την παραβίαση,

γ) την οικονομική ευρωστία του υπαίτιου φυσικού ή νομικού προσώπου,

δ) τη σημασία των κερδών που αποκομίστηκαν ή των ζημιών που αποφεύχθηκαν από το υπαίτιο φυσικό ή νομικό πρόσωπο, στον βαθμό που μπορούν να προσδιοριστούν,

ε) τις ζημίες τρίτων που προκλήθηκαν λόγω της παραβίασης, στον βαθμό που μπορούν να προσδιοριστούν,

στ) τον βαθμό συνεργασίας του υπαίτιου φυσικού ή νομικού προσώπου με την αρμόδια αρχή, με την επιφύλαξη της ανάγκης να διασφαλιστεί η παραίτηση του εν λόγω φυσικού ή νομικού προσώπου από αποκτηθέντα κέρδη ή αποφευχθείσες ζημίες,

ζ) προηγούμενες παραβιάσεις από το υπαίτιο φυσικό ή νομικό πρόσωπο.

Άρθρο 52

Ποινικές κυρώσεις

1. Τα κράτη μέλη δύνανται να αποφασίζουν να μην θεσπίσουν κανόνες σχετικά με τις διοικητικές κυρώσεις ή τα διορθωτικά μέτρα για παραβιάσεις που υπόκεινται σε ποινικές κυρώσεις βάσει του εθνικού τους δικαίου.

2. Σε περίπτωση που τα κράτη μέλη έχουν επιλέξει να θεσπίσουν ποινικές κυρώσεις σε περιπτώσεις παραβίασης του παρόντος κανονισμού, διασφαλίζουν ότι εφαρμόζονται κατάλληλα μέτρα ώστε οι αρμόδιες αρχές να διαθέτουν όλες τις απαραίτητες εξουσίες για να συνεργάζονται με τις δικαστικές, εισαγγελικές αρχές και τις αρχές ποινικής δικαιοσύνης εντός της δικαιοδοσίας τους, προκειμένου να λαμβάνουν συγκεκριμένες πληροφορίες σχετικά με ποινικές έρευνες ή κινηθείσες διαδικασίες σε σχέση με περιπτώσεις παραβίασης του παρόντος κανονισμού και να παρέχουν τις ίδιες πληροφορίες σε άλλες αρμόδιες αρχές, καθώς και στην ΕΑΤ, την ΕΑΚΑΑ και την ΕΑΑΕΣ, στο πλαίσιο της τήρησης των υποχρεώσεών τους όσον αφορά τη συνεργασία για τους σκοπούς του παρόντος κανονισμού.

Άρθρο 53

Απαιτήσεις κοινοποίησης

Τα κράτη μέλη κοινοποιούν τους νόμους, τους κανονισμούς και τις διοικητικές διατάξεις εφαρμογής του παρόντος κεφαλαίου, συμπεριλαμβανομένων ενδεχόμενων σχετικών ποινικών διατάξεων, στην Επιτροπή, την ΕΑΚΑΑ, την ΕΑΤ και την ΕΑΑΕΣ, έως τις 17 Ιανουαρίου 2025. Τα κράτη μέλη κοινοποιούν στην Επιτροπή, την ΕΑΚΑΑ, την ΕΑΤ και την ΕΑΑΕΣ, χωρίς αδικαιολόγητη καθυστέρηση, κάθε μεταγενέστερη τροποποίησή τους.

Άρθρο 54

Δημοσίευση διοικητικών κυρώσεων

1. Οι αρμόδιες αρχές δημοσιεύουν, χωρίς αδικαιολόγητη καθυστέρηση, στους επίσημους δικτυακούς τους τόπους κάθε απόφαση που επιβάλλει διοικητική κύρωση η οποία δεν επιδέχεται άσκηση προσφυγής, μόλις η απόφαση αυτή κοινοποιηθεί στο πρόσωπο στο οποίο επιβλήθηκε η κύρωση.

2. Η δημοσίευση που αναφέρεται στην παράγραφο 1 περιλαμβάνει πληροφορίες σχετικά με το είδος και τον χαρακτήρα της παραβίασης, την ταυτότητα των υπαίτιων προσώπων και τις επιβληθείσες κυρώσεις.

3. Όταν η αρμόδια αρχή, κατόπιν αξιολόγησης βάσει κατά περίπτωση εξέτασης, κρίνει ότι η δημοσίευση της ταυτότητας, στην περίπτωση νομικών προσώπων, ή της ταυτότητας και των δεδομένων προσωπικού χαρακτήρα, στην περίπτωση φυσικών προσώπων, θα ήταν δυσανάλογη, μεταξύ άλλων ενέχοντας κινδύνους σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα, θα έθετε σε κίνδυνο τη σταθερότητα των χρηματοοικονομικών αγορών ή τη διενέργεια υπό εξέλιξη ποινικής έρευνας, ή θα προξενούσε, στον βαθμό που μπορεί να προσδιοριστεί, δυσανάλογη ζημία στο συγκεκριμένο πρόσωπο, εγκρίνει μία από τις ακόλουθες λύσεις σε σχέση με την απόφαση επιβολής διοικητικής κύρωσης:

α) αναβάλλει τη δημοσίευσή της έως ότου παύσουν να συντρέχουν οι λόγοι για τη μη δημοσίευσή της,

β) τη δημοσιεύει σε ανώνυμη βάση, σύμφωνα με το εθνικό δίκαιο, ή

γ) απέχει από τη δημοσίευσή της, όταν οι επιλογές που αναφέρονται στα στοιχεία α) και β) θεωρούνται ανεπαρκείς ώστε να εγγυηθούν ότι δεν θα υπάρξει κίνδυνος για τη σταθερότητα των χρηματοοικονομικών αγορών ή σε περίπτωση που η δημοσίευση δεν θα ήταν αναλογική της επιείκειας της επιβληθείσας κύρωσης.

4. Σε περίπτωση απόφασης για δημοσίευση διοικητικής κύρωσης σε ανώνυμη βάση σύμφωνα με την παράγραφο 3 στοιχείο β), η δημοσίευση των σχετικών δεδομένων μπορεί να αναβληθεί.

5. Όταν αρμόδια αρχή δημοσιεύει απόφαση επιβολής διοικητικής κύρωσης κατά της οποίας ασκήθηκε προσφυγή ενώπιον των αρμόδιων δικαστικών αρχών, οι αρμόδιες αρχές προσθέτουν πάραυτα στον επίσημο δικτυακό τους τόπο τα στοιχεία αυτά και, σε μεταγενέστερο στάδιο, τυχόν επακόλουθες πληροφορίες σχετικά με την έκβαση της προσφυγής. Δημοσιεύεται επίσης κάθε δικαστική απόφαση που ακυρώνει απόφαση επιβολής διοικητικής κύρωσης.

6. Οι αρμόδιες αρχές διασφαλίζουν ότι τυχόν δημοσίευση σύμφωνα με τις παραγράφους 1 έως 4 θα παραμείνει στον επίσημο δικτυακό τόπο τους μόνο κατά το χρονικό διάστημα που απαιτείται για την προβολή του παρόντος άρθρου. Το διάστημα αυτό δεν υπερβαίνει τα πέντε έτη από τη δημοσίευση.

Άρθρο 55

Επαγγελματικό απόρρητο

1. Τυχόν εμπιστευτικές πληροφορίες που λαμβάνονται, ανταλλάσσονται ή διαβιβάζονται βάσει του παρόντος κανονισμού υπόκεινται στους όρους της παραγράφου 2 περί επαγγελματικού απορρήτου.

2. Η υποχρέωση τήρησης του επαγγελματικού απορρήτου ισχύει για όλα τα πρόσωπα που εργάζονται ή έχουν εργαστεί για τις αρμόδιες αρχές σύμφωνα με τον παρόντα κανονισμό ή για οποιαδήποτε αρχή ή επιχείρηση της αγοράς ή για οποιοδήποτε άλλο φυσικό ή νομικό πρόσωπο στο οποίο οι αρμόδιες αρχές έχουν αναθέσει τις εξουσίες τους, συμπεριλαμβανομένων των ελεγκτών και εμπειρογνωμόνων που προσλαμβάνονται από αυτές.

3. Απαγορεύεται η κοινοποίηση των πληροφοριών που καλύπτονται από το επαγγελματικό απόρρητο, συμπεριλαμβανομένης της ανταλλαγής πληροφοριών μεταξύ των αρμόδιων αρχών δυνάμει του παρόντος κανονισμού και των αρμόδιων αρχών που ορίζονται ή συστήνονται σύμφωνα την οδηγία (ΕΕ) 2022/2555 σε οποιοδήποτε άλλο πρόσωπο ή αρχή, εκτός εάν προβλέπεται από τις διατάξεις του ενωσιακού ή εθνικού δικαίου.·

4. Όλες οι πληροφορίες που ανταλλάσσονται μεταξύ των αρμόδιων αρχών δυνάμει του παρόντος κανονισμού και αφορούν επιχειρηματικές ή επιχειρησιακές συνθήκες και άλλες οικονομικές ή προσωπικές υποθέσεις θεωρούνται εμπιστευτικές και υπόκεινται στις απαιτήσεις τήρησης του επαγγελματικού απορρήτου, εκτός εάν η αρμόδια αρχή δηλώσει κατά τον χρόνο επικοινωνίας ότι η συγκεκριμένη πληροφορία δύναται να γνωστοποιηθεί ή εκτός εάν η γνωστοποίηση είναι αναγκαία στο πλαίσιο νομικών διαδικασιών.

Άρθρο 56

Προστασία δεδομένων

1. Οι ΕΕΑ και οι αρμόδιες αρχές επιτρέπεται να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα μόνον όταν αυτό είναι αναγκαίο για την εκπλήρωση των αντίστοιχων υποχρεώσεων και καθηκόντων τους δυνάμει του παρόντος κανονισμού, ιδίως όσον αφορά την έρευνα, την επιθεώρηση, το αίτημα παροχής πληροφοριών, την κοινοποίηση, τη δημοσίευση, την αξιολόγηση, την εξακρίβωση, την εκτίμηση και την κατάρτιση σχεδίων εποπτείας. Τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία σύμφωνα με τον κανονισμό (ΕΕ) 2016/679 ή τον κανονισμό (ΕΕ) 2018/1725, ανάλογα με την περίπτωση.

2. Εκτός εάν προβλέπεται διαφορετικά σε άλλες τομεακές πράξεις, τα δεδομένα προσωπικού χαρακτήρα που αναφέρονται στην παράγραφο 1 διατηρούνται μέχρι την εκπλήρωση των εφαρμοστέων εποπτικών καθηκόντων και, σε κάθε περίπτωση, για μέγιστο χρονικό διάστημα 15 ετών, εκτός από την περίπτωση εκκρεμών δικαστικών διαδικασιών που απαιτούν περαιτέρω διατήρηση των δεδομένων αυτών.

ΚΕΦΑΛΑΙΟ VIII

Κατ' εξουσιοδότηση πράξεις

Άρθρο 57

Άσκηση της εξουσιοδότησης

1. Ανατίθεται στην Επιτροπή η εξουσία να εκδίδει κατ' εξουσιοδότηση πράξεις υπό τους όρους του παρόντος άρθρου.

2. Η προβλεπόμενη στο άρθρο 31 παράγραφος 6 και στο άρθρο 43 παράγραφος 2 εξουσία έκδοσης κατ' εξουσιοδότηση πράξεων ανατίθεται στην Επιτροπή για περίοδο πέντε ετών από τις 17 Ιανουαρίου 2024. Η Επιτροπή υποβάλλει έκθεση σχετικά με τις εξουσίες που της έχουν ανατεθεί το αργότερο εννέα μήνες πριν από τη λήξη της περιόδου των πέντε ετών. Η εξουσιοδότηση ανανεώνεται σιωπηρά για περιόδους ίδιας διάρκειας, εκτός αν το Ευρωπαϊκό Κοινοβούλιο ή το Συμβούλιο προβάλουν αντιρρήσεις το αργότερο τρεις μήνες πριν από τη λήξη της κάθε περιόδου.

3. Η εξουσιοδότηση που προβλέπεται στο άρθρο 31 παράγραφος 6 και στο άρθρο 43 παράγραφος 2 μπορεί να ανακληθεί ανά πάσα στιγμή από το Ευρωπαϊκό Κοινοβούλιο ή το Συμβούλιο. Η απόφαση ανάκλησης περατώνει την εξουσιοδότηση που προσδιορίζεται στην εν λόγω απόφαση. Αρχίζει να ισχύει την επομένη της δημοσίευσης της απόφασης στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης* ή σε μεταγενέστερη ημερομηνία που ορίζεται σε αυτήν. Δεν θίγει το κύρος των κατ' εξουσιοδότηση πράξεων που ισχύουν ήδη.

4. Πριν από την έκδοση μιας κατ' εξουσιοδότηση πράξης, η Επιτροπή διεξάγει διαβουλεύσεις με εμπειρογνώμονες που ορίζουν τα κράτη μέλη σύμφωνα με τις αρχές της διοργανικής συμφωνίας της 13ης Απριλίου 2016 για τη βελτίωση του νομοθετικού έργου.

5. Μόλις εκδώσει μια κατ' εξουσιοδότηση πράξη, η Επιτροπή την κοινοποιεί ταυτόχρονα στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο.

6. Οι κατ' εξουσιοδότηση πράξεις που εκδίδονται σύμφωνα με το άρθρο 31 παράγραφος 6 και το άρθρο 43 παράγραφος 2 τίθενται σε ισχύ μόνον εάν δεν διατυπωθούν αντιρρήσεις είτε από το Ευρωπαϊκό Κοινοβούλιο είτε από το Συμβούλιο εντός προθεσμίας τριών μηνών από την κοινοποίηση της πράξης αυτής στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο ή εάν, πριν από τη λήξη της προθεσμίας αυτής, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο ενημερώσουν και τα δύο την Επιτροπή ότι δεν πρόκειται να προβάλουν αντιρρήσεις. Η προθεσμία αυτή παρατείνεται κατά τρεις μήνες κατόπιν πρωτοβουλίας του Ευρωπαϊκού Κοινοβουλίου ή του Συμβουλίου.

ΚΕΦΑΛΑΙΟ IX

Μεταβατικές και τελικές διατάξεις

Τμήμα I

Άρθρο 58

Ρήτρα επανεξέτασης

1. Έως τις 17 Ιανουαρίου 2028, η Επιτροπή, κατόπιν διαβούλευσης με τις ΕΕΑ και το ΕΣΣΚ, ανάλογα με την περίπτωση, επανεξετάζει και υποβάλλει στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο έκθεση, συνοδευόμενη από νομοθετική πρόταση. Η επανεξέταση περιλαμβάνει τουλάχιστον τα ακόλουθα:

α) τα κριτήρια ορισμού των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ σύμφωνα με το άρθρο 31 παράγραφος 2,

β) τον προαιρετικό χαρακτήρα της κοινοποίησης σημαντικών κυβερνοαπειλών, που αναφέρεται στο άρθρο 19,

γ) το καθεστώς που αναφέρεται στο άρθρο 31 παράγραφος 12 και τις εξουσίες του κύριου εποπτικού φορέα που προβλέπονται στο άρθρο 35 παράγραφος 1 στοιχείο δ) σημείο iv) πρώτη περίπτωση, με σκοπό την αξιολόγηση της αποτελεσματικότητας των εν λόγω διατάξεων όσον αφορά τη διασφάλιση της αποτελεσματικής εποπτείας κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ που είναι εγκατεστημένοι σε τρίτη χώρα, καθώς και της ανάγκης ίδρυσης θυγατρικής στην Ένωση.

Για τους σκοπούς του πρώτου εδαφίου του παρόντος στοιχείου, η επανεξέταση περιλαμβάνει ανάλυση του καθεστώτος που αναφέρεται στο άρθρο 31 παράγραφος 12, μεταξύ άλλων όσον αφορά την πρόσβαση των χρηματοοικονομικών οντοτήτων της Ένωσης σε υπηρεσίες από τρίτες χώρες και τη διαθεσιμότητα των εν λόγω υπηρεσιών στην αγορά της Ένωσης, και λαμβάνει υπόψη τις περαιτέρω εξελίξεις στις αγορές για τις υπηρεσίες που καλύπτονται από τον παρόντα κανονισμό, την πρακτική εμπειρία των χρηματοοικονομικών οντοτήτων και των χρηματοοικονομικών εποπτικών αρχών όσον αφορά την εφαρμογή και, αντίστοιχα, την εποπτεία του εν λόγω καθεστώτος, καθώς και τυχόν σχετικές ρυθμιστικές και εποπτικές εξελίξεις που σημειώνονται σε διεθνές επίπεδο,

δ) τη σκοπιμότητα της συμπερίληψης στο πεδίο εφαρμογής του παρόντος κανονισμού των χρηματοοικονομικών οντοτήτων που αναφέρονται στο άρθρο 2 παράγραφος 3 στοιχείο ε), οι οποίες κάνουν χρήση αυτοματοποιημένων συστημάτων πωλήσεων, υπό το πρίσμα των μελλοντικών εξελίξεων της αγοράς όσον αφορά τη χρήση των εν λόγω συστημάτων,

ε) τη λειτουργία και την αποτελεσματικότητα του ΔΚΕ όσον αφορά την υποστήριξη της συνέπειας της εποπτείας και της αποδοτικότητας της ανταλλαγής πληροφοριών εντός του πλαισίου εποπτείας.

2. Στο πλαίσιο της επανεξέτασης της οδηγίας (ΕΕ) 2015/2366, η Επιτροπή αξιολογεί την ανάγκη για αυξημένη κυβερνοανθεκτικότητα των συστημάτων πληρωμών και των δραστηριοτήτων επεξεργασίας πληρωμών, καθώς και τη σκοπιμότητα της επέκτασης του πεδίου εφαρμογής του παρόντος κανονισμού στους διαχειριστές συστημάτων πληρωμών και στις οντότητες που συμμετέχουν σε δραστηριότητες επεξεργασίας πληρωμών. Υπό το πρίσμα της αξιολόγησης αυτής, η Επιτροπή υποβάλλει, στο πλαίσιο της επανεξέτασης της οδηγίας (ΕΕ) 2015/2366, έκθεση στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο το αργότερο έως τις 17 Ιουλίου 2023.

Με βάση την εν λόγω έκθεση επανεξέτασης και κατόπιν διαβούλευσης με τις ΕΕΑ, την ΕΚΤ και το ΕΣΣΚ, η Επιτροπή μπορεί να υποβάλει, κατά περίπτωση και στο πλαίσιο της νομοθετικής πρότασης που μπορεί να εγκρίνει σύμφωνα με το άρθρο 108 δεύτερο εδάφιο της οδηγίας (ΕΕ) 2015/2366, πρόταση για να εξασφαλιστεί ότι όλοι οι φορείς εκμετάλλευσης συστημάτων πληρωμών και οι οντότητες που συμμετέχουν σε δραστηριότητες επεξεργασίας πληρωμών υπόκεινται σε κατάλληλη εποπτεία, λαμβάνοντας παράλληλα υπόψη την υφιστάμενη εποπτεία της κεντρικής τράπεζας.

3. Έως τις 17 Ιανουαρίου 2026, η Επιτροπή, κατόπιν διαβούλευσης με τις ΕΕΑ και την Επιτροπή Ευρωπαϊκών Φορέων Εποπτείας των Ελεγκτών, επανεξετάζει και υποβάλλει στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο έκθεση, συνοδευόμενη, κατά περίπτωση, από νομοθετική πρόταση, σχετικά με την καταλληλότητα των ενισχυμένων απαιτήσεων για τους νόμιμους ελεγκτές και τα ελεγκτικά γραφεία όσον αφορά την ψηφιακή επιχειρησιακή ανθεκτικότητα, μέσω της συμπερίληψης νόμιμων ελεγκτών και ελεγκτικών γραφείων στο πεδίο εφαρμογής του παρόντος κανονισμού ή μέσω τροποποιήσεων της οδηγίας 2006/43/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([39]).

ΤΜΉΜΑ ΙΙ

Τροποποιήσεις

Άρθρο 59

Τροποποιήσεις του κανονισμού (ΕΚ) αριθ. 1060/2009

Ο κανονισμός (ΕΚ) αριθ. 1060/2009 τροποποιείται ως εξής:

1) Στο παράρτημα Ι τμήμα Α σημείο 4), το πρώτο εδάφιο αντικαθίσταται από το ακόλουθο κείμενο:

«Ο οργανισμός αξιολόγησης πιστοληπτικής ικανότητας διαθέτει υγιείς διοικητικές και λογιστικές διαδικασίες, μηχανισμούς εσωτερικού ελέγχου, αποτελεσματικές διαδικασίες αξιολόγησης κινδύνων, καθώς και αποτελεσματικές ρυθμίσεις ελέγχου και προστασίας για τη διαχείριση των συστημάτων ΤΠΕ σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (*).

(*) Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (ΕΕ L 333 της 27.12.2022, σ. 1).».

2) Στο παράρτημα ΙΙΙ, το σημείο 12) αντικαθίσταται από το ακόλουθο κείμενο:

«12. Ο οργανισμός αξιολόγησης πιστοληπτικής ικανότητας παραβαίνει το άρθρο 6 παράγραφος 2, σε συνδυασμό με το σημείο 4) της ενότητας Α του παραρτήματος Ι, όταν δεν διαθέτει ορθές διοικητικές ή λογιστικές διαδικασίες, μηχανισμούς εσωτερικού ελέγχου, αποτελεσματικές διαδικασίες αξιολόγησης κινδύνων ή αποτελεσματικές ρυθμίσεις ελέγχου και προστασίας για τη διαχείριση συστημάτων ΤΠΕ σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554 ή όταν δεν εφαρμόζει ή δεν διατηρεί διαδικασίες λήψης αποφάσεων ή οργανωτική διάρθρωση κατά τα απαιτούμενα από το εν λόγω σημείο.».

Άρθρο 60

Τροποποιήσεις του κανονισμού (ΕΕ) αριθ. 648/2012

Ο κανονισμός (ΕΕ) αριθ. 648/2012 τροποποιείται ως εξής:

1) Το άρθρο 26 τροποποιείται ως εξής:

α) η παράγραφος 3 αντικαθίσταται από το ακόλουθο κείμενο:

«3. Ο κεντρικός αντισυμβαλλόμενος διατηρεί και εφαρμόζει οργανωτική δομή η οποία διασφαλίζει τη συνέχεια και την εύρυθμη λειτουργία κατά την παροχή των υπηρεσιών και την άσκηση των δραστηριοτήτων του. Χρησιμοποιεί κατάλληλα και ανάλογα συστήματα, πόρους και διαδικασίες, συμπεριλαμβανομένων συστημάτων ΤΠΕ τα οποία διαχειρίζεται σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (*).

(*) Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (ΕΕ L 333 της 27.12.2022, σ. 1).»·

([39]) Οδηγία 2006/43/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Μαΐου 2006**,** για τους υποχρεωτικούς ελέγχους των ετήσιων και των ενοποιημένων λογαριασμών, για την τροποποίηση των οδηγιών 78/660/ΕΟΚ και 83/349/ΕΟΚ του Συμβουλίου και για την κατάργηση της οδηγίας 84/253/ΕΟΚ του Συμβουλίου (ΕΕ L 157 της 9.6.2006, σ. 87).

β) η παράγραφος 6 διαγράφεται.

2) Το άρθρο 34 τροποποιείται ως εξής:

α) η παράγραφος 1 αντικαθίσταται από το ακόλουθο κείμενο:

«1. Ο κεντρικός αντισυμβαλλόμενος διαμορφώνει, εφαρμόζει και διατηρεί κατάλληλη πολιτική επιχειρησιακής συνέχειας και σχέδιο ανάκαμψης της λειτουργίας μετά από καταστροφή, στα οποία περιλαμβάνονται σχέδια πολιτικής επιχειρησιακής συνέχειας και αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ που λειτουργούν και εφαρμόζονται σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554 με σκοπό να διασφαλίσει τη διατήρηση των λειτουργιών του, την έγκαιρη αποκατάσταση των εργασιών και την εκπλήρωση των υποχρεώσεων του κεντρικού αντισυμβαλλομένου.»·

β) στην παράγραφο 3, το πρώτο εδάφιο αντικαθίσταται από το ακόλουθο κείμενο:

«3. Για να εξασφαλιστεί συνεπής εφαρμογή του παρόντος άρθρου, η ΕΑΚΑΑ, μετά από διαβούλευση με τα μέλη του ΕΣΚΤ, καταρτίζει σχέδια ρυθμιστικών τεχνικών προτύπων που να διευκρινίζουν το ελάχιστο περιεχόμενο και τις απαιτήσεις της πολιτικής επιχειρησιακής συνέχειας και του σχεδίου ανάκαμψης της λειτουργίας μετά από καταστροφή, με εξαίρεση τα σχέδια πολιτικής επιχειρησιακής συνέχειας και ανάκαμψης της λειτουργίας των ΤΠΕ μετά από καταστροφή.».

3) Στο άρθρο 56 παράγραφος 3, το πρώτο εδάφιο αντικαθίσταται από το ακόλουθο κείμενο:

«3. Προκειμένου να διασφαλίσει τη συνεπή εφαρμογή του παρόντος άρθρου, η ΕΑΚΑΑ καταρτίζει σχέδια ρυθμιστικών τεχνικών προτύπων για τον καθορισμό των λεπτομερών στοιχείων της αίτησης καταχώρισης που αναφέρεται στην παράγραφο 1, εκτός των απαιτήσεων που αφορούν τη διαχείριση κινδύνων ΤΠΕ.».

4) Στο άρθρο 79, οι παράγραφοι 1 και 2 αντικαθίστανται από το ακόλουθο κείμενο:

«1. Το αρχείο καταγραφής συναλλαγών εντοπίζει τις πηγές λειτουργικού κινδύνου και τις ελαχιστοποιεί, με την ανάπτυξη επίσης κατάλληλων συστημάτων, δικλείδων ασφάλειας και διαδικασιών, συμπεριλαμβανομένων συστημάτων ΤΠΕ τα οποία διαχειρίζεται σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554

2. Το αρχείο καταγραφής συναλλαγών διαμορφώνει, εφαρμόζει και διατηρεί κατάλληλη πολιτική επιχειρησιακής συνέχειας και σχέδιο ανάκαμψης της λειτουργίας μετά από καταστροφή, συμπεριλαμβανομένων σχεδίων πολιτικής επιχειρησιακής συνέχειας και αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ τα οποία καταρτίζονται σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554 με σκοπό να διασφαλίσει τη διατήρηση των λειτουργιών του, την έγκαιρη αποκατάσταση των εργασιών και την εκπλήρωση των υποχρεώσεων του αρχείου καταγραφής συναλλαγών.».

5) Στο άρθρο 80, η παράγραφος 1 διαγράφεται.

6) Στο παράρτημα Ι, το τμήμα ΙΙ τροποποιείται ως εξής:

α) τα στοιχεία α) και β) αντικαθίστανται από το ακόλουθο κείμενο:

«α) το αρχείο καταγραφής συναλλαγών παραβαίνει το άρθρο 79 παράγραφος 1 όταν δεν εντοπίζει τις πηγές λειτουργικού κινδύνου ή δεν ελαχιστοποιεί αυτούς τους κινδύνους με την ανάπτυξη κατάλληλων συστημάτων, δικλείδων ασφάλειας και διαδικασιών, συμπεριλαμβανομένων συστημάτων ΤΠΕ τα οποία διαχειρίζεται σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554

β) το αρχείο καταγραφής συναλλαγών παραβαίνει το άρθρο 79 παράγραφος 2 όταν δεν καταρτίζει, δεν εφαρμόζει ή δεν διατηρεί κατάλληλο σχέδιο επιχειρησιακής συνέχειας και ανάκαμψης της λειτουργίας μετά από καταστροφή, το οποίο καταρτίζεται σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554 με σκοπό να διασφαλίσει τη διατήρηση των λειτουργιών του, την έγκαιρη αποκατάσταση των εργασιών και την εκπλήρωση των υποχρεώσεων του αρχείου καταγραφής συναλλαγών·»·

β) το στοιχείο γ) διαγράφεται.

7) Το παράρτημα ΙΙΙ τροποποιείται ως εξής:

α) το τμήμα ΙΙ τροποποιείται ως εξής:

i) το στοιχείο γ) αντικαθίσταται από το ακόλουθο κείμενο:

«γ) κεντρικός αντισυμβαλλόμενος κατηγορίας 2 παραβαίνει το άρθρο 26 παράγραφος 3 όταν δεν διατηρεί ή δεν εφαρμόζει οργανωτική δομή που διασφαλίζει τη συνέχεια και την εύρυθμη λειτουργία κατά την εκτέλεση των υπηρεσιών και των δραστηριοτήτων του ή όταν δεν χρησιμοποιεί κατάλληλα και αναλογικά συστήματα, πόρους ή διαδικασίες, συμπεριλαμβανομένων των συστημάτων ΤΠΕ τα οποία διαχειρίζεται σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554»·

ii) το στοιχείο στ) διαγράφεται·

β) στο τμήμα III, το στοιχείο α) αντικαθίσταται από το ακόλουθο κείμενο:

«α) κεντρικός αντισυμβαλλόμενος κατηγορίας 2 παραβαίνει το άρθρο 34 παράγραφος 1 όταν δεν διαμορφώνει, δεν εφαρμόζει και δεν διατηρεί κατάλληλη πολιτική επιχειρησιακής συνέχειας και σχέδιο αντιμετώπισης και ανάκαμψης το οποίο καταρτίζεται σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554 με σκοπό να διασφαλίσει τη διατήρηση των λειτουργιών του, την έγκαιρη αποκατάσταση των εργασιών και την εκπλήρωση των υποχρεώσεων του κεντρικού αντισυμβαλλομένου, η οποία επιτρέπει τουλάχιστον την αποκατάσταση όλων των συναλλαγών κατά τη στιγμή της διαταραχής, ώστε να είναι σε θέση ο κεντρικός αντισυμβαλλόμενος να εξακολουθήσει να λειτουργεί με ασφάλεια και να ολοκληρώσει τον διακανονισμό στην καθορισμένη ημερομηνία·».

Άρθρο 61

Τροποποιήσεις του κανονισμού (ΕΕ) αριθ. 909/2014

Το άρθρο 45 του κανονισμού (ΕΕ) αριθ. 909/2014 τροποποιείται ως εξής:

1) Η παράγραφος 1 αντικαθίσταται από το ακόλουθο κείμενο:

«1. Το ΚΑΤ προσδιορίζει όλες τις πηγές λειτουργικού κινδύνου, εσωτερικές και εξωτερικές, και ελαχιστοποιεί τον αντίκτυπό τους μέσω της ανάπτυξης κατάλληλων εργαλείων, διαδικασιών και πολιτικών ΤΠΕ που έχουν θεσπιστεί και τελούν υπό διαχείριση σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (*), καθώς και μέσω οποιωνδήποτε άλλων σχετικών κατάλληλων εργαλείων, δικλείδων ασφάλειας και διαδικασιών για άλλα είδη λειτουργικού κινδύνου, μεταξύ άλλων για όλα τα συστήματα διακανονισμού αξιογράφων που διαχειρίζεται.

(*) Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014 και, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (ΕΕ L 333 της 27.12.2022, σ. 1).».

2) Η παράγραφος 2 διαγράφεται.

3) Οι παράγραφοι 3 και 4 αντικαθίστανται από το ακόλουθο κείμενο:

«3. Για τις υπηρεσίες που παρέχει καθώς και για κάθε σύστημα διακανονισμού αξιογράφων που διαχειρίζεται, το ΚΑΤ διαμορφώνει, εφαρμόζει και διατηρεί κατάλληλη πολιτική επιχειρησιακής συνέχειας και σχέδιο ανάκαμψης της λειτουργίας μετά από καταστροφή, συμπεριλαμβανομένων πολιτικής επιχειρησιακής συνέχειας και σχεδίων αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ μετά από καταστροφή τα οποία καταρτίζονται σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554 για να διασφαλίσει τη διατήρηση των υπηρεσιών του, την έγκαιρη αποκατάσταση των εργασιών και την εκπλήρωση των υποχρεώσεών του, σε περίπτωση γεγονότων που συνεπάγονται σημαντικό κίνδυνο διαταραχής των λειτουργιών.

4. Το σχέδιο που αναφέρεται στην παράγραφο 3 προβλέπει την αποκατάσταση όλων των συναλλαγών και των θέσεων των συμμετεχόντων κατά τον χρόνο της διακοπής, ώστε να μπορέσουν οι συμμετέχοντες του ΚΑΤ να εξακολουθήσουν να λειτουργούν με ασφάλεια και να ολοκληρώσουν τον διακανονισμό στην καθορισμένη ημερομηνία, μεταξύ άλλων διασφαλίζοντας ότι τα κρίσιμα συστήματα ΤΠ μπορούν ταχέως να αποκαταστήσουν τη λειτουργία τους ως είχε κατά τη στιγμή της διαταραχής, όπως προβλέπεται στο άρθρο 12 παράγραφοι 5 και 7 του κανονισμού (ΕΕ) 2022/2554».

4) Η παράγραφος 6 αντικαθίσταται από το ακόλουθο κείμενο:

«6. Το ΚΑΤ προσδιορίζει, παρακολουθεί και διαχειρίζεται τους κινδύνους που ενδέχεται να συνεπάγονται για τις δραστηριότητές του οι βασικοί συμμετέχοντες στα συστήματα διακανονισμού αξιογράφων που διαχειρίζεται, καθώς και οι πάροχοι υπηρεσιών και υπηρεσιών κοινής ωφελείας, άλλα ΚΑΤ ή άλλες υποδομές της αγοράς. Παρέχει πληροφορίες στις αρμόδιες και τις σχετικές αρχές, κατόπιν αιτήματος, σχετικά με οποιονδήποτε τέτοιον κίνδυνο εντοπιστεί. Ενημερώνει επίσης χωρίς καθυστέρηση την αρμόδια αρχή και τις σχετικές αρχές σχετικά με οποιαδήποτε περιστατικά που αφορούν τη λειτουργία του, εκτός των συμβάντων που σχετίζονται με κινδύνους ΤΠΕ, και οφείλονται στους εν λόγω κινδύνους.».

5) Στην παράγραφο 7, το πρώτο εδάφιο αντικαθίσταται από το ακόλουθο κείμενο:

«7. Η ΕΑΚΑΑ, σε στενή συνεργασία με τα μέλη του ΕΣΚΤ, καταρτίζει σχέδια ρυθμιστικών τεχνικών προτύπων για να εξειδικεύσει τους λειτουργικούς κινδύνους που αναφέρονται στις παραγράφους 1 και 6, πλην του κινδύνου ΤΠΕ, τις μεθόδους ελέγχου, αντιμετώπισης ή ελαχιστοποίησης των εν λόγω κινδύνων, συμπεριλαμβανομένων των πολιτικών επιχειρησιακής συνέχειας και των σχεδίων ανάκαμψης της λειτουργίας μετά από καταστροφή, που αναφέρονται στις παραγράφους 3 και 4, καθώς και των μεθόδων αξιολόγησής τους.».

Άρθρο 62

Τροποποιήσεις του κανονισμού (ΕΕ) αριθ. 600/2014

Ο κανονισμός (ΕΕ) αριθ. 600/2014 τροποποιείται ως εξής:

1) Το άρθρο 27ζ τροποποιείται ως εξής:

α) η παράγραφος 4 αντικαθίσταται από το ακόλουθο κείμενο:

«4. Οι ΕΜΔ συμμορφώνονται με τις απαιτήσεις σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών που ορίζονται στον κανονισμό (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (*).

_____

(*) Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014 και, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (ΕΕ L 333 της 27.12.2022, σ. 1).»·

β) στην παράγραφο 8, το στοιχείο γ) αντικαθίσταται από το ακόλουθο κείμενο:

«γ) τις συγκεκριμένες οργανωτικές απαιτήσεις που ορίζονται στις παραγράφους 3 και 5.».

2) Το άρθρο 27η τροποποιείται ως εξής:

α) η παράγραφος 5 αντικαθίσταται από το ακόλουθο κείμενο:

«5. Οι ΠΕΔ συμμορφώνονται με τις απαιτήσεις σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών που ορίζονται στον κανονισμό (ΕΕ) 2022/2554»·

β) στην παράγραφο 8, το στοιχείο ε) αντικαθίσταται από το ακόλουθο κείμενο:

«ε) τις συγκεκριμένες οργανωτικές απαιτήσεις που ορίζονται στην παράγραφο 4.».

3) Το άρθρο 27θ τροποποιείται ως εξής:

α) η παράγραφος 3 αντικαθίσταται από το ακόλουθο κείμενο:

«3. Οι ΕΜΑ συμμορφώνονται με τις απαιτήσεις σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών που ορίζονται στον κανονισμό (ΕΕ) 2022/2554»·

β) στην παράγραφο 5, το στοιχείο β) αντικαθίσταται από το ακόλουθο κείμενο:

«β) τις συγκεκριμένες οργανωτικές απαιτήσεις που ορίζονται στις παραγράφους 2 και 4.».

Άρθρο 63

Τροποποίηση του κανονισμού (ΕΕ) 2016/1011

Στο άρθρο 6 του κανονισμού (ΕΕ) 2016/1011, προστίθεται η ακόλουθη παράγραφος:

«6. Για τους δείκτες αναφοράς κρίσιμης σημασίας, ένας διαχειριστής διαθέτει υγιείς διοικητικές και λογιστικές διαδικασίες, μηχανισμούς εσωτερικού ελέγχου, αποτελεσματικές διαδικασίες αξιολόγησης κινδύνων, καθώς και αποτελεσματικές ρυθμίσεις ελέγχου και προστασίας για τη διαχείριση των συστημάτων ΤΠΕ σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (*).·

_____

(*) Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014 και, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (ΕΕ L 333 της 27.12.2022, σ. 1).».

Άρθρο 64

Έναρξη ισχύος και εφαρμογή

Ο παρών κανονισμός αρχίζει να ισχύει την εικοστή ημέρα από τη δημοσίευσή του στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

Εφαρμόζεται από τις 17 Ιανουαρίου 2025.

Ο παρών κανονισμός είναι δεσμευτικός ως προς όλα τα μέρη του και ισχύει άμεσα σε κάθε κράτος μέλος.

Στρασβούργο, 14 Δεκεμβρίου 2022.

Για το Ευρωπαϊκό Κοινοβούλιο	*Για το Συμβούλιο*
Η Πρόεδρος	*Ο Πρόεδρος*
R. METSOLA	M. BEK

ΟΔΗΓΙΕΣ

ΟΔΗΓΙΑ (ΕΕ) 2022/2555 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

της 14ης Δεκεμβρίου 2022

σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2)

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης, και ιδίως το άρθρο 114,

Έχοντας υπόψη την πρόταση της Ευρωπαϊκής Επιτροπής,

Κατόπιν διαβίβασης του σχεδίου νομοθετικής πράξης στα εθνικά κοινοβούλια,

Έχοντας υπόψη τη γνώμη της Ευρωπαϊκής Κεντρικής Τράπεζας ([1]),

Έχοντας υπόψη τη γνώμη της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής ([2]),

Αφού ζήτησαν τη γνώμη της Επιτροπής των Περιφερειών,

Αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία ([3]),

Εκτιμώντας τα ακόλουθα:

(1) Η οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([4]) αποσκοπούσε στην ανάπτυξη ικανοτήτων κυβερνοασφάλειας σε ολόκληρη την Ένωση, στον μετριασμό των απειλών για τα συστήματα δικτύου και πληροφοριών που χρησιμοποιούνται για την παροχή βασικών υπηρεσιών σε σημαντικούς τομείς και στη διασφάλιση της συνέχειας των υπηρεσιών αυτών κατά την αντιμετώπιση περιστατικών, ώστε να συμβάλει στην ασφάλεια και στην αποτελεσματική λειτουργία της οικονομίας και της κοινωνίας της Ένωσης.

(2) Μετά την έναρξη ισχύος της οδηγίας (ΕΕ) 2016/1148, έχει σημειωθεί σημαντική πρόοδος στην αύξηση του επιπέδου κυβερνοανθεκτικότητας της Ένωσης. Η επανεξέταση της εν λόγω οδηγίας κατέδειξε ότι αυτή λειτούργησε ως καταλύτης για τη θεσμική και κανονιστική προσέγγιση της κυβερνοασφάλειας στην Ένωση καθώς προετοίμασε το έδαφος για μια σημαντική αλλαγή νοοτροπίας. Με την οδηγία διασφαλίστηκε η ολοκλήρωση των εθνικών πλαισίων για την ασφάλεια των συστημάτων δικτύου και πληροφοριών με τη θέσπιση εθνικών στρατηγικών για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, τη θέσπιση εθνικών ικανοτήτων και με την εφαρμογή ρυθμιστικών μέτρων τα οποία καλύπτουν βασικές υποδομές και οντότητες που προσδιορίζονται από κάθε κράτος μέλος. Η οδηγία (ΕΕ) 2016/1148 συνέβαλε επίσης στη συνεργασία σε επίπεδο Ένωσης μέσω της σύστασης της ομάδας συνεργασίας και του δικτύου εθνικών ομάδων αντιμετώπισης περιστατικών ασφάλειας υπολογιστών. Παρά τα επιτεύγματα αυτά, η επανεξέταση της οδηγίας (ΕΕ) 2016/1148 αποκάλυψε εγγενείς αδυναμίες που την εμποδίζουν να αντιμετωπίσει αποτελεσματικά τις τρέχουσες και τις αναδυόμενες προκλήσεις στον τομέα της κυβερνοασφάλειας.

(3) Τα συστήματα δικτύου και πληροφοριών έχουν εξελιχθεί σε κεντρικό στοιχείο της καθημερινής ζωής με τον ταχύ ψηφιακό μετασχηματισμό και τη διασύνδεση της κοινωνίας, μεταξύ άλλων στις διασυνοριακές ανταλλαγές. Η εξέλιξη αυτή έχει οδηγήσει σε επέκταση του τοπίου των κυβερνοαπειλών, γεγονός που δημιουργεί νέες προκλήσεις οι οποίες απαιτούν προσαρμοσμένες, συντονισμένες και καινοτόμες αποκρίσεις σε όλα τα κράτη μέλη. Ο αριθμός, το μέγεθος, η επινοητικότητα, η συχνότητα και ο αντίκτυπος των περιστατικών αυξάνονται και συνιστούν μείζονα απειλή για τη λειτουργία των συστημάτων δικτύου και πληροφοριών. Ως εκ τούτου, τα περιστατικά μπορούν να παρεμποδίσουν την άσκηση οικονομικών δραστηριοτήτων στην εσωτερική αγορά, να προκαλέσουν οικονομικές απώλειες, να υπονομεύσουν την

([1]) ΕΕ C 233 της 16.6.2022, σ. 22.
([2]) ΕΕ C 286 της 16.7.2021, σ. 170.
([3]) Θέση του Ευρωπαϊκού Κοινοβουλίου της 10ης Νοεμβρίου 2022 (δεν έχει ακόμη δημοσιευθεί στην Επίσημη Εφημερίδα) και απόφαση του Συμβουλίου της 28ης Νοεμβρίου 2022.
([4]) Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση (ΕΕ L 194 της 19.7.2016, σ. 1).

εμπιστοσύνη των χρηστών και να προκαλέσουν σοβαρή ζημία στην οικονομία και την κοινωνία της Ένωσης. Ως εκ τούτου, η ετοιμότητα και η αποτελεσματικότητα στον τομέα της κυβερνοασφάλειας είναι πλέον πιο σημαντικές από ποτέ για την ορθή λειτουργία της εσωτερικής αγοράς. Επιπλέον, σε πολλούς κρίσιμους τομείς η κυβερνοασφάλεια αποτελεί βασικό παράγοντα για την αποδοχή του ψηφιακού μετασχηματισμού και την πλήρη αξιοποίηση των οικονομικών, κοινωνικών και βιώσιμων οφελών της ψηφιοποίησης.

(4) Η νομική βάση της οδηγίας (ΕΕ) 2016/1148 ήταν το άρθρο 114 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ), στόχος του οποίου είναι η εγκαθίδρυση και η λειτουργία της εσωτερικής αγοράς με την ενίσχυση των μέτρων για την προσέγγιση των εθνικών κανόνων. Οι απαιτήσεις κυβερνοασφάλειας που επιβάλλονται στις οντότητες που παρέχουν υπηρεσίες ή ασκούν οικονομικά σημαντικές δραστηριότητες ποικίλλουν σημαντικά μεταξύ των κρατών μελών ως προς το είδος των απαιτήσεων, τον βαθμό λεπτομέρειάς τους και τη μέθοδο εποπτείας. Οι διαφορές αυτές συνεπάγονται πρόσθετο κόστος και προκαλούν δυσκολίες στις οντότητες που προσφέρουν αγαθά ή υπηρεσίες διασυνοριακά. Απαιτήσεις που επιβάλλονται από ένα κράτος μέλος και οι οποίες διαφέρουν, ή ακόμη και έρχονται σε αντίθεση με αυτές που επιβάλλει άλλο κράτος μέλος, ενδέχεται να επηρεάσουν σημαντικά τις εν λόγω διασυνοριακές δραστηριότητες. Επιπλέον, η πιθανότητα ανεπαρκούς σχεδιασμού ή εφαρμογής των απαιτήσεων κυβερνοασφάλειας σε ένα κράτος μέλος είναι πιθανό να έχει επιπτώσεις στο επίπεδο κυβερνοασφάλειας άλλων κρατών μελών, ιδίως δεδομένης της έντασης των διασυνοριακών ανταλλαγών. Η επανεξέταση της οδηγίας (ΕΕ) 2016/1148 κατέδειξε μεγάλη απόκλιση στην εφαρμογή της από τα κράτη μέλη, μεταξύ άλλων όσον αφορά το πεδίο εφαρμογής της, η οριοθέτηση του οποίου επαφίεται σε μεγάλο βαθμό στη διακριτική ευχέρεια των κρατών μελών. Η οδηγία (ΕΕ) 2016/1148 παρείχε επίσης ευρύτατη διακριτική ευχέρεια στα κράτη μέλη όσον αφορά την εφαρμογή των υποχρεώσεων σχετικά με την ασφάλεια και την αναφορά των περιστατικών που ορίζονται στην εν λόγω οδηγία. Ως εκ τούτου, οι υποχρεώσεις αυτές εκπληρώθηκαν με πολύ διαφορετικούς τρόπους σε εθνικό επίπεδο. Παρόμοιες αποκλίσεις υπάρχουν στην εφαρμογή των διατάξεων της οδηγίας (ΕΕ) 2016/1148 για την εποπτεία και την επιβολή.

(5) Όλες αυτές οι αποκλίσεις έχουν ως αποτέλεσμα τον κατακερματισμό της εσωτερικής αγοράς και ενδέχεται να έχουν αρνητικές επιπτώσεις στη λειτουργία της, επηρεάζοντας ιδίως τη διασυνοριακή παροχή υπηρεσιών και το επίπεδο κυβερνοανθεκτικότητας λόγω της εφαρμογής πολλαπλών μέτρων. Εντέλει, οι αποκλίσεις αυτές θα μπορούσαν να οδηγήσουν στη μεγαλύτερη ευπάθεια ορισμένων κρατών μελών έναντι κυβερνοαπειλών, με δυνητικές δευτερογενείς επιπτώσεις σε ολόκληρη την Ένωση. Η παρούσα οδηγία αποσκοπεί στην εξάλειψη αυτών των μεγάλων αποκλίσεων μεταξύ των κρατών μελών, ιδίως με τον καθορισμό ελάχιστων κανόνων σχετικά με τη λειτουργία ενός συντονισμένου κανονιστικού πλαισίου, με τη θέσπιση μηχανισμών για την αποτελεσματική συνεργασία μεταξύ των αρμόδιων αρχών σε κάθε κράτος μέλος, με την επικαιροποίηση του καταλόγου των τομέων και δραστηριοτήτων που υπόκεινται σε υποχρεώσεις κυβερνοασφάλειας και με τη θέσπιση αποτελεσματικών ένδικων μέσων και μέτρων επιβολής που έχουν καθοριστική σημασία για την αποτελεσματική επιβολή των εν λόγω υποχρεώσεων. Ως εκ τούτου, η οδηγία (ΕΕ) 2016/1148 θα πρέπει να καταργηθεί και να αντικατασταθεί από την παρούσα οδηγία.

(6) Με την κατάργηση της οδηγίας (ΕΕ) 2016/1148, το πεδίο εφαρμογής ανά τομείς θα πρέπει να επεκταθεί σε μεγαλύτερο μέρος της οικονομίας για να παρέχεται ολοκληρωμένη κάλυψη των τομέων και υπηρεσιών ζωτικής σημασίας για βασικές κοινωνιακές και οικονομικές δραστηριότητες στην εσωτερική αγορά. Ειδικότερα, η παρούσα οδηγία αποσκοπεί στην αντιμετώπιση των ελλείψεων λόγω της διαφοροποίησης μεταξύ των φορέων εκμετάλλευσης βασικών υπηρεσιών και των παρόχων ψηφιακών υπηρεσιών, η οποία έχει αποδειχθεί παρωχημένη, δεδομένου ότι δεν αποτυπώνει τη σημασία των τομέων ή των υπηρεσιών για τις κοινωνικές και οικονομικές δραστηριότητες στην εσωτερική αγορά.

(7) Σύμφωνα με την οδηγία (ΕΕ) 2016/1148, τα κράτη μέλη έφεραν την ευθύνη του προσδιορισμού των οντοτήτων που πληρούν τα κριτήρια του ορισμού του φορέα εκμετάλλευσης βασικών υπηρεσιών. Προκειμένου να εξαλειφθούν οι μεγάλες αποκλίσεις μεταξύ των κρατών μελών ως προς το θέμα αυτό και να διασφαλιστεί για όλες τις σχετικές οντότητες ασφάλεια δικαίου όσον αφορά τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και τις υποχρεώσεις αναφοράς περιστατικών, θα πρέπει να θεσπιστεί ενιαίο κριτήριο για τον προσδιορισμό των οντοτήτων που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας. Το κριτήριο αυτό θα πρέπει να συνίσταται στην εφαρμογή ενός κανόνα ανώτατου ορίου μεγέθους, σύμφωνα με τον οποίο όλες οι οντότητες που χαρακτηρίζονται μεσαίες επιχειρήσεις δυνάμει του άρθρου 2 του παραρτήματος της σύστασης 2003/361/ΕΚ της Επιτροπής ([5]) ή υπερβαίνουν τα ανώτατα όρια για τις μεσαίες επιχειρήσεις

([5]) Σύσταση 2003/361/ΕΚ της Επιτροπής, της 6ης Μαΐου 2003, σχετικά με τον ορισμό των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων (ΕΕ L 124 της 20.5.2003, σ. 36).

που προβλέπονται στην παράγραφο 1 του εν λόγω άρθρου και που δραστηριοποιούνται στους τομείς και παρέχουν τα είδη υπηρεσιών ή ασκούν τις δραστηριότητες που καλύπτονται από την παρούσα οδηγία εμπίπτουν στο πεδίο εφαρμογής του. Τα κράτη μέλη θα πρέπει επίσης να προβλέπουν ότι ορισμένες μικρές επιχειρήσεις και πολύ μικρές επιχειρήσεις, όπως καθορίζονται στο άρθρο 2 παράγραφοι 2 και 3 του εν λόγω παραρτήματος, που πληρούν ειδικά κριτήρια τα οποία υποδεικνύουν βασικό ρόλο για την κοινωνία, την οικονομία ή για συγκεκριμένους τομείς ή τύπους υπηρεσιών εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας.

(8) Η εξαίρεση των οντοτήτων δημόσιας διοίκησης από το πεδίο εφαρμογής της παρούσας οδηγίας θα πρέπει να εφαρμόζεται σε οντότητες των οποίων οι δραστηριότητες εντάσσονται κατά κύριο λόγο στους τομείς της εθνικής ασφάλειας, της δημόσιας ασφάλειας, της άμυνας, ή της επιβολής του νόμου, συμπεριλαμβανομένης της πρόληψης, της διερεύνησης, της διαπίστωσης και της δίωξης ποινικών αδικημάτων. Ωστόσο, οι οντότητες δημόσιας διοίκησης των οποίων οι δραστηριότητες συνδέονται μόνο οριακά με τους εν λόγω τομείς δεν θα πρέπει να εξαιρεθούν από το πεδίο εφαρμογής της παρούσας οδηγίας. Για τους σκοπούς της παρούσας οδηγίας, οι οντότητες με ρυθμιστικές αρμοδιότητες δεν θεωρείται ότι ασκούν δραστηριότητες στον τομέα της επιβολής του νόμου και, επομένως, δεν εξαιρούνται για τον λόγο αυτό από το πεδίο εφαρμογής της παρούσας οδηγίας. Οι φορείς δημόσιας διοίκησης που ιδρύονται από κοινού με τρίτη χώρα σύμφωνα με διεθνή συμφωνία εξαιρούνται από το πεδίο εφαρμογής της παρούσας οδηγίας. Η παρούσα οδηγία δεν εφαρμόζεται στις διπλωματικές και προξενικές αποστολές κρατών μελών σε τρίτες χώρες ή στα συστήματα δικτύου και πληροφοριών τους, όταν τα συστήματα αυτά βρίσκονται στις εγκαταστάσεις της αποστολής ή λειτουργούν για χρήστες σε τρίτη χώρα.

(9) Τα κράτη μέλη θα πρέπει να είναι σε θέση να λαμβάνουν τα αναγκαία μέτρα για την προστασία των ουσιωδών συμφερόντων εθνικής ασφάλειας, τη διαφύλαξη της δημόσιας τάξης και ασφάλειας, καθώς και την πρόληψη, τη διερεύνηση, την ανίχνευση και τη δίωξη ποινικών αδικημάτων. Για τον σκοπό αυτό, τα κράτη μέλη θα πρέπει να μπορούν να εξαιρούν συγκεκριμένες οντότητες που ασκούν δραστηριότητες στους τομείς της εθνικής ασφάλειας, της δημόσιας ασφάλειας, της άμυνας, ή της επιβολής του νόμου, συμπεριλαμβανομένων και των δραστηριοτήτων που σχετίζονται με την πρόληψη, τη διερεύνηση, τον εντοπισμό και τη δίωξη ποινικών αδικημάτων, από ορισμένες υποχρεώσεις που ορίζονται στην παρούσα οδηγία όσον αφορά τις εν λόγω δραστηριότητες. Όταν μια οντότητα παρέχει υπηρεσίες αποκλειστικά σε οντότητα δημόσιας διοίκησης που εξαιρείται από το πεδίο εφαρμογής της παρούσας οδηγίας, τα κράτη μέλη θα πρέπει να μπορούν να αποφασίζουν ότι η εν λόγω οντότητα εξαιρείται από τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία όσον αφορά τις εν λόγω υπηρεσίες. Επιπλέον, σύμφωνα με το άρθρο 346 ΣΛΕΕ, κανένα κράτος μέλος δεν θα πρέπει να υποχρεούται να παρέχει πληροφορίες, η γνωστοποίηση των οποίων θα ήταν αντίθετη προς ουσιώδη συμφέροντα της εθνικής ασφάλειας, της δημόσιας ασφάλειας ή της άμυνάς του. Στο πλαίσιο αυτό, οι εθνικοί και ενωσιακοί κανόνες για την προστασία διαβαθμισμένων πληροφοριών, οι συμφωνίες εμπιστευτικότητας και οι άτυπες συμφωνίες εμπιστευτικότητας, όπως το πρωτόκολλο για την ανταλλαγή πληροφοριών «Traffic Light Protocol», θα πρέπει να λαμβάνονται υπόψη. Το πρωτόκολλο για την ανταλλαγή πληροφοριών πρέπει να νοείται ως μέσο που επιτρέπει την παροχή πληροφοριών σχετικά με τυχόν περιορισμούς στην περαιτέρω διάδοση των πληροφοριών. Χρησιμοποιείται σε όλες σχεδόν τις ομάδες αντιμετώπισης περιστατικών ασφαλείας σε υπολογιστές (CSIRT) και σε ορισμένα κέντρα ανάλυσης και ανταλλαγής πληροφοριών.

(10) Μολονότι η παρούσα οδηγία εφαρμόζεται σε οντότητες που ασκούν δραστηριότητες στον τομέα της παραγωγής ηλεκτρικής ενέργειας από πυρηνικούς σταθμούς, ορισμένες από τις εν λόγω δραστηριότητες μπορεί να συνδέονται με την εθνική ασφάλεια. Στην περίπτωση αυτή, τα κράτη μέλη θα πρέπει να είναι σε θέση να ασκούν την αρμοδιότητά τους για τη διαφύλαξη της εθνικής ασφάλειας όσον αφορά τις εν λόγω δραστηριότητες, συμπεριλαμβανομένων των δραστηριοτήτων εντός της αλυσίδας αξίας της πυρηνικής ενέργειας, σύμφωνα με τις Συνθήκες.

(11) Ορισμένες οντότητες ασκούν δραστηριότητες στους τομείς της εθνικής ασφάλειας, της δημόσιας ασφάλειας, της άμυνας ή της επιβολής του νόμου, συμπεριλαμβανομένης της πρόληψης, της διερεύνησης, της ανίχνευσης και της δίωξης ποινικών αδικημάτων, παρέχοντας παράλληλα υπηρεσίες εμπιστοσύνης. Οι πάροχοι υπηρεσιών εμπιστοσύνης που υπάγονται στο πεδίο εφαρμογής του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([6]) θα πρέπει να υπάγονται στο πεδίο εφαρμογής της παρούσας οδηγίας, προκειμένου να διασφαλίζεται το ίδιο επίπεδο απαιτήσεων ασφάλειας και εποπτείας με εκείνο που προβλεπόταν προηγουμένως στον εν λόγω κανονισμό σε σχέση με τους παρόχους υπηρεσιών εμπιστοσύνης. Σύμφωνα με την εξαίρεση κάποιων ορισμένων από τον κανονισμό (ΕΕ) αριθ. 910/2014 ειδικών υπηρεσιών, η παρούσα οδηγία δεν θα πρέπει να εφαρμόζεται στην παροχή υπηρεσιών εμπιστοσύνης που χρησιμοποιούνται αποκλειστικά στο πλαίσιο κλειστών συστημάτων που απορρέουν από το εθνικό δίκαιο ή από συμφωνίες μεταξύ καθορισμένου συνόλου συμμετεχόντων.

([6]) Κανονισμός (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Ιουλίου 2014, σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ (ΕΕ L 257 της 28.8.2014, σ. 73).

(12) Οι φορείς παροχής ταχυδρομικών υπηρεσιών κατά την έννοια της οδηγίας 97/67/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([7]), συμπεριλαμβανομένων των παρόχων υπηρεσιών ταχυμεταφοράς, θα πρέπει να εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας εάν παρέχουν τουλάχιστον ένα από τα στάδια της αλυσίδας ταχυδρομικής διανομής, και ιδίως την περισυλλογή, τη διαλογή, τη μεταφορά ή τη διανομή ταχυδρομικών αντικειμένων, συμπεριλαμβανομένων των υπηρεσιών παραλαβής, λαμβάνοντας παράλληλα υπόψη τον βαθμό εξάρτησής τους από τα συστήματα δικτύου και πληροφοριών. Οι υπηρεσίες μεταφορών που δεν πραγματοποιούνται σε συνδυασμό με ένα από τα στάδια αυτά θα πρέπει να εξαιρούνται από το πεδίο των ταχυδρομικών υπηρεσιών.

(13) Δεδομένης της εντατικοποίησης και της αυξημένης πολυπλοκότητας των κυβερνοαπειλών, τα κράτη μέλη θα πρέπει να επιδιώξουν να διασφαλίσουν ότι οι οντότητες που εξαιρούνται από το πεδίο εφαρμογής της παρούσας οδηγίας επιτυγχάνουν υψηλό επίπεδο κυβερνοασφάλειας και να στηρίξουν την εφαρμογή ισοδύναμων μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που αντικατοπτρίζουν τον ευαίσθητο χαρακτήρα των εν λόγω οντοτήτων.

(14) Το δίκαιο της Ένωσης για την προστασία των δεδομένων και το δίκαιο της Ένωσης για την προστασία της ιδιωτικότητας εφαρμόζονται σε κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα δυνάμει της παρούσας οδηγίας. Συγκεκριμένα, η παρούσα οδηγία εφαρμόζεται με την επιφύλαξη του κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([8]) και της οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([9]). Κατά συνέπεια, η παρούσα οδηγία δεν θα πρέπει να θίγει, μεταξύ άλλων, τα καθήκοντα και τις εξουσίες των αρχών που είναι αρμόδιες για την παρακολούθηση της συμμόρφωσης με το ισχύον ενωσιακό δίκαιο για την προστασία των δεδομένων και το ενωσιακό δίκαιο για την προστασία της ιδιωτικότητας.

(15) Οι οντότητες που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας για τους σκοπούς της συμμόρφωσης με τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και τις υποχρεώσεις υποβολής αναφορών θα πρέπει να ταξινομούνται σε δύο κατηγορίες, σε βασικές οντότητες και σημαντικές οντότητες, ώστε να αντικατοπτρίζονται ο βαθμός κρισιμότητάς τους, όσον αφορά τον τομέα τους ή το είδος της υπηρεσίας που παρέχουν, καθώς και το μέγεθός τους. Στο πλαίσιο αυτό, θα πρέπει να λαμβάνονται δεόντως υπόψη τυχόν σχετικές τομεακές εκτιμήσεις κινδύνου ή καθοδήγηση από τις αρμόδιες αρχές, κατά περίπτωση. Τα καθεστώτα εποπτείας και επιβολής για τις δύο αυτές κατηγορίες οντοτήτων θα πρέπει να διαφοροποιούνται ώστε να εξασφαλίζεται δίκαιη ισορροπία μεταξύ των απαιτήσεων και των υποχρεώσεων με βάση τον κίνδυνο, αφενός, και του διοικητικού φόρτου που προκύπτει από την εποπτεία της συμμόρφωσης, αφετέρου.

(16) Προκειμένου να αποφευχθεί το ενδεχόμενο, οντότητες που έχουν συνεργαζόμενες επιχειρήσεις ή είναι συνδεδεμένες επιχειρήσεις να θεωρούνται βασικές ή σημαντικές οντότητες όταν αυτό θα ήταν δυσανάλογο, τα κράτη μέλη μπορούν να λαμβάνουν υπόψη τον βαθμό ανεξαρτησίας που έχει μια οντότητα σε σχέση με τον εταίρο της ή τις συνδεδεμένες επιχειρήσεις, κατά την εφαρμογή του άρθρου 6 παράγραφος 2 του παραρτήματος της σύστασης 2003/361/ΕΚ. Πιο συγκεκριμένα, τα κράτη μέλη μπορούν να λαμβάνουν υπόψη το γεγονός ότι μια οντότητα είναι ανεξάρτητη από τον εταίρο της ή τις συνδεδεμένες επιχειρήσεις όσον αφορά τα συστήματα δικτύου και πληροφοριών που χρησιμοποιεί η εν λόγω οντότητα για την παροχή των υπηρεσιών της και όσον αφορά τις υπηρεσίες που παρέχει η οντότητα. Σε αυτή τη βάση, κατά περίπτωση, τα κράτη μέλη μπορούν να θεωρούν ότι μια τέτοια οντότητα δεν συνιστά μεσαία επιχείρηση δυνάμει του άρθρου 2 του παραρτήματος της σύστασης 2003/361/ΕΚ, ή δεν υπερβαίνει τα ανώτατα όρια για τις μεσαίες επιχειρήσεις που αναφέρονται στην παράγραφο 1 του εν λόγω άρθρου, εάν, αφού ληφθεί υπόψη ο βαθμός ανεξαρτησίας της εν λόγω οντότητας, η εν λόγω οντότητα δεν θα είχε θεωρηθεί ως μεσαία επιχείρηση ή ότι υπερβαίνει τα εν λόγω ανώτατα όρια σε περίπτωση που είχαν ληφθεί υπόψη μόνο τα δικά της δεδομένα. Αυτό δεν θίγει τις υποχρεώσεις που απορρέουν από την παρούσα οδηγία για τις συνεργαζόμενες και τις συνδεδεμένες επιχειρήσεις που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας.

(17) Τα κράτη μέλη θα πρέπει να είναι σε θέση να αποφασίσουν εάν οι οντότητες που προσδιορίστηκαν πριν από την έναρξη ισχύος της παρούσας οδηγίας ως φορείς εκμετάλλευσης βασικών υπηρεσιών σύμφωνα με την οδηγία (ΕΕ) 2016/1148, πρέπει να θεωρούνται βασικές οντότητες.

([7]) Οδηγία 97/67/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Δεκεμβρίου 1997, σχετικά με τους κοινούς κανόνες για την ανάπτυξη της εσωτερικής αγοράς κοινοτικών ταχυδρομικών υπηρεσιών και τη βελτίωση της ποιότητας των παρεχομένων υπηρεσιών (ΕΕ L 15 της 21.1.1998, σ. 14).

([8]) Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (ΕΕ L 119 της 4.5.2016, σ. 1).

([9]) Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) (ΕΕ L 201 της 31.7.2002, σ. 37).

(18) Προκειμένου να διασφαλιστεί σαφής επισκόπηση των οντοτήτων που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας, τα κράτη μέλη θα πρέπει να καταρτίσουν κατάλογο βασικών και σημαντικών οντοτήτων καθώς και οντοτήτων που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα. Για τον σκοπό αυτό, τα κράτη μέλη θα πρέπει να απαιτούν από τις οντότητες να υποβάλλουν στις αρμόδιες αρχές τουλάχιστον τις ακόλουθες πληροφορίες, συγκεκριμένα το όνομα, τη διεύθυνση και τα επικαιροποιημένα στοιχεία επικοινωνίας, συμπεριλαμβανομένων των διευθύνσεων ηλεκτρονικού ταχυδρομείου, των πεδίων IP και των αριθμών τηλεφώνου της οντότητας, και κατά περίπτωση, του σχετικού τομέα και υποτομέα που αναφέρονται στα παραρτήματα, καθώς και, κατά περίπτωση, κατάλογο των κρατών μελών στα οποία παρέχουν υπηρεσίες που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας. Για τον σκοπό αυτό, η Επιτροπή, με τη συνδρομή του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), θα πρέπει, χωρίς αδικαιολόγητη καθυστέρηση, να προβλέπει κατευθυντήριες γραμμές και υποδείγματα σχετικά με την υποχρέωση υποβολής πληροφοριών. Για να διευκολυνθεί η κατάρτιση και η επικαιροποίηση του καταλόγου των βασικών και σημαντικών οντοτήτων καθώς και των οντοτήτων που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα, τα κράτη μέλη θα πρέπει να είναι σε θέση να θεσπίζουν εθνικούς μηχανισμούς για την εγγραφή των οντοτήτων αυτών. Όταν υπάρχουν μητρώα σε εθνικό επίπεδο, τα κράτη μέλη μπορούν να αποφασίζουν σχετικά με τους κατάλληλους μηχανισμούς που επιτρέπουν τον προσδιορισμό των οντοτήτων που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας.

(19) Τα κράτη μέλη θα πρέπει να φέρουν την ευθύνη για την υποβολή στην Επιτροπή τουλάχιστον του αριθμού των βασικών και σημαντικών οντοτήτων για κάθε τομέα και υποτομέα που αναφέρεται στα παραρτήματα, καθώς και των πληροφοριών σχετικά με τον αριθμό των προσδιορισμένων οντοτήτων και τη διάταξη της παρούσας οδηγίας, βάσει της οποίας ορίστηκαν ως τέτοιες, και το είδος της υπηρεσίας που παρέχουν. Τα κράτη μέλη ενθαρρύνονται να ανταλλάσσουν με την Επιτροπή πληροφορίες σχετικά με βασικές και σημαντικές οντότητες και, σε περίπτωση περιστατικού μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας, σχετικές πληροφορίες όπως το όνομα της οικείας οντότητας.

(20) Η Επιτροπή θα πρέπει, σε συνεργασία με την Ομάδα Συνεργασίας και κατόπιν διαβούλευσης με τα ενδιαφερόμενα μέρη, να προβλέπει κατευθυντήριες γραμμές σχετικά με την εφαρμογή των κριτηρίων που ισχύουν για τις πολύ μικρές και τις μικρές επιχειρήσεις προκειμένου να αξιολογήσει εάν εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας. Η Επιτροπή θα πρέπει επίσης να διασφαλίσει ότι παρέχεται κατάλληλη καθοδήγηση στις πολύ μικρές και μικρές επιχειρήσεις που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας. Η Επιτροπή θα πρέπει, με τη βοήθεια των κρατών μελών, να θέτει σχετικές πληροφορίες στη διάθεση των πολύ μικρών και των μικρών επιχειρήσεων.

(21) Η Επιτροπή θα μπορούσε να παρέχει καθοδήγηση για να βοηθά τα κράτη μέλη στην εφαρμογή των διατάξεων της παρούσας οδηγίας σχετικά με το πεδίο εφαρμογής και την αξιολόγηση της αναλογικότητας των μέτρων που πρέπει να ληφθούν δυνάμει της παρούσας οδηγίας, ιδίως όσον αφορά οντότητες με σύνθετα επιχειρηματικά μοντέλα ή περιβάλλοντα λειτουργίας, σε περιπτώσεις όπου μια οντότητα μπορεί να πληροί ταυτόχρονα τα κριτήρια που αντιστοιχούν τόσο σε βασικές όσο και σε σημαντικές οντότητες ή να ασκεί ταυτόχρονα δραστηριότητες, ορισμένες από τις οποίες εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας και ορισμένες από τις οποίες εξαιρούνται από το πεδίο εφαρμογής της.

(22) Η παρούσα οδηγία καθορίζει τη βάση αναφοράς για τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και τις υποχρεώσεις αναφοράς περιστατικών σε όλους τους τομείς που εμπίπτουν στο πεδίο εφαρμογής της. Προκειμένου να αποφευχθεί ο κατακερματισμός των διατάξεων περί κυβερνοασφάλειας των νομικών πράξεων της Ένωσης, όταν περαιτέρω τομεακές νομικές πράξεις της Ένωσης που αφορούν μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και υποχρεώσεις υποβολής εκθέσεων θεωρούνται αναγκαίες για τη διασφάλιση υψηλού επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ένωση, η Επιτροπή θα πρέπει να αξιολογήσει κατά πόσον οι εν λόγω επιπλέον διατάξεις θα μπορούσαν να καθοριστούν σε εκτελεστική πράξη δυνάμει της παρούσας οδηγίας. Εάν οι εκτελεστική πράξη δεν είναι κατάλληλη για τον σκοπό αυτό, οι τομεακές νομικές πράξεις της Ένωσης θα μπορούσαν να συμβάλουν στη διασφάλιση υψηλού επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ένωση, λαμβάνοντας παράλληλα πλήρως υπόψη τις ιδιαιτερότητες και την πολυπλοκότητα των σχετικών τομέων. Για τον σκοπό αυτό, η παρούσα οδηγία δεν αποκλείει την έκδοση περαιτέρω τομεακών νομικών πράξεων της Ένωσης για την αντιμετώπιση των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και των υποχρεώσεων κοινοποίησης περιστατικών που λαμβάνουν δεόντως υπόψη την ανάγκη για ένα ολοκληρωμένο και συνεκτικό πλαίσιο κυβερνοασφάλειας. Η παρούσα οδηγία δεν θίγει τις υφιστάμενες εκτελεστικές αρμοδιότητες που έχουν ανατεθεί στην Επιτροπή σε διάφορους τομείς, συμπεριλαμβανομένων των μεταφορών και της ενέργειας.

(23) Όταν μια τομεακή νομική πράξη της Ένωσης περιέχει διατάξεις που απαιτούν από βασικές ή σημαντικές οντότητες να εγκρίνουν μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας ή να κοινοποιούν σημαντικά περιστατικά, και όταν οι εν λόγω απαιτήσεις είναι τουλάχιστον ισοδύναμες ως προς το αποτέλεσμα με τις υποχρεώσεις που ορίζονται στην

παρούσα οδηγία, οι εν λόγω διατάξεις, μεταξύ άλλων σχετικά με την εποπτεία και την επιβολή, θα πρέπει να εφαρμόζονται στις εν λόγω οντότητες. Εάν μια τομεακή νομική πράξη της Ένωσης δεν καλύπτει όλες τις οντότητες σε συγκεκριμένο τομέα που εμπίπτει στο πεδίο εφαρμογής της παρούσας οδηγίας, οι σχετικές διατάξεις της παρούσας οδηγίας θα πρέπει να εξακολουθήσουν να εφαρμόζονται στις οντότητες που δεν καλύπτονται από την εν λόγω πράξη.

(24) Όταν οι διατάξεις τομεακής νομικής πράξης της Ένωσης απαιτούν από βασικές ή σημαντικές οντότητες να συμμορφωθούν με υποχρεώσεις κοινοποίησης που είναι τουλάχιστον ισοδύναμου αποτελέσματος με τις υποχρεώσεις κοινοποίησης που ορίζονται στην παρούσα οδηγία, θα πρέπει να διασφαλίζεται η συνοχή και η αποτελεσματικότητα του χειρισμού των κοινοποιήσεων περιστατικών. Για τον σκοπό αυτό, οι διατάξεις της τομεακής νομικής πράξης της Ένωσης για την κοινοποίηση περιστατικών θα πρέπει να παρέχουν στις CSIRT, στις αρμόδιες αρχές ή στα ενιαία σημεία επαφής για την κυβερνοασφάλεια (ενιαία σημεία επαφής) δυνάμει της παρούσας οδηγίας άμεση πρόσβαση στις κοινοποιήσεις περιστατικών που υποβάλλονται σύμφωνα με την τομεακή νομική πράξη της Ένωσης. Ειδικότερα, η εν λόγω άμεση πρόσβαση μπορεί να διασφαλιστεί εάν οι κοινοποιήσεις περιστατικών διαβιβάζονται αμελλητί στην CSIRT, στην αρμόδια αρχή ή στο ενιαίο σημείο επαφής δυνάμει της παρούσας οδηγίας. Κατά περίπτωση, τα κράτη μέλη θα πρέπει να θεσπίσουν μηχανισμό αυτόματης και άμεσης αναφοράς που να διασφαλίζει τη συστηματική και άμεση ανταλλαγή πληροφοριών με τις CSIRT, τις αρμόδιες αρχές ή το ενιαίο σημείο επαφής σχετικά με τον χειρισμό των εν λόγω κοινοποιήσεων περιστατικών. Για τους σκοπούς της απλούστευσης της κοινοποίησης και της εφαρμογής του μηχανισμού αυτόματης και άμεσης υποβολής αναφορών, τα κράτη μέλη θα μπορούσαν, σύμφωνα με την τομεακή νομική πράξη της Ένωσης, να χρησιμοποιούν ενιαίο σημείο εισόδου.

(25) Οι τομεακές νομικές πράξεις της Ένωσης που προβλέπουν μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας ή υποχρεώσεις υποβολής εκθέσεων τουλάχιστον ισοδύναμου αποτελέσματος με εκείνες που ορίζονται στην παρούσα οδηγία, θα μπορούσαν να προβλέπουν ότι οι αρμόδιες αρχές δυνάμει των εν λόγω πράξεων ασκούν τις εποπτικές και εκτελεστικές αρμοδιότητές τους σε σχέση με τα εν λόγω μέτρα ή υποχρεώσεις με τη συνδρομή των αρμόδιων αρχών δυνάμει της παρούσας οδηγίας. Οι οικείες αρμόδιες αρχές θα μπορούσαν να προβούν σε ρυθμίσεις συνεργασίας για τον σκοπό αυτό. Οι εν λόγω ρυθμίσεις συνεργασίας θα μπορούσαν να προσδιορίζουν, μεταξύ άλλων, τις διαδικασίες που αφορούν τον συντονισμό των εποπτικών δραστηριοτήτων, συμπεριλαμβανομένων των διαδικασιών των ερευνών και των επιτόπιων επιθεωρήσεων σύμφωνα με το εθνικό δίκαιο και ενός μηχανισμού για την ανταλλαγή σχετικών πληροφοριών, σχετικά με την εποπτεία και την επιβολή μεταξύ των αρμόδιων αρχών, συμπεριλαμβανομένης της πρόσβασης σε σχετικές με τον κυβερνοχώρο πληροφορίες που ζητούν οι αρμόδιες αρχές δυνάμει της παρούσας οδηγίας.

(26) Όταν ειδικές τομεακές νομικές πράξεις της Ένωσης απαιτούν ή παρέχουν κίνητρα σε οντότητες για την κοινοποίηση σημαντικών κυβερνοαπειλών, τα κράτη μέλη θα πρέπει επίσης να ενθαρρύνουν την ανταλλαγή σημαντικών κυβερνοαπειλών με τις CSIRT, τις αρμόδιες αρχές ή τα ενιαία σημεία επαφής δυνάμει της παρούσας οδηγίας, προκειμένου να διασφαλίζεται ενισχυμένο επίπεδο ευαισθητοποίησης των εν λόγω οργάνων σχετικά με το τοπίο των κυβερνοαπειλών και να τους παρέχεται η δυνατότητα να ανταποκρίνονται αποτελεσματικά και εγκαίρως σε περίπτωση επέλευσης των σημαντικών κυβερνοαπειλών.

(27) Οι μελλοντικές τομεακές νομικές πράξεις της Ένωσης θα πρέπει να λαμβάνουν δεόντως υπόψη τους ορισμούς και το πλαίσιο εποπτείας και επιβολής που καθορίζονται στην παρούσα οδηγία.

(28) Ο κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([10]) θα πρέπει να θεωρείται τομεακή νομική πράξη της Ένωσης σε σχέση με την παρούσα οδηγία όσον αφορά τις οντότητες του χρηματοπιστωτικού τομέα. Αντί των διατάξεων που θεσπίζονται στην παρούσα οδηγία, θα πρέπει να εφαρμόζονται οι διατάξεις του κανονισμού (ΕΕ) 2022/2554 σχετικά με τη διαχείριση κινδύνων της τεχνολογίας πληροφοριών και επικοινωνιών (ΤΠΕ), τη διαχείριση περιστατικών που σχετίζονται με τις ΤΠΕ και ιδίως την αναφορά σοβαρών περιστατικών ΤΠΕ, καθώς και σχετικά με τις δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας, τις ρυθμίσεις ανταλλαγής πληροφοριών και τον κίνδυνο τρίτων παρόχων ΤΠΕ. Ως εκ τούτου, τα κράτη μέλη δεν θα πρέπει να εφαρμόζουν τις διατάξεις της παρούσας οδηγίας σχετικά με τις υποχρεώσεις διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και αναφοράς περιστατικών και την εποπτεία, καθώς και την επιβολή της νομοθεσίας στις χρηματοπιστωτικές οντότητες που καλύπτονται από τον κανονισμό (ΕΕ) 2022/2554. Ταυτόχρονα, είναι σημαντικό να διατηρηθεί στενή σχέση και ανταλλαγή πληροφοριών με τον χρηματοπιστωτικό τομέα στο πλαίσιο της παρούσας οδηγίας. Για τον σκοπό αυτό, ο κανονισμός (ΕΕ) 2022/2554 επιτρέπει στις Ευρωπαϊκές Εποπτικές Αρχές (ΕΕΑ) και στις αρμόδιες αρχές δυνάμει του εν λόγω κανονισμού να συμμετέχουν στις δραστηριότητες της Ομάδας Συνεργασίας και να ανταλλάσσουν πληροφορίες και να συνεργάζονται με τα ενιαία σημεία επαφής, καθώς και με τις CSIRT και τις αρμόδιες αρχές δυνάμει της παρούσας οδηγίας. Οι αρμόδιες αρχές δυνάμει του κανονισμού (ΕΕ) 2022/2554 θα

([10]) Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοπιστωτικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014 και (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (βλέπε σελίδα 1 της παρούσας Επίσημης Εφημερίδας).

πρέπει επίσης να διαβιβάζουν λεπτομερή στοιχεία για σημαντικά περιστατικά που σχετίζονται με τις ΤΠΕ και, κατά περίπτωση, σημαντικές κυβερνοαπειλές στις CSIRT, στις αρμόδιες αρχές ή στα ενιαία σημεία επαφής δυνάμει της παρούσας οδηγίας. Αυτό μπορεί να επιτευχθεί με την παροχή άμεσης πρόσβασης στην κοινοποίηση των περιστατικών και την διαβίβασή τους απευθείας ή μέσω ενός ενιαίου σημείου εισόδου. Επιπλέον, τα κράτη μέλη θα πρέπει να συνεχίσουν να περιλαμβάνουν τον χρηματοπιστωτικό τομέα στις στρατηγικές τους για την κυβερνοασφάλεια, και οι CSIRT μπορούν να περιλαμβάνουν τον χρηματοπιστωτικό τομέα στις δραστηριότητές τους.

(29) Προκειμένου να αποφευχθούν κενά ή αλληλεπικαλύψεις των υποχρεώσεων κυβερνοασφάλειας που επιβάλλονται σε οντότητες στον τομέα των αερομεταφορών, οι εθνικές αρχές δυνάμει των κανονισμών (ΕΚ) αριθ. 300/2008 ([11]) και (ΕΕ) 2018/1139 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([12]) και οι αρμόδιες αρχές δυνάμει της παρούσας οδηγίας θα πρέπει να συνεργάζονται σε σχέση με την εφαρμογή μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και την εποπτεία της συμμόρφωσης με τα εν λόγω μέτρα σε εθνικό επίπεδο. Η συμμόρφωση μιας οντότητας με τις απαιτήσεις ασφάλειας που καθορίζονται στους κανονισμούς (ΕΚ) αριθ. 300/2008 και (ΕΕ) 2018/1139 και στις σχετικές κατ' εξουσιοδότηση και εκτελεστικές πράξεις που εκδίδονται σύμφωνα με τους εν λόγω κανονισμούς θα μπορούσε να θεωρηθεί από τις αρμόδιες αρχές βάσει της παρούσας οδηγίας ότι συνιστά συμμόρφωση με τις αντίστοιχες απαιτήσεις που καθορίζονται στην παρούσα οδηγία.

(30) Λαμβανομένων υπόψη των διασυνδέσεων μεταξύ της κυβερνοασφάλειας και της φυσικής ασφάλειας των οντοτήτων, θα πρέπει να διασφαλιστεί μια συνεκτική προσέγγιση μεταξύ της οδηγίας (ΕΕ) 2022/2557 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([13]) και της παρούσας οδηγίας. Για να επιτευχθεί αυτό, οι οντότητες που χαρακτηρίζονται ως κρίσιμες οντότητες σύμφωνα με την οδηγία (ΕΕ) 2022/2557 θα πρέπει να θεωρούνται βασικές οντότητες δυνάμει της παρούσας οδηγίας. Επιπλέον, κάθε κράτος μέλος θα πρέπει να διασφαλίζει ότι η εθνική στρατηγική του για την κυβερνοασφάλεια προβλέπει ένα πλαίσιο πολιτικής για ενισχυμένο συντονισμό εντός του εν λόγω κράτους μέλους μεταξύ των αρμόδιων αρχών του δυνάμει της παρούσας οδηγίας και των αρχών που προβλέπονται στην οδηγία (ΕΕ) 2022/2557, στο πλαίσιο της ανταλλαγής πληροφοριών σχετικά με κινδύνους, απειλές και περιστατικά στον κυβερνοχώρο, καθώς και σχετικά με κινδύνους, απειλές και περιστατικά εκτός κυβερνοχώρου, και την άσκηση εποπτικών καθηκόντων. Οι αρμόδιες αρχές δυνάμει της παρούσας οδηγίας και οι αρμόδιες αρχές δυνάμει της οδηγίας (ΕΕ) 2022/2557 θα πρέπει να συνεργάζονται και να ανταλλάσσουν πληροφορίες αμελλητί, ιδίως όσον αφορά τον προσδιορισμό των κρίσιμων οντοτήτων, των κινδύνων, των κυβερνοαπειλών και των περιστατικών, καθώς και σε σχέση με κινδύνους, απειλές και περιστατικά μη σχετιζόμενα με τον κυβερνοχώρο, που επηρεάζουν κρίσιμες οντότητες, συμπεριλαμβανομένων των μέτρων κυβερνοασφάλειας και των φυσικών μέτρων που λαμβάνονται από κρίσιμες οντότητες, καθώς και των αποτελεσμάτων των εποπτικών δραστηριοτήτων που διεξάγονται σε σχέση με τις εν λόγω οντότητες.

Επιπλέον, προκειμένου να εξορθολογιστούν οι εποπτικές δραστηριότητες μεταξύ των αρμόδιων αρχών δυνάμει της παρούσας οδηγίας και των αρμοδίων αρχών δυνάμει της οδηγίας (ΕΕ) 2022/2557 και προκειμένου να ελαχιστοποιηθεί ο διοικητικός φόρτος για τις οικείες οντότητες, οι εν λόγω αρμόδιες αρχές θα πρέπει να προσπαθήσουν να εναρμονίσουν τα υποδείγματα κοινοποίησης περιστατικών και τις εποπτικές διαδικασίες. Κατά περίπτωση, οι αρμόδιες αρχές δυνάμει της οδηγίας (ΕΕ) 2022/2557, θα πρέπει να μπορούν να ζητούν από τις αρμόδιες αρχές δυνάμει της παρούσας οδηγίας να ασκούν τις εποπτικές και εκτελεστικές αρμοδιότητές τους σε σχέση με οντότητα η οποία προσδιορίζεται ως κρίσιμη οντότητα βάσει της οδηγίας (ΕΕ) 2022/2557. Οι αρμόδιες αρχές δυνάμει της παρούσας οδηγίας και οι αρμόδιες αρχές δυνάμει της οδηγίας (ΕΕ) 2022/2557 θα πρέπει, ει δυνατόν σε πραγματικό χρόνο, να συνεργάζονται και να ανταλλάσσουν πληροφορίες για τον σκοπό αυτό.

(31) Οι οντότητες που ανήκουν στον τομέα των ψηφιακών υποδομών στηρίζονται επί της ουσίας σε συστήματα δικτύου και πληροφοριών και, επομένως, οι υποχρεώσεις που επιβάλλονται σε αυτές σύμφωνα με την παρούσα οδηγία θα πρέπει να διαχειριστούν με ολοκληρωμένο τρόπο τη φυσική ασφάλεια των εν λόγω συστημάτων στο πλαίσιο των υποχρεώσεών τους όσον αφορά τη λήψη μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και την κοινοποίηση περιστατικών. Δεδομένου ότι τα θέματα αυτά καλύπτονται από την παρούσα οδηγία, οι υποχρεώσεις που προβλέπονται στα κεφάλαια III, IV και VI της οδηγίας (ΕΕ) 2022/2557 δεν ισχύουν για τις εν λόγω οντότητες.

([11]) Κανονισμός (ΕΚ) αριθ. 300/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαρτίου 2008, για τη θέσπιση κοινών κανόνων στο πεδίο της ασφάλειας της πολιτικής αεροπορίας και την κατάργηση του κανονισμού (ΕΚ) αριθ. 2320/2002 (ΕΕ L 97 της 9.4.2008, σ. 72).

([12]) Κανονισμός (ΕΕ) 2018/1139 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 4ης Ιουλίου 2018, για τη θέσπιση κοινών κανόνων στον τομέα της πολιτικής αεροπορίας και την ίδρυση Οργανισμού της Ευρωπαϊκής Ένωσης για την Αεροπορική Ασφάλεια, και για την τροποποίηση των κανονισμών (ΕΚ) αριθ. 2111/2005, (ΕΚ) αριθ. 1008/2008, (ΕΕ) αριθ. 996/2010, (ΕΕ) αριθ. 376/2014 και των οδηγιών 2014/30/ΕΕ και 2014/53/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, καθώς και για την κατάργηση των κανονισμών (ΕΚ) αριθ. 552/2004 και (ΕΚ) αριθ. 216/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και του κανονισμού (ΕΟΚ) αριθ. 3922/91 του Συμβουλίου (ΕΕ L 212 της 22.8.2018, σ. 1).

([13]) Οδηγία (ΕΕ) 2022/2557 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, για την ανθεκτικότητα των κρίσιμων οντοτήτων και την κατάργηση της οδηγίας 2008/114/ΕΚ του Συμβουλίου (βλέπε σελίδα 164 της παρούσας Επίσημης Εφημερίδας).

(32) Η υποστήριξη και η διατήρηση ενός αξιόπιστου, ανθεκτικού και ασφαλούς συστήματος ονομάτων χώρου (DNS) αποτελούν βασικό παράγοντα για τη διασφάλιση της ακεραιότητας του διαδικτύου και είναι ουσιαστικής σημασίας για τη συνεχή και σταθερή λειτουργία του, από την οποία εξαρτάται η ψηφιακή οικονομία και κοινωνία. Συνεπώς, η παρούσα οδηγία θα πρέπει να εφαρμόζεται στα μητρώα ονομάτων χώρου ανωτάτου επιπέδου (TLD) και στους παρόχους υπηρεσιών DNS που πρέπει να νοούνται ως οντότητες που παρέχουν δημόσια διαθέσιμες υπηρεσίες αναδρομικής επίλυσης ονομάτων χώρου για τελικούς χρήστες του διαδικτύου ή αυθεντικές υπηρεσίες επίλυσης ονομάτων χώρου για χρήση από τρίτους. Η παρούσα οδηγία δεν θα πρέπει να εφαρμόζεται σε εξυπηρετητές ονομάτων ρίζας (root name servers).

(33) Οι υπηρεσίες υπολογιστικού νέφους θα πρέπει να καλύπτουν ψηφιακές υπηρεσίες που καθιστούν δυνατή τη διαχείριση κατά παραγγελία και την ευρεία εξ αποστάσεως πρόσβαση σε κλιμακούμενη και ελαστική δεξαμενή διαμοιραζόμενων υπολογιστικών πόρων, συμπεριλαμβανομένων και των πόρων που είναι κατανεμημένοι σε διάφορες τοποθεσίες. Οι υπολογιστικοί πόροι περιλαμβάνουν πόρους όπως δίκτυα, εξυπηρετητές ή άλλες υποδομές, λειτουργικά συστήματα, λογισμικό, αποθήκευση, εφαρμογές και υπηρεσίες. Τα μοντέλα υπηρεσιών υπολογιστικού νέφους περιλαμβάνουν, μεταξύ άλλων, την υποδομή ως υπηρεσία (IaaS), την πλατφόρμα ως υπηρεσία (PaaS), το λογισμικό ως υπηρεσία (SaaS) και το δίκτυο ως υπηρεσία (NaaS). Τα μοντέλα ανάπτυξης της νεφοϋπολογιστικής θα πρέπει να περιλαμβάνουν το ιδιωτικό, το κοινοτικό, το δημόσιο και το υβριδικό υπολογιστικό νέφος. Τα μοντέλα υπηρεσιών και ανάπτυξης υπολογιστικού νέφους έχουν την ίδια έννοια με τους όρους παροχής υπηρεσιών και μοντέλων ανάπτυξης που ορίζονται στο πρότυπο ISO/IEC 17788:2014. Η ικανότητα του χρήστη του υπολογιστικού νέφους να λαμβάνει μονομερώς με ίδια μέσα υπολογιστικές ικανότητες, όπως ο χρόνος εξυπηρετητή ή η δικτυακή αποθήκευση, χωρίς ανθρώπινη αλληλεπίδραση από τον πάροχο υπηρεσιών νεφοϋπολογιστικής, θα μπορούσε να περιγραφεί ως διαχείριση κατά παραγγελία.

Ο όρος «ευρεία εξ αποστάσεως πρόσβαση» χρησιμοποιείται για να περιγράψει ότι οι δυνατότητες υπολογιστικού νέφους παρέχονται μέσω του δικτύου και είναι προσβάσιμες μέσω μηχανισμών που προωθούν τη χρήση ετερογενών πλατφορμών τύπου thin ή thick client, συμπεριλαμβανομένων κινητών τηλεφώνων, ταμπλετών, φορητών υπολογιστών και σταθμών εργασίας. Ο όρος «κλιμακοθετήσιμο» αναφέρεται σε υπολογιστικούς πόρους που κατανέμονται με ευελιξία από τον πάροχο των υπηρεσιών νεφοϋπολογιστικής, ανεξαρτήτως της γεωγραφικής θέσης των πόρων, προκειμένου να αντιμετωπιστούν διακυμάνσεις στη ζήτηση. Ο όρος «ελαστικό σύνολο» χρησιμοποιείται για να περιγράψει υπολογιστικούς πόρους που παρέχονται και γίνονται διαθέσιμοι ανάλογα με τη ζήτηση προκειμένου να καταστεί δυνατή η ταχεία αύξηση και μείωση των διαθέσιμων πόρων ανάλογα με τον φόρτο εργασίας. Ο όρος «διαμοιραζόμενοι» χρησιμοποιείται για να περιγράψει υπολογιστικούς πόρους που παρέχονται σε πολλούς χρήστες που μοιράζονται μία κοινή πρόσβαση στην υπηρεσία, αλλά όπου η επεξεργασία εκτελείται χωριστά για κάθε χρήστη, παρόλο που η υπηρεσία παρέχεται από τον ίδιο ηλεκτρονικό εξοπλισμό. Ο όρος «κατανεμημένοι» χρησιμοποιείται για να περιγράψει υπολογιστικούς πόρους που βρίσκονται σε διαφορετικούς χωρικά δικτυωμένους υπολογιστές ή συσκευές και οι οποίοι επικοινωνούν και συντονίζονται μεταξύ τους μέσω διαβίβασης μηνυμάτων.

(34) Δεδομένης της ανάδυσης καινοτόμων τεχνολογιών και νέων επιχειρηματικών μοντέλων, αναμένεται να εμφανιστούν στην εσωτερική αγορά νέα μοντέλα υπηρεσιών και ανάπτυξης υπολογιστικού νέφους τα οποία θα ανταποκρίνονται στις εξελισσόμενες ανάγκες των πελατών. Στο πλαίσιο αυτό, οι υπηρεσίες νεφοϋπολογιστικής μπορούν να παρέχονται σε έντονα κατανεμημένη μορφή, ακόμη εγγύτερα στον τόπο παραγωγής ή συλλογής των δεδομένων, μεταβαίνοντας έτσι από το παραδοσιακό μοντέλο σε ένα έντονα κατανεμημένο μοντέλο (υπολογιστική παρυφών).

(35) Οι υπηρεσίες που παρέχονται από τους παρόχους υπηρεσιών κέντρων δεδομένων ενδέχεται να μην παρέχονται πάντοτε στη μορφή υπηρεσιών υπολογιστικού νέφους. Ως εκ τούτου, τα κέντρα δεδομένων ενδέχεται να μην αποτελούν πάντοτε μέρος της υποδομής νεφοϋπολογιστικής. Για τη διαχείριση όλων των κινδύνων που αφορούν στην ασφάλεια των συστημάτων δικτύου και πληροφοριών, η παρούσα οδηγία θα πρέπει επομένως να καλύπτει και τους παρόχους τέτοιων υπηρεσιών κέντρων δεδομένων που δεν είναι υπηρεσίες υπολογιστικού νέφους. Για τους σκοπούς της παρούσας οδηγίας, ο όρος «υπηρεσία κέντρων δεδομένων» θα πρέπει να καλύπτει την παροχή υπηρεσίας που περιλαμβάνει δομές, ή ομάδες δομών, που προορίζονται για την κεντρική φιλοξενία, διασύνδεση και λειτουργία της τεχνολογίας πληροφοριών («ΤΠ») και του εξοπλισμού δικτύου που παρέχει υπηρεσίες αποθήκευσης, επεξεργασίας και μεταφοράς δεδομένων, καθώς και όλες τις εγκαταστάσεις και υποδομές διανομής ηλεκτρικής ενέργειας και περιβαλλοντικού ελέγχου. Ο όρος «υπηρεσία κέντρων δεδομένων» δεν θα πρέπει να ισχύει για ενδοεπιχειρησιακά εταιρικά κέντρα δεδομένων που ανήκουν στην οικεία οντότητα και λειτουργούν για ίδιους σκοπούς.

(36) Οι ερευνητικές δραστηριότητες διαδραματίζουν καίριο ρόλο στην ανάπτυξη νέων προϊόντων και διαδικασιών. Πολλές από τις δραστηριότητες αυτές διεξάγονται από οντότητες που μοιράζονται, διαθέτουν ή εκμεταλλεύονται τα αποτελέσματα της έρευνάς τους για εμπορικούς σκοπούς. Συνεπώς, οι εν λόγω οντότητες μπορούν να αποτελέσουν σημαντικούς παράγοντες στις αλυσίδες αξίας, γεγονός που καθιστά την ασφάλεια των συστημάτων δικτύου και πληροφοριών τους αναπόσπαστο μέρος της συνολικής κυβερνοασφάλειας της εσωτερικής αγοράς. Οι ερευνητικοί οργανισμοί θα πρέπει να νοούνται ως φορείς που εστιάζουν το κύριο μέρος των δραστηριοτήτων τους στη διεξαγωγή εφαρμοσμένης έρευνας ή πειραματικής

ανάπτυξης, κατά την έννοια του εγχειριδίου Frascati 2015 του Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης: Κατευθυντήριες γραμμές για τη συλλογή και την υποβολή δεδομένων σχετικά με την έρευνα και την πειραματική ανάπτυξη, με σκοπό την εκμετάλλευση των αποτελεσμάτων τους για εμπορικούς σκοπούς, όπως η κατασκευή ή η ανάπτυξη ενός προϊόντος, ή μιας διαδικασίας, η παροχή μιας υπηρεσίας, ή η εμπορία αυτών.

(37) Οι αυξανόμενες αλληλεξαρτήσεις είναι αποτέλεσμα ενός ολοένα και περισσότερο διασυνοριακού και αλληλεξαρτώμενου δικτύου παροχής υπηρεσιών που χρησιμοποιεί βασικές υποδομές σε ολόκληρη την Ένωση σε τομείς όπως της ενέργειας, των μεταφορών, των ψηφιακών υποδομών, του πόσιμου νερού και των λυμάτων, της υγείας, ορισμένων πτυχών της δημόσιας διοίκησης, καθώς και του διαστήματος, στον βαθμό που αφορά την παροχή ορισμένων υπηρεσιών που εξαρτώνται από επίγειες υποδομές των οποίων η κυριότητα, η διαχείριση και η λειτουργία ανήκει είτε σε κράτη μέλη είτε σε ιδιώτες, και, ως εκ τούτου, δεν καλύπτει τις υποδομές των οποίων η κυριότητα, η διαχείριση και η λειτουργία ανήκει στην Ένωση, ή γίνεται εξ ονόματος αυτής, στο πλαίσιο των διαστημικών προγραμμάτων της. Λόγω των αλληλεξαρτήσεων αυτών, οποιαδήποτε διατάραξη, ακόμη και αν αρχικά περιοριζόταν σε μία οντότητα ή σε έναν τομέα, μπορεί να έχει ευρύτερες αλυσιδωτές επιπτώσεις, με δυνητικά μεγάλης κλίμακας και μακροχρόνιο αρνητικό αντίκτυπο στην παροχή υπηρεσιών σε ολόκληρη την εσωτερική αγορά. Οι ενταθείσες κυβερνοεπιθέσεις στη διάρκεια της πανδημίας της COVID-19 κατέδειξαν την τρωτότητα των ολοένα και πιο αλληλεξαρτώμενων κοινωνιών απέναντι σε κινδύνους χαμηλής πιθανότητας.

(38) Δεδομένων των διαφορών στις εθνικές δομές διακυβέρνησης και προκειμένου να διασφαλιστούν οι ήδη υφιστάμενες τομεακές ρυθμίσεις ή οι εποπτικοί και ρυθμιστικοί φορείς της Ένωσης, τα κράτη μέλη θα πρέπει να είναι σε θέση να ορίσουν ή να συστήσουν μία ή περισσότερες αρμόδιες αρχές υπεύθυνες για την κυβερνοασφάλεια και για τα εποπτικά καθήκοντα δυνάμει της παρούσας οδηγίας.

(39) Για τη διευκόλυνση της διασυνοριακής συνεργασίας και επικοινωνίας μεταξύ των αρχών, και για να καταστεί δυνατή η αποτελεσματική εφαρμογή της παρούσας οδηγίας, είναι ανάγκη κάθε κράτος μέλος να ορίζει ένα ενιαίο σημείο επαφής υπεύθυνο για τον συντονισμό θεμάτων σχετικά με την ασφάλεια συστημάτων δικτύου και πληροφοριών και με τη διασυνοριακή συνεργασία σε επίπεδο Ένωσης.

(40) Τα ενιαία σημεία επαφής θα πρέπει να διασφαλίζουν την αποτελεσματική διασυνοριακή συνεργασία με τις αρμόδιες αρχές άλλων κρατών μελών και, κατά περίπτωση, με την Επιτροπή και τον ENISA. Συνεπώς, τα ενιαία σημεία επαφής θα πρέπει να είναι επιφορτισμένα με τη διαβίβαση των κοινοποιήσεων σημαντικών περιστατικών με διασυνοριακό αντίκτυπο στα ενιαία σημεία επαφής άλλων επηρεαζόμενων κρατών μελών κατόπιν αιτήματος της CSIRT ή της αρμόδιας αρχής. Σε εθνικό επίπεδο, τα ενιαία σημεία επαφής θα πρέπει να επιτρέπουν την ομαλή διατομεακή συνεργασία με άλλες αρμόδιες αρχές. Τα ενιαία σημεία επαφής θα μπορούσαν επίσης να είναι οι αποδέκτες σχετικών πληροφοριών σχετικά με περιστατικά που αφορούν χρηματοπιστωτικές οντότητες από τις αρμόδιες αρχές δυνάμει του κανονισμού (ΕΕ) 2022/2554, τις οποίες θα πρέπει να είναι σε θέση να διαβιβάζουν, κατά περίπτωση, στις CSIRT ή στις αρμόδιες αρχές δυνάμει της παρούσας οδηγίας.

(41) Τα κράτη μέλη θα πρέπει να είναι επαρκώς εξοπλισμένα, όσον αφορά τόσο τις τεχνικές όσο και τις οργανωτικές ικανότητες, για την πρόληψη, τον εντοπισμό, την αντιμετώπιση περιστατικών και κινδύνων, καθώς και για τον μετριασμό των επιπτώσεών τους. Τα κράτη μέλη θα πρέπει επομένως να συστήσουν ή ορίσουν μία ή περισσότερες CSIRT δυνάμει της παρούσας οδηγίας και να διασφαλίσουν ότι διαθέτουν επαρκείς πόρους και τεχνικές ικανότητες. Οι CSIRT θα πρέπει να συμμορφώνονται με τις απαιτήσεις που ορίζονται στην παρούσα οδηγία, προκειμένου να διασφαλίζονται αποτελεσματικές και συμβατές ικανότητες αντιμετώπισης περιστατικών και κινδύνων και να διασφαλίζεται αποτελεσματική συνεργασία σε επίπεδο Ένωσης. Τα κράτη μέλη δύνανται να ορίσουν υπάρχουσες ομάδες αντιμετώπισης περιστατικών ασφαλείας σε υπολογιστές (Computer Emergency Response Teams — CERT) ως CSIRT. Προκειμένου να ενισχυθεί η σχέση εμπιστοσύνης μεταξύ των οντοτήτων και των CSIRT, στις περιπτώσεις που μια CSIRT αποτελεί μέρος της αρμόδιας αρχής, τα κράτη μέλη θα πρέπει να μπορούν να εξετάσουν το ενδεχόμενο λειτουργικού διαχωρισμού μεταξύ των επιχειρησιακών καθηκόντων που επιτελούν οι CSIRT, ιδίως όσον αφορά την ανταλλαγή πληροφοριών και τη στήριξη προς τις οντότητες, και των εποπτικών δραστηριοτήτων των αρμόδιων αρχών.

(42) Οι CSIRT είναι επιφορτισμένες με τον χειρισμό περιστατικών. Αυτό περιλαμβάνει την επεξεργασία μεγάλων όγκων ενίοτε ευαίσθητων δεδομένων. Τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι οι CSIRT διαθέτουν υποδομή για την ανταλλαγή και επεξεργασία πληροφοριών, καθώς και καλά εξοπλισμένο προσωπικό, ώστε να διασφαλίζονται η εμπιστευτικότητα και η αξιοπιστία των δραστηριοτήτων τους. Οι CSIRT θα μπορούσαν επίσης να θεσπίσουν σχετικούς κώδικες δεοντολογίας.

(43) Όσον αφορά τα δεδομένα προσωπικού χαρακτήρα, οι CSIRT θα πρέπει να είναι σε θέση να παρέχουν, σύμφωνα με τον κανονισμό (ΕΕ) 2016/679, εξ ονόματος και κατόπιν αιτήματος βασικής ή σημαντικής οντότητας, προληπτική σάρωση των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούνται για την παροχή των υπηρεσιών τους. Κατά περίπτωση, τα κράτη μέλη θα πρέπει να στοχεύουν στην εξασφάλιση του ίδιου επιπέδου τεχνικών ικανοτήτων για όλες τις τομεακές CSIRT. Τα κράτη μέλη θα πρέπει να μπορούν να ζητούν τη συνδρομή του ENISA για την ανάπτυξη των CSIRT τους.

(44) Οι CSIRT θα πρέπει να έχουν τη δυνατότητα, κατόπιν αιτήματος μιας βασικής ή σημαντικής οντότητας, να παρακολουθούν τα στοιχεία της οντότητας που βρίσκονται στο διαδίκτυο, τόσο εντός όσο και εκτός των εγκαταστάσεων, προκειμένου να εντοπίζουν, να κατανοούν και να διαχειρίζονται τους συνολικούς οργανωτικούς κινδύνους της οντότητας όσον αφορά τις νεοεντοπισθείσες προσβολές της αλυσίδας εφοδιασμού ή τις κρίσιμες τρωτότητες. Η οντότητα θα πρέπει να ενθαρρύνεται να γνωστοποιεί στην CSIRT κατά πόσον διαχειρίζεται προνομιακή διεπαφή διαχείρισης, καθώς αυτό θα μπορούσε να επηρεάσει την ταχύτητα λήψης μέτρων μετριασμού.

(45) Δεδομένης της σημασίας της διεθνούς συνεργασίας για την κυβερνοασφάλεια, οι CSIRT θα πρέπει να έχουν τη δυνατότητα να συμμετέχουν σε διεθνή δίκτυα συνεργασίας πέραν του δικτύου CSIRT που θεσπίζεται με την παρούσα οδηγία. Κατά συνέπεια, για τους σκοπούς της εκτέλεσης των καθηκόντων τους, οι CSIRT και οι αρμόδιες αρχές θα πρέπει να είναι σε θέση να ανταλλάσσουν πληροφορίες, συμπεριλαμβανομένων των δεδομένων προσωπικού χαρακτήρα, με τις εθνικές ομάδες αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές ή με αρμόδιες αρχές τρίτων χωρών, υπό την προϋπόθεση ότι πληρούνται οι προϋποθέσεις της ενωσιακής νομοθεσίας για την προστασία των δεδομένων για τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες, μεταξύ άλλων εκείνες του άρθρου 49 του κανονισμού (ΕΕ) 2016/679.

(46) Είναι ουσιαστικής σημασίας η εξασφάλιση επαρκών πόρων για την επίτευξη των στόχων της παρούσας οδηγίας και για να παρασχεθεί στις αρμόδιες αρχές και στις CSIRT η δυνατότητα να εκτελούν τα καθήκοντα που ορίζονται στο παρόν. Τα κράτη μέλη μπορούν να θεσπίσουν σε εθνικό επίπεδο χρηματοδοτικό μηχανισμό για την κάλυψη των αναγκαίων δαπανών σε σχέση με την εκτέλεση των καθηκόντων των δημόσιων φορέων που είναι αρμόδιοι για την κυβερνοασφάλεια στο κράτος μέλος σύμφωνα με την παρούσα οδηγία. Ο εν λόγω μηχανισμός θα πρέπει να συμμορφώνεται με το δίκαιο της Ένωσης, να είναι αναλογικός και να μην εισάγει διακρίσεις, και να λαμβάνει υπόψη τις διαφορετικές προσεγγίσεις για την παροχή ασφαλών υπηρεσιών.

(47) Το δίκτυο CSIRT θα πρέπει να συνεχίσει να συμβάλλει στην ενίσχυση της αξιοπιστίας και της εμπιστοσύνης και να προωθεί την ταχεία και αποτελεσματική επιχειρησιακή συνεργασία μεταξύ των κρατών μελών. Για να ενισχυθεί η επιχειρησιακή συνεργασία σε επίπεδο Ένωσης, το δίκτυο CSIRT θα πρέπει να εξετάσει το ενδεχόμενο να προσκαλέσει όργανα και οργανισμούς της Ένωσης που εμπλέκονται στην πολιτική για την κυβερνοασφάλεια, όπως η Ευρωπόλ, να συμμετάσχουν στις εργασίες του.

(48) Για την επίτευξη και τη διατήρηση υψηλού επιπέδου κυβερνοασφάλειας, οι εθνικές στρατηγικές κυβερνοασφάλειας που απαιτούνται βάσει της παρούσας οδηγίας θα πρέπει να αποτελούνται από συνεκτικά πλαίσια που παρέχουν στρατηγικούς στόχους και προτεραιότητες στον τομέα της κυβερνοασφάλειας και της διακυβέρνησης για την επίτευξή τους. Οι στρατηγικές αυτές μπορούν να αποτελούνται από ένα ή περισσότερα νομοθετικά ή μη νομοθετικά μέσα.

(49) Οι πολιτικές κυβερνοϋγιεινής παρέχουν τα θεμέλια για την προστασία των υποδομών δικτυακών και πληροφοριακών συστημάτων, του υλικού, του λογισμικού και της ασφάλειας των διαδικτυακών εφαρμογών, καθώς και των δεδομένων των επιχειρήσεων ή των τελικών χρηστών στα οποία βασίζονται οι οντότητες. Οι πολιτικές κυβερνοϋγιεινής που περιλαμβάνουν κοινό βασικό σύνολο πρακτικών, συμπεριλαμβανομένων ενημερώσεων λογισμικού και αναβαθμίσεων υλικού, αλλαγών κωδικού πρόσβασης, διαχείρισης νέων εγκαταστάσεων, περιορισμού των λογαριασμών πρόσβασης σε επίπεδο διαχειριστή και δημιουργίας αντιγράφων ασφάλειας δεδομένων, δημιουργούν ένα προληπτικό πλαίσιο ετοιμότητας και γενικής ασφάλειας και προστασίας σε περίπτωση περιστατικών ή κυβερνοαπειλών. Ο ENISA θα πρέπει να παρακολουθεί και να αναλύει τις πολιτικές κυβερνοϋγιεινής των κρατών μελών.

(50) Η ευαισθητοποίηση στον τομέα της κυβερνοασφάλειας και η κυβερνοϋγιεινή είναι ουσιαστικής σημασίας για την ενίσχυση του επιπέδου κυβερνοασφάλειας εντός της Ένωσης, ιδίως μέσα από το πρίσμα του αυξανόμενου αριθμού συνδεδεμένων συσκευών που χρησιμοποιούνται όλο και περισσότερο σε κυβερνοεπιθέσεις. Θα πρέπει να καταβληθούν προσπάθειες για την ενίσχυση της συνολικής ευαισθητοποίησης σχετικά με τους κινδύνους που συνδέονται με τα εν λόγω ιατροτεχνολογικά προϊόντα, ενώ οι αξιολογήσεις σε επίπεδο Ένωσης θα μπορούσαν να συμβάλουν στη διασφάλιση κοινής αντίληψης των κινδύνων αυτών στην εσωτερική αγορά.

(51) Τα κράτη μέλη θα πρέπει να ενθαρρύνουν τη χρήση κάθε καινοτόμου τεχνολογίας, συμπεριλαμβανομένης της τεχνητής νοημοσύνης, η χρήση της οποίας θα μπορούσε να βελτιώσει τον εντοπισμό και την πρόληψη κυβερνοεπιθέσεων, καθιστώντας δυνατή την αποτελεσματικότερη διοχέτευση πόρων για την αντιμετώπιση κυβερνοεπιθέσεων. Για το σκοπό αυτό, τα κράτη μέλη θα πρέπει να ενθαρρύνουν, στο πλαίσιο της εθνικής στρατηγικής τους για την κυβερνοασφάλεια, τις δραστηριότητες έρευνας και ανάπτυξης για τη διευκόλυνση της χρήσης των εν λόγω τεχνολογιών, ιδίως εκείνων που σχετίζονται με αυτοματοποιημένα ή ημιαυτοματοποιημένα εργαλεία κυβερνοασφάλειας, και, κατά περίπτωση, την ανταλλαγή δεδομένων που απαιτούνται για την κατάρτιση των χρηστών της εν λόγω τεχνολογίας και για τη βελτίωσή της. Η χρήση κάθε καινοτόμου τεχνολογίας, συμπεριλαμβανομένης της τεχνητής νοημοσύνης, θα πρέπει να συμμορφώνεται με την ενωσιακή νομοθεσία για την προστασία των δεδομένων, συμπεριλαμβανομένων των αρχών προστασίας των δεδομένων που αφορούν την ακρίβεια των δεδομένων, την ελαχιστοποίηση των δεδομένων, τη δικαιοσύνη και τη διαφάνεια, καθώς και την ασφάλεια των δεδομένων, όπως η τελευταίας τεχνολογίας κρυπτογράφηση. Οι απαιτήσεις προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού που ορίζονται στον κανονισμό (ΕΕ) 2016/679 θα πρέπει να αξιοποιηθούν πλήρως.

(52) Τα εργαλεία και οι εφαρμογές κυβερνοασφάλειας ανοικτού κώδικα μπορούν να συμβάλουν σε υψηλότερο βαθμό διαφάνειας και δύνανται να έχουν θετικό αντίκτυπο στην αποδοτικότητα της βιομηχανικής καινοτομίας. Τα ανοικτά πρότυπα διευκολύνουν τη διαλειτουργικότητα μεταξύ των εργαλείων ασφάλειας, ωφελώντας την ασφάλεια των ενδιαφερόμενων μερών του βιομηχανικού κλάδου. Τα εργαλεία και οι εφαρμογές κυβερνοασφάλειας ανοικτού κώδικα μπορούν να αξιοποιήσουν την ευρύτερη κοινότητα των φορέων ανάπτυξης, καθιστώντας δυνατή τη διαφοροποίηση των προμηθευτών. Ο ανοικτός κώδικας μπορεί να οδηγήσει σε διαφανέστερη διαδικασία επαλήθευσης των εργαλείων που σχετίζονται με την κυβερνοασφάλεια και σε μια διαδικασία εντοπισμού ευπαθειών σε επίπεδο κοινότητας. Συνεπώς, τα κράτη μέλη θα πρέπει να μπορούν να προωθήσουν τη χρήση λογισμικού ανοικτού κώδικα και ανοικτών προτύπων με την εφαρμογή πολιτικών που συνδέονται με τη χρήση ανοικτών δεδομένων και ανοικτού κώδικα στο πλαίσιο της ασφάλειας μέσω διαφάνειας. Οι πολιτικές που προωθούν την εισαγωγή και τη βιώσιμη χρήση εργαλείων κυβερνοασφάλειας ανοικτού κώδικα έχουν ιδιαίτερη σημασία για τις μικρές και μεσαίες επιχειρήσεις που αντιμετωπίζουν σημαντικό κόστος υλοποίησης, το οποίο θα μπορούσε να ελαχιστοποιηθεί με τη μείωση της ανάγκης για συγκεκριμένες εφαρμογές ή εργαλεία.

(53) Οι υπηρεσίες κοινής ωφελείας συνδέονται όλο και περισσότερο με ψηφιακά δίκτυα στις πόλεις, με σκοπό τη βελτίωση των δικτύων αστικών μεταφορών, την αναβάθμιση των εγκαταστάσεων ύδρευσης και διάθεσης αποβλήτων και την αύξηση της αποδοτικότητας του φωτισμού και της θέρμανσης των κτιρίων. Αυτές οι ψηφιοποιημένες υπηρεσίες κοινής ωφελείας είναι ευπαθείς σε κυβερνοεπιθέσεις και διατρέχουν τον κίνδυνο, σε περίπτωση επιτυχούς κυβερνοεπίθεσης, να βλάψουν τους πολίτες σε μεγάλη κλίμακα λόγω της διασύνδεσής τους. Τα κράτη μέλη θα πρέπει να αναπτύξουν μια πολιτική που θα αντιμετωπίζει την ανάπτυξη των εν λόγω συνδεδεμένων ή έξυπνων πόλεων και τις πιθανές επιπτώσεις τους στην κοινωνία, στο πλαίσιο της εθνικής στρατηγικής τους για την κυβερνοασφάλεια.

(54) Τα τελευταία χρόνια, η Ένωση αντιμετώπισε εκθετική αύξηση των επιθέσεων λυτρισμικού, στις οποίες το κακόβουλο λογισμικό κρυπτογραφεί δεδομένα και συστήματα και απαιτεί την καταβολή λύτρων για την αποδέσμευση. Η αυξανόμενη συχνότητα και σοβαρότητα των επιθέσεων λυτρισμικού μπορεί να οφείλεται σε διάφορους παράγοντες, όπως οι διαφορετικές μορφές επιθέσεων, τα εγκληματικά επιχειρηματικά μοντέλα για την πραγματοποίηση επιθέσεων λυτρισμικού ως παροχή υπηρεσίας και τα κρυπτονομίσματα, οι απαιτήσεις λύτρων και η αύξηση των επιθέσεων στην αλυσίδα εφοδιασμού. Τα κράτη μέλη θα πρέπει να αναπτύξουν πολιτική για την αντιμετώπιση της αύξησης των επιθέσεων λυτρισμικού στο πλαίσιο της εθνικής στρατηγικής τους για την κυβερνοασφάλεια.

(55) Οι συμπράξεις δημόσιου και ιδιωτικού τομέα («ΣΔΙΤ») στον τομέα της κυβερνοασφάλειας μπορούν να προσφέρουν κατάλληλο πλαίσιο για την ανταλλαγή γνώσεων, την ανταλλαγή βέλτιστων πρακτικών και την καθιέρωση κοινού επιπέδου κατανόησης μεταξύ των ενδιαφερόμενων μερών. Τα κράτη μέλη θα πρέπει να θεσπίσουν πολιτικές που θα στηρίζουν τη δημιουργία ΣΔΙΤ για την κυβερνοασφάλεια. Οι πολιτικές αυτές θα πρέπει να αποσαφηνίζουν, μεταξύ άλλων, το πεδίο εφαρμογής και τα ενδιαφερόμενα μέρη, το μοντέλο διακυβέρνησης, τις διαθέσιμες επιλογές χρηματοδότησης και την αλληλεπίδραση μεταξύ των συμμετεχόντων ενδιαφερόμενων μερών σε σχέση με τις ΣΔΙΤ. Οι ΣΔΙΤ μπορούν να αξιοποιήσουν την εμπειρογνωσία οντοτήτων του ιδιωτικού τομέα για να συνδράμουν τις αρμόδιες αρχές στην ανάπτυξη προηγμένων υπηρεσιών και διαδικασιών που περιλαμβάνουν, μεταξύ άλλων, την ανταλλαγή πληροφοριών, έγκαιρες προειδοποιήσεις, ασκήσεις αντιμετώπισης κυβερνοαπειλών και περιστατικών στον κυβερνοχώρο, τη διαχείριση κρίσεων και τον σχεδιασμό ανθεκτικότητας.

(56) Τα κράτη μέλη θα πρέπει, στις εθνικές στρατηγικές τους για την κυβερνοασφάλεια, να αντιμετωπίζουν τις ειδικές ανάγκες των μικρών και μεσαίων επιχειρήσεων στον τομέα της κυβερνοασφάλειας. Οι μικρές και μεσαίες επιχειρήσεις αντιπροσωπεύουν, σε επίπεδο Ένωσης, μεγάλο ποσοστό της βιομηχανικής και επιχειρηματικής αγοράς και συχνά δυσκολεύονται να προσαρμοστούν στις νέες επιχειρηματικές πρακτικές σε έναν πιο συνδεδεμένο κόσμο, και στο ψηφιακό περιβάλλον, με τους εργαζομένους να εργάζονται κατ' οίκον και τις επιχειρήσεις να δραστηριοποιούνται διαρκώς περισσότερο στο διαδίκτυο. Ορισμένες μικρές και μεσαίες επιχειρήσεις αντιμετωπίζουν συγκεκριμένες προκλήσεις κυβερνοασφάλειας, όπως χαμηλή κυβερνοευαισθητοποίηση, έλλειψη τηλεματικής ασφάλειας ΤΠ, υψηλό κόστος λύσεων κυβερνοασφάλειας και αυξημένο επίπεδο απειλών, όπως το λυτρισμικό, για τις οποίες θα πρέπει να λαμβάνουν καθοδήγηση και βοήθεια. Οι μικρές και μεσαίες επιχειρήσεις καθίστανται όλο και περισσότερο στόχος επιθέσεων στην αλυσίδα εφοδιασμού λόγω των λιγότερο αυστηρών μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και της διαχείρισης επιθέσεων, καθώς και λόγω του γεγονότος ότι διαθέτουν περιορισμένους πόρους ασφάλειας. Οι εν λόγω επιθέσεις στην αλυσίδα εφοδιασμού όχι μόνο έχουν αντίκτυπο στις μικρές και μεσαίες επιχειρήσεις και στις δραστηριότητές

τους μεμονωμένα, αλλά μπορούν επίσης να έχουν αλυσιδωτές επιπτώσεις σε μεγαλύτερες επιθέσεις κατά οντοτήτων στις οποίες παρείχαν προμήθειες. Τα κράτη μέλη θα πρέπει, μέσω των εθνικών στρατηγικών τους για την κυβερνοασφάλεια, να βοηθούν τις μικρές και μεσαίες επιχειρήσεις να αντιμετωπίσουν τις προκλήσεις που αντιμετωπίζουν οι αλυσίδες εφοδιασμού τους. Τα κράτη μέλη θα πρέπει να διαθέτουν ένα σημείο επαφής για τις μικρές και μεσαίες επιχειρήσεις σε εθνικό ή περιφερειακό επίπεδο, το οποίο είτε θα παρέχει καθοδήγηση και συνδρομή στις μικρές και μεσαίες επιχειρήσεις είτε θα τις κατευθύνει στους κατάλληλους φορείς για καθοδήγηση και συνδρομή όσον αφορά ζητήματα κυβερνοασφάλειας. Τα κράτη μέλη ενθαρρύνονται επίσης να προσφέρουν υπηρεσίες όπως η παροχή δυνατότητας για διαμόρφωση ιστοτόπων και καταγραφή δεδομένων σε πολύ μικρές και μικρές επιχειρήσεις που δεν διαθέτουν τις σχετικές ικανότητες.

(57) Στο πλαίσιο των εθνικών στρατηγικών τους για την ασφάλεια στον κυβερνοχώρο, τα κράτη μέλη θα πρέπει να εγκρίνουν πολιτικές για την προώθηση της ενεργητικής κυβερνοπροστασίας στο πλαίσιο μιας ευρύτερης αμυντικής στρατηγικής. Σε αντιδιαστολή με την εκ των υστέρων ανταπόκριση, η ενεργητική κυβερνοπροστασία συνίσταται στην πρόληψη, τον εντοπισμό, την παρακολούθηση, την ανάλυση και τον μετριασμό των παραβιάσεων της ασφάλειας των δικτύων με ενεργό τρόπο, σε συνδυασμό με τη χρήση ικανοτήτων που αναπτύσσονται εντός και εκτός του δικτύου των θυμάτων. Αυτό θα μπορούσε να περιλαμβάνει την παροχή δωρεάν υπηρεσιών ή εργαλείων σε ορισμένες οντότητες από τα κράτη μέλη, συμπεριλαμβανομένων των ελέγχων αυτοεξυπηρέτησης, των εργαλείων ανίχνευσης και των υπηρεσιών απόσυρσης. Η ικανότητα ταχείας και αυτόματης ανταλλαγής και κατανόησης πληροφοριών και αναλύσεων απειλών, προειδοποιήσεων για δραστηριότητες στον κυβερνοχώρο, και δράσης αντιμετώπισης είναι ζωτικής σημασίας για να καταστεί δυνατή η ενότητα των προσπαθειών για την επιτυχή πρόληψη, ανίχνευση, αντιμετώπιση και παρεμπόδιση επιθέσεων κατά συστημάτων δικτύου και πληροφοριών. Η ενεργητική κυβερνοπροστασία βασίζεται σε μια αμυντική στρατηγική που αποκλείει τα επιθετικά μέτρα.

(58) Δεδομένου ότι η εκμετάλλευση των τρωτοτήτων στα συστήματα δικτύου και πληροφοριών μπορεί να προκαλέσει σημαντικές διαταράξεις και βλάβες, ο άμεσος εντοπισμός και η διόρθωση αυτών των τρωτοτήτων αποτελεί σημαντικό παράγοντα μείωσης του κινδύνου. Οι οντότητες που αναπτύσσουν ή διαχειρίζονται συστήματα δικτύου και πληροφοριών θα πρέπει, συνεπώς, να θεσπίσουν κατάλληλες διαδικασίες για την αντιμετώπιση των τρωτοτήτων όταν εντοπίζονται. Δεδομένου ότι οι ευπάθειες συχνά εντοπίζονται και γνωστοποιούνται από τρίτους, ο κατασκευαστής ή ο πάροχος προϊόντων ή υπηρεσιών ΤΠΕ θα πρέπει επίσης να θεσπίσει τις αναγκαίες διαδικασίες για τη λήψη πληροφοριών από τρίτους σχετικά με ευπάθειες. Στο πλαίσιο αυτό, τα διεθνή πρότυπα ISO/IEC 30111 και ISO/IEC 29147 παρέχουν καθοδήγηση σχετικά με τον χειρισμό τρωτοτήτων και τη γνωστοποίηση τρωτοτήτων. Η ενίσχυση του συντονισμού μεταξύ των αναφερόντων φυσικών και νομικών προσώπων και των κατασκευαστών ή παρόχων προϊόντων ΤΠΕ ή υπηρεσιών ΤΠΕ είναι ιδιαίτερα σημαντική για τον σκοπό της διευκόλυνσης του εθελοντικού πλαισίου γνωστοποίησης τρωτοτήτων. Η συντονισμένη γνωστοποίηση τρωτοτήτων καθορίζει μια δομημένη διαδικασία μέσω της οποίας αναφέρονται στον κατασκευαστή ή τον πάροχο των δυνητικά ευάλωτων προϊόντων ΤΠΕ ή υπηρεσιών ΤΠΕ οι τρωτότητες, κατά τρόπο που να του επιτρέπει να διαγιγνώσκει και να αποκαθιστά την τρωτότητα πριν από τη γνωστοποίηση λεπτομερών πληροφοριών για τρωτότητες σε τρίτους ή στο κοινό. Η συντονισμένη γνωστοποίηση τρωτοτήτων θα πρέπει επίσης να περιλαμβάνει συντονισμό μεταξύ του αναφέροντος φυσικού ή νομικού προσώπου και του κατασκευαστή ή του παρόχου των δυνητικά ευάλωτων προϊόντων ΤΠΕ ή υπηρεσιών ΤΠΕ όσον αφορά το χρονοδιάγραμμα αποκατάστασης και δημοσίευσης των τρωτοτήτων.

(59) Η Επιτροπή, ο ENISA και τα κράτη μέλη θα πρέπει να συνεχίσουν να προωθούν την ευθυγράμμιση με διεθνή πρότυπα και υπάρχουσες βέλτιστες πρακτικές της βιομηχανίας στον τομέα της διαχείρισης κινδύνων κυβερνοασφάλειας, για παράδειγμα στους τομείς των αξιολογήσεων ασφάλειας της αλυσίδας εφοδιασμού, της ανταλλαγής πληροφοριών και της γνωστοποίησης τρωτοτήτων.

(60) Τα κράτη μέλη, σε συνεργασία με τον ENISA, οφείλουν να λάβουν μέτρα για να διευκολύνουν τη συντονισμένη γνωστοποίηση τρωτοτήτων με τη θέσπιση σχετικής εθνικής πολιτικής. Στο πλαίσιο της εθνικής πολιτικής τους, τα κράτη μέλη θα πρέπει να στοχεύουν στην αντιμετώπιση, στο μέτρο του δυνατού, των προκλήσεων που αντιμετωπίζουν πρόσωπα που ερευνούν ευπάθειες, συμπεριλαμβανομένης της ενδεχόμενης έκθεσής τους σε ποινική ευθύνη, σύμφωνα με την εθνική νομοθεσία τους. Δεδομένου ότι τα φυσικά και νομικά πρόσωπα που ερευνούν ευπάθειες θα μπορούσαν σε ορισμένα κράτη μέλη να εκτεθούν σε ποινική και αστική ευθύνη, τα κράτη μέλη ενθαρρύνονται να εγκρίνουν κατευθυντήριες γραμμές όσον αφορά τη μη δίωξη των ερευνητών στον τομέα της ασφάλειας των πληροφοριών και την απαλλαγή από την αστική ευθύνη για τις δραστηριότητές τους.

(61) Τα κράτη μέλη θα πρέπει να ορίσουν μια από τις CSIRT τους ως συντονιστή η οποία να ενεργεί ως αξιόπιστος ενδιάμεσος φορέας μεταξύ των αναφερόντων φυσικών ή νομικών προσώπων και των κατασκευαστών προϊόντων ΤΠΕ ή παρόχων υπηρεσιών ΤΠΕ, που ενδέχεται να επηρεαστούν από την τρωτότητα, όπου απαιτείται. Τα καθήκοντα της CSIRT που ορίσθηκε ως συντονιστής θα πρέπει να περιλαμβάνουν τον προσδιορισμό των οικείων οντοτήτων και την επικοινωνία με αυτές, την παροχή συνδρομής στα φυσικά ή νομικά πρόσωπα που αναφέρουν ευπάθειες, τη διαπραγμάτευση χρονοδιαγραμμάτων γνωστοποίησης και τη διαχείριση τρωτοτήτων που επηρεάζουν πλείονες οντότητες (πολυμερής

συντονισμένη γνωστοποίηση ευπαθειών). Όταν η αναφερόμενη τρωτότητα θα μπορούσε να έχει σημαντικό αντίκτυπο σε οντότητες σε περισσότερα του ενός κράτη μέλη, οι CSIRT που ορίσθηκαν ως συντονιστές θα πρέπει να συνεργάζονται στο πλαίσιο του δικτύου CSIRT, κατά περίπτωση.

(62) Η πρόσβαση σε ορθές και έγκαιρες πληροφορίες σχετικά με ευπάθειες που επηρεάζουν τα προϊόντα και τις υπηρεσίες ΤΠΕ συμβάλλει στην ενίσχυση της διαχείρισης κινδύνων κυβερνοασφάλειας. Οι πηγές δημόσια διαθέσιμων πληροφοριών σχετικά με τρωτότητες αποτελούν σημαντικό εργαλείο για τις οντότητες και τους χρήστες των υπηρεσιών τους, αλλά και για τις εθνικές αρμόδιες αρχές και τις CSIRT. Για τον λόγο αυτό, ο ENISA θα πρέπει να καταρτίσει μια ευρωπαϊκή βάση δεδομένων ευπαθειών όπου οι οντότητες, ανεξαρτήτως από το αν εμπίπτουν στο πεδίο της παρούσας οδηγίας, και οι προμηθευτές τους για συστήματα δικτύου και πληροφοριών, όπως επίσης οι αρμόδιες αρχές και οι CSIRT, μπορούν να δημοσιοποιούν και να καταχωρούν, σε εθελοντική βάση, δημόσια γνωστές ευπάθειες ώστε να μπορούν οι χρήστες να λαμβάνουν κατάλληλα μέτρα μετριασμού. Σκοπός της εν λόγω βάσης δεδομένων είναι η αντιμετώπιση των μοναδικών προκλήσεων που συνιστούν οι κίνδυνοι κυβερνοασφάλειας για τις οντότητες στην Ένωση. Επιπλέον, ο ENISA θα πρέπει να θεσπίσει κατάλληλη διαδικασία σχετικά με τη διαδικασία δημοσίευσης, προκειμένου να δοθεί στις οντότητες ο χρόνος να λάβουν μέτρα μετριασμού όσον αφορά τις τρωτότητές τους και να εφαρμόσουν σύγχρονα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας, καθώς και μηχαναγνώσιμα σύνολα δεδομένων και αντίστοιχες διεπαφές. Για να ενθαρρυνθεί η νοοτροπία γνωστοποίησης ευπαθειών, η γνωστοποίηση δεν θα πρέπει να βλάπτει το αναφέρον φυσικό ή νομικό πρόσωπο.

(63) Μολονότι υπάρχουν παρόμοια μητρώα ή βάσεις δεδομένων ευπαθειών, αυτά φιλοξενούνται και τηρούνται από οντότητες που δεν είναι εγκατεστημένες στην Ένωση. Μια ευρωπαϊκή βάση δεδομένων ευπαθειών που θα τηρείται από τον ENISA θα προσέφερε βελτιωμένη διαφάνεια όσον αφορά στη διαδικασία δημοσίευσης προτού κάποια ευπάθεια γίνει δημόσια γνωστή, καθώς και ανθεκτικότητα σε περίπτωση διατάραξης ή διακοπής της παροχής παρόμοιων υπηρεσιών. Προκειμένου, στο μέτρο του δυνατού, να αποφευχθεί η αλληλεπικάλυψη των προσπαθειών και να επιδιωχθεί η συμπληρωματικότητα, ο ENISA θα πρέπει να διερευνήσει τη δυνατότητα σύναψης συμφωνιών διαρθρωμένης συνεργασίας με παρόμοια μητρώα ή βάσεις δεδομένων που υπάγονται στη δικαιοδοσία τρίτων χωρών. Ειδικότερα, ο ENISA θα πρέπει να διερευνήσει τη δυνατότητα στενής συνεργασίας με τους φορείς εκμετάλλευσης του συστήματος Κοινών Ευπαθειών και Εκτεθειμένων Σημείων (CVE).

(64) Η Ομάδα Συνεργασίας θα πρέπει να στηρίζει και να διευκολύνει τη στρατηγική συνεργασία και την ανταλλαγή πληροφοριών, καθώς και να ενισχύει την εμπιστοσύνη μεταξύ των κρατών μελών. Η Ομάδα Συνεργασίας θα πρέπει να καταρτίζει ανά διετία πρόγραμμα εργασίας. Το πρόγραμμα εργασίας θα πρέπει να περιλαμβάνει τις ενέργειες που θα αναλάβει η Ομάδα Συνεργασίας για την υλοποίηση των στόχων και των καθηκόντων της. Το χρονοδιάγραμμα για την κατάρτιση του πρώτου προγράμματος εργασιών βάσει της παρούσας οδηγίας θα πρέπει να ευθυγραμμιστεί με το χρονοδιάγραμμα του τελευταίου προγράμματος εργασίας που θεσπίστηκε δυνάμει της οδηγίας (ΕΕ) 2016/1148, προκειμένου να αποφευχθούν πιθανές διαταραχές στις εργασίες της ομάδας συνεργασίας.

(65) Κατά την κατάρτιση έγγραφων οδηγιών, η Ομάδα Συνεργασίας θα πρέπει να χαρτογραφεί με συνέπεια τις εθνικές λύσεις και εμπειρίες, να αξιολογεί τον αντίκτυπο των παραδοτέων της Ομάδας Συνεργασίας στις εθνικές προσεγγίσεις, να συζητά τις προκλήσεις εφαρμογής και να διατυπώνει ειδικές συστάσεις, ιδίως όσον αφορά τη διευκόλυνση της ευθυγράμμισης της μεταφοράς της παρούσας οδηγίας στο εθνικό δίκαιο των κρατών μελών, οι οποίες πρέπει να αντιμετωπιστούν μέσω της καλύτερης εφαρμογής των υφιστάμενων κανόνων. Η Ομάδα Συνεργασίας θα μπορούσε επίσης να χαρτογραφήσει τις εθνικές λύσεις, προκειμένου να προωθήσει τη συμβατότητα των λύσεων κυβερνοασφάλειας που εφαρμόζονται σε κάθε συγκεκριμένο τομέα σε ολόκληρη την Ένωση. Αυτό είναι ιδιαίτερα σημαντικό στους τομείς με διεθνή ή διασυνοριακό χαρακτήρα.

(66) Η Ομάδα Συνεργασίας θα πρέπει να παραμείνει ένα ευέλικτο φόρουμ και να είναι σε θέση να αντιδρά σε μεταβαλλόμενες και νέες πολιτικές προτεραιότητες και προκλήσεις, λαμβάνοντας παράλληλα υπόψη τη διαθεσιμότητα των πόρων. Θα μπορούσε να οργανώνει τακτικές κοινές συνεδριάσεις με σχετικά ενδιαφερόμενα μέρη του ιδιωτικού τομέα από ολόκληρη την Ένωση για τη συζήτηση των δραστηριοτήτων που διεξάγονται από την Ομάδα Συνεργασίας και τη συλλογή δεδομένων και στοιχείων σχετικά με τις αναδυόμενες προκλήσεις πολιτικής. Επιπλέον, η Ομάδα Συνεργασίας θα πρέπει να διενεργεί τακτική αξιολόγηση της κατάστασης σε σχέση με κυβερνοαπειλές ή περιστατικά στον κυβερνοχώρο, όπως επιθέσεις λυτρισμικού. Προκειμένου να ενισχυθεί η συνεργασία σε επίπεδο Ένωσης, η Ομάδα Συνεργασίας θα πρέπει να εξετάσει το

ενδεχόμενο να καλέσει τα σχετικά θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης που μετέχουν στην πολιτική για την κυβερνοασφάλεια, όπως το Ευρωπαϊκό Κοινοβούλιο, την Ευρωπόλ, το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Ασφάλεια της Αεροπορίας, που συστάθηκε με τον κανονισμό (ΕΕ) 2018/1139, και τον Οργανισμό της Ευρωπαϊκής Ένωσης για το διαστημικό πρόγραμμα, που θεσπίστηκε με τον κανονισμό (ΕΕ) 2021/696 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([14]), να συμμετάσχουν στις εργασίες της.

(67) Οι αρμόδιες αρχές και οι CSIRT θα πρέπει να μπορούν να συμμετέχουν σε προγράμματα ανταλλαγής υπαλλήλων από άλλα κράτη μέλη, εντός ειδικού πλαισίου και, κατά περίπτωση, με την επιφύλαξη της απαιτούμενης εξουσιοδότησης ασφαλείας των υπαλλήλων που συμμετέχουν στα εν λόγω συστήματα ανταλλαγής, προκειμένου να βελτιωθεί η συνεργασία και να ενισχυθεί η εμπιστοσύνη μεταξύ των κρατών μελών. Οι αρμόδιες αρχές θα πρέπει να λαμβάνουν τα αναγκαία μέτρα ώστε οι υπάλληλοι από άλλα κράτη μέλη να είναι σε θέση να συμμετέχουν αποτελεσματικά στις δραστηριότητες της φιλοξενούσας αρμόδιας αρχής ή της φιλοξενούσας CSIRT.

(68) Τα κράτη μέλη θα πρέπει να συμβάλουν στη δημιουργία του πλαισίου της ΕΕ για την αντιμετώπιση κρίσεων στον κυβερνοχώρο που ορίζεται στη σύσταση (ΕΕ) 2017/1584 της Επιτροπής ([15]) μέσω των υφιστάμενων δικτύων συνεργασίας, ιδίως του του ευρωπαϊκού δικτύου οργανισμών διασύνδεσης για κρίσεις στον κυβερνοχώρο (EU-CyCLONe), του δικτύου CSIRT και της ομάδας συνεργασίας. Το EU-CyCLONe και το δίκτυο CSIRT θα πρέπει να συνεργάζονται βάσει διαδικαστικών ρυθμίσεων που θα καθορίζουν τις λεπτομέρειες της εν λόγω συνεργασίας και να αποφεύγουν τυχόν αλληλοεπικάλυψη εργασιών. Οι διαδικαστικοί κανόνες του EU-CyCLONe θα πρέπει να προσδιορίζουν περαιτέρω τις ρυθμίσεις για τη λειτουργία του δικτύου, συμπεριλαμβανομένων των ρόλων, των τρόπων συνεργασίας, των αλληλεπιδράσεων του δικτύου με άλλους σχετικούς παράγοντες και των υποδειγμάτων για την ανταλλαγή πληροφοριών, καθώς και των μέσων επικοινωνίας. Για τη διαχείριση κρίσεων σε επίπεδο Ένωσης, τα ενδιαφερόμενα μέρη θα πρέπει να βασίζονται στις ολοκληρωμένες ρυθμίσεις της ΕΕ για την αντιμετώπιση πολιτικών κρίσεων δυνάμει της εκτελεστικής απόφασης (ΕΕ) 2018/1993 του Συμβουλίου ([16]) (ρυθμίσεις IPCR). Η Επιτροπή θα πρέπει να χρησιμοποιήσει για τον σκοπό αυτό την υψηλού επιπέδου διαδικασία ARGUS για τον συντονισμό σε περιπτώσεις διατομεακών κρίσεων. Εάν η κρίση ενέχει σημαντική εξωτερική διάσταση ή διάσταση κοινής πολιτικής ασφάλειας και άμυνας, θα πρέπει να ενεργοποιείται ο Μηχανισμός Αντιμετώπισης Κρίσεων της Ευρωπαϊκής Υπηρεσίας Εξωτερικής Δράσης.

(69) Σύμφωνα με το παράρτημα της σύστασης (ΕΕ) 2017/1584, ως περιστατικό μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας θα πρέπει να νοείται εκείνο το οποίο προκαλεί διατάραξη που υπερβαίνει την ικανότητα ενός κράτους μέλους να ανταποκριθεί σε αυτή ή το οποίο έχει σημαντικό αντίκτυπο σε τουλάχιστον δύο κράτη μέλη. Ανάλογα με την αιτία και τις συνέπειές τους, τα περιστατικά μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας ενδέχεται να κλιμακωθούν και να μετατραπούν σε πραγματικές κρίσεις που καθιστούν αδύνατη την ομαλή λειτουργία της εσωτερικής αγοράς ή θέτουν σε σοβαρό κίνδυνο τη δημόσια ασφάλεια οντοτήτων ή πολιτών σε διάφορα κράτη μέλη ή την Ένωση στο σύνολό της. Δεδομένου των ευρειών συνεπειών και, στις περισσότερες περιπτώσεις, του διασυνοριακού χαρακτήρα τέτοιων περιστατικών, τα κράτη μέλη και τα σχετικά θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης θα πρέπει να συνεργάζονται σε τεχνικό, επιχειρησιακό και πολιτικό επίπεδο για τον κατάλληλο συντονισμό της αντιμετώπισής τους σε ολόκληρη την Ένωση.

(70) Τα περιστατικά μεγάλης κλίμακας και οι κρίσεις στον τομέα της κυβερνοασφάλειας σε επίπεδο Ένωσης απαιτούν συντονισμένη δράση για τη διασφάλιση ταχείας και αποτελεσματικής αντίδρασης, λόγω του υψηλού βαθμού αλληλεξάρτησης μεταξύ τομέων και κρατών μελών. Η διαθεσιμότητα κυβερνοανθεκτικών συστημάτων δικτύων και πληροφοριών και η διαθεσιμότητα, η εμπιστευτικότητα και η ακεραιότητα των δεδομένων είναι ζωτικής σημασίας για την ασφάλεια της Ένωσης και για την προστασία των πολιτών, των επιχειρήσεων και των θεσμικών οργάνων της από περιστατικά και κυβερνοαπειλές, καθώς και για την ενίσχυση της εμπιστοσύνης των ατόμων και των οργανισμών στην ικανότητα της Ένωσης να προωθεί και να προστατεύει έναν παγκόσμιο, ανοικτό, ελεύθερο, σταθερό και ασφαλή κυβερνοχώρο που θα βασίζεται στα ανθρώπινα δικαιώματα, τις θεμελιώδεις ελευθερίες, τη δημοκρατία και το κράτος δικαίου.

([14]) Κανονισμός (ΕΕ) 2021/696 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 28ης Απριλίου 2021, για τη θέσπιση του ενωσιακού διαστημικού προγράμματος και του Οργανισμού της Ευρωπαϊκής Ένωσης για το διαστημικό πρόγραμμα, και για την κατάργηση των κανονισμών (ΕΕ) αριθ. 912/2010, (ΕΕ) αριθ. 1285/2013 και (ΕΕ) αριθ. 377/2014 και της απόφασης αριθ. 541/2014/ΕΕ (ΕΕ L 170 της 12.5.2021, σ. 69).

([15]) Σύσταση (ΕΕ) 2017/1584 της Επιτροπής, της 13ης Σεπτεμβρίου 2017, για τη συντονισμένη αντιμετώπιση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο (ΕΕ L 239 της 19.9.2017, σ. 36).

([16]) Εκτελεστική απόφαση (ΕΕ) 2018/1993 του Συμβουλίου, της 11ης Δεκεμβρίου 2018, ως προς τις ρυθμίσεις για την ολοκληρωμένη αντιμετώπιση πολιτικών κρίσεων της ΕΕ (ΕΕ L 320 της 17.12.2018, σ. 28).

(71) Το EU-CyCLONe θα πρέπει να λειτουργεί ως ενδιάμεσος μεταξύ του τεχνικού και του πολιτικού επιπέδου κατά τη διάρκεια περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας, να ενισχύει τη συνεργασία σε επιχειρησιακό επίπεδο και να στηρίζει τη λήψη αποφάσεων σε πολιτικό επίπεδο. Σε συνεργασία με την Επιτροπή, έχοντας υπόψη την αρμοδιότητα της Επιτροπής στον τομέα της διαχείρισης κρίσεων, το EU-CyCLONe θα πρέπει να αξιοποιεί τα πορίσματα του δικτύου CSIRT και να χρησιμοποιεί τις δικές του ικανότητες για τη δημιουργία ανάλυσης επιπτώσεων περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας.

(72) Οι κυβερνοεπιθέσεις έχουν διασυνοριακό χαρακτήρα και ένα σημαντικό περιστατικό μπορεί να διαταράξει και να βλάψει κρίσιμες υποδομές πληροφοριών από τις οποίες εξαρτάται η ομαλή λειτουργία της εσωτερικής αγοράς. Η σύσταση (ΕΕ) 2017/1584 προσδιορίζει τον ρόλο όλων των σχετικών φορέων. Επιπλέον, η Επιτροπή είναι υπεύθυνη, στο πλαίσιο του μηχανισμού πολιτικής προστασίας της Ένωσης που θεσπίστηκε με την απόφαση αριθ. 1313/2013/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([17]), για γενικές δράσεις ετοιμότητας, συμπεριλαμβανομένης της διαχείρισης του Κέντρου Συντονισμού Αντιμετώπισης Εκτάκτων Αναγκών και του Κοινού Συστήματος Επικοινωνίας και Πληροφόρησης Έκτακτης Ανάγκης, για τη διατήρηση και περαιτέρω ανάπτυξη ικανοτήτων επίγνωσης και ανάλυσης της κατάστασης, και για τη δημιουργία και διαχείριση της ικανότητας κινητοποίησης και αποστολής ομάδων εμπειρογνωμόνων σε περίπτωση αιτήματος παροχής βοήθειας από κράτος μέλος ή τρίτη χώρα. Η Επιτροπή είναι επίσης αρμόδια για την υποβολή αναλυτικών εκθέσεων σχετικά με τις ρυθμίσεις IPCR δυνάμει της εκτελεστικής απόφασης (ΕΕ) 2018/1993, μεταξύ άλλων σε σχέση με την επίγνωση της κατάστασης και την ετοιμότητα στον τομέα της κυβερνοασφάλειας, καθώς και για την επίγνωση της κατάστασης και την αντιμετώπιση κρίσεων στους τομείς της γεωργίας, των δυσμενών καιρικών συνθηκών, της χαρτογράφησης και των προβλέψεων συγκρούσεων, των συστημάτων έγκαιρης προειδοποίησης για φυσικές καταστροφές, των καταστάσεων έκτακτης ανάγκης στον τομέα της υγείας, της επιτήρησης λοιμώξεων, της υγείας των φυτών, των περιστατικών χημικής ασφάλειας, της ασφάλειας των τροφίμων και των ζωοτροφών, της υγείας των ζώων, της μετανάστευσης, των τελωνείων, των καταστάσεων έκτακτης ανάγκης στον τομέα της πυρηνικής και ραδιολογικής κατάστασης, και της ενέργειας.

(73) Η Ένωση μπορεί, κατά περίπτωση, να συνάπτει διεθνείς συμφωνίες σύμφωνα με το άρθρο 218 ΣΛΕΕ με τρίτες χώρες ή διεθνείς οργανισμούς, που επιτρέπουν και οργανώνουν τη συμμετοχή τους σε ορισμένες δραστηριότητες της Ομάδας Συνεργασίας και του δικτύου CSIRT και EU-CyCLONe. Οι συμφωνίες αυτές θα πρέπει να διασφαλίζουν τα συμφέροντα της Ένωσης και την επαρκή προστασία των δεδομένων. Αυτό δεν θα πρέπει να αποκλείει το δικαίωμα των κρατών μελών να συνεργάζονται με τρίτες χώρες για τη διαχείριση τρωτοτήτων και τη διαχείριση κινδύνων κυβερνοασφάλειας, διευκολύνοντας την κοινοποίηση και τη γενική ανταλλαγή πληροφοριών σύμφωνα με το δίκαιο της Ένωσης.

(74) Προκειμένου να διευκολυνθεί η αποτελεσματική εφαρμογή της παρούσας οδηγίας όσον αφορά, μεταξύ άλλων, τη διαχείριση τρωτοτήτων, τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας, τις υποχρεώσεις κοινοποίησης και τις ρυθμίσεις ανταλλαγής πληροφοριών στον τομέα της κυβερνοασφάλειας, τα κράτη μέλη μπορούν να συνεργάζονται με τρίτες χώρες και να αναλαμβάνουν δραστηριότητες που θεωρούνται κατάλληλες για τον σκοπό αυτό, συμπεριλαμβανομένης της ανταλλαγής πληροφοριών σχετικά με κυβερνοαπειλές, περιστατικά, τρωτότητες, εργαλεία και μεθόδους, τακτικές, τεχνικές και διαδικασίες, ετοιμότητα και ασκήσεις διαχείρισης κρίσεων στον τομέα της κυβερνοασφάλειας, κατάρτιση, οικοδόμηση εμπιστοσύνης και ρυθμίσεις για διαρθρωμένη ανταλλαγή πληροφοριών.

(75) Θα πρέπει να εισαχθούν αξιολογήσεις από ομοτίμους για να διευκολυνθεί η άντληση διδαγμάτων από τις κοινές εμπειρίες, να ενισχυθεί η αμοιβαία εμπιστοσύνη και να επιτευχθεί υψηλό κοινό επίπεδο κυβερνοασφάλειας. Οι αξιολογήσεις από ομοτίμους μπορούν να οδηγήσουν σε πολύτιμες πληροφορίες και συστάσεις που ενισχύουν τις συνολικές ικανότητες κυβερνοασφάλειας, δημιουργώντας μια ακόμη λειτουργική οδό για την ανταλλαγή βέλτιστων πρακτικών μεταξύ των κρατών μελών και συμβάλλοντας στην ενίσχυση των επιπέδων ωριμότητας των κρατών μελών στον τομέα της κυβερνοασφάλειας. Επιπλέον, οι αξιολογήσεις από ομοτίμους θα πρέπει να λαμβάνουν υπόψη τα αποτελέσματα παρόμοιων μηχανισμών, όπως το σύστημα αξιολόγησης από ομοτίμους του δικτύου CSIRT, και θα πρέπει να προσθέτουν αξία και να αποφεύγουν τις επικαλύψεις. Η εφαρμογή των αξιολογήσεων από ομοτίμους δεν θα πρέπει να θίγει το ενωσιακό ή το εθνικό δίκαιο σχετικά με την προστασία των εμπιστευτικών ή διαβαθμισμένων πληροφοριών.

(76) Η Ομάδα Συνεργασίας θα πρέπει να θεσπίσει μεθοδολογία αυτοαξιολόγησης για τα κράτη μέλη, με στόχο την κάλυψη παραγόντων όπως το επίπεδο εφαρμογής των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και των υποχρεώσεων υποβολής εκθέσεων, το επίπεδο ικανοτήτων και η αποτελεσματικότητα της άσκησης των καθηκόντων των αρμόδιων αρχών, οι επιχειρησιακές ικανότητες των CSIRT, το επίπεδο εφαρμογής της αμοιβαίας συνδρομής, το επίπεδο εφαρμογής των ρυθμίσεων ανταλλαγής πληροφοριών στον τομέα της κυβερνοασφάλειας ή ειδικά ζητήματα διασυνοριακού ή διατομεακού χαρακτήρα. Τα κράτη μέλη θα πρέπει να ενθαρρύνονται να διενεργούν αυτοαξιολογήσεις σε τακτική βάση, καθώς και να παρουσιάζουν και να συζητούν τα αποτελέσματα της αυτοαξιολόγησής τους στο πλαίσιο της Ομάδας Συνεργασίας.

([17]) Απόφαση αριθ. 1313/2013/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Δεκεμβρίου 2013, περί μηχανισμού πολιτικής προστασίας της Ένωσης (ΕΕ L 347 της 20.12.2013, σ. 924).

(77) Η ευθύνη για την εξασφάλιση της ασφάλειας των συστημάτων δικτύου και πληροφοριών εναπόκειται σε μεγάλο βαθμό στις βασικές και στις σημαντικές οντότητες. Θα πρέπει να προωθηθεί και να αναπτυχθεί μια αντίληψη διαχείρισης κινδύνων η οποία θα περιλαμβάνει εκτιμήσεις κινδύνου και την εφαρμογή μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας κατάλληλα για τους αντιμετωπιζόμενους κινδύνους.

(78) Τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας θα πρέπει να λαμβάνουν υπόψη τον βαθμό εξάρτησης της βασικής ή σημαντικής οντότητας από τα συστήματα δικτύου και πληροφοριών και να περιλαμβάνουν μέτρα για τον εντοπισμό τυχόν κινδύνων περιστατικών, για την πρόληψη, τον εντοπισμό, την αντιμετώπιση περιστατικών και την ανάκαμψη από αυτά, καθώς και για τον μετριασμό των επιπτώσεών τους. Η ασφάλεια των συστημάτων δικτύου και πληροφοριών θα πρέπει να περιλαμβάνει την ασφάλεια των αποθηκευμένων, διαβιβαζόμενων και υφιστάμενων σε επεξεργασία δεδομένων. Τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας θα πρέπει να προβλέπουν συστημική ανάλυση, λαμβάνοντας υπόψη τον ανθρώπινο παράγοντα, προκειμένου να υπάρχει πλήρης εικόνα της ασφάλειας του συστήματος δικτύου και πληροφοριών.

(79) Δεδομένου ότι οι απειλές για την ασφάλεια των συστημάτων δικτύου και πληροφοριών μπορεί να έχουν διαφορετικές προελεύσεις, τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας θα πρέπει να βασίζονται σε μια ολική προσέγγιση των κινδύνων, η οποία να αποσκοπεί στην προστασία των συστημάτων δικτύου και πληροφοριών και του φυσικού περιβάλλοντος των εν λόγω συστημάτων από περιστατικά όπως κλοπή, πυρκαγιά, πλημμύρες, αστοχίες στις τηλεπικοινωνίες ή την ηλεκτροδότηση, ή η μη εξουσιοδοτημένη φυσική πρόσβαση, καταστροφή και παρέμβαση στις εγκαταστάσεις επεξεργασίας πληροφοριών της βασικής ή σημαντικής οντότητας, οι οποίες θα μπορούσαν να θέσουν σε κίνδυνο τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή την εμπιστευτικότητα των αποθηκευμένων, διαβιβαζόμενων ή υφιστάμενων επεξεργασία δεδομένων ή των υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω συστημάτων δικτύου και πληροφοριών. Συνεπώς, τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας θα πρέπει επίσης να αφορούν τη φυσική και περιβαλλοντική ασφάλεια των συστημάτων δικτύου και πληροφοριών, συμπεριλαμβάνοντας μέτρα για την προστασία των εν λόγω συστημάτων από αστοχίες του συστήματος, ανθρώπινα σφάλματα, κακόβουλες πράξεις ή φυσικά φαινόμενα, σύμφωνα με τα ευρωπαϊκά και διεθνή πρότυπα, όπως αυτά που περιλαμβάνονται στη σειρά ISO/IEC 27000. Εν προκειμένω, οι βασικές και σημαντικές οντότητες θα πρέπει, στο πλαίσιο των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που εφαρμόζουν, να μεριμνούν και για την ασφάλεια των ανθρώπινων πόρων και να εφαρμόζουν κατάλληλες πολιτικές ελέγχου της πρόσβασης. Τα μέτρα αυτά θα πρέπει να συνάδουν με την οδηγία (ΕΕ) 2022/2557.

(80) Για τον σκοπό της απόδειξης της συμμόρφωσης με τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και ελλείψει κατάλληλων ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας που να έχουν εγκριθεί σύμφωνα με τον κανονισμό (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([18]), τα κράτη μέλη θα πρέπει, σε διαβούλευση με την Ομάδα Συνεργασίας και την ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας, να προωθούν τη χρήση σχετικών ευρωπαϊκών και διεθνών προτύπων από βασικές και σημαντικές οντότητες ή να απαιτούν από οντότητες να χρησιμοποιούν πιστοποιημένα προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ.

(81) Προκειμένου να αποφευχθεί η επιβολή δυσανάλογης οικονομικής και διοικητικής επιβάρυνσης σε βασικές και σημαντικές οντότητες, τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας θα πρέπει να είναι αναλογικά προς τους κινδύνους που εγκυμονεί το οικείο σύστημα δικτύου και πληροφοριών, λαμβάνοντας υπόψη την πλέον προηγμένη τεχνολογία των εν λόγω μέτρων και, κατά περίπτωση, τα σχετικά ευρωπαϊκά και διεθνή πρότυπα, καθώς και το κόστος εφαρμογής τους.

(82) Τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας θα πρέπει να είναι αναλογικά προς τον βαθμό έκθεσης της βασικής ή σημαντικής οντότητας σε κινδύνους και προς τον κοινωνικό και οικονομικό αντίκτυπο που θα είχε ένα περιστατικό. Κατά τη θέσπιση μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας, προσαρμοσμένων στις βασικές και σημαντικές οντότητες, θα πρέπει να λαμβάνονται δεόντως υπόψη ο διαφορετικός βαθμός έκθεσης στον κίνδυνο για τις βασικές και σημαντικές οντότητες, όπως η κρισιμότητα της οντότητας, οι κίνδυνοι, συμπεριλαμβανομένων των κοινωνικών κινδύνων στους οποίους είναι εκτεθειμένη, το μέγεθος της οντότητας και η πιθανότητα εμφάνισης περιστατικών και η σοβαρότητά τους, συμπεριλαμβανομένων των κοινωνικών και οικονομικών επιπτώσεών τους.

([18]) Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA (Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια) και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια) (ΕΕ L 151 της 7.6.2019, σ. 15).

(83) Οι βασικές και οι σημαντικές οντότητες θα πρέπει να εγγυώνται την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν στις δραστηριότητές τους. Τα συστήματα αυτά είναι κυρίως ιδιωτικά συστήματα δικτύου και πληροφοριών τα οποία διαχειρίζεται το εσωτερικό προσωπικό ΤΠ των βασικών και σημαντικών οντοτήτων ή των οποίων η ασφάλεια έχει ανατεθεί σε εξωτερικούς συνεργάτες. Τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και οι υποχρεώσεις υποβολής εκθέσεων που προβλέπονται στην παρούσα οδηγία θα πρέπει να εφαρμόζονται στις σχετικές βασικές και σημαντικές οντότητες, ανεξάρτητα από το αν οι εν λόγω οντότητες διατηρούν εσωτερικά τα συστήματα δικτύου και πληροφοριών τους ή αναθέτουν τη συντήρησή τους σε εξωτερικούς συνεργάτες.

(84) Λαμβανομένου υπόψη του διασυνοριακού χαρακτήρα τους, οι πάροχοι υπηρεσιών DNS, τα μητρώα ονομάτων TLD, οι πάροχοι υπηρεσιών υπολογιστικού νέφους, οι πάροχοι υπηρεσιών κέντρων δεδομένων, οι πάροχοι δικτύων διανομής περιεχομένου, οι πάροχοι υπηρεσιών υπό διαχείριση, οι πάροχοι υπηρεσιών ασφάλειας υπό διαχείριση, οι πάροχοι επιγραμμικών αγορών, επιγραμμικών μηχανών αναζήτησης και πλατφορμών κοινωνικής δικτύωσης και οι πάροχοι υπηρεσιών εμπιστοσύνης θα πρέπει να υπόκεινται σε υψηλό βαθμό εναρμόνισης σε επίπεδο Ένωσης. Κατά συνέπεια, η εφαρμογή των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας όσον αφορά τις εν λόγω οντότητες θα πρέπει να διευκολυνθεί με εκτελεστική πράξη.

(85) Η αντιμετώπιση των κινδύνων που απορρέουν από την αλυσίδα εφοδιασμού μιας οντότητας και τη σχέση της με τους προμηθευτές της, όπως οι πάροχοι υπηρεσιών αποθήκευσης και επεξεργασίας δεδομένων ή οι πάροχοι διαχειριζόμενης υπηρεσίας ασφάλειας και οι εκδότες λογισμικού, είναι ιδιαίτερα σημαντική δεδομένης της επικράτησης περιστατικών κατά τα οποία οντότητες έχουν πέσει θύματα κυβερνοεπιθέσεων και όπου κακόβουλοι δράστες μπόρεσαν να θέσουν σε κίνδυνο την ασφάλεια των συστημάτων δικτύου και πληροφοριών μιας οντότητας εκμεταλλευόμενοι ευπάθειες προϊόντων και υπηρεσιών τρίτων. Επομένως, οι βασικές και σημαντικές οντότητες θα πρέπει να αξιολογούν και να λαμβάνουν υπόψη τη συνολική ποιότητα και ανθεκτικότητα των προϊόντων και των υπηρεσιών, τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που ενσωματώνονται σε αυτά, καθώς και τις πρακτικές κυβερνοασφάλειας των προμηθευτών και των παρόχων υπηρεσιών τους, συμπεριλαμβανομένων των ασφαλών διαδικασιών ανάπτυξής τους. Οι βασικές και σημαντικές οντότητες θα πρέπει ιδίως να ενθαρρύνονται να ενσωματώνουν μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας στις συμβατικές ρυθμίσεις με τους άμεσους προμηθευτές και τους παρόχους υπηρεσιών τους. Οι εν λόγω οντότητες θα μπορούσαν να εξετάζουν τους κινδύνους που απορρέουν από άλλα επίπεδα προμηθευτών και παρόχων υπηρεσιών.

(86) Μεταξύ των παρόχων υπηρεσιών, οι πάροχοι υπηρεσίας διαχείρισης της ασφάλειας σε τομείς όπως η αντιμετώπιση περιστατικών, οι δοκιμές διείσδυσης, οι έλεγχοι ασφάλειας και η παροχή συμβουλών διαδραματίζουν ιδιαίτερα σημαντικό ρόλο στην παροχή συνδρομής σε οντότητες που καταβάλλουν προσπάθειες για την πρόληψη, τον εντοπισμό και την αντιμετώπιση περιστατικών ή την ανάκαμψη από αυτά. Ωστόσο, οι ίδιοι οι πάροχοι υπηρεσίας ασφάλειας που τελούν υπό διαχείριση αποτέλεσαν επίσης στόχο κυβερνοεπιθέσεων και, λόγω της στενής ενσωμάτωσής τους στη λειτουργία των οντοτήτων, εγκυμονούν ιδιαίτερο κίνδυνο. Συνεπώς, οι βασικές και σημαντικές οντότητες θα πρέπει να επιδεικνύουν αυξημένη επιμέλεια κατά την επιλογή παρόχου διαχειριζόμενης υπηρεσίας ασφάλειας.

(87) Οι αρμόδιες αρχές, στο πλαίσιο των εποπτικών καθηκόντων τους, μπορούν επίσης να επωφελούνται από υπηρεσίες κυβερνοασφάλειας, όπως οι έλεγχοι ασφάλειας και οι δοκιμές διείσδυσης ή η αντιμετώπιση περιστατικών.

(88) Οι βασικές και σημαντικές οντότητες θα πρέπει επίσης να αντιμετωπίζουν τους κινδύνους που απορρέουν από τις αλληλεπιδράσεις και τις σχέσεις τους με άλλα ενδιαφερόμενα μέρη εντός ενός ευρύτερου οικοσυστήματος, μεταξύ άλλων όσον αφορά την αντιμετώπιση της βιομηχανικής κατασκοπείας και την προστασία του εμπορικού απορρήτου. Ειδικότερα, οι εν λόγω οντότητες θα πρέπει να λαμβάνουν τα κατάλληλα μέτρα ώστε η συνεργασία τους με ακαδημαϊκά και ερευνητικά ιδρύματα να πραγματοποιείται σύμφωνα με τις πολιτικές τους για την κυβερνοασφάλεια και να ακολουθεί τις ορθές πρακτικές όσον αφορά την ασφαλή πρόσβαση και διάδοση των πληροφοριών εν γένει και την προστασία της πνευματικής ιδιοκτησίας ειδικότερα. Ομοίως, δεδομένης της σημασίας και της αξίας που έχουν τα δεδομένα για τις δραστηριότητες των βασικών και σημαντικών οντοτήτων, όταν βασίζονται σε υπηρεσίες μετασχηματισμού και ανάλυσης δεδομένων από τρίτα μέρη, οι εν λόγω οντότητες θα πρέπει να λαμβάνουν όλα τα κατάλληλα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας.

(89) Οι βασικές και σημαντικές οντότητες θα πρέπει να υιοθετήσουν ένα ευρύ φάσμα βασικών πρακτικών κυβερνοϋγιεινής, όπως τις αρχές μηδενικής εμπιστοσύνης, αναβαθμίσεις λογισμικού, παραμετροποίηση ρυθμίσεων συσκευών, κατάτμηση δικτύου, ταυτοποίηση και διαχείριση πρόσβασης ή ευαισθητοποίηση του χρήστη, να οργανώνουν προγράμματα κατάρτισης για το προσωπικό τους και να λαμβάνουν μέτρα ευαισθητοποίησης σχετικά με κυβερνοαπειλές μέσω εταιρικού ηλεκτρονικού ταχυδρομείου, ηλεκτρονικού «ψαρέματος» ή τεχνικών κοινωνικής μηχανικής. Επιπλέον, οι εν λόγω οντότητες θα πρέπει να αξιολογούν τις δικές τους ικανότητες κυβερνοασφάλειας και, κατά περίπτωση, να επιδιώκουν την ενσωμάτωση τεχνολογιών που ενισχύουν την κυβερνοασφάλεια, όπως η τεχνητή νοημοσύνη ή τα συστήματα μηχανικής μάθησης, για την ενίσχυση των ικανοτήτων τους και της ασφάλειας των συστημάτων δικτύου και πληροφοριών.

(90) Για την περαιτέρω αντιμετώπιση των βασικών κινδύνων της αλυσίδας εφοδιασμού και την παροχή βοήθειας σε βασικές και σημαντικές οντότητες που δραστηριοποιούνται σε τομείς που καλύπτονται από την παρούσα οδηγία για την κατάλληλη διαχείριση των κινδύνων που σχετίζονται με την αλυσίδα εφοδιασμού και τους προμηθευτές, η Ομάδα Συνεργασίας, σε συνεργασία με την Επιτροπή και τον ENISA, και, κατά περίπτωση, κατόπιν διαβούλευσης με τα σχετικά ενδιαφερόμενα μέρη, μεταξύ άλλων από τη βιομηχανία, θα πρέπει να διενεργεί συντονισμένες εκτιμήσεις κινδύνου για την ασφάλεια κρίσιμων αλυσίδων εφοδιασμού, όπως διενεργούνται για τα δίκτυα 5G σύμφωνα με τη σύσταση (ΕΕ) 2019/534 της Επιτροπής ([19]), με σκοπό τον προσδιορισμό, ανά τομέα, των κρίσιμων υπηρεσιών ΤΠΕ, των συστημάτων ΤΠΕ ή των προϊόντων ΤΠΕ, των σχετικών απειλών και ευπαθειών. Οι εν λόγω συντονισμένες εκτιμήσεις κινδύνου για την ασφάλεια θα πρέπει να προσδιορίζουν μέτρα, σχέδια μετριασμού και βέλτιστες πρακτικές για την αντιμετώπιση κρίσιμων εξαρτήσεων, πιθανών μεμονωμένων σημείων αστοχίας, απειλών, τρωτοτήτων και άλλων κινδύνων που συνδέονται με την αλυσίδα εφοδιασμού και θα πρέπει να διερευνούν τρόπους για την περαιτέρω ενθάρρυνση της ευρύτερης υιοθέτησής τους από τις βασικές και σημαντικές οντότητες. Πιθανοί μη τεχνικοί παράγοντες κινδύνου, όπως η αθέμιτη επιρροή τρίτης χώρας στους προμηθευτές και τους παρόχους υπηρεσιών, ιδίως στην περίπτωση εναλλακτικών μοντέλων διακυβέρνησης, ενέχουν κεκαλυμμένες ευπάθειες ή κερκόπορτες και δυνητικές συστημικές διαταραχές στον εφοδιασμό, ιδίως σε περίπτωση τεχνολογικού εγκλωβισμού ή εξάρτησης από παρόχους.

(91) Οι συντονισμένες εκτιμήσεις κινδύνου για την ασφάλεια κρίσιμων αλυσίδων εφοδιασμού, υπό το φως των χαρακτηριστικών του οικείου τομέα, θα πρέπει να λαμβάνουν υπόψη τόσο τεχνικούς όσο και, κατά περίπτωση, μη τεχνικούς παράγοντες, συμπεριλαμβανομένων εκείνων που ορίζονται στη σύσταση (ΕΕ) 2019/534, στην πανευρωπαϊκή συντονισμένη εκτίμηση κινδύνου της ασφάλειας των δικτύων 5G και στην εργαλειοθήκη της ΕΕ για την κυβερνοασφάλεια των δικτύων 5G που συμφωνήθηκε από την Ομάδα Συνεργασίας. Ο προσδιορισμός των αλυσίδων εφοδιασμού που θα πρέπει να υποβάλλονται σε συντονισμένη εκτίμηση κινδύνου για την ασφάλεια θα πρέπει να γίνεται με γνώμονα τα ακόλουθα κριτήρια: i) τον βαθμό στον οποίο βασικές και σημαντικές οντότητες χρησιμοποιούν και βασίζονται σε συγκεκριμένες κρίσιμες υπηρεσίες ΤΠΕ, συστήματα ΤΠΕ ή προϊόντα ΤΠΕ· ii) τη σημασία συγκεκριμένων κρίσιμων υπηρεσιών ΤΠΕ, συστημάτων ΤΠΕ ή προϊόντων ΤΠΕ για την εκτέλεση κρίσιμων ή ευαίσθητων λειτουργιών, συμπεριλαμβανομένης της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· iii) τη διαθεσιμότητα εναλλακτικών υπηρεσιών ΤΠΕ, συστημάτων ΤΠΕ ή προϊόντων ΤΠΕ· iv) την ανθεκτικότητα του συνόλου της αλυσίδας εφοδιασμού υπηρεσιών ΤΠΕ, συστημάτων ΤΠΕ ή προϊόντων ΤΠΕ καθ' όλη τη διάρκεια του κύκλου ζωής τους έναντι γεγονότων που προκαλούν διατάραξη και v) όσον αφορά αναδυόμενες υπηρεσίες ΤΠΕ, συστήματα ΤΠΕ ή προϊόντα ΤΠΕ, τη δυνητική μελλοντική τους σημασία για τις δραστηριότητες των οντοτήτων. Επιπλέον, θα πρέπει να δοθεί ιδιαίτερη έμφαση στις υπηρεσίες ΤΠΕ, τα συστήματα ΤΠΕ ή τα προϊόντα ΤΠΕ που υπόκεινται σε ειδικές απαιτήσεις που απορρέουν από τρίτες χώρες.

(92) Προκειμένου να εξορθολογιστούν οι υποχρεώσεις που επιβάλλονται στους παρόχους δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών και στους παρόχους υπηρεσιών εμπιστοσύνης, όσον αφορά την ασφάλεια των συστημάτων δικτύου και πληροφοριών τους, καθώς και να δοθεί η δυνατότητα στις εν λόγω οντότητες και στις αρμόδιες αρχές δυνάμει της οδηγίας (ΕΕ) 2018/1972 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([20]) και του κανονισμού (ΕΕ) αριθ. 910/2014 αντίστοιχα να επωφεληθούν από το νομικό πλαίσιο που θεσπίζεται με την παρούσα οδηγία, συμπεριλαμβανομένου του ορισμού μιας ομάδας CSIRT υπεύθυνης για τον χειρισμό περιστατικών, της συμμετοχής των οικείων αρμόδιων αρχών στις δραστηριότητες της ομάδας συνεργασίας και του δικτύου CSIRT, οι εν λόγω οντότητες θα πρέπει να υπάγονται στο πεδίο εφαρμογής της παρούσας οδηγίας. Συνεπώς, οι αντίστοιχες διατάξεις του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972 σχετικά με την επιβολή απαιτήσεων ασφάλειας και κοινοποίησης σε αυτούς τους τύπους οντοτήτων, θα πρέπει να καταργηθούν. Οι κανόνες σχετικά με τις υποχρεώσεις υποβολής αναφορών που ορίζονται στην παρούσα οδηγία δεν θα πρέπει να θίγουν τον κανονισμό (ΕΕ) 2016/679 και την οδηγία 2002/58/ΕΚ.

(93) Οι υποχρεώσεις κυβερνοασφάλειας που ορίζονται στην παρούσα οδηγία θα πρέπει να θεωρούνται συμπληρωματικές προς τις απαιτήσεις που επιβάλλονται στους παρόχους υπηρεσιών εμπιστοσύνης δυνάμει του κανονισμού (ΕΕ) αριθ. 910/2014. Οι πάροχοι υπηρεσιών εμπιστοσύνης θα πρέπει να υποχρεούνται να λαμβάνουν όλα τα κατάλληλα και αναλογικά μέτρα για τη διαχείριση των πιθανών κινδύνων για τις υπηρεσίες τους, μεταξύ άλλων σε σχέση με τους πελάτες και τα βασιζόμενα τρίτα μέρη, και να αναφέρουν περιστατικά δυνάμει της παρούσας οδηγίας. Οι εν λόγω υποχρεώσεις κυβερνοασφάλειας και αναφοράς περιστατικών θα πρέπει να αφορούν και τη φυσική προστασία των παρεχόμενων υπηρεσιών. Οι απαιτήσεις για τους αναγνωρισμένους παρόχους υπηρεσιών εμπιστοσύνης που ορίζονται στο άρθρο 24 του κανονισμού (ΕΕ) αριθ. 910/2014 εξακολουθούν να ισχύουν.

([19]) Σύσταση (ΕΕ) 2019/534 της Επιτροπής, της 26ης Μαρτίου 2019, Κυβερνοασφάλεια δικτύων 5G (ΕΕ L 88 της 29.3.2019, σ. 42).

([20]) Οδηγία (ΕΕ) 2018/1972 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Δεκεμβρίου 2018, για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών (ΕΕ L 321 της 17.12.2018, σ. 36).

(94) Τα κράτη μέλη μπορούν να αναθέσουν τον ρόλο των αρμόδιων αρχών για τις υπηρεσίες εμπιστοσύνης στους εποπτικούς φορείς δυνάμει του κανονισμού (ΕΕ) αριθ. 910/2014, προκειμένου να διασφαλιστεί η συνέχιση των τρεχουσών πρακτικών και να αξιοποιηθούν οι γνώσεις και η πείρα που αποκτήθηκαν κατά την εφαρμογή του εν λόγω κανονισμού. Σε τέτοια περίπτωση, οι αρμόδιες αρχές δυνάμει της παρούσας οδηγίας, θα πρέπει να συνεργάζονται στενά και εγκαίρως με τους εν λόγω εποπτικούς φορείς, ανταλλάσσοντας τις σχετικές πληροφορίες, προκειμένου να εξασφαλίζεται η αποτελεσματική εποπτεία και συμμόρφωση των παρόχων υπηρεσιών εμπιστοσύνης με τις απαιτήσεις που ορίζονται στην παρούσα οδηγία και στον κανονισμό (ΕΕ) αριθ. 910/2014. Κατά περίπτωση, η CSIRT ή η αρμόδια αρχή δυνάμει της παρούσας οδηγίας θα πρέπει να ενημερώνει αμέσως τον εποπτικό φορέα δυνάμει του κανονισμού (ΕΕ) αριθ. 910/2014 σχετικά με κάθε κοινοποιηθείσα σημαντική κυβερνοαπειλή ή περιστατικό με αντίκτυπο στις υπηρεσίες εμπιστοσύνης, καθώς και σχετικά με τυχόν παραβίασης της παρούσας οδηγίας εκ μέρους παρόχου υπηρεσιών εμπιστοσύνης. Για τους σκοπούς της κοινοποίησης, τα κράτη μέλη μπορούν να χρησιμοποιούν, κατά περίπτωση, το ενιαίο σημείο εισόδου που έχει θεσπιστεί για την επίτευξη κοινής και αυτόματης αναφοράς περιστατικών τόσο στον εποπτικό φορέα δυνάμει του κανονισμού (ΕΕ) αριθ. 910/2014 όσο και στην CSIRT ή στην αρμόδια αρχή δυνάμει της παρούσας οδηγίας.

(95) Κατά περίπτωση και προκειμένου να αποφευχθεί άσκοπη αναστάτωση, οι υφιστάμενες εθνικές κατευθυντήριες γραμμές που έχουν εγκριθεί για τη μεταφορά των κανόνων σχετικά με τα μέτρα ασφάλειας που προβλέπονται στα άρθρα 40 και 41 της οδηγίας (ΕΕ) 2018/1972, θα πρέπει να λαμβάνονται υπόψη κατά τη μεταφορά της παρούσας οδηγίας στο εθνικό δίκαιο, ώστε να αξιοποιηθούν οι γνώσεις και οι δεξιότητες που έχουν ήδη αποκτηθεί δυνάμει της οδηγίας (ΕΕ) 2018/1972 σχετικά με τα μέτρα ασφάλειας και τις κοινοποιήσεις περιστατικών. Ο ENISA μπορεί επίσης να καταρτίσει κατευθυντήριες γραμμές σχετικά με τις απαιτήσεις ασφάλειας και τις υποχρεώσεις αναφοράς περιστατικών για τους παρόχους δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, προκειμένου να διευκολυνθούν η εναρμόνιση και η μετάβαση και να ελαχιστοποιηθούν οι διαταράξεις. Τα κράτη μέλη μπορούν να αναθέσουν στις εθνικές ρυθμιστικές αρχές τον ρόλο των αρμόδιων αρχών για τις ηλεκτρονικές επικοινωνίες δυνάμει της οδηγίας (ΕΕ) 2018/1972 προκειμένου να εξασφαλιστεί η συνέχιση των τρεχουσών πρακτικών και να αξιοποιηθούν οι γνώσεις και η πείρα που αποκτήθηκαν ως αποτέλεσμα της μεταφοράς της εν λόγω οδηγίας.

(96) Δεδομένης της αυξανόμενης σημασίας των υπηρεσιών διαπροσωπικών επικοινωνιών ανεξαρτήτως αριθμού, όπως αυτές ορίζονται στην οδηγία (ΕΕ) 2018/1972, είναι αναγκαίο να εξασφαλίζεται ότι οι εν λόγω υπηρεσίες θα υπόκεινται επίσης σε κατάλληλες απαιτήσεις ασφάλειας σύμφωνα με τον συγκεκριμένο χαρακτήρα τους και την οικονομική τους σημασία. Καθώς η επιφάνεια επίθεσης συνεχίζει να επεκτείνεται, οι ανεξαρτήτως αριθμού υπηρεσίες διαπροσωπικών επικοινωνιών, όπως είναι οι υπηρεσίες ανταλλαγής μηνυμάτων, καθίστανται διαδεδομένοι φορείς επίθεσης. Οι κακόβουλοι δράστες χρησιμοποιούν πλατφόρμες για να επικοινωνούν με τα θύματα και να τα προσελκύουν να ανοίξουν παραβιασμένες ιστοσελίδες, με αποτέλεσμα να αυξάνεται η πιθανότητα περιστατικών που αφορούν στην εκμετάλλευση δεδομένων προσωπικού χαρακτήρα και, κατ' επέκταση, στην ασφάλεια των συστημάτων δικτύου και πληροφοριών. Οι πάροχοι υπηρεσιών διαπροσωπικών επικοινωνιών ανεξαρτήτως αριθμού θα πρέπει να διασφαλίζουν επίπεδο ασφάλειας των συστημάτων δικτύου και πληροφοριών κατάλληλο για τους κινδύνους που εγκυμονούν. Δεδομένου ότι οι πάροχοι υπηρεσιών διαπροσωπικών επικοινωνιών ανεξαρτήτως αριθμού κατά κανόνα δεν ασκούν πραγματικό έλεγχο επί της μετάδοσης σημάτων μέσω δικτύων, ο βαθμός κινδύνου για τις εν λόγω υπηρεσίες μπορεί να θεωρηθεί, από ορισμένες απόψεις, χαμηλότερος από ό,τι για τις παραδοσιακές υπηρεσίες ηλεκτρονικών επικοινωνιών. Το ίδιο ισχύει και για τις υπηρεσίες διαπροσωπικών επικοινωνιών όπως ορίζονται στην οδηγία (ΕΕ) 2018/1972 που χρησιμοποιούν αριθμούς και δεν ασκούν πραγματικό έλεγχο επί της μετάδοσης σημάτων.

(97) Η εσωτερική αγορά εξαρτάται περισσότερο από ποτέ από τη λειτουργία του διαδικτύου. Οι υπηρεσίες όλων, σχεδόν, των βασικών και των σημαντικών οντοτήτων εξαρτώνται από τις υπηρεσίες που παρέχονται μέσω του διαδικτύου. Προκειμένου να διασφαλιστεί η ομαλή παροχή υπηρεσιών που παρέχονται από βασικές και σημαντικές οντότητες, είναι σημαντικό όλοι οι πάροχοι δημόσιων δικτύων ηλεκτρονικών επικοινωνιών να διαθέτουν κατάλληλα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και να αναφέρουν σχετικά σημαντικά περιστατικά. Τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι διατηρείται η ασφάλεια των δημόσιων δικτύων ηλεκτρονικών επικοινωνιών και ότι τα ζωτικά συμφέροντά τους στον τομέα της ασφάλειας προστατεύονται από δολιοφθορά και κατασκοπεία. Δεδομένου ότι η διεθνής συνδεσιμότητα ενισχύει και επιταχύνει την ανταγωνιστική ψηφιοποίηση της Ένωσης και της οικονομίας της, τα περιστατικά που επηρεάζουν τα υποβρύχια καλώδια επικοινωνιών θα πρέπει να αναφέρονται στην CSIRT ή, κατά περίπτωση, στην αρμόδια αρχή. Η εθνική στρατηγική κυβερνοασφάλειας θα πρέπει, κατά περίπτωση, να λαμβάνει υπόψη την κυβερνοασφάλεια των υποθαλάσσιων καλωδίων επικοινωνιών και να περιλαμβάνει χαρτογράφηση των δυνητικών κινδύνων κυβερνοασφάλειας και μέτρα μετριασμού για τη διασφάλιση του υψηλότερου δυνατού επιπέδου προστασίας τους.

(98) Προκειμένου να προστατεύεται η ασφάλεια των δημόσιων δικτύων ηλεκτρονικών επικοινωνιών και των διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, θα πρέπει να προωθηθεί η χρήση τεχνολογιών κρυπτογράφησης, ιδίως διατερματικής κρυπτογράφησης, καθώς και εννοιών ασφάλειας με επίκεντρο τα δεδομένα, όπως χαρτογραφία, κατάτμηση, σήμανση, πολιτική πρόσβασης και διαχείριση πρόσβασης, καθώς και αποφάσεις αυτοματοποιημένης πρόσβασης. Όπου απαιτείται, η χρήση κρυπτογράφησης, ιδίως διατερματικής κρυπτογράφησης, θα πρέπει να είναι υποχρεωτική για τους παρόχους δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών σύμφωνα με τις αρχές της ασφάλειας και της ιδιωτικότητας εξ ορισμού και εκ σχεδιασμού για τους σκοπούς της παρούσας οδηγίας. Η χρήση της διατερματικής κρυπτογράφησης θα πρέπει να συμβιβάζεται με τις εξουσίες των κρατών μελών να διασφαλίζουν την προστασία των ουσιωδών συμφερόντων ασφάλειας και δημόσιας ασφάλειάς τους και να επιτρέπουν την πρόληψη, τη διερεύνηση, τον εντοπισμό και τη δίωξη ποινικών αδικημάτων σύμφωνα με το δίκαιο της Ένωσης. Ωστόσο, αυτό δεν θα πρέπει να αποδυναμώνει τη διατερματική κρυπτογράφηση, η οποία αποτελεί κρίσιμη τεχνολογία για την αποτελεσματική προστασία των δεδομένων, της ιδιωτικότητας και της ασφάλειας των επικοινωνιών.

(99) Προκειμένου να διαφυλαχθεί η ασφάλεια, και να αποτραπούν η κατάχρηση και η χειραγώγηση, των δημόσιων δικτύων ηλεκτρονικών επικοινωνιών και των διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, θα πρέπει να προωθηθεί η χρήση προτύπων ασφαλούς δρομολόγησης, ώστε να διασφαλιστεί η ακεραιότητα και η ευρωστία των λειτουργιών δρομολόγησης σε ολόκληρο το οικοσύστημα των παρόχων υπηρεσιών πρόσβασης στο διαδίκτυο.

(100) Προκειμένου να διασφαλιστούν η λειτουργικότητα και η ακεραιότητα του διαδικτύου και να προωθηθεί η ασφάλεια και η ανθεκτικότητα του DNS, τα σχετικά ενδιαφερόμενα μέρη, συμπεριλαμβανομένων των οντοτήτων του ιδιωτικού τομέα της Ένωσης, των παρόχων διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, ιδίως των παρόχων υπηρεσιών πρόσβασης στο διαδίκτυο και των παρόχων διαδικτυακών μηχανών αναζήτησης, θα πρέπει να ενθαρρυνθούν να υιοθετήσουν στρατηγική διαφοροποίησης της επίλυσης των ονομάτων DNS. Συνεπώς, τα κράτη μέλη θα πρέπει να ενθαρρύνουν την ανάπτυξη και χρήση μιας δημόσιας και ασφαλούς ευρωπαϊκής υπηρεσίας επίλυσης ονομάτων DNS.

(101) Η παρούσα οδηγία θεσπίζει μια προσέγγιση πολλαπλών σταδίων ως προς την αναφορά σοβαρών περιστατικών, προκειμένου να επιτευχθεί η σωστή ισορροπία μεταξύ, αφενός, της ταχείας αναφοράς, που συμβάλλει στον μετριασμό της πιθανής εξάπλωσης σοβαρών περιστατικών και επιτρέπει στις βασικές και σημαντικές οντότητες να αναζητούν στήριξη και, αφετέρου, της υποβολής εμπεριστατωμένων εκθέσεων που αντλούν πολύτιμα διδάγματα από μεμονωμένα περιστατικά και βελτιώνουν με την πάροδο του χρόνου την κυβερνοανθεκτικότητα μεμονωμένων οντοτήτων και ολόκληρων τομέων. Στο πλαίσιο αυτό, η παρούσα οδηγία θα πρέπει να περιλαμβάνει την αναφορά περιστατικών τα οποία, βάσει αρχικής αξιολόγησης που διενεργείται από την οικεία οντότητα, θα μπορούσαν να προκαλέσουν σοβαρή λειτουργική διατάραξη των υπηρεσιών ή οικονομική ζημία στην εν λόγω οντότητα ή να επηρεάσουν άλλα φυσικά ή νομικά πρόσωπα προκαλώντας σημαντική υλική ή μη υλική ζημία. Στην εν λόγω αρχική αξιολόγηση θα πρέπει να λαμβάνονται υπόψη, μεταξύ άλλων, τα επηρεαζόμενα συστήματα δικτύου και πληροφοριών, και ιδίως η σημασία τους για την παροχή των υπηρεσιών της οντότητας, η σοβαρότητα και τα τεχνικά χαρακτηριστικά της κυβερνοαπειλής και τυχόν υποκείμενων τρωτοτήτων που αποτελούν αντικείμενο εκμετάλλευσης, καθώς και η πείρα της οντότητας σε παρόμοια περιστατικά. Δείκτες όπως ο βαθμός στον οποίο επηρεάζεται η λειτουργία της υπηρεσίας, η διάρκεια ενός περιστατικού ή ο αριθμός των επηρεαζόμενων αποδεκτών των υπηρεσιών θα μπορούσαν να διαδραματίσουν σημαντικό ρόλο στον προσδιορισμό του κατά πόσον η λειτουργική διατάραξη της υπηρεσίας είναι σοβαρή.

(102) Όταν οι βασικές και σημαντικές οντότητες αντιληφθούν σημαντικό περιστατικό, θα πρέπει να υποχρεούνται να υποβάλλουν έγκαιρη προειδοποίηση χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 24 ωρών. Η έγκαιρη προειδοποίηση θα πρέπει να ακολουθείται από κοινοποίηση περιστατικού. Οι οικείες οντότητες θα πρέπει να υποβάλλουν αμελλητί κοινοποίηση περιστατικού και σε κάθε περίπτωση εντός 72 ωρών από τη στιγμή που αντιλαμβάνονται το σημαντικό περιστατικό, με σκοπό, ιδίως, την επικαιροποίηση των πληροφοριών που υποβάλλονται μέσω της έγκαιρης προειδοποίησης και την αναφορά αρχικής αξιολόγησης του σημαντικού περιστατικού, μεταξύ άλλων της σοβαρότητας και των επιπτώσεών του, καθώς και ενδείξεων προσβολής, εφόσον υπάρχουν. Η τελική έκθεση θα πρέπει να υποβάλλεται το αργότερο ένα μήνα μετά την κοινοποίηση του περιστατικού. Η έγκαιρη προειδοποίηση θα πρέπει να περιλαμβάνει μόνο τις πληροφορίες που είναι αναγκαίες προκειμένου η CSIRT ή, κατά περίπτωση, η αρμόδια αρχή, να γνωρίζει το σημαντικό περιστατικό και να επιτρέπει στην οικεία οντότητα να ζητήσει βοήθεια, εφόσον απαιτείται. Η εν λόγω έγκαιρη προειδοποίηση, κατά περίπτωση, θα πρέπει να αναφέρει αν το σημαντικό περιστατικό είναι ύποπτο για έκνομες ή κακόβουλες πράξεις και αν είναι πιθανό να έχει διασυνοριακές επιπτώσεις. Τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι η υποχρέωση υποβολής της εν λόγω έγκαιρης προειδοποίησης, ή η επακόλουθη κοινοποίηση περιστατικών, δεν εκτρέπει τους πόρους της κοινοποιούσας οντότητας από δραστηριότητες που σχετίζονται με τον χειρισμό περιστατικών κατά προτεραιότητα, προκειμένου οι υποχρεώσεις αναφοράς περιστατικών να μην εκτρέπουν πόρους από τον χειρισμό

σημαντικών περιστατικών ή να θέτουν άλλως σε κίνδυνο τις σχετικές προσπάθειες της οντότητας. Σε περίπτωση εν εξελίξει περιστατικού κατά τον χρόνο υποβολής της τελικής έκθεσης, τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι οι οικείες οντότητες υποβάλλουν έκθεση προόδου τη δεδομένη στιγμή και ότι έχει υποβληθεί τελική έκθεση εντός ενός μηνός από τον εκ μέρους τους χειρισμό του σημαντικού περιστατικού.

(103) Κατά περίπτωση, οι βασικές και σημαντικές οντότητες θα πρέπει να κοινοποιούν, χωρίς καθυστέρηση, στους αποδέκτες των υπηρεσιών τους τυχόν μέτρα ή διορθωτικά μέτρα που μπορούν να λάβουν για να μετριάσουν τους απορρέοντες κινδύνους από σημαντική κυβερνοαπειλή. Οι εν λόγω οντότητες θα πρέπει, κατά περίπτωση και ιδίως όταν η σημαντική κυβερνοαπειλή είναι πιθανό να συμβεί, να ενημερώνουν επίσης τους αποδέκτες των υπηρεσιών τους για την ίδια την απειλή. Η απαίτηση ενημέρωσης των αποδεκτών σημαντικών κυβερνοαπειλών θα πρέπει να τηρείται με τη μέγιστη δυνατή προσπάθεια, αλλά δεν θα πρέπει να απαλλάσσει τις εν λόγω οντότητες από την υποχρέωση να λαμβάνουν, με δικά τους έξοδα, κατάλληλα και άμεσα μέτρα για την πρόληψη ή την αντιμετώπιση τέτοιων απειλών και την αποκατάσταση του κανονικού επιπέδου ασφάλειας της υπηρεσίας. Η σχετική ενημέρωση προς τους αποδέκτες των υπηρεσιών σχετικά με σημαντικές κυβερνοαπειλές θα πρέπει να παρέχεται δωρεάν και να διατυπώνεται σε εύληπτη γλώσσα.

(104) Οι πάροχοι δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών θα πρέπει να εφαρμόζουν εκ σχεδιασμού και εξ ορισμού την ασφάλεια και να ενημερώνουν τους αποδέκτες των υπηρεσιών τους για σημαντικές κυβερνοαπειλές και για τα μέτρα που μπορούν να λάβουν για την προστασία της ασφάλειας των συσκευών και των επικοινωνιών τους, για παράδειγμα με τη χρήση ειδικών τύπων λογισμικού ή τεχνολογιών κρυπτογράφησης.

(105) Η προληπτική προσέγγιση των κυβερνοαπειλών αποτελεί ζωτικής σημασίας συνιστώσα των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας, η οποία θα πρέπει να επιτρέπει στις αρμόδιες αρχές να αποτρέπουν αποτελεσματικά τη μετεξέλιξη κυβερνοαπειλών σε περιστατικά που ενδέχεται να προκαλέσουν σημαντική υλική ή μη υλική ζημία. Για τον σκοπό αυτό, η κοινοποίηση κυβερνοαπειλών έχει καθοριστική σημασία. Για τον σκοπό αυτό, οι οντότητες ενθαρρύνονται να αναφέρουν σε εθελοντική βάση τις κυβερνοαπειλές.

(106) Προκειμένου να απλουστευθεί η υποβολή των πληροφοριών που απαιτούνται βάσει της παρούσας οδηγίας, καθώς και να μειωθεί ο διοικητικός φόρτος για τις οντότητες, τα κράτη μέλη θα πρέπει να παρέχουν τεχνικά μέσα, όπως ενιαίο σημείο εισόδου, αυτοματοποιημένα συστήματα, διαδικτυακές φόρμες, φιλικές προς τον χρήστη διεπαφές, υποδείγματα, ειδικές πλατφόρμες για χρήση από οντότητες, ανεξαρτήτως του αν εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας, για την υποβολή των σχετικών πληροφοριών που πρέπει να αναφερθούν. Η ενωσιακή χρηματοδότηση για τη στήριξη της εφαρμογής της παρούσας οδηγίας, ιδίως στο πλαίσιο του προγράμματος «Ψηφιακή Ευρώπη» που θεσπίστηκε με τον κανονισμό (ΕΕ) 2021/694 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([21]), θα μπορούσε να περιλαμβάνει στήριξη για τα ενιαία σημεία εισόδου. Επιπλέον, οι οντότητες βρίσκονται συχνά αντιμέτωπες με καταστάσεις κατά τις οποίες ένα συγκεκριμένο περιστατικό, λόγω των χαρακτηριστικών του, πρέπει να αναφερθεί σε διαφορετικές αρχές, ως αποτέλεσμα των υποχρεώσεων κοινοποίησης που περιλαμβάνονται σε διάφορες νομικές πράξεις. Οι περιπτώσεις αυτές δημιουργούν πρόσθετο διοικητικό φόρτο και θα μπορούσαν επίσης να οδηγήσουν σε αβεβαιότητες όσον αφορά τη μορφή και τις διαδικασίες των εν λόγω κοινοποιήσεων. Όταν δημιουργείται ενιαίο σημείο εισόδου, τα κράτη μέλη ενθαρρύνονται επίσης να χρησιμοποιούν το εν λόγω ενιαίο σημείο εισόδου για κοινοποιήσεις περιστατικών ασφάλειας που απαιτούνται βάσει άλλης ενωσιακής νομοθεσίας, όπως ο κανονισμός (ΕΕ) 2016/679 και η οδηγία 2002/58/ΕΚ. Η χρήση του εν λόγω ενιαίου σημείου εισόδου για την αναφορά περιστατικών ασφάλειας βάσει του κανονισμού (ΕΕ) 2016/679 και της οδηγίας 2002/58/ΕΚ δεν θα πρέπει να επηρεάζει την εφαρμογή των διατάξεων του κανονισμού (ΕΕ) 2016/679 και της οδηγίας 2002/58/ΕΚ, ιδίως εκείνων που αφορούν την ανεξαρτησία των αρχών που αναφέρονται σε αυτά. Ο ENISA, σε συνεργασία με την Ομάδα Συνεργασίας, θα πρέπει να αναπτύξει κοινά υποδείγματα κοινοποίησης μέσω κατευθυντήριων γραμμών για την απλούστευση και τον εξορθολογισμό των πληροφοριών που πρέπει να αναφερθούν δυνάμει του δικαίου της Ένωσης και τη μείωση του διοικητικού φόρτου των κοινοποιουσών οντοτήτων.

(107) Όταν υπάρχει υπόνοια ότι ένα περιστατικό σχετίζεται με σοβαρές εγκληματικές δραστηριότητες δυνάμει ενωσιακής ή εθνικής νομοθεσίας, τα κράτη μέλη θα πρέπει να παροτρύνουν τις βασικές και τις σημαντικές οντότητες με βάση τους ισχύοντες στο ενωσιακό δίκαιο κανόνες ποινικών διαδικασιών, να αναφέρουν περιστατικά εικαζόμενης σοβαρής εγκληματικής φύσεως στις αρμόδιες αρχές επιβολής του νόμου. Κατά περίπτωση, και με την επιφύλαξη των κανόνων προστασίας των δεδομένων προσωπικού χαρακτήρα που ισχύουν για την Ευρωπόλ, είναι επιθυμητό ο συντονισμός μεταξύ των αρμόδιων αρχών και των αρχών επιβολής του νόμου των διαφόρων κρατών μελών να διευκολύνεται από το Ευρωπαϊκό Κέντρο για το Κυβερνοέγκλημα (EC3), και από τον ENISA.

([21]) Κανονισμός (ΕΕ) 2021/694 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 29ης Απριλίου 2021, για τη θέσπιση του προγράμματος Ψηφιακή Ευρώπη και την κατάργηση της απόφασης (ΕΕ) 2015/2240 (ΕΕ L 166 της 11.5.2021, σ. 1).

(108) Ως αποτέλεσμα περιστατικών, σε πολλές περιπτώσεις διακυβεύονται δεδομένα προσωπικού χαρακτήρα. Στο πλαίσιο αυτό, οι αρμόδιες αρχές θα πρέπει να συνεργάζονται και να ανταλλάσσουν πληροφορίες σχετικά με όλα τα σχετικά θέματα με τις αρχές που αναφέρονται στον κανονισμό (ΕΕ) 2016/679 και στην οδηγία 2002/58/ΕΚ.

(109) Η διατήρηση επακριβών και πλήρων βάσεων δεδομένων για δεδομένα καταχώρισης ονομάτων τομέα (τα λεγόμενα «δεδομένα WHOIS») και η παροχή νόμιμης πρόσβασης στα εν λόγω δεδομένα είναι ουσιαστικής σημασίας για τη διασφάλιση της ασφάλειας, της σταθερότητας και της ανθεκτικότητας του DNS, γεγονός που με τη σειρά του συμβάλλει σε υψηλό κοινό επίπεδο κυβερνοασφάλειας εντός της Ένωσης. Για τον συγκεκριμένο σκοπό, τα μητρώα ονομάτων TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα θα πρέπει να υποχρεούνται να επεξεργάζονται ορισμένα δεδομένα που είναι αναγκαία για την επίτευξη του εν λόγω σκοπού. Η εν λόγω επεξεργασία θα πρέπει να συνιστά νομική υποχρέωση κατά την έννοια του άρθρου 6 παράγραφος 1 στοιχείο γ) του κανονισμού (ΕΕ) 2016/679. Η υποχρέωση αυτή δεν θίγει τη δυνατότητα συλλογής δεδομένων καταχώρισης ονομάτων τομέα για άλλους σκοπούς, για παράδειγμα βάσει συμβατικών ρυθμίσεων ή νομικών απαιτήσεων που καθορίζονται σε άλλο ενωσιακό ή εθνικό δίκαιο. Η υποχρέωση αυτή αποσκοπεί στην επίτευξη ενός πλήρους και ακριβούς συνόλου δεδομένων καταχώρισης και δεν θα πρέπει να έχει ως αποτέλεσμα την επανειλημμένη συλλογή των ίδιων δεδομένων. Τα μητρώα ονομάτων TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα θα πρέπει να συνεργάζονται μεταξύ τους προκειμένου να αποφεύγεται η αλληλεπικάλυψη του εν λόγω καθήκοντος.

(110) Η διαθεσιμότητα και η έγκαιρη προσβασιμότητα των δεδομένων καταχώρισης ονομάτων τομέα στους νομίμως αιτούντες πρόσβαση είναι ουσιαστικής σημασίας για την πρόληψη και την καταπολέμηση της κατάχρησης του DNS, καθώς και για την πρόληψη και τον εντοπισμό και την αντιμετώπιση περιστατικών. Ως νομίμως αιτούντες πρόσβαση νοούνται τα φυσικά ή νομικά πρόσωπα που υποβάλλουν αίτηση βάσει του ενωσιακού ή του εθνικού δικαίου. Μπορούν να περιλαμβάνονται αρχές που είναι αρμόδιες δυνάμει της παρούσας οδηγίας και αρχές που είναι αρμόδιες δυνάμει του ενωσιακού ή του εθνικού δικαίου για την πρόληψη, τη διερεύνηση, την ανίχνευση ή τη δίωξη ποινικών αδικημάτων, καθώς και CERT ή CSIRT. Τα μητρώα ονομάτων TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα θα πρέπει να υποχρεούνται να επιτρέπουν τη νόμιμη πρόσβαση σε συγκεκριμένα δεδομένα καταχώρισης ονομάτων τομέα, τα οποία είναι αναγκαία για τους σκοπούς του αιτήματος πρόσβασης, σε νομίμως αιτούντες πρόσβαση σύμφωνα με το ενωσιακό και το εθνικό δίκαιο. Το αίτημα των νομίμως αιτούντων πρόσβαση θα πρέπει να συνοδεύεται από αιτιολόγηση που να επιτρέπει την αξιολόγηση της αναγκαιότητας πρόσβασης στα δεδομένα.

(111) Προκειμένου να διασφαλιστεί η διαθεσιμότητα ακριβών και πλήρων δεδομένων καταχώρισης ονομάτων χώρου, τα μητρώα ονομάτων TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων χώρου θα πρέπει να συλλέγουν και να εγγυώνται την ακεραιότητα και τη διαθεσιμότητα των δεδομένων καταχώρισης ονομάτων χώρου. Ειδικότερα, τα μητρώα ονομάτων TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα θα πρέπει να θεσπίσουν πολιτικές και διαδικασίες για τη συλλογή και τη διατήρηση ακριβών και πλήρων δεδομένων καταχώρισης ονομάτων τομέα, καθώς και για την πρόληψη και διόρθωση ανακριβών δεδομένων καταχώρισης σύμφωνα με τη νομοθεσία της Ένωσης για την προστασία των δεδομένων. Οι εν λόγω πολιτικές και διαδικασίες θα πρέπει να λαμβάνουν υπόψη, στο μέτρο του δυνατού, τα πρότυπα που αναπτύσσονται από τις πολυσυμμετοχικές δομές διακυβέρνησης σε διεθνές επίπεδο. Τα μητρώα ονομάτων TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα θα πρέπει να καθιερώσουν και να εφαρμόζουν αναλογικές διαδικασίες για την επαλήθευση των δεδομένων καταχώρισης ονομάτων τομέα. Οι διαδικασίες αυτές θα πρέπει να αντικατοπτρίζουν τις βέλτιστες πρακτικές που χρησιμοποιούνται στον κλάδο και, στο μέτρο του δυνατού, την πρόοδο που έχει σημειωθεί στον τομέα της ηλεκτρονικής ταυτοποίησης. Παραδείγματα διαδικασιών επαλήθευσης μπορεί να είναι οι προληπτικοί που διενεργούνται κατά την καταχώριση και οι κατασταλτικοί έλεγχοι που διενεργούνται μετά την καταχώριση. Τα μητρώα ονομάτων TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα θα πρέπει, ιδίως, να επαληθεύουν τουλάχιστον ένα στοιχείο επικοινωνίας του καταχωρίζοντος.

(112) Τα μητρώα ονομάτων TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα θα πρέπει να υποχρεούνται να δημοσιοποιούν δεδομένα καταχώρισης ονομάτων τομέα που δεν εμπίπτουν στο πεδίο εφαρμογής της ενωσιακής νομοθεσίας για την προστασία των δεδομένων, όπως δεδομένα που αφορούν νομικά πρόσωπα, σύμφωνα με το προοίμιο του κανονισμού (ΕΕ) 2016/679. Για τα νομικά πρόσωπα, τα μητρώα ονομάτων TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα θα πρέπει να δημοσιοποιούν τουλάχιστον το όνομα του καταχωρίζοντος και τον αριθμό τηλεφώνου επικοινωνίας. Η διεύθυνση ηλεκτρονικού ταχυδρομείου επικοινωνίας θα πρέπει επίσης να δημοσιεύεται υπό την προϋπόθεση ότι δεν περιέχει δεδομένα προσωπικού χαρακτήρα, όπως ψευδώνυμα ηλεκτρονικού ταχυδρομείου ή λογαριασμούς υπηρεσίας. Τα μητρώα ονομάτων TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα θα πρέπει επίσης να καθιστούν δυνατή τη νόμιμη πρόσβαση από νομίμως αιτούντες πρόσβαση σε συγκεκριμένα δεδομένα καταχώρισης ονομάτων τομέα που αφορούν φυσικά πρόσωπα, σύμφωνα με το δίκαιο της Ένωσης για την προστασία των δεδομένων. Τα κράτη μέλη θα πρέπει να απαιτούν από τα μητρώα ονομάτων TLD και τις οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα να απαντούν χωρίς αδικαιολόγητη καθυστέρηση σε αιτήματα γνωστοποίησης δεδομένων καταχώρισης ονομάτων τομέα από νομίμως αιτούντες πρόσβαση. Τα μητρώα ονομάτων TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα θα πρέπει να θεσπίσουν πολιτικές και διαδικασίες για τη δημοσίευση και γνωστοποίηση δεδομένων καταχώρισης, συμπεριλαμβανομένων συμφωνιών

σε επίπεδο υπηρεσιών για την αντιμετώπιση αιτημάτων πρόσβασης από νομίμως αιτούντες πρόσβαση. Οι εν λόγω πολιτικές και διαδικασίες θα πρέπει να λαμβάνουν υπόψη, στο μέτρο του δυνατού, τυχόν κατευθύνσεις που έχουν δοθεί καθώς και τα πρότυπα που αναπτύσσονται από τις πολυσυμμετοχικές δομές διακυβέρνησης σε διεθνές επίπεδο. Η διαδικασία πρόσβασης θα μπορούσε να περιλαμβάνει τη χρήση διεπαφής, πύλης ή άλλου τεχνικού εργαλείου για την παροχή αποτελεσματικού συστήματος υποβολής αιτημάτων για δεδομένα καταχώρισης και την πρόσβαση σε αυτά. Για την προώθηση εναρμονισμένων πρακτικών σε ολόκληρη την εσωτερική αγορά, η Επιτροπή μπορεί, με την επιφύλαξη των αρμοδιοτήτων του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων, να προβλέπει κατευθυντήριες γραμμές σχετικά με τις εν λόγω διαδικασίες, οι οποίες λαμβάνουν υπόψη, στο μέτρο του δυνατού, τα πρότυπα που έχουν αναπτυχθεί από τις πολυμερείς δομές διακυβέρνησης σε διεθνές επίπεδο. Τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι όλοι οι τύποι πρόσβασης σε προσωπικά και μη προσωπικά δεδομένα καταχώρισης ονομάτων τομέα είναι δωρεάν.

(113) Οι οντότητες που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας θα πρέπει να θεωρείται ότι εμπίπτουν στη δικαιοδοσία του κράτους μέλους στο οποίο είναι εγκατεστημένες. Ωστόσο, οι πάροχοι δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή οι πάροχοι διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών θα πρέπει να θεωρείται ότι εμπίπτουν στη δικαιοδοσία του κράτους μέλους στο οποίο παρέχουν τις υπηρεσίες τους. Οι πάροχοι υπηρεσιών DNS, τα μητρώα ονομάτων TLD, οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα, οι πάροχοι υπηρεσιών υπολογιστικού νέφους, οι πάροχοι υπηρεσιών κέντρων δεδομένων, οι πάροχοι δικτύων διανομής περιεχομένου, οι πάροχοι διαχειριζομένων υπηρεσιών, οι πάροχοι διαχειριζομένων υπηρεσιών ασφάλειας, καθώς και οι πάροχοι επιγραμμικών αγορών, επιγραμμικών μηχανών αναζήτησης και πλατφορμών υπηρεσιών κοινωνικής δικτύωσης θα πρέπει να θεωρείται ότι εμπίπτουν στη δικαιοδοσία του κράτους μέλους στο οποίο έχουν την κύρια εγκατάστασή τους στην Ένωση. Οι οντότητες της δημόσιας διοίκησης πρέπει να υπάγονται στη δικαιοδοσία του κράτους μέλους που τις έχει συστήσει. Εάν η οντότητα παρέχει υπηρεσίες ή είναι εγκατεστημένη σε περισσότερα του ενός κράτη μέλη, θα πρέπει να υπάγεται στη χωριστή και συντρέχουσα δικαιοδοσία καθενός από αυτά τα κράτη μέλη. Οι αρμόδιες αρχές των εν λόγω κρατών μελών θα πρέπει να συνεργάζονται, να παρέχουν αμοιβαία συνδρομή μεταξύ τους και, κατά περίπτωση, να εκτελούν κοινές εποπτικές δράσεις. Όταν τα κράτη μέλη ασκούν δικαιοδοσία, δεν θα πρέπει να προβλέπουν πάνω από μία φορά μέτρα επιβολής ή κυρώσεις για την ίδια συμπεριφορά, σύμφωνα με την αρχή ne bis in idem.

(114) Προκειμένου να ληφθεί υπόψη ο διασυνοριακός χαρακτήρας των υπηρεσιών και των λειτουργιών των παρόχων υπηρεσιών DNS, των μητρώων ονομάτων TLD, των οντοτήτων που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα, των παρόχων υπηρεσιών υπολογιστικού νέφους, των παρόχων υπηρεσιών κέντρων δεδομένων, των παρόχων δικτύων διανομής περιεχομένου, των παρόχων διαχειριζομένων υπηρεσιών, των παρόχων διαχειριζομένων υπηρεσιών ασφάλειας, καθώς και των παρόχων επιγραμμικών αγορών, επιγραμμικών μηχανών αναζήτησης και πλατφορμών υπηρεσιών κοινωνικής δικτύωσης, μόνο ένα κράτος μέλος θα πρέπει να έχει δικαιοδοσία επί των εν λόγω οντοτήτων. Η δικαιοδοσία θα πρέπει να ανατίθεται στο κράτος μέλος στο οποίο η οικεία οντότητα έχει την κύρια εγκατάστασή της στην Ένωση. Το κριτήριο της εγκατάστασης για τους σκοπούς της παρούσας οδηγίας συνεπάγεται την πραγματική άσκηση δραστηριότητας μέσω σταθερών ρυθμίσεων. Από αυτή την άποψη, ο νομικός τύπος των ρυθμίσεων αυτών, είτε πρόκειται για παράρτημα είτε για θυγατρική με νομική προσωπικότητα, δεν είναι καθοριστικής σημασίας. Το κατά πόσον πληρούται το συγκεκριμένο κριτήριο δεν θα πρέπει να εξαρτάται από το αν τα συστήματα δικτύου και πληροφοριών βρίσκονται σε συγκεκριμένο τόπο· η παρουσία και η χρήση τέτοιων συστημάτων δεν συνιστούν από μόνες τους βασική εγκατάσταση και συνεπώς δεν συνιστούν αποφασιστικά κριτήρια για τον καθορισμό της βασικής εγκατάστασης. Η κύρια εγκατάσταση θα πρέπει να θεωρείται ότι είναι στο κράτος μέλος όπου λαμβάνονται κατά κύριο λόγο στην Ένωση οι αποφάσεις που σχετίζονται με τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας. Αυτό συνήθως αντιστοιχεί στον τόπο της κεντρικής διοίκησης των οντοτήτων εντός της Ένωσης. Εάν το εν λόγω κράτος μέλος δεν μπορεί να προσδιοριστεί ή εάν δεν ληφθούν τέτοιες αποφάσεις στην Ένωση, η κύρια εγκατάσταση θα πρέπει να θεωρείται ότι βρίσκεται στο κράτος μέλος στο οποίο διεξάγονται οι επιχειρήσεις κυβερνοασφάλειας. Εάν το εν λόγω κράτος μέλος δεν μπορεί να προσδιοριστεί, η κύρια εγκατάσταση θα πρέπει να θεωρείται ότι βρίσκεται στο κράτος μέλος στο οποίο η οντότητα έχει την εγκατάσταση με τον μεγαλύτερο αριθμό εργαζομένων στην Ένωση. Όταν οι υπηρεσίες παρέχονται από όμιλο επιχειρήσεων, η κύρια εγκατάσταση της ελέγχουσας επιχείρησης θα πρέπει να θεωρείται ως η κύρια εγκατάσταση του ομίλου επιχειρήσεων.

(115) Όταν μια διαθέσιμη στο κοινό υπηρεσία DNS παρέχεται από πάροχο δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών μόνο ως μέρος της υπηρεσίας πρόσβασης στο διαδίκτυο, η οντότητα θα πρέπει να θεωρείται ότι εμπίπτει στη δικαιοδοσία όλων των κρατών μελών στα οποία παρέχονται οι υπηρεσίες της.

(116) Όταν πάροχος υπηρεσιών DNS, μητρώο ονομάτων TLD, οντότητα που παρέχει υπηρεσίες καταχώρισης ονομάτων τομέα, πάροχος υπηρεσιών υπολογιστικού νέφους, πάροχος υπηρεσιών κέντρου δεδομένων, πάροχος δικτύου διανομής περιεχομένου, πάροχος διαχειριζομένων υπηρεσιών, πάροχος διαχειριζομένων υπηρεσιών ασφάλειας ή πάροχος επιγραμμικών αγορών, επιγραμμικών μηχανών αναζήτησης ή πλατφορμών κοινωνικής δικτύωσης, ο οποίος δεν είναι εγκατεστημένος στην Ένωση, προσφέρει υπηρεσίες εντός της Ένωσης, θα πρέπει να ορίζει εκπρόσωπο στην Ένωση. Για να προσδιοριστεί κατά πόσον μια τέτοια οντότητα προσφέρει υπηρεσίες εντός της Ένωσης, θα πρέπει να εξακριβώνεται αν η εν λόγω οντότητα σχεδιάζει να προσφέρει υπηρεσίες σε πρόσωπα σε ένα η περισσότερα κράτη μέλη. Η απλή προσβασιμότητα στην Ένωση του δικτυακού τόπου της οντότητας ή ενός ενδιάμεσου φορέα ή μιας διεύθυνσης ηλεκτρονικού ταχυδρομείου ή άλλων στοιχείων επικοινωνίας, ή η χρήση γλώσσας που χρησιμοποιείται γενικά στην τρίτη χώρα όπου είναι εγκατεστημένη η οντότητα θα πρέπει να θεωρείται ανεπαρκής για την επιβεβαίωση της εν λόγω πρόθεσης. Ωστόσο, παράγοντες όπως η χρήση γλώσσας ή νομίσματος που χρησιμοποιείται γενικά σε ένα ή περισσότερα κράτη μέλη με δυνατότητα παραγγελίας υπηρεσιών στη γλώσσα αυτή, ή η αναφορά πελατών ή χρηστών που βρίσκονται στην Ένωση, θα μπορούσαν να καταστήσουν σαφές ότι η οντότητα σχεδιάζει να προσφέρει υπηρεσίες εντός της Ένωσης. Ο εκπρόσωπος πρέπει να ενεργεί εξ ονόματος της οντότητας και οι αρμόδιες αρχές ή οι CSIRT θα πρέπει να έχουν τη δυνατότητα να απευθύνονται στον εκπρόσωπο. Ο εκπρόσωπος θα πρέπει να ορίζεται ρητώς με γραπτή εντολή της οντότητας να ενεργεί για λογαριασμό της τελευταίας όσον αφορά τις υποχρεώσεις της που απορρέουν από την παρούσα οδηγία, συμπεριλαμβανομένης της αναφοράς περιστατικών.

(117) Προκειμένου να διασφαλιστεί σαφής επισκόπηση των παρόχων υπηρεσιών DNS, των μητρώων ονομάτων TLD, των οντοτήτων που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα, των παρόχων υπηρεσιών υπολογιστικού νέφους, των παρόχων υπηρεσιών κέντρων δεδομένων, των παρόχων δικτύων διανομής περιεχομένου, των παρόχων διαχειριζομένων υπηρεσιών, των παρόχων διαχειριζομένων υπηρεσιών ασφάλειας, καθώς και των παρόχων επιγραμμικών αγορών, επιγραμμικών μηχανών αναζήτησης και πλατφορμών κοινωνικής δικτύωσης, οι οποίες παρέχουν υπηρεσίες σε ολόκληρη την Ένωση που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας, ο ENISA θα πρέπει να δημιουργήσει και να τηρεί μητρώο των εν λόγω οντοτήτων, με βάση τις πληροφορίες που λαμβάνουν τα κράτη μέλη, κατά περίπτωση μέσω εθνικών μηχανισμών που έχουν θεσπιστεί για την καταχώριση των οντοτήτων. Τα ενιαία σημεία επαφής θα πρέπει να διαβιβάζουν στον ENISA τις πληροφορίες και τυχόν αλλαγές τους. Προκειμένου να εξασφαλίζονται η ακρίβεια και η πληρότητα των πληροφοριών που πρέπει να περιλαμβάνονται στο εν λόγω μητρώο, τα κράτη μέλη μπορούν να υποβάλλουν στον ENISA τις πληροφορίες που είναι διαθέσιμες σε τυχόν εθνικά μητρώα των εν λόγω οντοτήτων. Ο ENISA και τα κράτη μέλη θα πρέπει να λάβουν μέτρα για να διευκολύνουν τη διαλειτουργικότητα των εν λόγω μητρώων, διασφαλίζοντας παράλληλα την προστασία των εμπιστευτικών ή διαβαθμισμένων πληροφοριών. Ο ENISA θα πρέπει να θεσπίζει κατάλληλα πρωτόκολλα ταξινόμησης και διαχείρισης πληροφοριών για την εγγύηση της ασφάλειας και της εμπιστευτικότητας γνωστοποιημένων πληροφοριών, και να περιορίζει την πρόσβαση, αποθήκευση και διαβίβαση τέτοιου είδους πληροφοριών στους χρήστες για τους οποίους προορίζονται.

(118) Όταν οι πληροφορίες που είναι διαβαθμισμένες σύμφωνα με το ενωσιακό ή το εθνικό δίκαιο, ανταλλάσσονται, αναφέρονται ή κοινοποιούνται με άλλον τρόπο δυνάμει της παρούσας οδηγίας, θα πρέπει να εφαρμόζονται οι αντίστοιχοι κανόνες για τον χειρισμό των διαβαθμισμένων πληροφοριών. Επιπλέον, ο ENISA θα πρέπει να διαθέτει υποδομές, διαδικασίες και κανόνες ώστε να χειρίζεται ευαίσθητες και διαβαθμισμένες πληροφορίες σύμφωνα με τους ισχύοντες κανόνες ασφάλειας της ΕΕ για την προστασία διαβαθμισμένων πληροφοριών.

(119) Καθώς οι κυβερνοαπειλές καθίστανται πιο σύνθετες και εξελιγμένες, ο ορθός εντοπισμός αυτών των απειλών και τα μέτρα για την πρόληψή τους εξαρτώνται σε μεγάλο βαθμό από την τακτική ανταλλαγή πληροφοριών σχετικά με απειλές και τρωτότητες μεταξύ των οντοτήτων. Η ανταλλαγή πληροφοριών συμβάλλει στην αύξηση της ευαισθητοποίησης σχετικά με τις κυβερνοαπειλές, γεγονός που, με τη σειρά του, ενισχύει την ικανότητα των οντοτήτων να αποτρέπουν την επέλευση τέτοιων απειλών σε περιστατικά και επιτρέπει στις οντότητες να περιορίζουν καλύτερα τις επιπτώσεις των περιστατικών και να ανακάμπτουν αποτελεσματικότερα. Ελλείψει καθοδήγησης σε επίπεδο Ένωσης, διάφοροι παράγοντες φαίνεται ότι εμπόδισαν την εν λόγω ανταλλαγή πληροφοριών, ιδίως η αβεβαιότητα σχετικά με τη συμβατότητα με τους κανόνες περί ανταγωνισμού και ευθύνης.

(120) Οι οντότητες θα πρέπει να ενθαρρύνονται και να επικουρούνται από τα κράτη μέλη ώστε να αξιοποιούν συλλογικά τις ατομικές γνώσεις και την πρακτική πείρα τους σε στρατηγικό, τακτικό και επιχειρησιακό επίπεδο, με σκοπό την ενίσχυση των ικανοτήτων τους να προλαμβάνουν, να εντοπίζουν, να αντιμετωπίζουν ή να ανακάμπτουν από περιστατικά ή να μετριάζουν τις επιπτώσεις τους. Συνεπώς, είναι αναγκαίο να καταστεί δυνατή η δημιουργία ρυθμίσεων εθελοντικής ανταλλαγής πληροφοριών στον τομέα της κυβερνοασφάλειας σε επίπεδο Ένωσης. Για τον σκοπό αυτό, τα κράτη μέλη θα πρέπει να συνδράμουν ενεργά και να ενθαρρύνουν επίσης οντότητες όπως αυτές που παρέχουν υπηρεσίες και έρευνα κυβερνοασφάλειας, καθώς και τις σχετικές οντότητες που δεν εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας, να συμμετέχουν στις εν λόγω ρυθμίσεις ανταλλαγής πληροφοριών στον τομέα της κυβερνοασφάλειας. Οι ρυθμίσεις αυτές θα πρέπει να θεσπιστούν σε πλήρη συμμόρφωση με τους κανόνες ανταγωνισμού της Ένωσης και το δίκαιο της Ένωσης για την προστασία των δεδομένων.

(121) Η επεξεργασία δεδομένων προσωπικού χαρακτήρα, στον βαθμό που είναι αναγκαία και αναλογική για τον σκοπό της προστασίας της ασφάλειας των συστημάτων δικτύου και πληροφοριών από βασικές και σημαντικές οντότητες, θα μπορούσε να θεωρηθεί σύννομη λόγω του ότι η εν λόγω επεξεργασία συμμορφώνεται με νομική υποχρέωση στην οποία υπόκειται ο υπεύθυνος επεξεργασίας, σύμφωνα με τις απαιτήσεις του άρθρου 6 παράγραφος 1 στοιχείο γ) και του άρθρου 6 παράγραφος 3 του κανονισμού (ΕΕ) 2016/679. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα θα μπορούσε επίσης να είναι απαραίτητη για έννομα συμφέροντα που επιδιώκονται από βασικές και σημαντικές οντότητες, καθώς και από παρόχους τεχνολογιών και υπηρεσιών ασφάλειας που ενεργούν για λογαριασμό των εν λόγω οντοτήτων, σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο στ) του κανονισμού (ΕΕ) 2016/679, μεταξύ άλλων όταν η εν λόγω επεξεργασία είναι απαραίτητη για ρυθμίσεις ανταλλαγής πληροφοριών για την κυβερνοασφάλεια ή για την εθελοντική κοινοποίηση σχετικών πληροφοριών σύμφωνα με την παρούσα οδηγία. Μέτρα σχετικά με την πρόληψη, τον εντοπισμό, τον προσδιορισμό, τον περιορισμό, την ανάλυση και την αντιμετώπιση περιστατικών, μέτρα για την ευαισθητοποίηση σχετικά με συγκεκριμένες κυβερνοαπειλές, την ανταλλαγή πληροφοριών στο πλαίσιο της αποκατάστασης ευπαθειών και της συντονισμένης γνωστοποίησης ευπαθειών, την εθελούσια ανταλλαγή πληροφοριών σχετικά με τα εν λόγω περιστατικά, τις κυβερνοαπειλές και τις ευπάθειες, τους δείκτες έκθεσης σε κίνδυνο, τις τακτικές, τις τεχνικές και τις διαδικασίες, τις ειδοποιήσεις επαγρύπνησης για την κυβερνοασφάλεια και τα εργαλεία διαμόρφωσης θα μπορούσαν να απαιτούν την επεξεργασία ορισμένων κατηγοριών δεδομένων προσωπικού χαρακτήρα, όπως διευθύνσεις IP, ενιαίους εντοπιστές πόρων (URL), ονόματα τομέα, διευθύνσεις ηλεκτρονικού ταχυδρομείου, και, στον βαθμό που αυτά αποκαλύπτουν προσωπικά δεδομένα, χρονοσφραγίδες. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές, ενιαία σημεία επαφής και CSIRT θα μπορούσε να συνιστά νομική υποχρέωση ή να θεωρείται αναγκαία για την εκτέλεση καθήκοντος δημοσίου συμφέροντος ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο γ) ή ε) και το άρθρο 6 παράγραφος 3 του κανονισμού (ΕΕ) 2016/679, ή για την επιδίωξη έννομου συμφέροντος των βασικών και σημαντικών οντοτήτων, όπως αναφέρεται στο άρθρο 6 παράγραφος 1 στοιχείο στ) του εν λόγω κανονισμού. Επιπλέον, το εθνικό δίκαιο θα μπορούσε να θεσπίζει κανόνες που θα επιτρέπουν στις αρμόδιες αρχές, στα ενιαία σημεία επαφής και στις CSIRT, στον βαθμό που είναι αναγκαίο και αναλογικό για τον σκοπό της προστασίας της ασφάλειας των συστημάτων δικτύου και πληροφοριών βασικών και σημαντικών οντοτήτων, να επεξεργάζονται ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα σύμφωνα με το άρθρο 9 του κανονισμού (ΕΕ) 2016/679, ιδίως με την πρόβλεψη κατάλληλων και ειδικών μέτρων για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων των φυσικών προσώπων, συμπεριλαμβανομένων τεχνικών περιορισμών στην περαιτέρω χρήση των εν λόγω δεδομένων και της χρήσης προηγμένων μέτρων ασφάλειας και προστασίας της ιδιωτικής ζωής, όπως η ψευδωνυμοποίηση, ή η κρυπτογράφηση όταν η ανωνυμοποίηση μπορεί να επηρεάσει σημαντικά τον επιδιωκόμενο σκοπό.

(122) Προκειμένου να ενισχυθούν οι εποπτικές εξουσίες και τα μέτρα που συμβάλλουν στη διασφάλιση της αποτελεσματικής συμμόρφωσης, η παρούσα οδηγία θα πρέπει να προβλέπει έναν ελάχιστο κατάλογο εποπτικών μέτρων και μέσων μέσω των οποίων οι αρμόδιες αρχές μπορούν να εποπτεύουν βασικές και σημαντικές οντότητες. Επιπλέον, η παρούσα οδηγία θα πρέπει να καθιερώσει μια διαφοροποίηση του εποπτικού καθεστώτος μεταξύ βασικών και σημαντικών οντοτήτων, με σκοπό την εξασφάλιση δίκαιης ισορροπίας των υποχρεώσεων τόσο για τις εν λόγω οντότητες όσο και για τις αρμόδιες αρχές. Συνεπώς, οι βασικές οντότητες θα πρέπει να υπόκεινται σε πλήρες εκ των προτέρων και εκ των υστέρων καθεστώς εποπτείας, ενώ οι σημαντικές οντότητες θα πρέπει να υπόκεινται σε απλοποιημένο, μόνο εκ των υστέρων, εποπτικό καθεστώς. Δεν θα πρέπει επομένως να απαιτείται από τις σημαντικές οντότητες να τεκμηριώνουν συστηματικά τη συμμόρφωση με τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας, ενώ οι αρμόδιες αρχές θα πρέπει να εφαρμόζουν μια εκ των υστέρων προσέγγιση της εποπτείας και, ως εκ τούτου, να μην έχουν γενική υποχρέωση εποπτείας των εν λόγω οντοτήτων. Η εκ των υστέρων εποπτεία σημαντικών οντοτήτων μπορεί να ενεργοποιείται με αποδεικτικά στοιχεία, ενδείξεις ή πληροφορίες που περιέρχονται σε γνώση των αρμόδιων αρχών τις οποίες οι εν λόγω αρχές θεωρούν ότι υποδηλώνουν πιθανές παραβιάσεις των υποχρεώσεων της παρούσας οδηγίας. Για παράδειγμα, τέτοια αποδεικτικά στοιχεία, ενδείξεις ή πληροφορίες θα μπορούσαν να είναι του είδους που παρέχονται στις αρμόδιες αρχές από άλλες αρχές, οντότητες, πολίτες, μέσα ενημέρωσης ή άλλες πηγές, πληροφορίες διαθέσιμες στο κοινό, ή θα μπορούσαν να προκύπτουν από άλλες δραστηριότητες που διεξάγουν οι αρμόδιες αρχές κατά την εκτέλεση των καθηκόντων τους.

(123) Η εκτέλεση εποπτικών καθηκόντων από τις αρμόδιες αρχές δεν θα πρέπει να παρεμποδίζει αδικαιολόγητα τις επιχειρηματικές δραστηριότητες της οικείας οντότητας. Όταν οι αρμόδιες αρχές εκτελούν τα εποπτικά τους καθήκοντα σε σχέση με βασικές οντότητες, συμπεριλαμβανομένης της διενέργειας επιτόπιων επιθεωρήσεων και της εποπτείας εκτός των εγκαταστάσεων, της διερεύνησης περιπτώσεων παραβιάσεων της παρούσας οδηγίας, και της διενέργειας ελέγχων ασφάλειας ή σαρώσεων ασφαλείας, θα πρέπει να ελαχιστοποιούν τον αντίκτυπο στις επιχειρηματικές δραστηριότητες της οικείας οντότητας.

(124) Στο πλαίσιο της άσκησης της εκ των προτέρων εποπτείας, οι αρμόδιες αρχές θα πρέπει να είναι σε θέση να αποφασίζουν πώς θα ιεραρχήσουν τη χρήση των εποπτικών μέτρων και μέσων που έχουν στη διάθεσή τους με αναλογικό τρόπο. Τούτο συνεπάγεται ότι οι αρμόδιες αρχές μπορούν να αποφασίζουν σχετικά με την εν λόγω ιεράρχηση βάσει εποπτικών μεθοδολογιών οι οποίες θα πρέπει να ακολουθούν προσέγγιση που βασίζεται στους κινδύνους. Πιο συγκεκριμένα, οι μεθοδολογίες αυτές θα μπορούσαν να περιλαμβάνουν κριτήρια ή στοιχεία αναφοράς για την κατάταξη των βασικών οντοτήτων σε κατηγορίες κινδύνου, και αντίστοιχα εποπτικά μέτρα και μέσα που συνιστώνται ανά κατηγορία κινδύνου, όπως χρήση, συχνότητα ή είδος επιτόπιων επιθεωρήσεων, ή στοχευμένων ελέγχων ασφαλείας ή σαρώσεων ασφαλείας, είδος πληροφοριών που πρέπει να ζητούνται και βαθμός λεπτομέρειας των εν λόγω πληροφοριών. Οι εν λόγω εποπτικές

μεθοδολογίες θα μπορούσαν επίσης να συνοδεύονται από προγράμματα εργασίας και να αξιολογούνται και να επανεξετάζονται τακτικά, μεταξύ άλλων όσον αφορά πτυχές όπως η κατανομή των πόρων και οι ανάγκες σε πόρους. Όσον αφορά τους φορείς δημόσιας διοίκησης, οι εποπτικές εξουσίες θα πρέπει να ασκούνται σύμφωνα με το εθνικό νομοθετικό και θεσμικό πλαίσιο.

(125) Οι αρμόδιες αρχές θα πρέπει να διασφαλίζουν ότι τα εποπτικά τους καθήκοντα σε σχέση με βασικές και σημαντικές οντότητες ασκούνται από καταρτισμένους επαγγελματίες, οι οποίοι θα πρέπει να διαθέτουν τις απαραίτητες δεξιότητες για την εκτέλεση των εν λόγω καθηκόντων, ιδίως όσον αφορά τη διενέργεια επιτόπιων επιθεωρήσεων και την εποπτεία εκτός των εγκαταστάσεων, συμπεριλαμβανομένου του εντοπισμού αδυναμιών στις βάσεις δεδομένων, το υλικό, τα τείχη προστασίας, την κρυπτογράφηση και τα δίκτυα. Οι εν λόγω επιθεωρήσεις και εποπτεία θα πρέπει να διενεργούνται με αντικειμενικό τρόπο.

(126) Σε δεόντως αιτιολογημένες περιπτώσεις όπου αντιλαμβάνεται σημαντική κυβερνοαπειλή ή επικείμενο κίνδυνο, η αρμόδια αρχή θα πρέπει να είναι σε θέση να λαμβάνει άμεσες αποφάσεις επιβολής με σκοπό την πρόληψη ή την αντιμετώπιση περιστατικού.

(127) Προκειμένου να καταστεί αποτελεσματική η επιβολή, θα πρέπει να καταρτιστεί ένας ελάχιστος κατάλογος μέσων επιβολής που μπορούν να ασκηθούν σε περίπτωση παραβίασης των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και των υποχρεώσεων υποβολής εκθέσεων που προβλέπονται στην παρούσα οδηγία, με τη θέσπιση σαφούς και συνεκτικού πλαισίου για τα εν λόγω μέσα επιβολής σε ολόκληρη την Ένωση. Θα πρέπει να λαμβάνονται δεόντως υπόψη η φύση, η σοβαρότητα και η διάρκεια της παράβασης της παρούσας οδηγίας, η υλική ή μη υλική ζημία που προκλήθηκε, το κατά πόσον η παράβαση ήταν εκ προθέσεως ή εξ αμελείας, οι ενέργειες που πραγματοποιήθηκαν για την πρόληψη ή τον μετριασμό της υλικής ή μη υλικής ζημίας, ο βαθμός ευθύνης ή τυχόν σχετικών προηγούμενων παραβάσεων, ο βαθμός συνεργασίας με την αρμόδια αρχή και κάθε άλλη επιβαρυντική ή ελαφρυντική περίσταση. Τα μέσα επιβολής, περιλαμβανομένων των διοικητικών προστίμων, θα πρέπει να είναι αναλογικές και η επιβολή τους θα πρέπει να υπόκειται σε κατάλληλες δικονομικές εγγυήσεις σύμφωνα με τις γενικές αρχές του ενωσιακού δικαίου και του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης («ο Χάρτης»), συμπεριλαμβανομένου του δικαιώματος αποτελεσματικής δικαστικής προστασίας και δίκαιης δίκης, του τεκμηρίου αθωότητας και του δικαιώματος υπεράσπισης.

(128) Η παρούσα οδηγία δεν απαιτεί από τα κράτη μέλη να προβλέπουν ποινική ή αστική ευθύνη έναντι φυσικών προσώπων που είναι υπεύθυνα να διασφαλίζουν ότι μια οντότητα συμμορφώνεται με την παρούσα οδηγία για ζημία που υπέστησαν τρίτοι ως αποτέλεσμα παραβίασης της παρούσας οδηγίας.

(129) Προκειμένου να διασφαλιστεί η αποτελεσματική επιβολή των υποχρεώσεων που ορίζονται στην παρούσα οδηγία, κάθε αρμόδια αρχή θα πρέπει να έχει την εξουσία να επιβάλλει ή να ζητεί την επιβολή διοικητικών προστίμων.

(130) Σε περίπτωση που επιβάλλονται διοικητικά πρόστιμα σε βασική ή σημαντική οντότητα που είναι επιχείρηση, η επιχείρηση θα πρέπει να νοείται ως επιχείρηση σύμφωνα με τα άρθρα 101 και 102 ΣΛΕΕ για τους σκοπούς αυτούς. Σε περίπτωση που επιβάλλονται διοικητικά πρόστιμα σε πρόσωπα που δεν είναι επιχειρήσεις, η αρμόδια αρχή θα πρέπει να λαμβάνει υπόψη το γενικό επίπεδο εισοδημάτων στο κράτος μέλος, καθώς και την οικονομική κατάσταση του προσώπου, όταν εξετάζει το ενδεδειγμένο ποσό του προστίμου. Θα πρέπει να εναπόκειται στα κράτη μέλη να αποφασίζουν εάν και σε ποιο βαθμό μπορούν να επιβάλλονται διοικητικά πρόστιμα σε δημόσιες αρχές. Η επιβολή διοικητικού προστίμου δεν θίγει την άσκηση άλλων εξουσιών από τις αρμόδιες αρχές ή άλλων κυρώσεων που προβλέπονται στους εθνικούς κανόνες μεταφοράς της παρούσας οδηγίας.

(131) Τα κράτη μέλη θα πρέπει να μπορούν να θεσπίζουν κανόνες σχετικά με τις ποινικές κυρώσεις για παραβάσεις των εθνικών κανόνων μεταφοράς της παρούσας οδηγίας. Ωστόσο, η επιβολή ποινικών κυρώσεων για παραβάσεις τέτοιων εθνικών κανόνων και συναφών διοικητικών κυρώσεων δεν θα πρέπει να οδηγεί σε παραβίαση της αρχής ne bis in idem, όπως την ερμηνεύει το Δικαστήριο της Ευρωπαϊκής Ένωσης.

(132) Όταν η παρούσα οδηγία δεν εναρμονίζει τις διοικητικές κυρώσεις ή όταν είναι αναγκαίο σε άλλες περιπτώσεις, π.χ. σε περίπτωση σοβαρής παράβασης των υποχρεώσεων της παρούσας οδηγίας, τα κράτη μέλη θα πρέπει να εφαρμόζουν σύστημα που προβλέπει αποτελεσματικές, αναλογικές και αποτρεπτικές κυρώσεις. Η φύση των εν λόγω κυρώσεων (ποινικών ή διοικητικών) θα πρέπει να προσδιορίζεται από το εθνικό δίκαιο.

(133) Προκειμένου να ενισχυθεί περαιτέρω η αποτελεσματικότητα και η αποτρεπτικότητα των εφαρμοστέων μέσων επιβολής σε περίπτωση παράβασης των υποχρεώσεων της παρούσας οδηγίας, οι αρμόδιες αρχές θα πρέπει να έχουν την εξουσία να αναστέλλουν προσωρινά ή να ζητούν την προσωρινή αναστολή πιστοποίησης ή εξουσιοδότησης που αφορά μέρος ή το σύνολο των σχετικών υπηρεσιών που παρέχονται ή των δραστηριοτήτων που ασκούνται από βασική οντότητα και να ζητούν την επιβολή προσωρινής απαγόρευσης της άσκησης διευθυντικών καθηκόντων από οποιοδήποτε φυσικό πρόσωπο ασκεί διευθυντικά καθήκοντα σε επίπεδο διευθύνοντος συμβούλου ή νομικού εκπροσώπου. Δεδομένης της σοβαρότητας και του αντικτύπου τους στις δραστηριότητες των οντοτήτων και, εν τέλει, στους χρήστες, οι εν λόγω προσωρινές αναστολές ή απαγορεύσεις θα πρέπει να εφαρμόζονται μόνο κατ' αναλογία προς τη σοβαρότητα της παράβασης και λαμβανομένων υπόψη των περιστάσεων κάθε μεμονωμένης περίπτωσης, συμπεριλαμβανομένου του κατά πόσον η παράβαση ήταν εκ προθέσεως ή εξ αμελείας, καθώς και οποιωνδήποτε ενεργειών που αναλαμβάνονται για την πρόληψη ή τον μετριασμό της υλικής ή μη υλικής ζημίας. Οι εν λόγω προσωρινές αναστολές ή απαγορεύσεις θα πρέπει να εφαρμόζονται μόνο ως έσχατη λύση, δηλαδή μόνο αφού εξαντληθούν τα άλλα σχετικά μέτρα επιβολής που προβλέπονται στην παρούσα οδηγία, και μόνο έως ότου η οικεία οντότητα λάβει τα αναγκαία μέτρα για να διορθώσει τις ελλείψεις ή να συμμορφωθεί με τις απαιτήσεις της αρμόδιας αρχής για τις οποίες εφαρμόστηκαν οι εν λόγω προσωρινές αναστολές ή απαγορεύσεις. Η επιβολή τέτοιων προσωρινών αναστολών ή απαγορεύσεων θα πρέπει να υπόκειται σε κατάλληλες διαδικαστικές εγγυήσεις σύμφωνα με τις γενικές αρχές του δικαίου της Ένωσης και του Χάρτη, συμπεριλαμβανομένου του δικαιώματος αποτελεσματικής δικαστικής προστασίας και δίκαιης δίκης, του τεκμηρίου αθωότητας και του δικαιώματος υπεράσπισης.

(134) Για τη διασφάλιση της συμμόρφωσης των οντοτήτων με τις υποχρεώσεις τους δυνάμει της παρούσας οδηγίας, τα κράτη μέλη θα πρέπει να συνεργάζονται και να αλληλοβοηθούνται όσον αφορά τα μέτρα εποπτείας και επιβολής, ιδίως όταν μια οντότητα παρέχει υπηρεσίες σε περισσότερα του ενός κράτη μέλη ή όταν τα συστήματα δικτύου και πληροφοριών της βρίσκονται σε κράτος μέλος διαφορετικό από εκείνο στο οποίο παρέχει υπηρεσίες. Κατά την παροχή συνδρομής, η αρμόδια αρχή στην οποία υποβάλλεται το αίτημα θα πρέπει να λαμβάνει μέτρα εποπτείας ή επιβολής σύμφωνα με το εθνικό δίκαιο. Προκειμένου να διασφαλιστεί η ομαλή λειτουργία της αμοιβαίας συνδρομής δυνάμει της παρούσας οδηγίας, οι αρμόδιες αρχές θα πρέπει να χρησιμοποιούν την Ομάδα Συνεργασίας ως φόρουμ για τη συζήτηση υποθέσεων και ειδικών αιτημάτων συνδρομής.

(135) Προκειμένου να διασφαλιστεί η αποτελεσματική εποπτεία και επιβολή, ιδίως σε περίπτωση κατάστασης με διασυνοριακή διάσταση, τα κράτη μέλη που έχουν λάβει αίτηση αμοιβαίας συνδρομής θα πρέπει, εντός των ορίων του εν λόγω αιτήματος, να λαμβάνουν κατάλληλα μέτρα εποπτείας και επιβολής σε σχέση με την οντότητα αποτελεί αντικείμενο του αιτήματος αυτού και που παρέχει υπηρεσίες ή διαθέτει σύστημα δικτύου και πληροφοριών στην επικράτειά τους.

(136) Η παρούσα οδηγία θα πρέπει να θεσπίσει κανόνες συνεργασίας μεταξύ των αρμόδιων αρχών και των εποπτικών αρχών δυνάμει του κανονισμού (ΕΕ) 2016/679 για την αντιμετώπιση παραβάσεων της παρούσας οδηγίας που σχετίζονται με δεδομένα προσωπικού χαρακτήρα.

(137) Η παρούσα οδηγία θα πρέπει να αποσκοπεί στη διασφάλιση υψηλού επιπέδου ευθύνης για τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και τις υποχρεώσεις υποβολής εκθέσεων στο επίπεδο των βασικών και σημαντικών οντοτήτων. Συνεπώς, τα διοικητικά όργανα των βασικών και σημαντικών οντοτήτων θα πρέπει να εγκρίνουν τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και να επιβλέπουν την εφαρμογή τους.

(138) Προκειμένου να διασφαλιστεί υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση βάσει της παρούσας οδηγίας, θα πρέπει να ανατεθεί στην Επιτροπή η εξουσία έκδοσης πράξεων σύμφωνα με το άρθρο 290 ΣΛΕΕ όσον αφορά τη συμπλήρωση της παρούσας οδηγίας με τον προσδιορισμό των κατηγοριών βασικών και σημαντικών οντοτήτων που πρέπει να χρησιμοποιούν ορισμένα πιστοποιημένα προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ ή να αποκτούν πιστοποιητικό στο πλαίσιο ευρωπαϊκού καθεστώτος πιστοποίησης κυβερνοασφάλειας. Είναι ιδιαίτερα σημαντικό η Επιτροπή να διεξάγει, κατά τις προπαρασκευαστικές της εργασίες, τις κατάλληλες διαβουλεύσεις, μεταξύ άλλων σε επίπεδο εμπειρογνωμόνων, και οι διαβουλεύσεις αυτές να πραγματοποιούνται σύμφωνα με τις αρχές που ορίζονται στη διοργανική συμφωνία της 13ης Απριλίου 2016 για τη βελτίωση του νομοθετικού έργου ([22]). Πιο συγκεκριμένα, προκειμένου να διασφαλιστεί η ίση συμμετοχή στην προετοιμασία των κατ' εξουσιοδότηση πράξεων, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο λαμβάνουν όλα τα έγγραφα κατά τον ίδιο χρόνο με τους εμπειρογνώμονες των κρατών μελών, και οι εμπειρογνώμονές τους έχουν συστηματικά πρόσβαση στις συνεδριάσεις των ομάδων εμπειρογνωμόνων της Επιτροπής που ασχολούνται με την προετοιμασία κατ' εξουσιοδότηση πράξεων.

([22]) ΕΕ L 123 της 12.5.2016, σ. 1.

(139) Προκειμένου να διασφαλιστούν ενιαίες προϋποθέσεις για την εφαρμογή της παρούσας οδηγίας, θα πρέπει να ανατεθούν στην Επιτροπή εκτελεστικές αρμοδιότητες για τον καθορισμό των διαδικαστικών ρυθμίσεων που απαιτούνται για τη λειτουργία της ομάδας συνεργασίας και των τεχνικών και μεθοδολογικών και τομεακών απαιτήσεων σχετικά με τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας, καθώς και για τον περαιτέρω προσδιορισμό του είδους των πληροφοριών, του μορφότυπου και της διαδικασίας των κοινοποιήσεων περιστατικών, κυβερνοαπειλών και κοινοποιήσεων παρ' ολίγον περιστατικών, και της κοινοποίησης σημαντικών κυβερνοαπειλών, καθώς και των περιπτώσεων στις οποίες ένα περιστατικό πρέπει να θεωρείται σημαντικό. Οι εν λόγω αρμοδιότητες θα πρέπει να ασκούνται σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 182/2011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([23]).

(140) Η Επιτροπή θα πρέπει να επανεξετάζει περιοδικά την παρούσα οδηγία, κατόπιν διαβούλευσης με τα ενδιαφερόμενα μέρη, ιδίως προκειμένου να καθορίζεται κατά πόσον είναι σκόπιμο να προτείνονται τροποποιήσεις υπό το φως αλλαγών στις κοινωνικές, πολιτικές, τεχνολογικές συνθήκες ή στις συνθήκες της αγοράς. Στο πλαίσιο των εν λόγω επανεξετάσεων, η Επιτροπή θα πρέπει να αξιολογεί τη συνάφεια του μεγέθους των οικείων οντοτήτων και των τομέων, των υποτομέων και των τύπων οντοτήτων που αναφέρονται στα παραρτήματα της παρούσας οδηγίας για τη λειτουργία της οικονομίας και της κοινωνίας σε σχέση με την κυβερνοασφάλεια. Η Επιτροπή θα πρέπει να αξιολογεί, μεταξύ άλλων, κατά πόσον οι πάροχοι που χαρακτηρίζονται ως πολύ μεγάλες επιγραμμικές πλατφόρμες κατά την έννοια του άρθρου 33 του κανονισμού (ΕΕ) 2022/2065 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([24]) θα μπορούσαν να χαρακτηριστούν βασικές οντότητες βάσει της παρούσας οδηγίας.

(141) Η παρούσα οδηγία δημιουργεί νέα καθήκοντα για τον ENISA, ενισχύοντας έτσι τον ρόλο του, και θα μπορούσε επίσης να έχει ως αποτέλεσμα να απαιτείται από τον ENISA να εκτελεί τα υφιστάμενα καθήκοντά του δυνάμει του κανονισμού (ΕΕ) 2019/881 σε υψηλότερο επίπεδο από ό, τι στο παρελθόν. Προκειμένου να διασφαλιστεί ότι ο ENISA διαθέτει τους αναγκαίους οικονομικούς και ανθρώπινους πόρους για την εκτέλεση των υφιστάμενων και των νέων καθηκόντων, καθώς και για την κάλυψη οποιουδήποτε υψηλότερου επιπέδου εκτέλεσης των εν λόγω καθηκόντων που απορρέει από τον ενισχυμένο ρόλο του, ο προϋπολογισμός του θα πρέπει να αυξηθεί αναλόγως. Επιπλέον, προκειμένου να διασφαλιστεί η αποδοτική χρήση των πόρων, ο ENISA θα πρέπει να διαθέτει μεγαλύτερη ευελιξία όσον αφορά τον τρόπο με τον οποίο είναι σε θέση να κατανέμει τους πόρους εσωτερικά με σκοπό την αποτελεσματική εκτέλεση των καθηκόντων του και την ικανοποίηση των προσδοκιών.

(142) Δεδομένου ότι ο στόχος της παρούσας οδηγίας, ήτοι η επίτευξη υψηλού ενιαίου επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ένωση, δεν μπορεί να επιτευχθεί ικανοποιητικά από τα κράτη μέλη αλλά μπορεί, λόγω των επιπτώσεων της δράσης, να επιτευχθεί καλύτερα σε ενωσιακό επίπεδο, η Ένωση μπορεί να λάβει μέτρα, σύμφωνα με την αρχή της επικουρικότητας του άρθρου 5 της Συνθήκης για την Ευρωπαϊκή Ένωση. Σύμφωνα με την αρχή της αναλογικότητας του ιδίου άρθρου, η παρούσα οδηγία δεν υπερβαίνει τα αναγκαία για την επίτευξη του στόχου αυτού.

(143) Η παρούσα οδηγία σέβεται τα θεμελιώδη δικαιώματα και τηρεί τις αρχές που αναγνωρίζονται από τον Χάρτη, ιδίως το δικαίωμα στον σεβασμό της ιδιωτικότητας και των επικοινωνιών, την προστασία των δεδομένων προσωπικού χαρακτήρα, την επιχειρηματική ελευθερία, το δικαίωμα ιδιοκτησίας, το δικαίωμα αποτελεσματικής δικαστικής προστασίας και δίκαιης δίκης, το τεκμήριο αθωότητας και το δικαίωμα υπεράσπισης. Το δικαίωμα αποτελεσματικής δικαστικής προστασίας εκτείνεται στους αποδέκτες υπηρεσιών που παρέχονται από βασικές και σημαντικές οντότητες. Η παρούσα οδηγία θα πρέπει να εφαρμόζεται σύμφωνα με τα δικαιώματα και τις αρχές αυτές.

(144) Ζητήθηκε η γνώμη του Ευρωπαίου Επόπτη Προστασίας Δεδομένων σύμφωνα με το άρθρο 42 παράγραφος 1 του κανονισμού (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([25]) και διατύπωσε γνώμη στις 11 Μαρτίου 2021 ([26]),

([23]) Κανονισμός (ΕΕ) αριθ. 182/2011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 16ης Φεβρουαρίου 2011, για τη θέσπιση κανόνων και γενικών αρχών σχετικά με τους τρόπους ελέγχου από τα κράτη μέλη της άσκησης των εκτελεστικών αρμοδιοτήτων από την Επιτροπή (ΕΕ L 55 της 28.2.2011, σ. 13).

([24]) Κανονισμός (ΕΕ) 2022/2065 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 19ης Οκτωβρίου 2022, σχετικά με την ενιαία αγορά ψηφιακών υπηρεσιών και την τροποποίηση της οδηγίας 2000/31/ΕΚ (πράξη για τις ψηφιακές υπηρεσίες) (ΕΕ L 277 της 27.10.2022, σ. 1).

([25]) Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2018, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ (ΕΕ L 295 της 21.11.2018, σ. 39).

([26]) ΕΕ C 183 της 11.5.2021, σ. 3.

ΕΞΕΔΩΣΑΝ ΤΗΝ ΠΑΡΟΥΣΑ ΟΔΗΓΙΑ:

ΚΕΦΑΛΑΙΟ I

ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 1

Αντικείμενο

1. Η παρούσα οδηγία θεσπίζει μέτρα που αποσκοπούν στην επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ένωση, με σκοπό τη βελτίωση της λειτουργίας της εσωτερικής αγοράς.

2. Για τον σκοπό αυτό, η παρούσα οδηγία καθορίζει:

α) υποχρεώσεις που απαιτούν από τα κράτη μέλη να εγκρίνουν εθνικές στρατηγικές κυβερνοασφάλειας και να ορίσουν ή να συστήσουν αρμόδιες αρχές, αρχές διαχείρισης κυβερνοκρίσεων, ενιαία σημεία επαφής για την κυβερνοασφάλεια (ενιαία σημεία επαφής) και ομάδες αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές (CSIRT)·

β) μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και υποχρεώσεις υποβολής αναφορών για οντότητες του τύπου που αναφέρεται στο παράρτημα I ή II καθώς και για οντότητες που χαρακτηρίζονται ως κρίσιμες δυνάμει της οδηγίας (ΕΕ) 2022/2557·

γ) κανόνες και υποχρεώσεις σχετικά με την ανταλλαγή πληροφοριών για την κυβερνοασφάλεια·

δ) υποχρεώσεις των κρατών μελών σχετικά με την εποπτεία και την επιβολή.

Άρθρο 2

Πεδίο εφαρμογής

1. Η παρούσα οδηγία εφαρμόζεται σε δημόσιες ή ιδιωτικές οντότητες των τύπων που αναφέρονται στο παράρτημα I ή II οι οποίες χαρακτηρίζονται ως μεσαίες επιχειρήσεις δυνάμει του άρθρου 2 του παραρτήματος της σύστασης 2003/361/ΕΚ ή υπερβαίνουν τα ανώτατα όρια για τις μεσαίες επιχειρήσεις που αναφέρονται στο εν λόγω άρθρο και οι οποίες παρέχουν τις υπηρεσίες τους ή ασκούν τις δραστηριότητές τους εντός της Ένωσης.

Το άρθρο 3 παράγραφος 4 του παραρτήματος της εν λόγω σύστασης δεν εφαρμόζεται για τους σκοπούς της παρούσας οδηγίας.

2. Ανεξάρτητα από το μέγεθός τους, η παρούσα οδηγία εφαρμόζεται επίσης στις οντότητες τύπου που αναφέρεται στο παράρτημα I ή II, εφόσον:

α) οι υπηρεσίες παρέχονται από:

i) παρόχους δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών·

ii) παρόχους υπηρεσιών εμπιστοσύνης·

iii) μητρώα ονομάτων τομέα ανωτάτου επιπέδου, και παρόχους υπηρεσιών συστήματος ονομάτων τομέα·

β) η οντότητα είναι ο μοναδικός πάροχος, σε ένα κράτος μέλος, υπηρεσίας που είναι ουσιώδης για τη διατήρηση κρίσιμων κοινωνικών ή οικονομικών δραστηριοτήτων·

γ) η διατάραξη της υπηρεσίας που παρέχει η οντότητα θα μπορούσε να έχει σημαντικό αντίκτυπο στη δημόσια ασφάλεια, στη δημόσια τάξη ή στη δημόσια υγεία·

δ) η διατάραξη της υπηρεσίας που παρέχεται από την οντότητα θα μπορούσε να προκαλέσει σημαντικό συστημικό κίνδυνο, ιδίως για τομείς στους οποίους η διατάραξη αυτή θα μπορούσε να έχει διασυνοριακό αντίκτυπο·

ε) η οντότητα είναι κρίσιμη λόγω της ιδιαίτερης σημασίας της σε εθνικό ή περιφερειακό επίπεδο για τον συγκεκριμένο τομέα ή είδος υπηρεσίας ή για άλλους αλληλοεξαρτώμενους τομείς στο κράτος μέλος·

στ) η οντότητα είναι φορέας δημόσιας διοίκησης:

i) της κεντρικής κυβέρνησης όπως ορίζεται από κράτος μέλος σύμφωνα με το εθνικό δίκαιο·

ii) σε περιφερειακό επίπεδο, όπως ορίζεται από κράτος μέλος σύμφωνα με το εθνικό δίκαιο, ο οποίος, μετά από αξιολόγηση βάσει κινδύνου, παρέχει υπηρεσίες των οποίων η διατάραξη θα μπορούσε να έχει σημαντικό αντίκτυπο σε κρίσιμες κοινωνικές ή οικονομικές δραστηριότητες.

3. Ανεξαρτήτως του μεγέθους τους, η παρούσα οδηγία εφαρμόζεται σε οντότητες που χαρακτηρίζονται ως κρίσιμες οντότητες δυνάμει της οδηγίας (ΕΕ) 2022/2557·

4. Ανεξαρτήτως του μεγέθους τους, η παρούσα οδηγία εφαρμόζεται σε οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα.

5. Τα κράτη μέλη μπορούν να προβλέπουν ότι η παρούσα οδηγία εφαρμόζεται:

α) σε οντότητες δημόσιας διοίκησης σε τοπικό επίπεδο·

β) σε εκπαιδευτικά ιδρύματα, ιδίως όταν διεξάγουν κρίσιμες ερευνητικές δραστηριότητες.

6. Η παρούσα οδηγία εφαρμόζεται με την επιφύλαξη της ευθύνης των κρατών μελών για τη διαφύλαξη της εθνικής ασφάλειας και κυριαρχικού τους δικαιώματος να διαφυλάσσουν άλλες ουσιώδεις λειτουργίες του κράτους, συμπεριλαμβανομένων της διασφάλισης της εδαφικής ακεραιότητας του κράτους και της διατήρησης της δημόσιας τάξης.

7. Η παρούσα οδηγία δεν εφαρμόζεται σε οντότητες δημόσιας διοίκησης που ασκούν τις δραστηριότητές τους στους τομείς της εθνικής ασφάλειας, της δημόσιας τάξης, της άμυνας ή της επιβολής του νόμου, συμπεριλαμβανομένων της πρόληψης, της διακρίβωσης, της διαπίστωσης και της δίωξης ποινικών αδικημάτων.

8. Τα κράτη μέλη μπορούν να εξαιρούν συγκεκριμένες οντότητες που ασκούν δραστηριότητες στους τομείς της εθνικής ασφάλειας, της δημόσιας τάξης, της άμυνας ή της επιβολής του νόμου, συμπεριλαμβανομένων δραστηριοτήτων που σχετίζονται με την πρόληψη, τη διερεύνηση, τη διακρίβωση και τη δίωξη ποινικών αδικημάτων, ή οι οποίες παρέχουν υπηρεσίες αποκλειστικά στους φορείς δημόσιας διοίκησης που αναφέρονται στην παράγραφο 7 του παρόντος άρθρου, από τις υποχρεώσεις που ορίζονται στο άρθρο 21 ή 23 όσον αφορά τις εν λόγω δραστηριότητες ή υπηρεσίες. Στις περιπτώσεις αυτές, τα μέτρα εποπτείας και επιβολής που αναφέρονται στο κεφάλαιο VII δεν εφαρμόζονται σε σχέση με τις συγκεκριμένες δραστηριότητες ή υπηρεσίες. Όταν οι οντότητες ασκούν δραστηριότητες ή παρέχουν υπηρεσίες αποκλειστικά του τύπου που αναφέρεται στην παρούσα παράγραφο, τα κράτη μέλη μπορούν επίσης να αποφασίσουν να εξαιρέσουν τις εν λόγω οντότητες από τις υποχρεώσεις που ορίζονται στα άρθρα 3 και 27.

9. Οι παράγραφοι 7 και 8 δεν εφαρμόζονται όταν μια οντότητα ενεργεί ως πάροχος υπηρεσιών εμπιστοσύνης.

10. Η παρούσα οδηγία δεν εφαρμόζεται σε οντότητες τις οποίες τα κράτη μέλη έχουν εξαιρέσει από το πεδίο εφαρμογής του κανονισμού (ΕΕ) 2022/2554 σύμφωνα με το άρθρο 2 παράγραφος 4 του εν λόγω κανονισμού.

11. Οι υποχρεώσεις που προβλέπονται στην παρούσα οδηγία δεν συνεπάγονται την παροχή πληροφοριών, η γνωστοποίηση των οποίων θα ήταν αντίθετη προς τα ουσιώδη συμφέροντα εθνικής ασφάλειας, δημόσιας τάξης ή άμυνας των κρατών μελών.

12. Η παρούσα οδηγία εφαρμόζεται με την επιφύλαξη του κανονισμού (ΕΕ) 2016/679, της οδηγίας 2002/58/ΕΚ, των οδηγιών 2011/93/ΕΕ ([27]) και 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([28]) και της οδηγίας (ΕΕ) 2022/2557.

13. Με την επιφύλαξη του άρθρου 346 ΣΛΕΕ, πληροφορίες που είναι εμπιστευτικές σύμφωνα με ενωσιακούς ή εθνικούς κανόνες, όπως κανόνες περί επιχειρηματικού απορρήτου, ανταλλάσσονται με την Επιτροπή και άλλες αρμόδιες αρχές σύμφωνα με την παρούσα οδηγία, μόνον εφόσον η ανταλλαγή αυτή είναι αναγκαία για την εφαρμογή της παρούσας οδηγίας. Οι ανταλλασσόμενες πληροφορίες περιορίζονται σε ό,τι είναι συναφές και αναλογικό προς τον σκοπό της ανταλλαγής αυτής. Η ανταλλαγή πληροφοριών διαφυλάσσει το απόρρητο αυτών των πληροφοριών και προστατεύει τα συμφέροντα ασφάλειας και τα εμπορικά συμφέροντα των οικείων οντοτήτων.

([27]) Οδηγία 2011/93/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 2011, σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας και την αντικατάσταση της απόφασης-πλαίσιο 2004/68/ΔΕΥ του Συμβουλίου (ΕΕ L 335 της 17.12.2011, σ. 1).

([28]) Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Αυγούστου 2013, για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου (ΕΕ L 218 της 14.8.2013, σ. 8).

14. Οι οντότητες, οι αρμόδιες αρχές, τα ενιαία σημεία επαφής και οι CSIRT επεξεργάζονται δεδομένα προσωπικού χαρακτήρα στον βαθμό που είναι αναγκαίο για τους σκοπούς της παρούσας οδηγίας και σύμφωνα με τον κανονισμό (ΕΕ) 2016/679, και πιο συγκεκριμένα η εν λόγω επεξεργασία βασίζεται στο άρθρο 6 του εν λόγω κανονισμού.

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα δυνάμει της παρούσας οδηγίας από παρόχους δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή παρόχους διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών πραγματοποιείται σύμφωνα με το δίκαιο της Ένωσης για την προστασία των δεδομένων και το δίκαιο της Ένωσης για την προστασία της ιδιωτικότητας, ιδίως την οδηγία 2002/58/ΕΚ.

Άρθρο 3

Βασικές και σημαντικές οντότητες

1. Για τους σκοπούς της παρούσας οδηγίας, βασικές οντότητες θεωρούνται οι ακόλουθες οντότητες:

α) οντότητες των τύπων που αναφέρονται στο παράρτημα Ι, οι οποίες υπερβαίνουν τα ανώτατα όρια για τις μεσαίες επιχειρήσεις που προβλέπονται στο άρθρο 2 παράγραφος 1 του παραρτήματος της σύστασης 2003/361/ΕΚ·

β) εγκεκριμένοι πάροχοι υπηρεσιών εμπιστοσύνης και μητρώα ονομάτων τομέα ανωτάτου επιπέδου, καθώς και πάροχοι υπηρεσιών DNS, ανεξάρτητα από το μέγεθός τους·

γ) πάροχοι δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών που χαρακτηρίζονται ως μεσαίες επιχειρήσεις, δυνάμει 2 του παραρτήματος της σύστασης 2003/361/ΕΚ·

δ) οντότητες δημόσιας διοίκησης που αναφέρονται στο άρθρο 2 παράγραφος 2 στοιχείο στ) σημείο i)·

ε) οποιεσδήποτε άλλες οντότητες των τύπων που αναφέρονται στο παράρτημα Ι ή ΙΙ, οι οποίες προσδιορίζονται από κράτος μέλος ως βασικές οντότητες βάσει του άρθρου 2 παράγραφος 2 στοιχεία β) έως ε)·

στ) οντότητες που προσδιορίζονται ως κρίσιμες οντότητες βάσει της οδηγίας (ΕΕ) 2022/2557, που αναφέρονται στο άρθρο 2 παράγραφος 3 της παρούσας οδηγίας·

ζ) αν υπάρχει σχετική πρόβλεψη στο κράτος μέλος, οντότητες που το κράτος μέλος αναγνώρισε πριν από τις 16 Ιανουαρίου 2023 ως φορείς εκμετάλλευσης βασικών υπηρεσιών σύμφωνα με την οδηγία (ΕΕ) 2016/1148 ή το εθνικό δίκαιο.

2. Για τους σκοπούς της παρούσας οδηγίας, οι οντότητες των τύπων που αναφέρονται στο παράρτημα Ι ή ΙΙ, οι οποίες δεν θεωρούνται βασικές οντότητες σύμφωνα με την παράγραφο 1 του παρόντος άρθρου, θεωρούνται σημαντικές οντότητες. Σε αυτές περιλαμβάνονται οντότητες που προσδιορίζονται από τα κράτη μέλη ως σημαντικές οντότητες βάσει του άρθρου 2 παράγραφος 2 στοιχεία β) έως ε).

3. Έως τις 17 Απριλίου 2025, τα κράτη μέλη καταρτίζουν κατάλογο βασικών και σημαντικών οντοτήτων καθώς και οντοτήτων που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα. Τα κράτη μέλη επανεξετάζουν και, κατά περίπτωση, επικαιροποιούν τον εν λόγω κατάλογο σε τακτική βάση και στη συνέχεια τουλάχιστον ανά διετία.

4. Για τους σκοπούς της κατάρτισης του καταλόγου που αναφέρεται στην παράγραφο 3, τα κράτη μέλη απαιτούν από τις οντότητες που αναφέρονται στην εν λόγω παράγραφο να υποβάλλουν τουλάχιστον τις ακόλουθες πληροφορίες στις αρμόδιες αρχές:

α) την επωνυμία της οντότητας·

β) τη διεύθυνση και τα επικαιροποιημένα στοιχεία επικοινωνίας, συμπεριλαμβανομένων των ηλεκτρονικών διευθύνσεων, των πεδίων IP και των αριθμών τηλεφώνου·

γ) κατά περίπτωση, τον σχετικό τομέα και υποτομέα που αναφέρεται στο παράρτημα Ι ή ΙΙ· και

δ) κατά περίπτωση, κατάλογο των κρατών μελών στα οποία παρέχουν υπηρεσίες που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας.

Οι οντότητες που αναφέρονται στην παράγραφο 3 κοινοποιούν τυχόν αλλαγές στα στοιχεία που υποβάλλονται σύμφωνα με το πρώτο εδάφιο της παρούσας παραγράφου αμελλητί και, σε κάθε περίπτωση, εντός δύο εβδομάδων από την ημερομηνία της αλλαγής.

Η Επιτροπή, με τη συνδρομή του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), θεσπίζει αμελλητί κατευθυντήριες γραμμές και υποδείγματα σχετικά με τις υποχρεώσεις που καθορίζονται στην παρούσα παράγραφο.

Τα κράτη μέλη μπορούν να θεσπίζουν εθνικούς μηχανισμούς για να εγγράφονται οι ίδιες οι οντότητες.

5. Έως τις 17 Απριλίου 2025 και στη συνέχεια ανά διετία, οι αρμόδιες αρχές κοινοποιούν:

α) στην Επιτροπή και στην Ομάδα Συνεργασίας τον αριθμό των βασικών και σημαντικών οντοτήτων που απαριθμούνται σύμφωνα με την παράγραφο 3 για κάθε τομέα και υποτομέα που αναφέρεται στο παράρτημα I ή II· και

β) στην Επιτροπή σχετικές πληροφορίες σχετικά με τον αριθμό των βασικών και σημαντικών οντοτήτων που προσδιορίζονται βάσει του άρθρου 2 παράγραφος 2 στοιχεία β) έως ε), τον τομέα και υποτομέα που αναφέρονται στο παράρτημα I ή II στον οποίο ανήκουν, το είδος της υπηρεσίας που παρέχουν και την διάταξη βάσει των οποίων προσδιορίστηκαν, μεταξύ εκείνων που ορίζονται στο άρθρο 2 παράγραφος 2 στοιχεία β) έως ε).

6. Έως τις 17 Απριλίου 2025 και κατόπιν αιτήματος της Επιτροπής, τα κράτη μέλη μπορούν να κοινοποιούν στην Επιτροπή τα ονόματα των βασικών και σημαντικών οντοτήτων που αναφέρονται στην παράγραφο 5 στοιχείο β).

Άρθρο 4

Τομεακές νομικές πράξεις της Ένωσης

1. Όταν οι τομεακές νομικές πράξεις της Ένωσης απαιτούν από βασικές ή σημαντικές οντότητες να εγκρίνουν μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας ή να κοινοποιούν σημαντικά περιστατικά και όταν οι εν λόγω απαιτήσεις είναι τουλάχιστον ισοδύναμες ως προς το αποτέλεσμα με τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία, οι σχετικές διατάξεις της παρούσας οδηγίας, συμπεριλαμβανομένων των διατάξεων για την εποπτεία και την επιβολή που προβλέπονται στο κεφάλαιο VII, δεν εφαρμόζονται στις εν λόγω οντότητες. Όταν οι τομεακές νομικές πράξεις της Ένωσης δεν καλύπτουν όλες τις οντότητες σε συγκεκριμένο τομέα που εμπίπτει στο πεδίο εφαρμογής της παρούσας οδηγίας, οι σχετικές διατάξεις της παρούσας οδηγίας εξακολουθούν να εφαρμόζονται στις οντότητες που δεν καλύπτονται από τις εν λόγω τομεακές νομικές πράξεις της Ένωσης.

2. Οι απαιτήσεις που αναφέρονται στην παράγραφο 1 του παρόντος άρθρου θεωρούνται ισοδύναμες ως προς το αποτέλεσμα με τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία όταν:

α) τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας είναι τουλάχιστον ισοδύναμα ως προς το αποτέλεσμα με εκείνα που προβλέπονται στο άρθρο 21 παράγραφοι 1 και 2· ή

β) η τομεακή νομική πράξη της Ένωσης προβλέπει άμεση πρόσβαση, κατά περίπτωση αυτόματη και απευθείας, στις κοινοποιήσεις περιστατικών από τις CSIRT, τις αρμόδιες αρχές ή τα ενιαία σημεία επαφής δυνάμει της παρούσας οδηγίας και εάν οι απαιτήσεις για την κοινοποίηση σημαντικών περιστατικών είναι τουλάχιστον ισοδύναμες ως προς το αποτέλεσμα με εκείνες που ορίζονται στο άρθρο 23 παράγραφοι 1 έως 6 της παρούσας οδηγίας.

3. Έως τις 17 Ιουλίου 2023, η Επιτροπή θεσπίζει κατευθυντήριες γραμμές για την αποσαφήνιση της εφαρμογής των παραγράφων 1 και 2. Η Επιτροπή επανεξετάζει τις εν λόγω κατευθυντήριες γραμμές σε τακτική βάση. Κατά την κατάρτιση των εν λόγω κατευθυντήριων γραμμών, η Επιτροπή λαμβάνει υπόψη τυχόν παρατηρήσεις της Ομάδας Συνεργασίας και του ENISA.

Άρθρο 5

Ελάχιστη εναρμόνιση

Η παρούσα οδηγία δεν εμποδίζει τα κράτη μέλη να θεσπίζουν ή να διατηρούν διατάξεις που διασφαλίζουν υψηλότερο επίπεδο κυβερνοασφάλειας, υπό την προϋπόθεση ότι οι εν λόγω διατάξεις συνάδουν με τις υποχρεώσεις των κρατών μελών δυνάμει του ενωσιακού δικαίου.

Άρθρο 6

Ορισμοί

Για τους σκοπούς της παρούσας οδηγίας, ισχύουν οι ακόλουθοι ορισμοί:

1) «δικτυακό και πληροφοριακό σύστημα»:

α) δίκτυο ηλεκτρονικών επικοινωνιών όπως ορίζεται στο άρθρο 2 σημείο 1) της οδηγίας (ΕΕ) 2018/1972·

β) κάθε συσκευή ή ομάδα διασυνδεδεμένων ή συναφών συσκευών, μία ή περισσότερες από τις οποίες, σύμφωνα με ένα πρόγραμμα, διενεργούν αυτόματη επεξεργασία ψηφιακών δεδομένων· ή

γ) ψηφιακά δεδομένα που αποθηκεύονται, υποβάλλονται σε επεξεργασία, ανακτώνται ή μεταδίδονται από στοιχεία που καλύπτονται στα στοιχεία α) και β) για τους σκοπούς της λειτουργίας, χρήσης, προστασίας και συντήρησής τους·

2) «ασφάλεια συστημάτων δικτύου και πληροφοριών»: η ικανότητα των συστημάτων δικτύου και πληροφοριών να ανθίστανται, σε δεδομένο επίπεδο εμπιστοσύνης, σε κάθε συμβάν που ενδέχεται να θέσει σε κίνδυνο τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή την εμπιστευτικότητα των αποθηκευμένων, διαβιβαζόμενων ή επεξεργασμένων δεδομένων ή των υπηρεσιών που προσφέρονται από τα εν λόγω συστήματα δικτύου και πληροφοριών ή είναι προσβάσιμες μέσω αυτών·

3) «κυβερνοασφάλεια»: η κυβερνοασφάλεια όπως ορίζεται στο άρθρο 2 σημείο 1) του κανονισμού (ΕΕ) 2019/881·

4) «εθνική στρατηγική κυβερνοασφάλειας»: συνεκτικό πλαίσιο ενός κράτους μέλους το οποίο παρέχει στρατηγικούς στόχους και προτεραιότητες στον τομέα της κυβερνοασφάλειας και της διακυβέρνησης για την επίτευξή τους στο εν λόγω κράτος μέλος·

5) «παρ' ολίγον περιστατικό»: περιστατικό το οποίο θα μπορούσε να έχει θέσει σε κίνδυνο τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή την εμπιστευτικότητα των αποθηκευμένων, διαβιβαζόμενων ή υφιστάμενων επεξεργασία δεδομένων ή των υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω συστημάτων δικτύου και πληροφοριών, αλλά το οποίο εμποδίστηκε ή δεν υλοποιήθηκε επιτυχώς·

6) «περιστατικό»: κάθε συμβάν που θέτει σε κίνδυνο τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή το απόρρητο των δεδομένων που αποθηκεύονται, μεταδίδονται ή υποβάλλονται σε επεξεργασία ή των υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω συστημάτων δικτύου και πληροφοριών·

7) «περιστατικό μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας»: περιστατικό το οποίο προκαλεί διατάραξη που υπερβαίνει την ικανότητα ενός κράτους μέλους να ανταποκριθεί σε αυτή ή το οποίο έχει σημαντικό αντίκτυπο σε τουλάχιστον δύο κράτη μέλη·

8) «χειρισμός περιστατικών»: κάθε ενέργεια και διαδικασία που αποσκοπεί στην πρόληψη, τη διαπίστωση, την ανάλυση και τον περιορισμό ή την αντίδραση σε περιστατικό και την ανάκαμψη από αυτό·

9) «κίνδυνος»: η πιθανότητα απώλειας ή διατάραξης που προκαλείται από περιστατικό και εκφράζεται ως συνδυασμός του μεγέθους της εν λόγω απώλειας ή διατάραξης και της πιθανότητας επέλευσης του εν λόγω περιστατικού·

10) «κυβερνοαπειλή»: κυβερνοαπειλή όπως ορίζεται στο άρθρο 2 σημείο 8) του κανονισμού (ΕΕ) 2019/881·

11) «σημαντική κυβερνοαπειλή»: κυβερνοαπειλή η οποία, βάσει των τεχνικών χαρακτηριστικών της, μπορεί να θεωρηθεί ότι έχει τη δυνατότητα να επηρεάσει σοβαρά τα συστήματα δικτύου και πληροφοριών μιας οντότητας ή των χρηστών υπηρεσιών της οντότητας προκαλώντας σημαντική υλική ή μη υλική ζημία·

12) «προϊόν ΤΠΕ»: προϊόν ΤΠΕ όπως ορίζεται στο άρθρο 2 σημείο 12) του κανονισμού (ΕΕ) 2019/881·

13) «υπηρεσία ΤΠΕ»: υπηρεσία ΤΠΕ όπως ορίζεται στο άρθρο 2 σημείο 13) του κανονισμού (ΕΕ) 2019/881·

14) «διαδικασία ΤΠΕ»: διαδικασία ΤΠΕ όπως ορίζεται στο άρθρο 2 σημείο 14) του κανονισμού (ΕΕ) 2019/881·

15) «ευπάθεια»: αδυναμία, ευαισθησία ή ελάττωμα προϊόντων ΤΠΕ ή υπηρεσιών ΤΠΕ που μπορεί να αποτελέσει αντικείμενο εκμετάλλευσης από κυβερνοαπειλή·

16) «πρότυπο»: πρότυπο όπως ορίζεται στο άρθρο 2 σημείο 1) του κανονισμού (ΕΕ) αριθ. 1025/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου [29]·

17) «τεχνική προδιαγραφή»: τεχνική προδιαγραφή όπως ορίζεται στο άρθρο 2 σημείο 4) του κανονισμού (ΕΕ) αριθ. 1025/2012·

[29] Κανονισμός (ΕΕ) αριθ. 1025/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Οκτωβρίου 2012, σχετικά με την ευρωπαϊκή τυποποίηση, την τροποποίηση των οδηγιών του Συμβουλίου 89/686/ΕΟΚ και 93/15/ΕΟΚ και των οδηγιών του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου 94/9/ΕΚ, 94/25/ΕΚ, 95/16/ΕΚ, 97/23/ΕΚ, 98/34/ΕΚ, 2004/22/ΕΚ, 2007/23/ΕΚ, 2009/23/ΕΚ και 2009/105/ΕΚ και την κατάργηση της απόφασης 87/95/ΕΟΚ του Συμβουλίου και της απόφασης αριθ. 1673/2006/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (ΕΕ L 316 της 14.11.2012, σ. 12).

18) «σημείο ανταλλαγής κίνησης διαδικτύου»: δικτυακή διευκόλυνση που επιτρέπει τη διασύνδεση περισσότερων από δύο ανεξάρτητων δικτύων (αυτόνομων συστημάτων), κυρίως με σκοπό τη διευκόλυνση της ανταλλαγής κίνησης στο διαδίκτυο, η οποία παρέχει διασύνδεση μόνο για αυτόνομα συστήματα και η οποία ούτε απαιτεί η κυκλοφορία στο διαδίκτυο που διέρχεται μεταξύ οποιουδήποτε ζεύγους συμμετεχόντων αυτόνομων συστημάτων να διέρχεται μέσω οποιουδήποτε τρίτου αυτόνομου συστήματος ούτε μεταβάλλει ή επηρεάζει με άλλο τρόπο την εν λόγω κίνηση·

19) «σύστημα ονομάτων χώρου» ή «DNS»: ιεραρχικό κατανεμημένο σύστημα ονοματοδοσίας που επιτρέπει τον προσδιορισμό των διαδικτυακών υπηρεσιών και πόρων, επιτρέποντας στις συσκευές των τελικών χρηστών να χρησιμοποιούν υπηρεσίες δρομολόγησης και συνδεσιμότητας στο διαδίκτυο για την πρόσβαση στις εν λόγω υπηρεσίες και πόρους·

20) «πάροχος υπηρεσιών DNS»: οντότητα που παρέχει:

α) δημόσια διαθέσιμες υπηρεσίες αναδρομικής επίλυσης ονομάτων τομέα για τελικούς χρήστες του διαδικτύου· ή

β) έγκυρες υπηρεσίες επίλυσης ονομάτων τομέα για χρήση από τρίτους, με εξαίρεση τους εξυπηρετητές ονομάτων ρίζας·

21) «μητρώο ονομάτων τομέα ανωτάτου επιπέδου» ή «μητρώο ονομάτων TLD»: οντότητα στην οποία έχει ανατεθεί συγκεκριμένος TLD και είναι υπεύθυνη για τη διαχείριση του TLD, συμπεριλαμβανομένης της καταχώρισης ονομάτων τομέα στο πλαίσιο του TLD και της τεχνικής λειτουργίας του TLD, συμπεριλαμβανομένης της λειτουργίας των εξυπηρετητών ονομάτων του, της συντήρησης των βάσεων δεδομένων του και της διανομής αρχείων ζώνης TLD σε διακομιστές ονομάτων, ανεξάρτητα από το αν οποιαδήποτε από τις εν λόγω πράξεις εκτελείται από την ίδια την οντότητα ή ανατίθεται εξωτερικά, αλλά εξαιρουμένων των περιπτώσεων στις οποίες τα ονόματα TLD χρησιμοποιούνται από μητρώο μόνο για δική της χρήση·

22) «οντότητα που παρέχει υπηρεσίες καταχώρισης ονομάτων τομέα»: καταχωρητής ή αντιπρόσωπος που ενεργεί για λογαριασμό καταχωρητών, όπως πάροχος υπηρεσιών καταχώρισης δεδομένων προσωπικού χαρακτήρα ή πληρεξούσιος ή μεταπωλητής·

23) «ψηφιακή υπηρεσία»: υπηρεσία όπως ορίζεται στο άρθρο 1 παράγραφος 1 στοιχείο β) της οδηγίας (ΕΕ) 2015/1535 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([30])·

24) «τεχνική προδιαγραφή»: τεχνική προδιαγραφή όπως ορίζεται στο άρθρο 3 σημείο 16) του κανονισμού (ΕΕ) αριθ. 910/2014·

25) «πάροχος υπηρεσιών εμπιστοσύνης»: πάροχος υπηρεσιών εμπιστοσύνης όπως ορίζεται στο άρθρο 3 σημείο 19) του κανονισμού (ΕΕ) αριθ. 910/2014·

26) «εγκεκριμένη υπηρεσία εμπιστοσύνης»: εγκεκριμένη υπηρεσία εμπιστοσύνης όπως ορίζεται στο άρθρο 3 σημείο 17) του κανονισμού (ΕΕ) αριθ. 910/2014·

27) «εγκεκριμένος πάροχος υπηρεσιών εμπιστοσύνης»: εγκεκριμένος πάροχος υπηρεσιών εμπιστοσύνης όπως ορίζεται στο άρθρο 3 σημείο 20) του κανονισμού (ΕΕ) αριθ. 910/2014·

28) «επιγραμμική αγορά»: επιγραμμική αγορά όπως ορίζεται στο άρθρο 2 στοιχείο ιδ) της οδηγίας 2005/29/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([31])·

29) «επιγραμμική μηχανή αναζήτησης»: επιγραμμική μηχανή αναζήτησης όπως ορίζεται στο άρθρο 2 σημείο 5) του κανονισμού (ΕΕ) 2019/1150 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([32])·

30) «υπηρεσία υπολογιστικού νέφους»: ψηφιακή υπηρεσία που καθιστά δυνατή τη διαχείριση κατά παραγγελία και την ευρεία εξ αποστάσεως πρόσβαση σε κλιμακούμενη και ελαστική δεξαμενή κοινών υπολογιστικών πόρων, μεταξύ άλλων όταν οι πόροι αυτοί κατανέμονται σε διάφορα σημεία·

([30]) Οδηγία (ΕΕ) 2015/1535 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Σεπτεμβρίου 2015, για την καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προδιαγραφών και των κανόνων σχετικά με τις υπηρεσίες της κοινωνίας των πληροφοριών (ΕΕ L 241 της 17.9.2015, σ. 1).

([31]) Οδηγία 2005/29/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαΐου 2005, για τις αθέμιτες εμπορικές πρακτικές των επιχειρήσεων προς τους καταναλωτές στην εσωτερική αγορά και για την τροποποίηση της οδηγίας 84/450/ΕΟΚ του Συμβουλίου, των οδηγιών 97/7/ΕΚ, 98/27/ΕΚ, 2002/65/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και του κανονισμού (ΕΚ) αριθ. 2006/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου («Οδηγία για τις αθέμιτες εμπορικές πρακτικές») (ΕΕ L 149 της 11.6.2005, σ. 22).

([32]) Κανονισμός (ΕΕ) 2019/1150 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Ιουνίου 2019, για την προώθηση της δίκαιης μεταχείρισης και της διαφάνειας για τους επιχειρηματικούς χρήστες επιγραμμικών υπηρεσιών διαμεσολάβησης (ΕΕ L 186 της 11.7.2019, σ. 57).

31) «υπηρεσία κέντρου δεδομένων»: υπηρεσία που περιλαμβάνει δομές, ή ομάδες δομών, οι οποίες προορίζονται για την κεντρική φιλοξενία, διασύνδεση και λειτουργία εξοπλισμού ΤΠ και δικτύων και παρέχουν υπηρεσίες αποθήκευσης, επεξεργασίας και μεταφοράς δεδομένων, καθώς και όλες τις εγκαταστάσεις και υποδομές διανομής ισχύος και περιβαλλοντικού ελέγχου·

32) «δίκτυο διανομής περιεχομένου»: δίκτυο γεωγραφικά κατανεμημένων εξυπηρετητών που αποσκοπεί στη διασφάλιση υψηλής διαθεσιμότητας και προσβασιμότητας ή ταχείας παράδοσης ψηφιακού περιεχομένου και ψηφιακών υπηρεσιών στους χρήστες του διαδικτύου για λογαριασμό παρόχων περιεχομένου και υπηρεσιών·

33) «πλατφόρμα υπηρεσιών κοινωνικής δικτύωσης»: πλατφόρμα που επιτρέπει στους τελικούς χρήστες να συνδέονται, να ανταλλάσσουν, να ανακαλύπτουν και να επικοινωνούν μεταξύ τους μέσω πολλαπλών συσκευών, ιδίως μέσω συνομιλιών, αναρτήσεων, βίντεο και συστάσεων·

34) «εκπρόσωπος»: φυσικό ή νομικό πρόσωπο εγκατεστημένο στην Ένωση που έχει οριστεί ρητά να ενεργεί εξ ονόματος παρόχου υπηρεσιών DNS, μητρώου ονομάτων TLD, οντότητας που παρέχει υπηρεσίες καταχώρισης ονομάτων τομέα, παρόχου υπηρεσιών υπολογιστικού νέφους, παρόχου υπηρεσιών κέντρου δεδομένων, παρόχου δικτύου διανομής περιεχομένου, παρόχου διαχειριζομένων υπηρεσιών, παρόχου διαχειριζομένων υπηρεσιών ασφάλειας, παρόχου επιγραμμικής αγοράς, επιγραμμικής μηχανής αναζήτησης ή πλατφόρμας υπηρεσιών κοινωνικής δικτύωσης που δεν είναι εγκατεστημένος στην Ένωση, στον οποίο μπορεί να απευθύνεται αρμόδια αρχή ή CSIRT αντί της ίδιας της οντότητας όσον αφορά τις υποχρεώσεις της εν λόγω οντότητας δυνάμει της παρούσας οδηγίας·

35) «οντότητα δημόσιας διοίκησης»: οντότητα που αναγνωρίζεται ως τέτοια σε κράτος μέλος σύμφωνα με το εθνικό δίκαιο, μη συμπεριλαμβανομένων των δικαστηρίων, των κοινοβουλίων ή των κεντρικών τραπεζών, η οποία πληροί τα ακόλουθα κριτήρια:

α) έχει συσταθεί με σκοπό την κάλυψη αναγκών γενικού συμφέροντος και δεν έχει βιομηχανικό ή εμπορικό χαρακτήρα·

β) έχει νομική προσωπικότητα ή δικαιούται εκ του νόμου να ενεργεί για λογαριασμό άλλης οντότητας με νομική προσωπικότητα·

γ) χρηματοδοτείται κατά το μεγαλύτερο μέρος από το κράτος, τις περιφερειακές αρχές ή άλλους οργανισμούς δημοσίου δικαίου, υπόκειται σε έλεγχο διαχείρισης από τις εν λόγω αρχές ή οργανισμούς ή έχει διοικητικό, διευθυντικό ή εποπτικό συμβούλιο, του οποίου περισσότερα από τα μισά μέλη διορίζονται από το κράτος, τις περιφερειακές αρχές ή άλλους οργανισμούς δημοσίου δικαίου·

δ) έχει την εξουσία να απευθύνει σε φυσικά ή νομικά πρόσωπα διοικητικές ή κανονιστικές αποφάσεις που επηρεάζουν τα δικαιώματά τους στη διασυνοριακή κυκλοφορία προσώπων, αγαθών, υπηρεσιών ή κεφαλαίων·

36) «δημόσιο δίκτυο ηλεκτρονικών επικοινωνιών»: δημόσιο δίκτυο ηλεκτρονικών επικοινωνιών, όπως ορίζεται στο άρθρο 2 σημείο 8) της οδηγίας (ΕΕ) 2018/1972·

37) «υπηρεσία ηλεκτρονικών επικοινωνιών»: υπηρεσία ηλεκτρονικών επικοινωνιών, όπως ορίζεται στο άρθρο 2 σημείο 4) της οδηγίας (ΕΕ) 2018/1972·

38) «οντότητα»: φυσικό ή νομικό πρόσωπο που έχει συσταθεί και αναγνωρίζεται ως τέτοιο βάσει του εθνικού δικαίου του τόπου εγκατάστασής του, το οποίο μπορεί, ενεργώντας για ίδιο λογαριασμό, να ασκεί δικαιώματα και να υπόκειται σε υποχρεώσεις·

39) «πάροχος διαχειριζόμενων υπηρεσιών»: οντότητα που παρέχει υπηρεσίες σχετικές με την εγκατάσταση, τη διαχείριση, τη λειτουργία ή τη συντήρηση προϊόντων, δικτύων, υποδομών, εφαρμογών ΤΠΕ ή οποιωνδήποτε άλλων συστημάτων δικτύου και πληροφοριών, μέσω συνδρομής ή ενεργού διαχείρισης που εκτελείται είτε στις εγκαταστάσεις των πελατών είτε εξ αποστάσεως·

40) «πάροχος διαχειριζόμενων υπηρεσιών ασφάλειας»: πάροχος διαχειριζόμενων υπηρεσιών που εκτελεί ή παρέχει υποστήριξη για δραστηριότητες που σχετίζονται με τη διαχείριση κινδύνων κυβερνοασφάλειας·

41) «ερευνητικός οργανισμός»: οντότητα που έχει ως πρωταρχικό στόχο τη διεξαγωγή εφαρμοσμένης έρευνας ή πειραματικής ανάπτυξης με σκοπό την εκμετάλλευση των αποτελεσμάτων της εν λόγω έρευνας για εμπορικούς σκοπούς, αλλά η οποία δεν περιλαμβάνει εκπαιδευτικά ιδρύματα.

ΚΕΦΑΛΑΙΟ II

ΣΥΝΤΟΝΙΣΜΕΝΑ ΚΑΝΟΝΙΣΤΙΚΑ ΠΛΑΙΣΙΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Άρθρο 7

Εθνική στρατηγική κυβερνοασφάλειας

1. Κάθε κράτος μέλος θεσπίζει εθνική στρατηγική κυβερνοασφάλειας που προβλέπει τους στρατηγικούς στόχους, τους πόρους που απαιτούνται για την επίτευξη των εν λόγω στόχων και κατάλληλα μέτρα πολιτικής και ρυθμιστικά μέτρα, με σκοπό την επίτευξη και τη διατήρηση υψηλού επιπέδου κυβερνοασφάλειας. Η εθνική στρατηγική κυβερνοασφάλειας περιλαμβάνει:

α) στόχους και προτεραιότητες της στρατηγικής κυβερνοασφάλειας του κράτους μέλους που καλύπτουν ιδίως τους τομείς που αναφέρονται στα παραρτήματα I και II·

β) πλαίσιο διακυβέρνησης για την επίτευξη των στόχων και των προτεραιοτήτων που αναφέρονται στο στοιχείο α) της παρούσας παραγράφου, συμπεριλαμβανομένων των πολιτικών που αναφέρονται στην παράγραφο 2·

γ) πλαίσιο διακυβέρνησης που αποσαφηνίζει τους ρόλους και τις αρμοδιότητες των σχετικών ενδιαφερόμενων μερών σε εθνικό επίπεδο, το οποίο υποστηρίζει τη συνεργασία και τον συντονισμό σε εθνικό επίπεδο μεταξύ των αρμόδιων αρχών, των ενιαίων κέντρων επαφής και των CSIRT, δυνάμει της παρούσας οδηγίας, καθώς και τον συντονισμό και τη συνεργασία μεταξύ των εν λόγω φορέων και των αρμόδιων αρχών βάσει τομεακών νομικών πράξεων της Ένωσης·

δ) μηχανισμό για τον προσδιορισμό των σχετικών πάγιων στοιχείων και εκτίμηση των κινδύνων στο εν λόγω κράτος μέλος·

ε) προσδιορισμό των μέτρων για τη διασφάλιση της ετοιμότητας, της απόκρισης και της αποκατάστασης από περιστατικά, συμπεριλαμβανομένης της συνεργασίας μεταξύ του δημόσιου και του ιδιωτικού τομέα·

στ) κατάλογο των διαφόρων αρχών και ενδιαφερόμενων μερών που συμμετέχουν στην εφαρμογή της εθνικής στρατηγικής κυβερνοασφάλειας·

ζ) πλαίσιο πολιτικής για ενισχυμένο συντονισμό μεταξύ των αρμόδιων αρχών δυνάμει της παρούσας οδηγίας και των αρμόδιων αρχών που προβλέπονται στην οδηγία (ΕΕ) 2022/2557, για τον σκοπό της ανταλλαγής πληροφοριών σχετικά με κινδύνους, κυβερνοαπειλές και περιστατικά, καθώς και σχετικά με κινδύνους, απειλές και περιστατικά εκτός κυβερνοχώρου, και την άσκηση εποπτικών καθηκόντων, κατά περίπτωση·

η) σχέδιο, συμπεριλαμβανομένων των αναγκαίων μέτρων, για την ενίσχυση του γενικού επιπέδου ευαισθητοποίησης των πολιτών στον τομέα της κυβερνοασφάλειας.

2. Στο πλαίσιο της εθνικής στρατηγικής κυβερνοασφάλειας, τα κράτη μέλη θεσπίζουν ιδίως πολιτικές:

α) αντιμετώπισης της κυβερνοασφάλειας στην αλυσίδα εφοδιασμού προϊόντων ΤΠΕ και υπηρεσιών ΤΠΕ που χρησιμοποιούνται από οντότητες για την παροχή των υπηρεσιών τους·

β) σχετικά με τη συμπερίληψη και τον προσδιορισμό των σχετικών με την κυβερνοασφάλεια απαιτήσεων για τα προϊόντα ΤΠΕ και τις υπηρεσίες ΤΠΕ στις δημόσιες συμβάσεις, συμπεριλαμβανομένων των σχετικών με την πιστοποίηση της κυβερνοασφάλειας, την κρυπτογράφηση και τη χρήση προϊόντων κυβερνοασφάλειας ανοικτού κώδικα·

γ) διαχείρισης ευπαθειών, συμπεριλαμβανομένης της προώθησης και της διευκόλυνσης της συντονισμένης γνωστοποίησης τρωτοτήτων δυνάμει του άρθρου 12 παράγραφος 1·

δ) σχετικές με τη διατήρηση της γενικής διαθεσιμότητας, της ακεραιότητας και της εμπιστευτικότητας του δημόσιου πυρήνα του ανοικτού διαδικτύου, συμπεριλαμβανομένης, κατά περίπτωση, της κυβερνοασφάλειας των υποβρύχιων καλωδίων επικοινωνιών·

ε) προώθησης της ανάπτυξης και της ενσωμάτωσης σχετικών προηγμένων τεχνολογιών με στόχο την εφαρμογή προηγμένων μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας·

στ) προώθησης και ανάπτυξης της εκπαίδευσης και της κατάρτισης στην κυβερνοασφάλεια, τις δεξιότητες κυβερνοασφάλειας, την ευαισθητοποίηση και τις πρωτοβουλίες έρευνας και ανάπτυξης, καθώς και καθοδήγηση σχετικά με ορθές πρακτικές και ελέγχους κυβερνοϋγιεινής, με στόχο τους πολίτες, τα ενδιαφερόμενα μέρη και τις οντότητες·

ζ) στήριξης ακαδημαϊκών και ερευνητικών ιδρυμάτων για την ανάπτυξη, την ενίσχυση και την προώθηση της ανάπτυξης εργαλείων κυβερνοασφάλειας και ασφαλών υποδομών δικτύου·

η) συμπερίληψης σχετικών διαδικασιών και κατάλληλων εργαλείων ανταλλαγής πληροφοριών για τη στήριξη της εθελοντικής ανταλλαγής πληροφοριών για την κυβερνοασφάλεια μεταξύ οντοτήτων σύμφωνα με το δίκαιο της Ένωσης·

θ) ενίσχυσης της κυβερνοανθεκτικότητας και της βάσης για την κυβερνοϋγιεινή των μικρών και μεσαίων επιχειρήσεων, ιδίως εκείνων που εξαιρούνται από το πεδίο εφαρμογής της παρούσας οδηγίας, με την παροχή εύκολα προσβάσιμης καθοδήγησης και συνδρομής για τις ειδικές ανάγκες τους·

ι) προώθησης της ενεργητικής κυβερνοπροστασίας.

3. Τα κράτη μέλη κοινοποιούν τις εθνικές στρατηγικές κυβερνοασφάλειας στην Επιτροπή εντός τριών μηνών από την έγκρισή τους. Τα κράτη μέλη μπορούν να εξαιρούν από τις εν λόγω κοινοποιήσεις τις πληροφορίες που αφορούν την εθνική τους ασφάλεια.

4. Τα κράτη μέλη αξιολογούν τις εθνικές στρατηγικές κυβερνοασφάλειας σε τακτική βάση και τουλάχιστον ανά πενταετία με βάση βασικούς δείκτες επιδόσεων και, όπου απαιτείται, τους επικαιροποιούν. Ο ENISA επικουρεί τα κράτη μέλη, κατόπιν αιτήματός τους, στην ανάπτυξη ή την επικαιροποίηση εθνικής στρατηγικής για την ασφάλεια στον κυβερνοχώρο και βασικών δεικτών επιδόσεων για την αξιολόγηση της εν λόγω στρατηγικής, με σκοπό την ευθυγράμμισή της με τις απαιτήσεις και τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία.

Άρθρο 8

Αρμόδιες αρχές και ενιαία σημεία επαφής

1. Κάθε κράτος μέλος ορίζει ή συστήνει μία ή περισσότερες αρμόδιες αρχές ως υπεύθυνες για την κυβερνοασφάλεια και για τα εποπτικά καθήκοντα που αναφέρονται στο κεφάλαιο VII (αρμόδιες αρχές).

2. Οι αρμόδιες αρχές που αναφέρονται στην παράγραφο 1 παρακολουθούν την εφαρμογή της παρούσας οδηγίας σε εθνικό επίπεδο.

3. Κάθε κράτος μέλος ορίζει ή συστήνει ένα ή περισσότερα σημεία επαφής. Όταν ένα κράτος μέλος ορίζει ή συστήνει μόνο μία αρμόδια αρχή σύμφωνα με την παράγραφο 1, η εν λόγω αρμόδια αρχή αποτελεί επίσης το ενιαίο σημείο επαφής για το εν λόγω κράτος μέλος.

4. Κάθε ενιαίο σημείο επαφής ασκεί καθήκοντα συνδέσμου για τη διασφάλιση της διασυνοριακής συνεργασίας των αρχών του κράτους μέλους του με τις αρμόδιες αρχές άλλων κρατών μελών και, κατά περίπτωση, με την Επιτροπή και τον ENISA, καθώς και για τη διασφάλιση διατομεακής συνεργασίας με άλλες αρμόδιες αρχές εντός του οικείου κράτους μέλους.

5. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές τους διαθέτουν τις απαιτούμενες εξουσίες και επαρκείς πόρους για να επιτελούν αποτελεσματικά και αποδοτικά τα καθήκοντα που τους ανατίθενται και να επιτυγχάνουν, με τον τρόπο αυτό, τους στόχους του παρόντος κανονισμού.

6. Κάθε κράτος μέλος κοινοποιεί αμελλητί στην Επιτροπή την ταυτότητα της αρμόδιας αρχής της παραγράφου 1 και του ενιαίου σημείου επαφής της παραγράφου 3, τα καθήκοντα των εν λόγω αρχών, καθώς και κάθε μεταγενέστερη τροποποίηση. Κάθε κράτος μέλος δημοσιοποιεί την ταυτότητα της αρμόδιας αρχής του. Η Επιτροπή δημοσιοποιεί κατάλογο των ενιαίων σημείων επαφής.

Άρθρο 9

Εθνικά πλαίσια διαχείρισης κυβερνοκρίσεων

1. Κάθε κράτος μέλος ορίζει ή συστήνει μία ή περισσότερες αρμόδιες αρχές ως υπεύθυνες για τη διαχείριση περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας (αρχές διαχείρισης κυβερνοκρίσεων). Τα κράτη μέλη διασφαλίζουν ότι οι οικείες αρμόδιες αρχές διαθέτουν επαρκείς πόρους για την αποτελεσματική και αποδοτική εκτέλεση των καθηκόντων που τους ανατίθενται. Τα κράτη μέλη διασφαλίζουν τη συνοχή με τα υφιστάμενα πλαίσια για τη γενική εθνική διαχείριση κρίσεων.

2. Όταν ένα κράτος μέλος ορίζει ή συστήνει περισσότερες από μία αρχές διαχείρισης κυβερνοκρίσεων σύμφωνα με την παράγραφο 1, αναφέρει σαφώς ποια από τις εν λόγω αρχές θα λειτουργεί ως συντονιστής στη διαχείριση περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας.

3. Κάθε κράτος μέλος προσδιορίζει τις ικανότητες, τα πάγια στοιχεία και τις διαδικασίες που μπορούν να χρησιμοποιηθούν στην περίπτωση κρίσης για τους σκοπούς της παρούσας οδηγίας.

4. Κάθε κράτος μέλος θεσπίζει εθνικό σχέδιο αντιμετώπισης περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας, στο οποίο καθορίζονται οι στόχοι και οι ρυθμίσεις για τη διαχείριση περιστατικών μεγάλης κλίμακας και κρίσεων στον τομέα της κυβερνοασφάλειας. Το εν λόγω σχέδιο καθορίζει ιδίως:

α) τους στόχους των εθνικών μέτρων και δραστηριοτήτων ετοιμότητας·

β) τα καθήκοντα και τις αρμοδιότητες των αρχών διαχείρισης κυβερνοκρίσεων·

γ) τις διαδικασίες διαχείρισης κυβερνοκρίσεων, συμπεριλαμβανομένης της ενσωμάτωσής τους στο γενικό εθνικό πλαίσιο διαχείρισης κρίσεων και στους διαύλους ανταλλαγής πληροφοριών·

δ) τα εθνικά μέτρα ετοιμότητας, συμπεριλαμβανομένων ασκήσεων και δραστηριοτήτων κατάρτισης·

ε) τα σχετικά ενδιαφερόμενα μέρη δημόσιου και ιδιωτικού τομέα και τις σχετικές υποδομές·

στ) τις εθνικές διαδικασίες και ρυθμίσεις μεταξύ των αρμόδιων εθνικών αρχών και φορέων για να διασφαλίζεται η αποτελεσματική συμμετοχή και η παροχή υποστήριξης εκ μέρους του κράτους μέλους στη συντονισμένη διαχείριση περιστατικών μεγάλης κλίμακας και κρίσεων στον τομέα της κυβερνοασφάλειας σε επίπεδο Ένωσης.

5. Εντός τριών μηνών από τον ορισμό ή τη σύσταση της αρχής διαχείρισης κυβερνοκρίσεων που αναφέρεται στην παράγραφο 1, κάθε κράτος μέλος κοινοποιεί στην Επιτροπή την ταυτότητα της αρμόδιας αρχής του και τυχόν μεταγενέστερες αλλαγές. Τα κράτη μέλη υποβάλλουν στην Επιτροπή και στο ευρωπαϊκό δίκτυο οργανισμών διασύνδεσης για κυβερνοκρίσεις (EU-CyCLONe) σχετικές πληροφορίες σχετικά με τις απαιτήσεις της παραγράφου 4 όσον αφορά τα εθνικά σχέδια αντιμετώπισης περιστατικών μεγάλης κλίμακας και κρίσεων στον τομέα της κυβερνοασφάλειας εντός τριών μηνών από την έγκριση των εν λόγω σχεδίων. Τα κράτη μέλη μπορούν να εξαιρούν συγκεκριμένες πληροφορίες όταν και στον βαθμό που η εξαίρεση αυτή είναι αναγκαία για την εθνική τους ασφάλεια.

Άρθρο 10

Ομάδες αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές (CSIRT)

1. Κάθε κράτος μέλος ορίζει ή συστήνει μία ή περισσότερες CSIRT. Οι CSIRT μπορούν να ορίζονται ή να συστήνονται στο πλαίσιο αρμόδιας αρχής. Οι CSIRT συμμορφώνονται με τις απαιτήσεις που ορίζονται στο άρθρο 11 παράγραφος 1, καλύπτουν τουλάχιστον τους τομείς, τους υποτομείς και τους τύπους οντοτήτων που αναφέρονται στα παραρτήματα I και II και είναι υπεύθυνες για τον χειρισμό περιστατικών σύμφωνα με σαφώς καθορισμένη διαδικασία.

2. Τα κράτη μέλη διασφαλίζουν ότι κάθε CSIRT διαθέτει επαρκείς πόρους για την αποτελεσματική εκτέλεση των καθηκόντων της, όπως ορίζονται στο άρθρο 11 παράγραφος 3.

3. Τα κράτη μέλη διασφαλίζουν ότι κάθε CSIRT διαθέτει κατάλληλη, ασφαλή και ανθεκτική υποδομή επικοινωνίας και πληροφοριών μέσω της οποίας ανταλλάσσει πληροφορίες με βασικές και σημαντικές οντότητες και άλλα σχετικά ενδιαφερόμενα μέρη. Για τον σκοπό αυτό, τα κράτη μέλη διασφαλίζουν ότι κάθε CSIRT συμβάλλει στην ανάπτυξη ασφαλών εργαλείων ανταλλαγής πληροφοριών.

4. Οι CSIRT συνεργάζονται και, κατά περίπτωση, ανταλλάσσουν σχετικές πληροφορίες σύμφωνα με το άρθρο 29 με τομεακές ή διατομεακές κοινότητες βασικών και σημαντικών οντοτήτων.

5. Οι CSIRT συμμετέχουν σε αξιολογήσεις από ομοτίμους που διοργανώνονται σύμφωνα με το άρθρο 19.

6. Τα κράτη μέλη διασφαλίζουν την αποτελεσματική, αποδοτική και ασφαλή συνεργασία των CSIRT τους στο δίκτυο CSIRT.

7. Οι CSIRT μπορούν να συνάπτουν σχέσεις συνεργασίας με τις εθνικές ομάδες αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές τρίτης χώρας. Στο πλαίσιο αυτών των σχέσεων συνεργασίας, τα κράτη μέλη διευκολύνουν την αποτελεσματική, αποδοτική και ασφαλή ανταλλαγή πληροφοριών με τις εν λόγω εθνικές ομάδες αντιμετώπισης περιστατικών ασφαλείας σε υπολογιστές τρίτης χώρας, χρησιμοποιώντας σχετικά πρωτόκολλα ανταλλαγής πληροφοριών, συμπεριλαμβανομένου του πρωτοκόλλου φωτεινού σηματοδότη. Οι CSIRT μπορούν να ανταλλάσσουν σχετικές πληροφορίες με εθνικές ομάδες αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές τρίτης χώρας, συμπεριλαμβανομένων δεδομένων προσωπικού χαρακτήρα σύμφωνα με τη νομοθεσία της Ένωσης για την προστασία των δεδομένων.

8. Οι CSIRT μπορούν να συνεργάζονται με εθνικές ομάδες αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές τρίτης χώρας ή με ισοδύναμους φορείς τρίτης χώρας, ιδίως με σκοπό την παροχή συνδρομής στον τομέα της κυβερνοασφάλειας.

9. Κάθε κράτος μέλος κοινοποιεί αμελλητί στην Επιτροπή την ταυτότητα της CSIRT που αναφέρεται στην παράγραφο 1 του παρόντος άρθρου και της CSIRT στην οποία έχουν ανατεθεί καθήκοντα συντονισμού σύμφωνα με το άρθρο 12 παράγραφος 1, τα αντίστοιχα καθήκοντά τους σε σχέση με βασικές και σημαντικές οντότητες, και τυχόν μεταγενέστερες αλλαγές τους.

10. Τα κράτη μέλη μπορούν να ζητούν τη συνδρομή του ENISA για την ανάπτυξη των CSIRT τους.

Άρθρο 11

Απαιτήσεις, τεχνικές ικανότητες και καθήκοντα των CSIRT

1. Οι CSIRT συμμορφώνονται με τις ακόλουθες απαιτήσεις:

α) οι CSIRT εξασφαλίζουν υψηλό επίπεδο διαθεσιμότητας των διαύλων επικοινωνίας τους αποφεύγοντας μοναδικά σημεία αστοχίας και διαθέτουν διάφορους τρόπους για εισερχόμενη και εξερχόμενη επικοινωνία με τρίτους ανά πάσα στιγμή. προσδιορίζουν σαφώς τους διαύλους επικοινωνίας και τους γνωστοποιούν στα μέλη της περιοχής ευθύνης τους και στους συνεργαζόμενους εταίρους·

β) οι εγκαταστάσεις των CSIRT και τα υποστηρικτικά πληροφοριακά συστήματα βρίσκονται σε ασφαλείς χώρους·

γ) οι CSIRT είναι εφοδιασμένες με κατάλληλο σύστημα διαχείρισης και δρομολόγησης αιτημάτων, ιδίως προκειμένου να διευκολύνεται η αποτελεσματική και αποδοτική παράδοση καθηκόντων·

δ) οι CSIRT διασφαλίζουν την εμπιστευτικότητα και την αξιοπιστία των δραστηριοτήτων τους·

ε) οι CSIRT είναι επαρκώς στελεχωμένες ώστε να διασφαλίζουν τη διαθεσιμότητα των υπηρεσιών τους ανά πάσα στιγμή και διασφαλίζουν ότι το προσωπικό τους είναι κατάλληλα καταρτισμένο·

στ) οι CSIRT είναι εξοπλισμένες με πλεονάζοντα συστήματα και εφεδρικό χώρο εργασίας για τη διασφάλιση της συνέχειας των υπηρεσιών τους.

Οι CSIRT μπορούν να συμμετέχουν σε διεθνή δίκτυα συνεργασίας.

2. Τα κράτη μέλη διασφαλίζουν ότι οι CSIRT τους διαθέτουν από κοινού τις τεχνικές ικανότητες που απαιτούνται για την εκτέλεση των καθηκόντων που αναφέρονται στην παράγραφο 3. Τα κράτη μέλη διασφαλίζουν ότι διατίθενται επαρκείς πόροι στις CSIRT τους ώστε να εξασφαλίζονται επαρκή επίπεδα στελέχωσης για να μπορούν οι CSIRT να αναπτύξουν τις τεχνικές τους ικανότητες.

3. Οι CSIRT είναι επιφορτισμένες με τα ακόλουθα καθήκοντα:

α) παρακολούθηση και ανάλυση κυβερνοαπειλών, ευπαθειών και περιστατικών σε εθνικό επίπεδο και, κατόπιν αιτήματος, παροχή συνδρομής σε επηρεαζόμενες βασικές και σημαντικές οντότητες σχετικά με την παρακολούθηση των συστημάτων δικτύου και πληροφοριών τους σε πραγματικό χρόνο ή σχεδόν σε πραγματικό χρόνο·

β) παροχή έγκαιρων προειδοποιήσεων, ειδοποιήσεων, ανακοινώσεων και διάδοσης πληροφοριών σε εμπλεκόμενες βασικές και σημαντικές οντότητες, καθώς και σε αρμόδιες αρχές και άλλα σχετικά ενδιαφερόμενα μέρη σχετικά με κυβερνοαπειλές, τρωτότητες και περιστατικά, ει δυνατόν σε σχεδόν πραγματικό χρόνο·

γ) αντιμετώπιση περιστατικών και παροχή συνδρομής στις επηρεαζόμενες βασικές και σημαντικές οντότητες, κατά περίπτωση·

δ) συλλογή και ανάλυση εγκληματολογικών δεδομένων και δυναμική ανάλυση κινδύνων και περιστατικών και επίγνωση της κατάστασης σε θέματα κυβερνοασφάλειας·

ε) παροχή, κατόπιν αιτήματος βασικής ή σημαντικής οντότητας, προληπτικής σάρωσης των συστημάτων δικτύου και πληροφοριών της οικείας οντότητας για τον εντοπισμό ευπαθειών με δυνητικό σημαντικό αντίκτυπο·

στ) συμμετοχή στο δίκτυο CSIRT και παροχή αμοιβαίας συνδρομής σύμφωνα με τις ικανότητες και τις αρμοδιότητές τους σε άλλα μέλη του δικτύου CSIRT κατόπιν αιτήματός τους·

ζ) κατά περίπτωση, ανάληψη συντονιστικού ρόλου για τους σκοπούς της συντονισμένης διαδικασίας γνωστοποίησης τρωτοτήτων δυνάμει του άρθρου 12 παράγραφος 1·

η) συμβολή στην ανάπτυξη ασφαλών εργαλείων ανταλλαγής πληροφοριών σύμφωνα με το άρθρο 10 παράγραφος 3.

Οι CSIRT μπορούν να διενεργούν προληπτική μη παρεμβατική σάρωση των δημοσίως προσβάσιμων συστημάτων δικτύου και πληροφοριών βασικών και σημαντικών οντοτήτων. Η εν λόγω σάρωση διενεργείται για τον εντοπισμό ευπαθών ή επισφαλώς διαμορφωμένων συστημάτων δικτύου και πληροφοριών και για την ενημέρωση των οικείων οντοτήτων. Η εν λόγω σάρωση δεν έχει αρνητικές συνέπειες για τη λειτουργία των υπηρεσιών των οντοτήτων.

Κατά την εκτέλεση των καθηκόντων που αναφέρονται στο πρώτο εδάφιο, οι CSIRT μπορούν να δίνουν προτεραιότητα σε συγκεκριμένα καθήκοντα στο πλαίσιο προσέγγισης βάσει κινδύνου.

4. Οι CSIRT συνάπτουν σχέσεις συνεργασίας με τα σχετικά ενδιαφερόμενα μέρη του ιδιωτικού τομέα, με σκοπό την επίτευξη των στόχων της παρούσας οδηγίας.

5. Προκειμένου να διευκολυνθεί η συνεργασία που αναφέρεται στην παράγραφο 4, οι CSIRT προωθούν την υιοθέτηση και τη χρήση κοινών ή τυποποιημένων πρακτικών, συστημάτων ταξινόμησης και ταξινομιών σε σχέση με:

α) διαδικασίες χειρισμού περιστατικών·

β) διαχείριση κρίσεων· και

γ) συντονισμένη γνωστοποίηση ευπαθειών δυνάμει του άρθρου 12 παράγραφος 1.

Άρθρο 12

Συντονισμένη γνωστοποίηση ευπαθειών και ευρωπαϊκή βάση δεδομένων ευπαθειών

1. Κάθε κράτος μέλος αναθέτει σε μία από τις CSIRT του συντονιστικό ρόλο για τους σκοπούς της συντονισμένης γνωστοποίησης ευπαθειών. Η CSIRT στην οποία ανατίθενται συντονιστικά καθήκοντα ενεργεί ως αξιόπιστος διαμεσολαβητής, διευκολύνοντας, όπου απαιτείται, την αλληλεπίδραση μεταξύ του φυσικού ή νομικού προσώπου που αναφέρει την ευπάθεια και του κατασκευαστή ή του παρόχου των δυνητικά ευπαθών προϊόντων ΤΠΕ ή υπηρεσιών ΤΠΕ, κατόπιν αιτήματος ενός εκ των μερών. Τα καθήκοντα της CSIRT στην οποία έχει ανατεθεί συντονιστικός ρόλος περιλαμβάνουν:

α) τον προσδιορισμό των οικείων οντοτήτων και την επικοινωνία με αυτές·

β) την παροχή συνδρομής στα φυσικά ή νομικά πρόσωπα που αναφέρουν ευπάθειες· και

γ) τη διαπραγμάτευση χρονοδιαγραμμάτων γνωστοποίησης και τη διαχείριση ευπαθειών που επηρεάζουν πλείονες οντότητες.

Τα κράτη μέλη διασφαλίζουν ότι τα φυσικά ή νομικά πρόσωπα μπορούν να αναφέρουν ανώνυμα, εφόσον το ζητήσουν, ευπάθειες στην CSIRT στην οποία έχει ανατεθεί ο συντονισμός. Η CSIRT στην οποία έχει ανατεθεί ο συντονισμός διασφαλίζει ότι εκτελούνται επιμελείς ενέργειες παρακολούθησης όσον αφορά την αναφερθείσα τρωτότητα και διασφαλίζει την ανωνυμία του φυσικού ή νομικού προσώπου που αναφέρει την τρωτότητα. Στις περιπτώσεις όπου μια αναφερόμενη ευπάθεια θα μπορούσε να έχει σημαντικό αντίκτυπο σε οντότητες σε περισσότερα του ενός κράτη μέλη, η CSIRT στην οποία έχει ανατεθεί ο συντονισμός σε κάθε ενδιαφερόμενο κράτος μέλος συνεργάζεται, κατά περίπτωση, με άλλες CSIRT στις οποίες έχει ανατεθεί συντονιστικός ρόλος στο πλαίσιο του δικτύου CSIRT.

2. Ο ENISA αναπτύσσει και διατηρεί, κατόπιν διαβούλευσης με την Ομάδα Συνεργασίας, ευρωπαϊκή βάση δεδομένων ευπαθειών. Για τον σκοπό αυτό, ο ENISA καταρτίζει και διατηρεί τα κατάλληλα συστήματα πληροφοριών, πολιτικές και διαδικασίες και θεσπίζει τα αναγκαία τεχνικά και οργανωτικά μέτρα για τη διαφύλαξη της ασφάλειας και της ακεραιότητας της ευρωπαϊκής βάσης δεδομένων ευπαθειών, με σκοπό ιδίως να δοθεί η δυνατότητα στις οντότητες, ανεξαρτήτως από το αν εμπίπτουν στο πεδίο της παρούσας οδηγίας, και στους προμηθευτές συστημάτων δικτύου και πληροφοριών τους να δημοσιοποιούν και να καταχωρίζουν, σε εθελοντική βάση, δημόσια γνωστές ευπάθειες σε προϊόντα ΤΠΕ ή υπηρεσίες ΤΠΕ. Παρέχεται σε όλα τα ενδιαφερόμενα μέρη πρόσβαση στις πληροφορίες σχετικά με τις ευπάθειες που περιέχονται στην ευρωπαϊκή βάση δεδομένων ευπαθειών. Η εν λόγω βάση δεδομένων περιλαμβάνει:

α) πληροφορίες που περιγράφουν την ευπάθεια·

β) τα επηρεαζόμενα προϊόντα ΤΠΕ ή υπηρεσίες ΤΠΕ και τη σοβαρότητα της ευπάθειας όσον αφορά τις περιστάσεις υπό τις οποίες μπορεί να αποτελέσει αντικείμενο εκμετάλλευσης·

γ) τη διαθεσιμότητα διορθωτικών προγραμμάτων και, ελλείψει διορθωτικών προγραμμάτων, υλικό καθοδήγησης που παρέχεται από τις αρμόδιες αρχές ή CSIRT και απευθύνεται στους χρήστες προϊόντων ΤΠΕ και υπηρεσιών ΤΠΕ που εμφανίζουν την ευπάθεια, σχετικά με τον τρόπο μετριασμού των κινδύνων που απορρέουν από τις γνωστοποιηθείσες ευπάθειες.

Άρθρο 13

Συνεργασία σε εθνικό επίπεδο

1. Εφόσον πρόκειται για διακριτές οντότητες, οι αρμόδιες αρχές, το ενιαίο σημείο επαφής και οι CSIRT του ίδιου κράτους μέλους συνεργάζονται μεταξύ τους για τους σκοπούς της τήρησης των υποχρεώσεων που προβλέπονται στην παρούσα οδηγία.

2. Τα κράτη μέλη διασφαλίζουν ότι οι CSIRT ή, κατά περίπτωση, οι αρμόδιες αρχές τους λαμβάνουν αναφορές σοβαρών περιστατικών σύμφωνα με το άρθρο 23, καθώς και περιστατικών, κυβερνοαπειλών και παρ' ολίγον περιστατικών σύμφωνα με το άρθρο 30.

3. Κάθε κράτος μέλος μεριμνά ώστε οι CSIRT του ή, κατά περίπτωση, οι αρμόδιες αρχές του να ενημερώνουν τα ενιαία σημεία επαφής τους για κοινοποιήσεις περιστατικών, κυβερνοαπειλών και παρ' ολίγον περιστατικών που υποβάλλονται σύμφωνα με την παρούσα οδηγία.

4. Προκειμένου να διασφαλιστεί η αποτελεσματική εκτέλεση των καθηκόντων και των υποχρεώσεων των αρμόδιων αρχών, των ενιαίων σημείων επαφής, και των CSIRT, τα κράτη μέλη διασφαλίζουν, στο μέτρο του δυνατού, την κατάλληλη συνεργασία μεταξύ των εν λόγω φορέων και των αρχών επιβολής του νόμου, των αρχών προστασίας δεδομένων, των εθνικών αρχών δυνάμει των κανονισμών (ΕΚ) αριθ. 300/2008 και (ΕΕ) 2018/1139, των εποπτικών φορέων δυνάμει του κανονισμού (ΕΕ) αριθ. 910/2014, των αρμόδιων αρχών δυνάμει του κανονισμού (ΕΕ) 2022/2554, των εθνικών ρυθμιστικών αρχών δυνάμει της οδηγίας (ΕΕ) 2018/1972, των αρμόδιων αρχών δυνάμει της οδηγίας (ΕΕ) 2022/2557, καθώς και των αρμόδιων αρχών βάσει άλλων τομεακών νομικών πράξεων της Ένωσης, εντός του εν λόγω κράτους μέλους.

5. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές τους δυνάμει της παρούσας οδηγίας και οι αρμόδιες αρχές τους δυνάμει της οδηγίας (ΕΕ) 2022/2557 συνεργάζονται και ανταλλάσσουν πληροφορίες σε τακτική βάση όσον αφορά τον προσδιορισμό των κρίσιμων οντοτήτων, τους κινδύνους, τις κυβερνοαπειλές και τα περιστατικά, καθώς και τους κινδύνους, τις απειλές και τα περιστατικά εκτός του κυβερνοχώρου, που επηρεάζουν βασικές οντότητες που προσδιορίζονται ως κρίσιμες οντότητες βάσει της οδηγίας (ΕΕ) 2022/2557, και τα μέτρα που λαμβάνονται για την αντιμετώπιση των εν λόγω κινδύνων, απειλών και περιστατικών. Τα κράτη μέλη διασφαλίζουν επίσης ότι οι αρμόδιες αρχές τους δυνάμει της παρούσας οδηγίας και οι αρμόδιες αρχές τους δυνάμει του κανονισμού (ΕΕ) αριθ. 910/2014, του κανονισμού (ΕΕ) 2022/2554 και της οδηγίας (ΕΕ) 2018/1972 ανταλλάσσουν σχετικές πληροφορίες σε τακτική βάση, μεταξύ άλλων όσον αφορά συναφή περιστατικά και κυβερνοαπειλές.

6. Τα κράτη μέλη απλουστεύουν την υποβολή αναφορών με τεχνικά μέσα για τις κοινοποιήσεις που αναφέρονται στα άρθρα 23 και 30.

ΚΕΦΑΛΑΙΟ III

ΣΥΝΕΡΓΑΣΙΑ ΣΕ ΕΝΩΣΙΑΚΟ ΚΑΙ ΔΙΕΘΝΕΣ ΕΠΙΠΕΔΟ

Άρθρο 14

Ομάδα Συνεργασίας

1. Για την υποστήριξη και τη διευκόλυνση της στρατηγικής συνεργασίας και την ανταλλαγή πληροφοριών μεταξύ των κρατών μελών, καθώς και την ενίσχυση της πίστης και της εμπιστοσύνης, συστήνεται Ομάδα Συνεργασίας.

2. Η Ομάδα Συνεργασίας εκτελεί τα καθήκοντά της βάσει διετών προγραμμάτων εργασιών τα οποία αναφέρονται στην παράγραφο 7.

3. Η Ομάδα Συνεργασίας απαρτίζεται από εκπροσώπους των κρατών μελών, της Επιτροπής και του ENISA. Η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης συμμετέχει στις δραστηριότητες της ομάδας συνεργασίας ως παρατηρητής. Οι Ευρωπαϊκές Εποπτικές Αρχές (ΕΕΑ) και οι αρμόδιες αρχές δυνάμει του κανονισμού (ΕΕ) 2022/2554 μπορούν να συμμετέχουν στις δραστηριότητες της ομάδας συνεργασίας σύμφωνα με το άρθρο 47 παράγραφος 1 του εν λόγω κανονισμού.

Όποτε είναι σκόπιμο, η Ομάδα Συνεργασίας μπορεί να καλεί εκπροσώπους του Ευρωπαϊκού Κοινοβουλίου και σχετικών ενδιαφερόμενων μερών για να συμμετάσχουν στις εργασίες της.

Η Επιτροπή παρέχει τη γραμματειακή υποστήριξη.

4. Τα καθήκοντα της Ομάδας Συνεργασίας είναι τα εξής:

α) παροχή καθοδήγησης στις αρμόδιες αρχές όσον αφορά τη μεταφορά στο εθνικό δίκαιο και την εφαρμογή της παρούσας οδηγίας·

β) παροχή καθοδήγησης στις αρμόδιες αρχές σε σχέση με την ανάπτυξη και την εφαρμογή πολιτικών για τη συντονισμένη γνωστοποίηση ευπαθειών, όπως αναφέρεται στο άρθρο 7 παράγραφος 2 στοιχείο γ)·

γ) ανταλλαγή βέλτιστων πρακτικών και πληροφοριών σχετικά με την εφαρμογή της παρούσας οδηγίας, μεταξύ άλλων όσον αφορά κυβερνοαπειλές, περιστατικά, ευπάθειες, παρ' ολίγον περιστατικά, πρωτοβουλίες ευαισθητοποίησης, προγράμματα κατάρτισης, ασκήσεις και δεξιότητες, ανάπτυξη ικανοτήτων, προτύπων και τεχνικών προδιαγραφών, καθώς και τον προσδιορισμό βασικών και σημαντικών οντοτήτων βάσει του άρθρου 2 παράγραφος 2 στοιχεία β) έως ε)·

δ) ανταλλαγή συμβουλών και συνεργασία με την Επιτροπή σχετικά με αναδυόμενες πρωτοβουλίες πολιτικής σε θέματα κυβερνοασφάλειας και τη συνολική συνεκτικότητα των ειδικών ανά τομέα απαιτήσεων κυβερνοασφάλειας·

ε) ανταλλαγή συμβουλών και συνεργασία με την Επιτροπή σχετικά με σχέδια εκτελεστικών πράξεων που εκδίδονται δυνάμει της παρούσας οδηγίας·

στ) ανταλλαγή βέλτιστων πρακτικών και πληροφοριών με τα αρμόδια θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης·

ζ) ανταλλαγή απόψεων σχετικά με την εφαρμογή τομεακών νομικών πράξεων της Ένωσης που περιέχουν διατάξεις για την κυβερνοασφάλεια·

η) κατά περίπτωση, εξέταση των εκθέσεων σχετικά με την αξιολόγηση από ομοτίμους που αναφέρεται στο άρθρο 19 παράγραφος 9 και σύνταξη συμπερασμάτων και συστάσεων·

θ) διεξαγωγή συντονισμένων εκτιμήσεων κινδύνου για την ασφάλεια κρίσιμων αλυσίδων εφοδιασμού σύμφωνα με το άρθρο 22 παράγραφος 1·

ι) εξέταση περιπτώσεων αμοιβαίας συνδρομής, συμπεριλαμβανομένων εμπειριών και αποτελεσμάτων από διασυνοριακές κοινές εποπτικές δράσεις όπως αναφέρεται στο άρθρο 37·

ια) κατόπιν αιτήματος ενός ή περισσότερων ενδιαφερόμενων κρατών μελών, εξέταση συγκεκριμένων αιτήσεων αμοιβαίας συνδρομής που αναφέρονται στο άρθρο 37·

ιβ) παροχή στρατηγικής καθοδήγησης στο δίκτυο CSIRT και στην EU-CyCLONe σχετικά με συγκεκριμένα αναδυόμενα ζητήματα·

ιγ) ανταλλαγή απόψεων σχετικά με την πολιτική για τις δράσεις παρακολούθησης μετά από περιστατικά μεγάλης κλίμακας και κρίσεις, στον τομέα της κυβερνοασφάλειας με βάση τα διδάγματα που αντλήθηκαν από το δίκτυο CSIRT και την EU-CyCLONe·

ιδ) συμβολή στις ικανότητες κυβερνοασφάλειας σε ολόκληρη την Ένωση, διευκολύνοντας την ανταλλαγή εθνικών υπαλλήλων μέσω προγράμματος ανάπτυξης ικανοτήτων με τη συμμετοχή προσωπικού από τις αρμόδιες αρχές ή τις CSIRT·

ιε) διοργάνωση τακτικών κοινών συνεδριάσεων με σχετικά ενδιαφερόμενα μέρη του ιδιωτικού τομέα από ολόκληρη την Ένωση για τη συζήτηση των δραστηριοτήτων που πραγματοποιεί η Ομάδα Συνεργασίας και τη συγκέντρωση στοιχείων σχετικά με αναδυόμενες προκλήσεις πολιτικής·

ιστ) εξέταση του έργου που έχει αναληφθεί σε σχέση με τις ασκήσεις κυβερνοασφάλειας, συμπεριλαμβανομένου του έργου που επιτελεί ο ENISA·

ιζ) καθορισμός της μεθοδολογίας και των οργανωτικών πτυχών των αξιολογήσεων από ομοτίμους που αναφέρονται στο άρθρο 19 παράγραφος 1, καθώς και της μεθοδολογίας αυτοαξιολόγησης για τα κράτη μέλη σύμφωνα με το άρθρο 19 παράγραφος 5, με τη βοήθεια της Επιτροπής και του ENISA, και, σε συνεργασία με την Επιτροπή και τον ENISA, κατάρτιση κωδίκων δεοντολογίας στους οποίους στηρίζονται οι μέθοδοι εργασίας των ορισθέντων εμπειρογνωμόνων κυβερνοασφάλειας σύμφωνα με το άρθρο 19 παράγραφος 6·

ιη) κατάρτιση εκθέσεων για τους σκοπούς της επανεξέτασης που αναφέρεται στο άρθρο 40 σχετικά με την πείρα που αποκτήθηκε σε στρατηγικό επίπεδο και από αξιολογήσεις από ομοτίμους·

ιθ) συζήτηση και τακτική αξιολόγηση της κατάστασης σε σχέση με κυβερνοαπειλές ή περιστατικά, όπως επιθέσεις λυτρισμικού.

Η Ομάδα Συνεργασίας υποβάλλει τις εκθέσεις που αναφέρονται στο πρώτο εδάφιο στοιχείο ιη) στην Επιτροπή, στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο.

5. Τα κράτη μέλη μεριμνούν για την αποτελεσματική, αποδοτική και ασφαλή συνεργασία των αντιπροσώπων τους στο πλαίσιο της ομάδας συνεργασίας.

6. Η Ομάδα Συνεργασίας μπορεί να ζητήσει από το δίκτυο CSIRT να εκπονήσει τεχνική έκθεση σχετικά με επιλεγμένα θέματα.

7. Έως την 1η Φεβρουαρίου 2024, και στη συνέχεια ανά διετία, η Ομάδα Συνεργασίας καταρτίζει πρόγραμμα εργασιών σχετικά με τις δράσεις που πρέπει να αναληφθούν για την υλοποίηση των στόχων και των καθηκόντων της.

8. Η Επιτροπή μπορεί να εκδίδει εκτελεστικές πράξεις που καθορίζουν τις διαδικαστικές ρυθμίσεις που είναι αναγκαίες για τη λειτουργία της Ομάδας Συνεργασίας.

Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης στην οποία παραπέμπει το άρθρο 39 παράγραφος 2.

Η Επιτροπή ανταλλάσσει συμβουλές και συνεργάζεται με την Ομάδα Συνεργασίας σχετικά με τα σχέδια εκτελεστικών πράξεων που αναφέρονται στο πρώτο εδάφιο της παρούσας παραγράφου σύμφωνα με την παράγραφο 4 στοιχείο ε).

9. Η Ομάδα Συνεργασίας συνεδριάζει σε τακτική βάση, και σε κάθε περίπτωση τουλάχιστον μία φορά ετησίως, με την ομάδα για την ανθεκτικότητα των κρίσιμων οντοτήτων που συστάθηκε βάσει της οδηγίας (ΕΕ) 2022/2557 για την προώθηση και τη διευκόλυνση της στρατηγικής συνεργασίας και της ανταλλαγής πληροφοριών.

Άρθρο 15

Δίκτυο CSIRT

1. Δημιουργείται δίκτυο εθνικών CSIRT με σκοπό τη συμβολή στην ανάπτυξη πίστης και εμπιστοσύνης και την προώθηση ταχείας και αποτελεσματικής επιχειρησιακής συνεργασίας μεταξύ των κρατών μελών.

2. Το δίκτυο CSIRT απαρτίζεται από εκπροσώπους των CSIRT που ορίζονται ή συγκροτούνται σύμφωνα με το άρθρο 10 και της Ομάδας Αντιμετώπισης Έκτακτων αναγκών στην πληροφορική για τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης (CERT-EU). Η Επιτροπή συμμετέχει στο δίκτυο CSIRT ως παρατηρητής. Ο ENISA παρέχει γραμματειακή υποστήριξη και παρέχει ενεργά συνδρομή για τη συνεργασία μεταξύ των CSIRT.

3. Τα καθήκοντα του δικτύου CSIRT είναι τα εξής:

α) ανταλλαγή πληροφοριών σχετικά με τις ικανότητες των CSIRT·

β) διευκόλυνση του διαμοιρασμού, μεταφοράς και ανταλλαγής τεχνολογίας και σχετικών μέτρων, πολιτικών, εργαλείων, διαδικασιών, βέλτιστων πρακτικών και πλαισίων μεταξύ των CSIRT·

γ) ανταλλαγή πληροφοριών σχετικά με περιστατικά, παρ' ολίγον περιστατικά, κυβερνοαπειλές, κινδύνους και ευπάθειες·

δ) ανταλλαγή πληροφοριών σχετικά με δημοσιεύσεις και συστάσεις για την κυβερνοασφάλεια·

ε) εξασφάλιση διαλειτουργικότητας όσον αφορά τις προδιαγραφές και τα πρωτόκολλα ανταλλαγής πληροφοριών·

στ) κατόπιν αιτήματος μέλους του δικτύου CSIRT, το οποίο επηρεάζεται δυνητικά από περιστατικό, ανταλλαγή και συζήτηση πληροφοριών σχετικά με το εν λόγω περιστατικό και τις συναφείς κυβερνοαπειλές, τους κινδύνους και τις ευπάθειες·

ζ) κατόπιν αιτήματος μέλους του δικτύου CSIRT, συζήτηση και, ει δυνατόν, εφαρμογή συντονισμένης αντίδρασης σε περιστατικό που έχει εντοπιστεί εντός της δικαιοδοσίας του εν λόγω κράτους μέλους·

η) παροχή συνδρομής στα κράτη μέλη για την αντιμετώπιση διασυνοριακών περιστατικών σύμφωνα με την παρούσα οδηγία·

θ) συνεργασία, ανταλλαγή βέλτιστων πρακτικών και παροχή βοήθειας στις CSIRT στις οποίες ανατίθεται συντονισμός σύμφωνα με το άρθρο 12 παράγραφος 1 όσον αφορά τη διαχείριση της συντονισμένης δημοσιοποίησης ευπαθειών που θα μπορούσαν να έχουν σημαντικό αντίκτυπο σε οντότητες σε περισσότερα από ένα κράτη μέλη·

ι) συζήτηση και προσδιορισμός περαιτέρω μορφών επιχειρησιακής συνεργασίας, μεταξύ άλλων σε σχέση με:

i) τις κατηγορίες κυβερνοαπειλών και περιστατικών·

ii) τις έγκαιρες προειδοποιήσεις·

iii) την αμοιβαία συνδρομή·

iv) τις αρχές και τις ρυθμίσεις συντονισμού για την αντιμετώπιση διασυνοριακών κινδύνων και περιστατικών·

v) τη συμβολή στο εθνικό σχέδιο αντιμετώπισης περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας που αναφέρεται στο άρθρο 9 παράγραφος 4 κατόπιν αιτήματος κράτους μέλους·

ια) ενημέρωση της Ομάδας Συνεργασίας σχετικά με τις δραστηριότητές του και τις περαιτέρω μορφές επιχειρησιακής συνεργασίας που συζητούνται σύμφωνα με το στοιχείο ι) και, όπου κρίνεται αναγκαίο, υποβολή σχετικού αιτήματος καθοδήγησης·

ιβ) απολογισμός των ασκήσεων κυβερνοασφάλειας, συμπεριλαμβανομένων εκείνων που διοργανώνει ο ENISA·

ιγ) κατόπιν αιτήματος επιμέρους CSIRT, συζήτηση των ικανοτήτων και της ετοιμότητας του εν λόγω CSIRT·

ιδ) συνεργασία και ανταλλαγή πληροφοριών με περιφερειακά και ενωσιακά κέντρα επιχειρήσεων ασφάλειας (SOCs) με σκοπό τη βελτίωση της κοινής επίγνωσης της κατάστασης σχετικά με περιστατικά και κυβερνοαπειλές σε ολόκληρη την Ένωση·

ιε) κατά περίπτωση, συζήτηση των εκθέσεων αξιολόγησης από ομοτίμους που αναφέρονται στο άρθρο 19 παράγραφος 9·

ιστ) θέσπιση κατευθυντήριων γραμμών προκειμένου να διευκολυνθεί η σύγκλιση των επιχειρησιακών πρακτικών όσον αφορά την εφαρμογή των διατάξεων του παρόντος άρθρου σχετικά με την επιχειρησιακή συνεργασία.

4. Έως τις 17 Ιανουαρίου 2025, και στη συνέχεια ανά διετία, το δίκτυο CSIRT αξιολογεί, για τους σκοπούς της επανεξέτασης που αναφέρεται στο άρθρο 40, την πρόοδο που έχει σημειωθεί όσον αφορά την επιχειρησιακή συνεργασία και εγκρίνει έκθεση. Ειδικότερα, η έκθεση διατυπώνει συμπεράσματα και συστάσεις με βάση τα αποτελέσματα των αξιολογήσεων από ομοτίμους που αναφέρονται στο άρθρο 19, οι οποίες διενεργούνται σε σχέση με τις εθνικές CSIRT. Η εν λόγω έκθεση υποβάλλεται στην Ομάδα Συνεργασίας.

5. Το δίκτυο CSIRT εγκρίνει τον εσωτερικό του κανονισμό.

6. Το δίκτυο CSIRT και η EU-CyCLONe συμφωνούν επί των διαδικαστικών ρυθμίσεων και συνεργάζονται βάσει αυτών.

Άρθρο 16

Ευρωπαϊκό δίκτυο οργανώσεων διασύνδεσης για κρίσεις στον κυβερνοχώρο (EU-CyCLONe)

1. Το EU-CyCLONe συστήνεται για να στηρίζει τη συντονισμένη διαχείριση περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας σε επιχειρησιακό επίπεδο και να διασφαλίζει την τακτική ανταλλαγή σχετικών πληροφοριών μεταξύ των κρατών μελών και των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης.

2. Το EU-CyCLONe απαρτίζεται από εκπροσώπους των αρχών διαχείρισης κρίσεων στον κυβερνοχώρο των κρατών μελών, καθώς και, σε περιπτώσεις όπου ένα δυνητικό ή εν εξελίξει περιστατικό μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας έχει ή ενδέχεται να έχει σημαντικό αντίκτυπο σε υπηρεσίες και δραστηριότητες που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας, από εκπροσώπους της Επιτροπής. Στις άλλες περιπτώσεις, η Επιτροπή συμμετέχει στις δραστηριότητες του EU-CyCLONe με καθεστώς παρατηρητή.

Ο ENISA παρέχει γραμματειακή υποστήριξη στο EU-CyCLONe και υποστηρίζει την ασφαλή ανταλλαγή πληροφοριών, παρέχει δε επίσης τα απαιτούμενα εργαλεία για τη στήριξη της συνεργασίας μεταξύ των κρατών μελών, διασφαλίζοντας την ασφαλή ανταλλαγή πληροφοριών.

Κατά περίπτωση, το EU-CyCLONe μπορεί να καλεί το Ευρωπαϊκό Κοινοβούλιο και εκπροσώπους των σχετικών ενδιαφερόμενων μερών να συμμετάσχουν στις εργασίες του.

3. Τα καθήκοντα του EU-CyCLONe είναι τα εξής:

α) αύξηση του επιπέδου ετοιμότητας για τη διαχείριση περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας·

β) ανάπτυξη κοινής επίγνωσης της κατάστασης για περιστατικά και κρίσεις μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας·

γ) αξιολόγηση των συνεπειών και του αντικτύπου των σχετικών περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας και υποβολή προτάσεων για πιθανά μέτρα μετριασμού·

δ) συντονισμός της διαχείρισης περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας και στήριξη της λήψης αποφάσεων σε πολιτικό επίπεδο σε σχέση με τέτοια περιστατικά και κρίσεις·

ε) συμβολή στο εθνικό σχέδιο αντιμετώπισης περιστατικών και κρίσεων μεγάλης κλίμακας που αναφέρεται στο άρθρο 9 παράγραφος 4, κατόπιν αιτήματος ενδιαφερόμενου κράτους μέλους.

4. Το δίκτυο EU-CyCLONe θεσπίζει τον εσωτερικό κανονισμό του.

5. Το EU-CyCLONe υποβάλλει τακτικά εκθέσεις στην Ομάδα Συνεργασίας σχετικά με τη διαχείριση των περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας, καθώς και τις τάσεις, εστιάζοντας ιδίως στον αντίκτυπό τους στις βασικές και τις σημαντικές οντότητες.

6. Το EU-CyCLONe συνεργάζεται με το δίκτυο CSIRT βάσει συμφωνημένων διαδικαστικών ρυθμίσεων που προβλέπονται στο άρθρο 15 παράγραφος 6.

7. Έως τις 17 Ιουλίου 2024, και στη συνέχεια κάθε 18 μήνες, το EU-CyCLONe υποβάλλει στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο έκθεση αξιολόγησης του έργου του.

Άρθρο 17

Διεθνής συνεργασία

Η Ένωση μπορεί, κατά περίπτωση, να συνάπτει διεθνείς συμφωνίες σύμφωνα με το άρθρο 218 ΣΛΕΕ με τρίτες χώρες ή διεθνείς οργανισμούς, που επιτρέπουν και οργανώνουν τη συμμετοχή τους σε ορισμένες δραστηριότητες της ομάδας συνεργασίας και του δικτύου CSIRT και του EU-CyCLONe. Οι εν λόγω συμφωνίες συμμορφώνονται με το δίκαιο της Ένωσης για την προστασία των δεδομένων.

Άρθρο 18

Έκθεση σχετικά με την κατάσταση της κυβερνοασφάλειας στην Ένωση

1. Ο ENISA εκδίδει, σε συνεργασία με την Επιτροπή και την Ομάδα Συνεργασίας, διετή έκθεση σχετικά με την κατάσταση της κυβερνοασφάλειας στην Ένωση, την οποία υποβάλλει και υποβάλλει στο Ευρωπαϊκό Κοινοβούλιο. Η έκθεση διατίθεται, μεταξύ άλλων, σε μηχαναγνώσιμα δεδομένα και περιλαμβάνει τα εξής:

α) αξιολόγηση κινδύνου κυβερνοασφάλειας σε επίπεδο Ένωσης, λαμβάνοντας υπόψη το τοπίο των κυβερνοαπειλών·

β) αξιολόγηση της ανάπτυξης ικανοτήτων κυβερνοασφάλειας στον δημόσιο και τον ιδιωτικό τομέα σε ολόκληρη την Ένωση·

γ) αξιολόγηση του γενικού επιπέδου ευαισθητοποίησης σε θέματα κυβερνοασφάλειας και κυβερνοϋγιεινής μεταξύ των πολιτών και των οντοτήτων, συμπεριλαμβανομένων των μικρών και μεσαίων επιχειρήσεων·

δ) συγκεντρωτική αξιολόγηση των αποτελεσμάτων των αξιολογήσεων από ομοτίμους που αναφέρονται στο άρθρο 19·

ε) συγκεντρωτική αξιολόγηση του επιπέδου ωριμότητας των ικανοτήτων και των πόρων κυβερνοασφάλειας σε ολόκληρη την Ένωση, συμπεριλαμβανομένων εκείνων σε τομεακό επίπεδο, καθώς και του βαθμού ευθυγράμμισης των εθνικών στρατηγικών κυβερνοασφάλειας των κρατών μελών.

2. Η έκθεση περιλαμβάνει συγκεκριμένες συστάσεις πολιτικής για την αντιμετώπιση αδυναμιών και την αύξηση του επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ένωση και σύνοψη των ευρημάτων για περιστατικά και κυβερνοαπειλές που αφορούν τη συγκεκριμένη περίοδο από τις τεχνικές εκθέσεις για την κατάσταση της κυβερνοασφάλειας στην ΕΕ που εκδίδει ο ENISA σύμφωνα με το άρθρο 7 παράγραφος 6 του κανονισμού (ΕΕ) 2019/881.

3. Ο ENISA, σε συνεργασία με την Επιτροπή, την Ομάδα Συνεργασίας και το δίκτυο CSIRT, αναπτύσσει τη μεθοδολογία, της συγκεντρωτικής αξιολόγησης που αναφέρεται στην παράγραφο 1 στοιχείο ε), συμπεριλαμβανομένων των σχετικών μεταβλητών, όπως ποσοτικούς και ποιοτικούς δείκτες.

Άρθρο 19

Αξιολογήσεις από ομότιμους

1. Η Ομάδα Συνεργασίας, με τη βοήθεια της Επιτροπής και του ENISA και, κατά περίπτωση, του δικτύου CSIRT καθορίζει, έως τις 17 Ιανουαρίου 2025, τη μεθοδολογία και τις οργανωτικές πτυχές των αξιολογήσεων από ομοτίμους με σκοπό την άντληση διδαγμάτων από κοινές εμπειρίες, την ενίσχυση της αμοιβαίας εμπιστοσύνης, την επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας, καθώς και την ενίσχυση των ικανοτήτων και των πολιτικών κυβερνοασφάλειας των κρατών μελών που είναι αναγκαίες για την εφαρμογή της παρούσας οδηγίας. Η συμμετοχή σε αξιολογήσεις από ομοτίμους είναι προαιρετική. Οι αξιολογήσεις από ομοτίμους διενεργούνται από εμπειρογνώμονες στον τομέα της κυβερνοασφάλειας. Οι εμπειρογνώμονες στον τομέα της κυβερνοασφάλειας ορίζονται από τουλάχιστον δύο κράτη μέλη, διαφορετικά από το κράτος μέλος που εξετάζεται.

Οι αξιολογήσεις από ομοτίμους καλύπτουν τουλάχιστον ένα από τα ακόλουθα:

α) το επίπεδο εφαρμογής των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και των υποχρεώσεων υποβολής εκθέσεων που προβλέπονται στα άρθρα 21 και 23·

β) το επίπεδο των ικανοτήτων, συμπεριλαμβανομένων των διαθέσιμων οικονομικών, τεχνικών και ανθρώπινων πόρων, και την αποτελεσματικότητα της άσκησης των καθηκόντων εκ μέρους των αρμόδιων αρχών·

γ) τις επιχειρησιακές ικανότητες των CSIRT·

δ) το επίπεδο υλοποίησης της αμοιβαίας συνδρομής που αναφέρεται στο άρθρο 37·

ε) το επίπεδο υλοποίησης των ρυθμίσεων ανταλλαγής πληροφοριών στον τομέα της κυβερνοασφάλειας που αναφέρεται στο άρθρο 29·

στ) ειδικά ζητήματα διασυνοριακού ή διατομεακού χαρακτήρα.

2. Η μεθοδολογία που αναφέρεται στην παράγραφο 1 περιλαμβάνει αντικειμενικά, αμερόληπτα, δίκαια και διαφανή κριτήρια βάσει των οποίων τα κράτη μέλη ορίζουν εμπειρογνώμονες στον τομέα της κυβερνοασφάλειας προς επιλογή για τη διενέργεια των αξιολογήσεων από ομοτίμους. Η Επιτροπή και ο ENISA συμμετέχουν ως παρατηρητές στις αξιολογήσεις από ομοτίμους.

3. Τα κράτη μέλη μπορούν να προσδιορίσουν συγκεκριμένα ζητήματα όπως αναφέρεται στην παράγραφο 1 στοιχείο στ) για τους σκοπούς της αξιολόγησης από ομοτίμους.

4. Πριν από την έναρξη της αξιολόγησης από ομοτίμους, όπως αναφέρεται στην παράγραφο 1, τα κράτη μέλη κοινοποιούν στα συμμετέχοντα κράτη μέλη το πεδίο εφαρμογής της, μεταξύ άλλων και τα συγκεκριμένα ζητήματα που προσδιορίζονται βάσει της παραγράφου 3.

5. Πριν από την έναρξη της αξιολόγησης από ομοτίμους, τα κράτη μέλη μπορούν να διενεργούν αυτοαξιολόγηση των αξιολογούμενων πτυχών και να παρέχουν την εν λόγω αυτοαξιολόγηση στους ορισθέντες εμπειρογνώμονες κυβερνοασφάλειας. Η Ομάδα Συνεργασίας, με τη συνδρομή της Επιτροπής και του ENISA, καθορίζει τη μεθοδολογία για την αυτοαξιολόγηση των κρατών μελών.

6. Οι αξιολογήσεις από ομοτίμους περιλαμβάνουν φυσικές ή εικονικές επιτόπιες επισκέψεις και ανταλλαγές πληροφοριών εκτός των εγκαταστάσεων. Με γνώμονα την αρχή της καλής συνεργασίας, τα κράτη μέλη που υποβάλλονται σε αξιολόγηση από ομοτίμους παρέχουν στους ορισθέντες εμπειρογνώμονες κυβερνοασφάλειας τις πληροφορίες που είναι αναγκαίες για την αξιολόγηση, με την επιφύλαξη του ενωσιακού ή του εθνικού δικαίου σχετικά με την προστασία εμπιστευτικών ή διαβαθμισμένων πληροφοριών και τη διασφάλιση ουσιωδών λειτουργιών του κράτους, όπως η εθνική ασφάλεια. Η Ομάδα Συνεργασίας, σε συνεργασία με την Επιτροπή και τον ENISA, καταρτίζει κατάλληλους κώδικες δεοντολογίας στους οποίους στηρίζονται οι μέθοδοι εργασίας των ορισθέντων εμπειρογνωμόνων κυβερνοασφάλειας. Κάθε πληροφορία που λαμβάνεται μέσω της αξιολόγησης από ομοτίμους χρησιμοποιείται αποκλειστικά για τον σκοπό αυτό. Οι εμπειρογνώμονες κυβερνοασφάλειας που συμμετέχουν στην αξιολόγηση από ομοτίμους δεν αποκαλύπτουν σε τρίτους τυχόν ευαίσθητες ή εμπιστευτικές πληροφορίες που απέκτησαν κατά τη διάρκεια της εν λόγω αξιολόγησης από ομοτίμους.

7. Αφού υποβληθούν σε αξιολόγηση από ομοτίμους, τα σημεία που εξετάζονται σε ένα κράτος μέλος δεν υποβάλλονται σε περαιτέρω αξιολόγηση από ομοτίμους εντός του εν λόγω κράτους μέλους για διάστημα δύο ετών μετά την ολοκλήρωση της αξιολόγησης από ομοτίμους, εκτός εάν αποφασιστεί διαφορετικά από το κράτος μέλος ή συμφωνηθεί μετά από πρόταση της ομάδας συνεργασίας.

8. Τα κράτη μέλη μεριμνούν για τη γνωστοποίηση οποιουδήποτε κινδύνου σύγκρουσης συμφερόντων που αφορά τους ορισθέντες εμπειρογνώμονες κυβερνοασφάλειας στα άλλα κράτη μέλη, στην Ομάδα Συνεργασίας, στην Επιτροπή και στον ENISA, πριν από την έναρξη της αξιολόγησης από ομοτίμους. Το κράτος μέλος που υπόκειται στην αξιολόγηση από ομοτίμους μπορεί να αντιταχθεί στον ορισμό συγκεκριμένων εμπειρογνωμόνων για δεόντως αιτιολογημένους λόγους που κοινοποιούνται στο ορίζον κράτος μέλος.

9. Οι εμπειρογνώμονες κυβερνοασφάλειας που συμμετέχουν σε αξιολογήσεις από ομοτίμους συντάσσουν εκθέσεις με τα ευρήματα και τα συμπεράσματα των αξιολογήσεων. Τα υπό αξιολόγηση από ομοτίμους κράτη μέλη μπορούν να υποβάλλουν παρατηρήσεις σχετικά με τα σχέδια εκθέσεων που τα αφορούν και τα σχόλια αυτά επισυνάπτονται στις εκθέσεις. Οι εκθέσεις περιλαμβάνουν συστάσεις που επιτρέπουν τη βελτίωση των πτυχών που καλύπτονται από την αξιολόγηση από ομοτίμους. Οι εκθέσεις υποβάλλονται στην Ομάδα Συνεργασίας και στο δίκτυο CSIRT, κατά περίπτωση. Τα υπό αξιολόγηση από ομοτίμους κράτη μέλη μπορούν να αποφασίσουν να δημοσιοποιήσουν την έκθεσή τους ή μια αναδιατυπωμένη έκδοσή της.

ΚΕΦΑΛΑΙΟ IV

ΜΕΤΡΑ ΔΙΑΧΕΙΡΙΣΗΣ ΚΙΝΔΥΝΩΝ ΣΤΟΝ ΤΟΜΕΑ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΑΙ ΥΠΟΧΡΕΩΣΕΙΣ ΑΝΑΦΟΡΑΣ ΠΕΡΙΣΤΑΤΙΚΩΝ

Άρθρο 20

Διακυβέρνηση

1. Τα κράτη μέλη διασφαλίζουν ότι η ανώτατη διοίκηση των βασικών και σημαντικών οντοτήτων εγκρίνει τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που λαμβάνουν οι εν λόγω οντότητες προκειμένου να συμμορφώνονται με το άρθρο 21, επιβλέπει την εφαρμογή τους και μπορεί να λογοδοτεί για την εκ μέρους των οντοτήτων παραβίαση των υποχρεώσεων του εν λόγω άρθρου.

Η εφαρμογή της παρούσας παραγράφου δεν θίγει το εθνικό δίκαιο όσον αφορά τους κανόνες περί ευθύνης που ισχύουν για τους δημόσιους οργανισμούς, καθώς και την ευθύνη δημοσίων υπαλλήλων και αιρετών ή διορισμένων αξιωματούχων.

2. Τα κράτη μέλη διασφαλίζουν ότι τα μέλη της ανώτατης διοίκησης των βασικών και σημαντικών οντοτήτων υποχρεούνται να παρακολουθούν εκπαίδευση και να ενθαρρύνουν τις βασικές και σημαντικές οντότητες να προσφέρουν παρόμοια κατάρτιση στους υπαλλήλους τους σε τακτική βάση, προκειμένου να αποκτούν επαρκείς γνώσεις και δεξιότητες που θα τους επιτρέπουν να εντοπίζουν τους κινδύνους και να αξιολογούν τις πρακτικές διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και τον αντίκτυπό τους στις υπηρεσίες που παρέχει η οντότητα.

Άρθρο 21

Μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας

1. Τα κράτη μέλη εξασφαλίζουν ότι οι βασικές και σημαντικές οντότητες λαμβάνουν κατάλληλα και αναλογικά τεχνικά, επιχειρησιακά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων όσον αφορά την ασφάλεια συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν οι εν λόγω οντότητες για τις δραστηριότητές τους ή για την παροχή των υπηρεσιών τους και για την πρόληψη ή ελαχιστοποίηση των επιπτώσεων των περιστατικών στους αποδέκτες των υπηρεσιών τους ή σε άλλες υπηρεσίες.

Λαμβάνοντας υπόψη τα πλέον σύγχρονα και, κατά περίπτωση, τα σχετικά ευρωπαϊκά και διεθνή πρότυπα, καθώς και το κόστος εφαρμογής, τα μέτρα που αναφέρονται στο πρώτο εδάφιο εξασφαλίζουν επίπεδο ασφάλειας των συστημάτων δικτύου και πληροφοριών ανάλογο προς τον εκάστοτε κίνδυνο. Κατά την αξιολόγηση της αναλογικότητας των εν λόγω μέτρων, λαμβάνονται δεόντως υπόψη ο βαθμός έκθεσης της οντότητας σε κινδύνους, το μέγεθος της οντότητας και η πιθανότητα εμφάνισης περιστατικών και η σοβαρότητά τους, συμπεριλαμβανομένων των κοινωνικών και οικονομικών επιπτώσεών τους.

2. Τα μέτρα που αναφέρονται στην παράγραφο 1 βασίζονται σε ολιστική προσέγγιση του κινδύνου που αποσκοπεί στην προστασία των συστημάτων δικτύου και πληροφοριών και του φυσικού περιβάλλοντος των εν λόγω συστημάτων από περιστατικά, περιλαμβάνουν δε τουλάχιστον τα ακόλουθα:

α) πολιτικές για την ανάλυση κινδύνου και την ασφάλεια των πληροφοριακών συστημάτων·

β) χειρισμό περιστατικών·

γ) επιχειρησιακή συνέχεια, όπως διαχείριση αντιγράφων ασφαλείας και αποκατάσταση έπειτα από καταστροφή, και διαχείριση των κρίσεων·

δ) ασφάλεια της αλυσίδας εφοδιασμού, συμπεριλαμβανομένων των σχετικών με την ασφάλεια πτυχών που αφορούν τις σχέσεις μεταξύ κάθε οντότητας και των άμεσων προμηθευτών ή παρόχων υπηρεσιών της·

ε) ασφάλεια στην απόκτηση, ανάπτυξη και συντήρηση συστημάτων δικτύου και πληροφοριών, συμπεριλαμβανομένου του χειρισμού και της γνωστοποίησης ευπαθειών·

στ) πολιτικές και διαδικασίες για την αξιολόγηση της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας·

ζ) βασικές πρακτικές κυβερνοϋγιεινής και κατάρτιση στην κυβερνοασφάλεια·

η) πολιτικές και διαδικασίες σχετικά με τη χρήση κρυπτογραφίας και, κατά περίπτωση, κρυπτογράφησης·

θ) ασφάλεια ανθρώπινων πόρων, πολιτικές ελέγχου πρόσβασης και διαχείριση πάγιων στοιχείων·

ι) χρήση λύσεων πολυπαραγοντικής επαλήθευσης ταυτότητας ή συνεχούς επαλήθευσης ταυτότητας, ασφαλών φωνητικών επικοινωνιών, επικοινωνιών βίντεο και κειμένου και ασφαλών συστημάτων επικοινωνιών έκτακτης ανάγκης εντός της οντότητας, κατά περίπτωση.

3. Τα κράτη μέλη διασφαλίζουν ότι, όταν εξετάζουν ποια από τα μέτρα που αναφέρονται στην παράγραφο 2 στοιχείο δ) του παρόντος άρθρου είναι κατάλληλα, οι οντότητες λαμβάνουν υπόψη τις ευπάθειες που χαρακτηρίζουν κάθε άμεσο προμηθευτή και πάροχο υπηρεσιών και τη συνολική ποιότητα των προϊόντων και των πρακτικών κυβερνοασφάλειας των προμηθευτών και των παρόχων υπηρεσιών τους, συμπεριλαμβανομένων των ασφαλών διαδικασιών ανάπτυξής τους. Τα κράτη μέλη διασφαλίζουν επίσης ότι, όταν εξετάζουν ποια από τα μέτρα που αναφέρονται στο εν λόγω στοιχείο είναι κατάλληλα, οι οντότητες υποχρεούνται να λαμβάνουν υπόψη τα αποτελέσματα των συντονισμένων εκτιμήσεων κινδύνου των κρίσιμων αλυσίδων εφοδιασμού που διενεργούνται σύμφωνα με το άρθρο 22 παράγραφος 1.

4. Τα κράτη μέλη διασφαλίζουν ότι μια οντότητα που διαπιστώνει ότι δεν συμμορφώνεται με τα μέτρα που προβλέπονται στην παράγραφο 2 λαμβάνει αμελλητί όλα τα αναγκαία, κατάλληλα και αναλογικά διορθωτικά μέτρα.

5. Έως τις 17 Οκτωβρίου 2024, η Επιτροπή εκδίδει εκτελεστικές πράξεις για τον καθορισμό των τεχνικών και μεθοδολογικών απαιτήσεων των μέτρων που αναφέρονται στην παράγραφο 2 όσον αφορά τους παρόχους υπηρεσιών DNS, τα μητρώα ονομάτων TLD, τους παρόχους υπηρεσιών υπολογιστικού νέφους, τους παρόχους υπηρεσιών κέντρου δεδομένων, τους παρόχους δικτύων παράδοσης περιεχομένου, τους παρόχους διαχειριζόμενων υπηρεσιών, τους παρόχους διαχειριζόμενων υπηρεσιών ασφάλειας, τους παρόχους επιγραμμικών αγορών, επιγραμμικών μηχανών αναζήτησης και πλατφορμών κοινωνικής δικτύωσης και τους παρόχους υπηρεσιών εμπιστοσύνης.

Η Επιτροπή μπορεί να εκδίδει εκτελεστικές πράξεις για τον καθορισμό των τεχνικών και μεθοδολογικών απαιτήσεων, καθώς και των τομεακών απαιτήσεων, κατά περίπτωση, των μέτρων που αναφέρονται στην παράγραφο 2 όσον αφορά βασικές και σημαντικές οντότητες διαφορετικές από εκείνες που αναφέρονται στο πρώτο εδάφιο της παρούσας παραγράφου.

Κατά την κατάρτιση των εκτελεστικών πράξεων που αναφέρονται στο πρώτο και δεύτερο εδάφιο της παρούσας παραγράφου, η Επιτροπή ακολουθεί, στο μέτρο του δυνατού, τα ευρωπαϊκά και διεθνή πρότυπα, καθώς και τις σχετικές τεχνικές προδιαγραφές. Η Επιτροπή ανταλλάσσει συμβουλές και συνεργάζεται με την Ομάδα Συνεργασίας και τον ENISA σχετικά με τα σχέδια εκτελεστικών πράξεων σύμφωνα με το άρθρο 14 παράγραφος 4 στοιχείο ε).

Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης στην οποία παραπέμπει το άρθρο 39 παράγραφος 2.

Άρθρο 22

Συντονισμένες σε ενωσιακό επίπεδο εκτιμήσεις κινδύνου για τις κρίσιμες αλυσίδες εφοδιασμού

1. Η Ομάδα Συνεργασίας, σε συνεργασία με την Επιτροπή και τον ENISA, μπορεί να διενεργεί συντονισμένες εκτιμήσεις κινδύνου για την ασφάλεια συγκεκριμένων κρίσιμων υπηρεσιών ΤΠΕ, συστημάτων ΤΠΕ ή αλυσίδων εφοδιασμού προϊόντων ΤΠΕ, λαμβάνοντας υπόψη τεχνικούς και, κατά περίπτωση, μη τεχνικούς παράγοντες κινδύνου.

2. Η Επιτροπή, κατόπιν διαβούλευσης με την Ομάδα Συνεργασίας και τον ENISA, και, κατά περίπτωση, τα σχετικά ενδιαφερόμενα μέρη, προσδιορίζει τις συγκεκριμένες κρίσιμες υπηρεσίες ΤΠΕ, τα συστήματα ΤΠΕ ή τα προϊόντα ΤΠΕ που ενδέχεται να υπόκεινται στη συντονισμένη εκτίμηση κινδύνου ασφάλειας που αναφέρεται στην παράγραφο 1.

Άρθρο 23

Υποχρεώσεις αναφοράς περιστατικών

1. Κάθε κράτος μέλος διασφαλίζει ότι οι βασικές και σημαντικές οντότητες κοινοποιούν αμελλητί στην CSIRT του ή, κατά περίπτωση, στην αρμόδια αρχή του σύμφωνα με την παράγραφο 4 κάθε περιστατικό που έχει σημαντικό αντίκτυπο στην παροχή των υπηρεσιών τους, όπως αναφέρεται στην παράγραφο 3 (σημαντικό περιστατικό). Κατά περίπτωση, οι οικείες οντότητες κοινοποιούν, χωρίς αδικαιολόγητη καθυστέρηση, στους αποδέκτες των υπηρεσιών τους σημαντικά περιστατικά που ενδέχεται να επηρεάσουν αρνητικά την παροχή των εν λόγω υπηρεσιών. Κάθε κράτος μέλος διασφαλίζει ότι οι εν λόγω οντότητες αναφέρουν, μεταξύ άλλων, κάθε πληροφορία που επιτρέπει στην CSIRT ή, κατά περίπτωση, στην αρμόδια αρχή να προσδιορίσει τυχόν διασυνοριακές επιπτώσεις του περιστατικού. Η απλή πράξη κοινοποίησης δεν συνεπάγεται αυξημένη ευθύνη της κοινοποιούσας οντότητας.

Όταν οι οικείες οντότητες κοινοποιούν στην αρμόδια αρχή σημαντικό περιστατικό σύμφωνα με το πρώτο εδάφιο, το κράτος μέλος διασφαλίζει ότι η εν λόγω αρμόδια αρχή διαβιβάζει την κοινοποίηση στην CSIRT με την παραλαβή της.

Σε περίπτωση διασυνοριακού ή διατομεακού σημαντικού περιστατικού, τα κράτη μέλη διασφαλίζουν ότι τα ενιαία σημεία επαφής τους λαμβάνουν εγκαίρως τις σχετικές πληροφορίες που κοινοποιούνται σύμφωνα με την παράγραφο 4.

2. Κατά περίπτωση, τα κράτη μέλη διασφαλίζουν ότι οι βασικές και σημαντικές οντότητες κοινοποιούν αμελλητί στους αποδέκτες των υπηρεσιών τους, που ενδέχεται να επηρεαστούν από σημαντική κυβερνοαπειλή, τυχόν μέτρα ή διορθωτικές ενέργειες που μπορούν να αυτοί να λάβουν για την αντιμετώπιση της συγκεκριμένης απειλής. Κατά περίπτωση, οι οντότητες ενημερώνουν επίσης τους εν λόγω αποδέκτες για τη σημαντική κυβερνοαπειλή.

3. Ένα περιστατικό θεωρείται σημαντικό εάν:

α) έχει προκαλέσει ή μπορεί να προκαλέσει σοβαρή λειτουργική διατάραξη των υπηρεσιών ή οικονομική ζημία για την οικεία οντότητα·

β) έχει επηρεάσει ή μπορεί να επηρεάσει άλλα φυσικά ή νομικά πρόσωπα προκαλώντας σημαντική υλική ή μη υλική ζημία.

4. Τα κράτη μέλη διασφαλίζουν ότι, για τους σκοπούς της κοινοποίησης δυνάμει της παραγράφου 1, οι οικείες οντότητες υποβάλλουν στην CSIRT ή, κατά περίπτωση, στην αρμόδια αρχή:

α) χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 24 ωρών από τη στιγμή που αντιλήφθηκε το σημαντικό περιστατικό, έγκαιρη προειδοποίηση, η οποία, κατά περίπτωση, αναφέρει αν υπάρχει υποψία ότι το σημαντικό περιστατικό προκλήθηκε από έκνομες ή κακόβουλες ενέργειες ή θα μπορούσε να έχει διασυνοριακό αντίκτυπο·

β) χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 72 ωρών από τη στιγμή που έγινε αντιληπτό το σημαντικό περιστατικό, κοινοποίηση περιστατικού, η οποία, κατά περίπτωση, επικαιροποιεί τις πληροφορίες που αναφέρονται στο στοιχείο α) και αναφέρει μια αρχική αξιολόγηση του σημαντικού περιστατικού, μεταξύ άλλων της σοβαρότητας και των επιπτώσεών του, καθώς και, εφόσον υπάρχουν, τις ενδείξεις της παραβίασης·

γ) κατόπιν αιτήματος μιας CSIRT ή, κατά περίπτωση, της αρμόδιας αρχής, ενδιάμεση έκθεση σχετικά με τις σχετικές επικαιροποιήσεις της κατάστασης·

δ) τελική έκθεση το αργότερο ένα μήνα μετά την υποβολή της κοινοποίησης περιστατικού σύμφωνα με το στοιχείο β), η οποία περιλαμβάνει τα ακόλουθα:

i) λεπτομερή περιγραφή του περιστατικού, μεταξύ άλλων της σοβαρότητάς του και των επιπτώσεών του·

ii) το είδος της απειλής ή τη βασική αιτία που ενδεχομένως προκάλεσε το περιστατικό·

iii) εφαρμοζόμενα και εν εξελίξει μέτρα μετριασμού·

iv) κατά περίπτωση, τον διασυνοριακό αντίκτυπο του περιστατικού·

ε) σε περίπτωση εν εξελίξει περιστατικού κατά τον χρόνο υποβολής της τελικής έκθεσης που αναφέρεται στο στοιχείο δ), τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι οι οικείες οντότητες υποβάλλουν έκθεση προόδου τη δεδομένη στιγμή και τελική έκθεση εντός ενός μηνός από τον εκ μέρους τους χειρισμό του σημαντικού περιστατικού.

Κατά παρέκκλιση από το πρώτο εδάφιο στοιχείο β), ο πάροχος υπηρεσιών εμπιστοσύνης ενημερώνει την CSIRT ή, κατά περίπτωση, την αρμόδια αρχή, όσον αφορά σημαντικά περιστατικά που επηρεάζουν την παροχή των υπηρεσιών εμπιστοσύνης του, χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 24 ωρών από τη στιγμή που έλαβε γνώση του σημαντικού περιστατικού.

5. Η CSIRT ή η αρμόδια αρχή παρέχει στην κοινοποιούσα οντότητα, αμελλητί και ει δυνατόν εντός 24 ωρών από τη λήψη της έγκαιρης προειδοποίησης που αναφέρεται στην παράγραφο 4 στοιχείο α), απάντηση που συμπεριλαμβάνει αρχική ανάδραση σχετικά με το σημαντικό περιστατικό και, κατόπιν αιτήματος της οντότητας, καθοδήγηση ή επιχειρησιακές συμβουλές σχετικά με την εφαρμογή πιθανών μέτρων μετριασμού. Σε περίπτωση που η CSIRT δεν είναι η αρχική αποδέκτρια της κοινοποίησης που αναφέρεται στην παράγραφο 1, η καθοδήγηση παρέχεται από την αρμόδια αρχή σε συνεργασία με την CSIRT. Η CSIRT παρέχει πρόσθετη τεχνική υποστήριξη εφόσον το ζητήσει η οικεία οντότητα. Όταν υπάρχουν υπόνοιες ότι το σημαντικό περιστατικό είναι ποινικού χαρακτήρα, η CSIRT ή η αρμόδια αρχή παρέχει επίσης καθοδήγηση σχετικά με την αναφορά του σημαντικού περιστατικού στις αρχές επιβολής του νόμου.

6. Κατά περίπτωση, και ιδίως όταν το σημαντικό περιστατικό αφορά δύο ή περισσότερα κράτη μέλη, η CSIRT, η αρμόδια αρχή ή το ενιαίο σημείο επαφής ενημερώνουν αμελλητί τα άλλα επηρεαζόμενα κράτη μέλη και τον ENISA σχετικά με το σημαντικό περιστατικό. Οι πληροφορίες αυτές περιλαμβάνουν το είδος των πληροφοριών που λαμβάνονται σύμφωνα με την παράγραφο 4. Στο πλαίσιο αυτό, η CSIRT, η αρμόδια αρχή ή το ενιαίο σημείο επαφής διαφυλάσσουν, σύμφωνα με το ενωσιακό ή το εθνικό δίκαιο, την ασφάλεια και τα εμπορικά συμφέροντα της οντότητας, καθώς και την εμπιστευτικότητα των παρεχόμενων πληροφοριών.

7. Όταν η ευαισθητοποίηση του κοινού είναι αναγκαία για την πρόληψη σημαντικού περιστατικού ή για την αντιμετώπιση συνεχιζόμενου σημαντικού περιστατικού, ή όταν η γνωστοποίηση του σημαντικού περιστατικού είναι άλλως προς το δημόσιο συμφέρον, η CSIRT ενός κράτους μέλους ή, κατά περίπτωση, η αρμόδια αρχή του και, κατά περίπτωση, οι CSIRT ή οι αρμόδιες αρχές άλλων ενδιαφερόμενων κρατών μελών, μπορούν, κατόπιν διαβούλευσης με την οικεία οντότητα, να ενημερώσουν το κοινό σχετικά με το σημαντικό περιστατικό ή να απαιτήσουν από την οντότητα να το πράξει.

8. Κατόπιν αιτήματος της CSIRT ή της αρμόδιας αρχής, το ενιαίο σημείο επαφής διαβιβάζει τις κοινοποιήσεις που λαμβάνονται σύμφωνα με την παράγραφο 1 στα ενιαία σημεία επαφής άλλων επηρεαζόμενων κρατών μελών.

9. Το ενιαίο σημείο επαφής υποβάλλει στον ENISA ανά τρίμηνο συνοπτική έκθεση, η οποία περιλαμβάνει ανωνυμοποιημένα και συγκεντρωτικά δεδομένα σχετικά με σημαντικά περιστατικά, περιστατικά, κυβερνοαπειλές και παρ' ολίγον περιστατικά που κοινοποιούνται σύμφωνα με την παράγραφο 1 του παρόντος άρθρου και με το άρθρο 30. Προκειμένου να συμβάλει στην παροχή συγκρίσιμων πληροφοριών, ο ENISA μπορεί να εκδίδει τεχνικές οδηγίες σχετικά με τις παραμέτρους των πληροφοριών που πρέπει να περιλαμβάνονται στη συνοπτική έκθεση. Ο ENISA ενημερώνει την Ομάδα Συνεργασίας και το δίκτυο CSIRT σχετικά με τα πορίσματά του σχετικά με τις κοινοποιήσεις που λαμβάνει κάθε έξι μήνες.

10. Οι CSIRT ή, κατά περίπτωση, οι αρμόδιες αρχές παρέχουν στις αρμόδιες αρχές δυνάμει της οδηγίας (ΕΕ) 2022/2557 πληροφορίες σχετικά με σημαντικά περιστατικά, περιστατικά, κυβερνοαπειλές και παρ' ολίγον περιστατικά που κοινοποιούνται σύμφωνα με την παράγραφο 1 του παρόντος άρθρου και το άρθρο 30 από οντότητες που προσδιορίζονται ως κρίσιμες οντότητες βάσει της οδηγίας (ΕΕ) 2022/2557.

11. Η Επιτροπή μπορεί να εκδίδει εκτελεστικές πράξεις για τον περαιτέρω προσδιορισμό του είδους των πληροφοριών, του μορφότυπου και της διαδικασίας κοινοποίησης που υποβάλλεται σύμφωνα με την παράγραφο 1 του παρόντος άρθρου και το άρθρο 30, καθώς και της κοινοποίησης που υποβάλλεται σύμφωνα με την παράγραφο 2 του παρόντος άρθρου.

Έως τις 17 Οκτωβρίου 2024, η Επιτροπή εκδίδει, όσον αφορά τους παρόχους υπηρεσιών DNS, τα μητρώα ονομάτων TLD, τους παρόχους υπηρεσιών υπολογιστικού νέφους, τους παρόχους υπηρεσιών κέντρων δεδομένων, τους παρόχους δικτύων διανομής περιεχομένου, τους παρόχους διαχειριζόμενων υπηρεσιών, τους παρόχους διαχειριζόμενων υπηρεσιών ασφάλειας, καθώς και τους παρόχους επιγραμμικών αγορών, επιγραμμικών μηχανών αναζήτησης και πλατφορμών υπηρεσιών κοινωνικής δικτύωσης, εκτελεστικές πράξεις για τον περαιτέρω προσδιορισμό των περιπτώσεων στις οποίες ένα περιστατικό θεωρείται σημαντικό, όπως αναφέρεται στην παράγραφο 3. Η Επιτροπή μπορεί να εκδίδει τέτοιες εκτελεστικές πράξεις όσον αφορά άλλες βασικές και σημαντικές οντότητες.

Η Επιτροπή ανταλλάσσει συμβουλές και συνεργάζεται με την Ομάδα Συνεργασίας και τον ENISA σχετικά με τα σχέδια εκτελεστικών πράξεων σύμφωνα με το άρθρο 14 παράγραφος 4 στοιχείο ε).

Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης στην οποία παραπέμπει το άρθρο 39 παράγραφος 2.

Άρθρο 24

Χρήση των ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας

1. Προκειμένου να αποδειχθεί η συμμόρφωση με τις ειδικές απαιτήσεις του άρθρου 21, τα κράτη μέλη μπορούν να απαιτούν από βασικές και σημαντικές οντότητες να χρησιμοποιούν συγκεκριμένα προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ, που αναπτύσσονται από τη βασική ή σημαντική οντότητα ή παρέχονται από τρίτους και πιστοποιούνται στο πλαίσιο ευρωπαϊκών συστημάτων πιστοποίησης κυβερνοασφάλειας που θεσπίζονται σύμφωνα με το άρθρο 49 του κανονισμού (ΕΕ) 2019/881. Επιπλέον, τα κράτη μέλη ενθαρρύνουν τις βασικές και σημαντικές οντότητες να χρησιμοποιούν αναγνωρισμένες υπηρεσίες εμπιστοσύνης.

2. Η Επιτροπή εξουσιοδοτείται να εκδίδει κατ' εξουσιοδότηση πράξεις, σύμφωνα με το άρθρο 38, για να συμπληρώνει την παρούσα οδηγία προσδιορίζοντας τις κατηγορίες βασικών και σημαντικών οντοτήτων από τις οποίες θα απαιτείται να χρησιμοποιούν ορισμένα πιστοποιημένα προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ ή να λαμβάνουν πιστοποιητικό δυνάμει ευρωπαϊκού συστήματος πιστοποίησης κυβερνοασφάλειας εγκεκριμένου σύμφωνα με το άρθρο 49 του κανονισμού (ΕΕ) 2019/881. Οι εν λόγω κατ' εξουσιοδότηση πράξεις εκδίδονται όταν έχουν εντοπιστεί ανεπαρκή επίπεδα κυβερνοασφάλειας, και περιλαμβάνουν περίοδο εφαρμογής.

Πριν από την έκδοση των εν λόγω κατ' εξουσιοδότηση πράξεων, η Επιτροπή διενεργεί εκτίμηση επιπτώσεων και διενεργεί διαβουλεύσεις σύμφωνα με το άρθρο 56 του κανονισμού (ΕΕ) 2019/881.

3. Όταν δεν είναι διαθέσιμο κατάλληλο ευρωπαϊκό σύστημα πιστοποίησης κυβερνοασφάλειας για τους σκοπούς της παραγράφου 2 του παρόντος άρθρου, η Επιτροπή μπορεί, κατόπιν διαβούλευσης με την Ομάδα Συνεργασίας και την Ευρωπαϊκή Ομάδα Πιστοποίησης Κυβερνοασφάλειας, να ζητήσει από τον ENISA να καταρτίσει υποψήφιο σύστημα σύμφωνα με το άρθρο 48 παράγραφος 2 του κανονισμού (ΕΕ) 2019/881.

Άρθρο 25

Τυποποίηση

1. Προκειμένου να προωθηθεί η συγκλίνουσα εφαρμογή του άρθρου 21 παράγραφοι 1 και 2, τα κράτη μέλη, χωρίς να επιβάλλουν ούτε να ευνοούν τη χρήση συγκεκριμένου είδους τεχνολογίας, ενθαρρύνουν τη χρήση ευρωπαϊκών και διεθνώς αποδεκτών προτύπων και τεχνικών προδιαγραφών σχετικών με την ασφάλεια συστημάτων δικτύου και πληροφοριών.

2. Ο ENISA, σε συνεργασία με τα κράτη μέλη και, κατά περίπτωση, κατόπιν διαβούλευσης με τα ενδιαφερόμενα μέρη, καταρτίζει συμβουλές και κατευθυντήριες γραμμές σχετικά με τους τεχνικούς τομείς που πρέπει να εξεταστούν σε σχέση με την παράγραφο 1, καθώς και σχετικά με τα ήδη υφιστάμενα πρότυπα, συμπεριλαμβανομένων των εθνικών προτύπων, που θα επιτρέψουν την κάλυψη των εν λόγω τομέων.

ΚΕΦΑΛΑΙΟ V

ΔΙΚΑΙΟΔΟΣΙΑ ΚΑΙ ΚΑΤΑΧΩΡΙΣΗ

Άρθρο 26

Δικαιοδοσία και εδαφικότητα

1. Οι οντότητες που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας θεωρούνται ότι εμπίπτουν στη δικαιοδοσία του κράτους μέλους στο οποίο είναι εγκατεστημένες, εκτός αν πρόκειται για:

α) παρόχους δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή παρόχους διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, οι οποίοι θεωρείται ότι εμπίπτουν στη δικαιοδοσία του κράτους μέλους στο οποίο παρέχουν τις υπηρεσίες τους·

β) παρόχους υπηρεσιών DNS, μητρώα ονομάτων TLD, οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα, παρόχους υπηρεσιών υπολογιστικού νέφους, παρόχους υπηρεσιών κέντρων δεδομένων, παρόχους δικτύων διανομής περιεχομένου, παρόχους διαχειριζομένων υπηρεσιών, παρόχους διαχειριζομένων υπηρεσιών ασφάλειας, καθώς και παρόχους επιγραμμικών αγορών, επιγραμμικών μηχανών αναζήτησης ή πλατφορμών υπηρεσιών κοινωνικής δικτύωσης, που θεωρείται ότι εμπίπτουν στη δικαιοδοσία του κράτους μέλους στο οποίο έχουν την κύρια εγκατάστασή τους στην Ένωση σύμφωνα με την παράγραφο 2·

γ) οντότητες δημόσιας διοίκησης, που θεωρείται ότι υπάγονται στη δικαιοδοσία του κράτους μέλους που τις έχει συστήσει.

2. Για τους σκοπούς της παρούσας οδηγίας, οντότητα που αναφέρεται στην παράγραφο 1 στοιχείο β) θεωρείται ότι έχει την κύρια εγκατάστασή της στην Ένωση στο κράτος μέλος στο οποίο λαμβάνονται κυρίως οι αποφάσεις που σχετίζονται με τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας. Εάν το εν λόγω κράτος μέλος δεν μπορεί να προσδιοριστεί ή εάν οι αποφάσεις αυτές δεν λαμβάνονται στην Ένωση, η κύρια εγκατάσταση θεωρείται ότι βρίσκεται στο κράτος μέλος στο οποίο διεξάγονται οι επιχειρήσεις κυβερνοασφάλειας. Εάν το εν λόγω κράτος μέλος δεν μπορεί να προσδιοριστεί, η κύρια εγκατάσταση θα πρέπει να θεωρείται ότι βρίσκεται στο κράτος μέλος στο οποίο η οικεία οντότητα έχει την εγκατάσταση με τον μεγαλύτερο αριθμό εργαζομένων στην Ένωση.

3. Εάν μια οντότητα που αναφέρεται στην παράγραφο 1 στοιχείο β) δεν είναι εγκατεστημένη στην Ένωση, αλλά προσφέρει υπηρεσίες εντός της Ένωσης, ορίζει εκπρόσωπο στην Ένωση. Ο εκπρόσωπος είναι εγκατεστημένος σε ένα από τα κράτη μέλη στα οποία προσφέρονται οι υπηρεσίες. Μια τέτοια οντότητα θεωρείται ότι υπόκειται στη δικαιοδοσία του κράτους μέλους στο οποίο είναι εγκατεστημένος ο εκπρόσωπος. Ελλείψει εκπροσώπου στην Ένωση που ορίζεται σύμφωνα με την παρούσα παράγραφο, κάθε κράτος μέλος στο οποίο η οντότητα παρέχει υπηρεσίες μπορεί να κινήσει νομικές διαδικασίες κατά της οντότητας για παραβίαση των υποχρεώσεων της παρούσας οδηγίας.

4. Ο ορισμός εκπροσώπου από οντότητα που αναφέρεται στην παράγραφο 1 στοιχείο β) δεν θίγει τις νομικές ενέργειες που θα μπορούσαν να κινηθούν κατά της ίδιας της οντότητας.

5. Τα κράτη μέλη που έχουν λάβει αίτημα αμοιβαίας συνδρομής σε σχέση με οντότητα που αναφέρεται στην παράγραφο 1, μπορούν, εντός των ορίων του εν λόγω αιτήματος, να λαμβάνουν κατάλληλα μέτρα εποπτείας και επιβολής σε σχέση με την οικεία οντότητα η οποία παρέχει υπηρεσίες ή διαθέτει το σύστημα δικτύου και πληροφοριών στην επικράτειά τους.

Άρθρο 27

Μητρώο οντοτήτων

1. Ο ENISA δημιουργεί και τηρεί μητρώο με παρόχους υπηρεσιών DNS, μητρώα ονομάτων TLD, οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα, παρόχους υπηρεσιών υπολογιστικού νέφους, παρόχους υπηρεσιών κέντρων δεδομένων, παρόχους δικτύων διανομής περιεχομένου, παρόχους διαχειριζομένων υπηρεσιών, παρόχους διαχειριζομένων υπηρεσιών ασφάλειας, καθώς και παρόχους επιγραμμικών αγορών, επιγραμμικών μηχανών αναζήτησης ή πλατφορμών υπηρεσιών κοινωνικής δικτύωσης, βάσει των πληροφοριών που λαμβάνει από τα ενιαία σημεία επαφής σύμφωνα με την παράγραφο 4. Κατόπιν αιτήματος, ο ENISA επιτρέπει την πρόσβαση των αρμόδιων αρχών στο εν λόγω μητρώο, διασφαλίζοντας παράλληλα την προστασία της εμπιστευτικότητας των πληροφοριών, κατά περίπτωση.

2. Τα κράτη μέλη απαιτούν από τις οντότητες που αναφέρονται στην παράγραφο 1 να υποβάλουν τις ακόλουθες πληροφορίες στις αρμόδιες αρχές έως τις 17 Ιανουαρίου 2025:

α) την επωνυμία της οντότητας·

β) τον σχετικό τομέα, υποτομέα και τύπο οντότητας που αναφέρεται στα παραρτήματα I και II, κατά περίπτωση·

γ) τη διεύθυνση της κύριας εγκατάστασης της οντότητας και των άλλων νομικών εγκαταστάσεών της στην Ένωση ή, εάν δεν είναι εγκατεστημένη στην Ένωση, της διεύθυνσης του εκπροσώπου της που έχει οριστεί σύμφωνα με το άρθρο 26 παράγραφος 3·

δ) επικαιροποιημένα στοιχεία επικοινωνίας, συμπεριλαμβανομένων των διευθύνσεων ηλεκτρονικού ταχυδρομείου και των αριθμών τηλεφώνου της οντότητας και, κατά περίπτωση, του εκπροσώπου της ο οποίος έχει οριστεί σύμφωνα με το άρθρο 26 παράγραφος 3·

ε) τα κράτη μέλη στα οποία η οντότητα παρέχει υπηρεσίες· και

στ) το εύρος IP της οντότητας.

3. Τα κράτη μέλη διασφαλίζουν ότι οι οντότητες που αναφέρονται στην παράγραφο 1 κοινοποιούν στην αρμόδια αρχή τυχόν αλλαγές στις πληροφορίες που υπέβαλαν δυνάμει της παραγράφου 2 αμελλητί και, σε κάθε περίπτωση, εντός τριών μηνών από την ημερομηνία πραγματοποίησης της αλλαγής.

4. Με την παραλαβή των πληροφοριών που αναφέρονται στις παραγράφους 2 και 3, εκτός από τις πληροφορίες που αναφέρονται στην παράγραφο 2 στοιχείο στ), το ενιαίο σημείο επαφής του οικείου κράτους μέλους τις διαβιβάζει), στον ENISA χωρίς αδικαιολόγητη καθυστέρηση.

5. Κατά περίπτωση, οι πληροφορίες που αναφέρονται στις παραγράφους 2 και 3 του παρόντος άρθρου υποβάλλονται μέσω του εθνικού μηχανισμού που αναφέρεται στο άρθρο 3 παράγραφος 4 τέταρτο εδάφιο.

Άρθρο 28

Βάση δεδομένων καταχώρισης ονομάτων τομέα

1. Για τους σκοπούς της συμβολής στην ασφάλεια, τη σταθερότητα και την ανθεκτικότητα του DNS, τα κράτη μέλη απαιτούν από τα μητρώα ονομάτων TLD και τις οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα να συλλέγουν και να διατηρούν ακριβή και πλήρη δεδομένα καταχώρισης ονομάτων τομέα σε ειδική βάση δεδομένων με τη δέουσα επιμέλεια σύμφωνα με την ενωσιακή νομοθεσία για την προστασία των δεδομένων όσον αφορά τα δεδομένα προσωπικού χαρακτήρα.

2. Για τους σκοπούς της παραγράφου 1, τα κράτη μέλη απαιτούν η βάση δεδομένων καταχώρισης ονομάτων τομέα να περιέχει τις αναγκαίες πληροφορίες για την ταυτοποίηση και την επικοινωνία με τους κατόχους των ονομάτων τομέα και τα σημεία επαφής που διαχειρίζονται τα ονόματα τομέα στο πλαίσιο των TLD. Οι πληροφορίες αυτές περιλαμβάνουν:

α) το όνομα τομέα·

β) την ημερομηνία καταχώρισης·

γ) το όνομα, την ηλεκτρονική διεύθυνση επικοινωνίας και τον αριθμό τηλεφώνου του καταχωρίζοντος·

δ) τη διεύθυνση ηλεκτρονικού ταχυδρομείου επικοινωνίας και τον αριθμό τηλεφώνου του σημείου επαφής που διαχειρίζεται το όνομα τομέα σε περίπτωση που διαφέρουν από εκείνα του καταχωρίζοντος.

3. Τα κράτη μέλη απαιτούν από τα μητρώα ονομάτων TLD και τις οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα να διαθέτουν πολιτικές και διαδικασίες, συμπεριλαμβανομένων διαδικασιών επαλήθευσης, ώστε να διασφαλίζεται ότι οι βάσεις δεδομένων που αναφέρονται στην παράγραφο 1 περιλαμβάνουν ακριβείς και πλήρεις πληροφορίες. Τα κράτη μέλη απαιτούν να δημοσιοποιούνται οι εν λόγω πολιτικές και διαδικασίες.

4. Τα κράτη μέλη απαιτούν από τα μητρώα ονομάτων TLD και από τις οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα να δημοσιοποιούν αμελλητί μετά από την καταχώριση ονόματος τομέα, τα δεδομένα καταχώρισης ονομάτων τομέα που δεν είναι δεδομένα προσωπικού χαρακτήρα.

5. Τα κράτη μέλη απαιτούν από τα μητρώα ονομάτων TLD και τις οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα να παρέχουν πρόσβαση σε συγκεκριμένα δεδομένα καταχώρισης ονομάτων τομέα κατόπιν νομίμων και δεόντως αιτιολογημένων αιτημάτων από νόμιμους αιτούντες πρόσβαση, σύμφωνα με τη νομοθεσία της Ένωσης για την προστασία των δεδομένων. Τα κράτη μέλη απαιτούν από τα μητρώα ονομάτων TLD και τις οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα να απαντούν χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 72 ωρών από την παραλαβή τυχόν αιτημάτων πρόσβασης. Τα κράτη μέλη απαιτούν να δημοσιοποιούνται οι πολιτικές και οι διαδικασίες γνωστοποίησης των εν λόγω δεδομένων.

6. Η συμμόρφωση με τις υποχρεώσεις που ορίζονται στις παραγράφους 1 έως 5 δεν οδηγεί σε επικάλυψη της συλλογής δεδομένων καταχώρισης ονομάτων τομέα. Για τον σκοπό αυτό, τα κράτη μέλη απαιτούν από τα μητρώα ονομάτων TLD και τις οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα να συνεργάζονται μεταξύ τους.

ΚΕΦΑΛΑΙΟ VI

ΑΝΤΑΛΛΑΓΗ ΠΛΗΡΟΦΟΡΙΩΝ

Άρθρο 29

Ρυθμίσεις για την ανταλλαγή πληροφοριών στον τομέα της κυβερνοασφάλειας

1. Τα κράτη μέλη διασφαλίζουν ότι οι οντότητες που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας και, κατά περίπτωση, άλλες οντότητες που δεν εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας είναι σε θέση να ανταλλάσσουν μεταξύ τους, σε εθελοντική βάση, πληροφορίες σχετικές με την κυβερνοασφάλεια, συμπεριλαμβανομένων πληροφοριών που αφορούν κυβερνοαπειλές, παρ' ολίγον περιστατικά, ευπάθειες, τεχνικές και διαδικασίες, ενδείξεις της παραβίασης, εχθρικές τακτικές, πληροφορίες που αφορούν συγκεκριμένους παράγοντες απειλής, προειδοποιήσεις για την κυβερνοασφάλεια και συστάσεις σχετικά με την παραμετροποίηση εργαλείων κυβερνοασφάλειας για τον εντοπισμό κυβερνοεπιθέσεων, στον βαθμό που η εν λόγω ανταλλαγή πληροφοριών:

α) αποσκοπεί στην πρόληψη, τον εντοπισμό, την αντιμετώπιση ή την ανάκαμψη από περιστατικά ή στον μετριασμό των επιπτώσεών τους·

β) ενισχύει το επίπεδο της κυβερνοασφάλειας, ιδίως μέσω της ευαισθητοποίησης σχετικά με τις κυβερνοαπειλές, του περιορισμού ή της παρεμπόδισης της ικανότητας διάδοσης των εν λόγω απειλών, της στήριξης μιας σειράς αμυντικών ικανοτήτων, της αποκατάστασης και της γνωστοποίησης ευπαθειών, της ανίχνευσης απειλών, των τεχνικών περιορισμού και πρόληψης, των στρατηγικών μετριασμού ή των σταδίων αντίδρασης και ανάκαμψης ή της προώθησης της συνεργατικής έρευνας για τις κυβερνοαπειλές μεταξύ δημόσιων και ιδιωτικών φορέων.

2. Τα κράτη μέλη διασφαλίζουν ότι η ανταλλαγή πληροφοριών πραγματοποιείται στο πλαίσιο κοινοτήτων βασικών και σημαντικών οντοτήτων και, κατά περίπτωση, των προμηθευτών ή των παρόχων υπηρεσιών τους. Η εν λόγω ανταλλαγή πραγματοποιείται μέσω ρυθμίσεων για την ανταλλαγή πληροφοριών στον τομέα της κυβερνοασφάλειας όσον αφορά τον δυνητικά ευαίσθητο χαρακτήρα των ανταλλασσόμενων πληροφοριών.

3. Τα κράτη μέλη διευκολύνουν τη θέσπιση ρυθμίσεων για την ανταλλαγή πληροφοριών στον τομέα της κυβερνοασφάλειας που αναφέρονται στην παράγραφο 2 του παρόντος άρθρου. Οι ρυθμίσεις αυτές μπορούν να προσδιορίζουν επιχειρησιακά στοιχεία, συμπεριλαμβανομένων της χρήσης ειδικών πλατφορμών ΤΠΕ και εργαλείων αυτοματισμού, του περιεχομένου και των όρων των ρυθμίσεων ανταλλαγής πληροφοριών. Κατά τον καθορισμό των λεπτομερειών της συμμετοχής των δημόσιων αρχών στις εν λόγω ρυθμίσεις, τα κράτη μέλη μπορούν να επιβάλλουν όρους όσον αφορά τις πληροφορίες που διατίθενται από τις αρμόδιες αρχές ή τις CSIRT. Τα κράτη μέλη παρέχουν βοήθεια για την εφαρμογή των εν λόγω ρυθμίσεων σύμφωνα με τις πολιτικές τους που αναφέρονται στο άρθρο 7 παράγραφος 2 στοιχείο η).

4. Τα κράτη μέλη διασφαλίζουν ότι οι βασικές και σημαντικές οντότητες γνωστοποιούν στις αρμόδιες αρχές τη συμμετοχή τους στις ρυθμίσεις ανταλλαγής πληροφοριών στον τομέα της κυβερνοασφάλειας που αναφέρονται στην παράγραφο 2, αμέσως μετά τη σύναψη των εν λόγω ρυθμίσεων ή, κατά περίπτωση, την ανάκληση της συμμετοχής τους στις ρυθμίσεις αυτές, μόλις αυτή πραγματοποιηθεί.

5. Ο ENISA παρέχει συνδρομή για τη θέσπιση ρυθμίσεων ανταλλαγής πληροφοριών στον τομέα της κυβερνοασφάλειας που αναφέρονται στην παράγραφο 2, ανταλλάσσοντας βέλτιστες πρακτικές και παρέχοντας καθοδήγηση.

Άρθρο 30

Εθελούσια κοινοποίηση των σχετικών πληροφοριών

1. Τα κράτη μέλη διασφαλίζουν ότι, επιπλέον της υποχρέωσης κοινοποίησης που προβλέπεται στο άρθρο 23, οι κοινοποιήσεις μπορούν να υποβάλλονται στις CSIRT ή, κατά περίπτωση, στις αρμόδιες αρχές, σε εθελοντική βάση, από:

α) βασικές και σημαντικές οντότητες όσον αφορά περιστατικά, κυβερνοαπειλές και παρ' ολίγον περιστατικά·

β) οντότητες διαφορετικές από εκείνες που αναφέρονται στο στοιχείο α), ανεξαρτήτως του αν εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας, όσον αφορά σημαντικά περιστατικά, κυβερνοαπειλές και παρ' ολίγον περιστατικά.

2. Τα κράτη μέλη επεξεργάζονται τις κοινοποιήσεις που αναφέρονται στην παράγραφο 1 του παρόντος άρθρου με τη διαδικασία του άρθρου 23. Τα κράτη μέλη μπορούν να δίνουν προτεραιότητα στην επεξεργασία των υποχρεωτικών έναντι των εθελούσιων κοινοποιήσεων.

Όπου είναι αναγκαίο, οι CSIRT και, κατά περίπτωση, οι αρμόδιες αρχές παρέχουν στα ενιαία σημεία επαφής τις πληροφορίες σχετικά με τις κοινοποιήσεις που λαμβάνουν σύμφωνα με το παρόν άρθρο, διασφαλίζοντας παράλληλα την εμπιστευτικότητα και την κατάλληλη προστασία των πληροφοριών που παρέχονται από την αναφέρουσα οντότητα. Με την επιφύλαξη της πρόληψης, της διερεύνησης, της διακρίβωσης και της δίωξης ποινικών αδικημάτων, η εθελούσια αναφορά δεν συνεπάγεται την επιβολή πρόσθετων υποχρεώσεων στην κοινοποιούσα οντότητα, τις οποίες δεν θα υπείχε αν δεν είχε υποβάλει την κοινοποίηση.

ΚΕΦΑΛΑΙΟ VII

ΕΠΟΠΤΕΙΑ ΚΑΙ ΕΠΙΒΟΛΗ

Άρθρο 31

Γενικές πτυχές που αφορούν την εποπτεία και την επιβολή

1. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές τους εποπτεύουν αποτελεσματικά και λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν τη συμμόρφωση με την παρούσα οδηγία.

2. Τα κράτη μέλη μπορούν να επιτρέπουν στις αρμόδιες αρχές τους να δίνουν προτεραιότητα στα εποπτικά καθήκοντα. Η προτεραιοποίηση αυτή βασίζεται σε προσέγγιση βάσει κινδύνου. Για τον σκοπό αυτό, κατά την άσκηση των εποπτικών καθηκόντων τους που προβλέπονται στα άρθρα 32 και 33, οι αρμόδιες αρχές μπορούν να θεσπίζουν μεθοδολογίες εποπτείας που επιτρέπουν την ιεράρχηση των εν λόγω καθηκόντων με μια προσέγγιση βάσει κινδύνου.

3. Οι αρμόδιες αρχές συνεργάζονται στενά με τις εποπτικές αρχές δυνάμει του κανονισμού (ΕΕ) 2016/679 στην αντιμετώπιση περιστατικών που οδηγούν σε παραβιάσεις δεδομένων προσωπικού χαρακτήρα, με την επιφύλαξη της αρμοδιότητας και των καθηκόντων των εποπτικών αρχών δυνάμει του εν λόγω κανονισμού.

4. Με την επιφύλαξη των εθνικών νομοθετικών και θεσμικών πλαισίων, τα κράτη μέλη διασφαλίζουν ότι, κατά την εποπτεία της συμμόρφωσης των φορέων δημόσιας διοίκησης με την παρούσα οδηγία και την πρόβλεψη μέτρων επιβολής για παραβιάσεις της παρούσας οδηγίας, οι αρμόδιες αρχές διαθέτουν κατάλληλες εξουσίες για την εκτέλεση των καθηκόντων αυτών με λειτουργική ανεξαρτησία έναντι των εποπτευόμενων φορέων δημόσιας διοίκησης. Τα κράτη μέλη μπορούν να αποφασίσουν την επιβολή κατάλληλων, αναλογικών και αποτελεσματικών μέτρων εποπτείας και επιβολής σε σχέση με τις εν λόγω οντότητες σύμφωνα με το εθνικό νομοθετικό και θεσμικό πλαίσιο.

Άρθρο 32

Μέτρα εποπτείας και επιβολής σε σχέση με βασικές οντότητες

1. Τα κράτη μέλη διασφαλίζουν ότι τα μέτρα εποπτείας ή επιβολής που επιβάλλονται σε βασικές οντότητες σε σχέση με τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία είναι αποτελεσματικά, αναλογικά και αποτρεπτικά, λαμβάνοντας υπόψη τις περιστάσεις κάθε μεμονωμένης περίπτωσης.

2. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές, κατά την άσκηση των εποπτικών τους καθηκόντων σε σχέση με βασικές οντότητες, έχουν την εξουσία να υποβάλλουν τις εν λόγω οντότητες σε διαδικασίες που αφορούν τουλάχιστον:

α) επιτόπιες επιθεωρήσεις και εποπτεία εκτός των εγκαταστάσεων, συμπεριλαμβανομένων δειγματοληπτικών ελέγχων, που διεξάγονται από καταρτισμένους επαγγελματίες·

β) τακτικούς και στοχευμένους ελέγχους ασφάλειας που διενεργούνται από ειδικευμένο ανεξάρτητο όργανο ή αρμόδια αρχή·

γ) έκτακτους ειδικούς ελέγχους, μεταξύ άλλων, όταν αυτό δικαιολογείται λόγω σημαντικού περιστατικού ή παραβίασης της παρούσας οδηγίας από τη βασική οντότητα·

δ) σαρώσεις ασφαλείας βάσει αντικειμενικών, αμερόληπτων, δίκαιων και διαφανών κριτηρίων αξιολόγησης του κινδύνου, όπου απαιτείται με τη συνεργασία της οικείας οντότητας·

ε) αιτήματα παροχής πληροφοριών αναγκαίων για την εκ των υστέρων αξιολόγηση των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που λαμβάνει η οικεία οντότητα, συμπεριλαμβανομένων τεκμηριωμένων πολιτικών κυβερνοασφάλειας, καθώς και της συμμόρφωσης με την υποχρέωση διαβίβασης πληροφοριών στις αρμόδιες αρχές σύμφωνα με το άρθρο 27·

στ) αιτήματα πρόσβασης σε δεδομένα, έγγραφα και πληροφορίες που απαιτούνται για την εκτέλεση των εποπτικών καθηκόντων τους·

ζ) αιτήματα για αποδεικτικά στοιχεία που αφορούν την εφαρμογή των πολιτικών κυβερνοασφάλειας, όπως τα αποτελέσματα των ελέγχων ασφάλειας που διενεργούνται από εξουσιοδοτημένο επιθεωρητή και τα αντίστοιχα υποκείμενα αποδεικτικά στοιχεία.

Οι στοχευμένοι έλεγχοι ασφάλειας που αναφέρονται στο πρώτο εδάφιο στοιχείο β) βασίζονται σε εκτιμήσεις κινδύνου που διενεργούνται από την αρμόδια αρχή ή την ελεγχόμενη οντότητα ή σε άλλες σχετικές με κινδύνους διαθέσιμες πληροφορίες.

Τα αποτελέσματα κάθε στοχευμένου ελέγχου ασφάλειας τίθενται στη διάθεση της αρμόδιας αρχής. Το κόστος του εν λόγω στοχευμένου ελέγχου ασφάλειας που διενεργείται από ανεξάρτητο όργανο καλύπτεται από την ελεγχόμενη οντότητα, εκτός από δεόντως αιτιολογημένες περιπτώσεις για τις οποίες η αρμόδια αρχή αποφασίζει διαφορετικά.

3. Κατά την άσκηση των εξουσιών τους σύμφωνα με την παράγραφο 2 στοιχείο ε), στ) ή ζ), οι αρμόδιες αρχές δηλώνουν τον σκοπό του αιτήματος και προσδιορίζουν τις ζητούμενες πληροφορίες.

4. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές τους, κατά την άσκηση των εποπτικών καθηκόντων τους σε σχέση με βασικές οντότητες, έχουν την εξουσία τουλάχιστον για τα ακόλουθα:

α) να εκδίδουν προειδοποιήσεις σχετικά με παραβιάσεις της παρούσας οδηγίας από τις οικείες οντότητες·

β) να εκδίδουν δεσμευτικές οδηγίες, μεταξύ άλλων όσον αφορά τα μέτρα που είναι αναγκαία για την πρόληψη ή την αποκατάσταση περιστατικού, καθώς και προθεσμίες για την εφαρμογή των εν λόγω μέτρων και για την υποβολή εκθέσεων σχετικά με την εφαρμογή τους, ή εντολή με την οποία ζητείται από τις οικείες οντότητες να αποκαταστήσουν τις ελλείψεις που εντοπίστηκαν ή τις παραβιάσεις της παρούσας οδηγίας·

γ) να εντέλλουν τις οικείες οντότητες να παύσουν συμπεριφορά που παραβιάζει την παρούσα οδηγία και να απόσχουν από την επανάληψη της εν λόγω συμπεριφοράς·

δ) να εντέλλουν τις οικείες οντότητες να διασφαλίσουν ότι τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας συμμορφώνονται με το άρθρο 21 ή να εκπληρώσουν τις υποχρεώσεις υποβολής εκθέσεων που ορίζονται στο άρθρο 23, με συγκεκριμένο τρόπο και εντός καθορισμένου χρονικού διαστήματος·

ε) να εντέλλουν τις οικείες οντότητες να ενημερώσουν τα φυσικά ή νομικά πρόσωπα σε σχέση με τα οποία παρέχουν υπηρεσίες ή ασκούν δραστηριότητες που ενδέχεται να επηρεαστούν από σημαντική κυβερνοαπειλή σχετικά με τη φύση της απειλής, καθώς και σχετικά με τυχόν μέτρα προστασίας ή αποκατάστασης που μπορούν να λάβουν τα εν λόγω φυσικά ή νομικά πρόσωπα για την αντιμετώπιση της εν λόγω απειλής·

στ) να δίνουν εντολή στις οικείες οντότητες να εφαρμόσουν τις συστάσεις που διατυπώθηκαν ως αποτέλεσμα ελέγχου ασφάλειας εντός εύλογης προθεσμίας·

ζ) να ορίζουν υπεύθυνο παρακολούθησης με σαφώς καθορισμένα καθήκοντα για καθορισμένο χρονικό διάστημα, προκειμένου να επιβλέπει τη συμμόρφωση των οικείων οντοτήτων με τα άρθρα 21 και 23·

η) να εντέλλουν τις οικείες οντότητες να δημοσιοποιούν πτυχές των παραβιάσεων της παρούσας οδηγία με συγκεκριμένο τρόπο·

θ) να επιβάλλουν, ή να απαιτούν την επιβολή από τα αρμόδια όργανα ή δικαστήρια, σύμφωνα με το εθνικό δίκαιο, διοικητικού προστίμου δυνάμει του άρθρου 34 επιπλέον οποιουδήποτε από τα μέτρα που αναφέρονται στα στοιχεία α) έως η) της παρούσας παραγράφου.

5. Όταν τα μέτρα επιβολής που θεσπίζονται σύμφωνα με την παράγραφο 4 στοιχεία α) έως δ) και στ) είναι αναποτελεσματικά, τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές τους έχουν την εξουσία να ορίζουν προθεσμία εντός της οποίας η βασική οντότητα καλείται να λάβει τα αναγκαία μέτρα για την αποκατάσταση των ελλείψεων ή για τη συμμόρφωση με τις απαιτήσεις των εν λόγω αρχών. Εάν τα ζητούμενα μέτρα δεν ληφθούν εντός της καθορισμένης προθεσμίας, τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές έχουν την εξουσία:

α) να αναστείλουν προσωρινά ή να ζητήσουν από φορέα πιστοποίησης ή εξουσιοδότησης, ή από δικαστήριο, σύμφωνα με το εθνικό δίκαιο, την προσωρινή αναστολή πιστοποίησης ή εξουσιοδότησης που αφορά μέρος ή το σύνολο των σχετικών υπηρεσιών που παρέχονται ή των δραστηριοτήτων που εκτελούνται από τη βασική οντότητα·

β) να ζητούν από τα αρμόδια όργανα ή δικαστήρια, σύμφωνα με το εθνικό δίκαιο, να απαγορεύουν προσωρινά σε κάθε φυσικό πρόσωπο που είναι υπεύθυνο για την άσκηση διευθυντικών καθηκόντων σε επίπεδο διευθύνοντος συμβούλου ή νομικού εκπροσώπου στη βασική οντότητα να ασκεί διευθυντικά καθήκοντα στην εν λόγω οντότητα.

Οι προσωρινές αναστολές ή απαγορεύσεις που επιβάλλονται σύμφωνα με την παρούσα παράγραφο εφαρμόζονται μόνο έως ότου η οικεία οντότητα λάβει τα αναγκαία μέτρα για να διορθώσει τις ελλείψεις ή να συμμορφωθεί με τις απαιτήσεις της αρμόδιας αρχής για τις οποίες εφαρμόστηκαν τέτοια μέτρα επιβολής. Η επιβολή τέτοιων προσωρινών αναστολών ή απαγορεύσεων υπόκειται σε κατάλληλες διαδικαστικές εγγυήσεις σύμφωνα με τις γενικές αρχές του δικαίου της Ένωσης και του Χάρτη, συμπεριλαμβανομένου του δικαιώματος αποτελεσματικής δικαστικής προστασίας και δίκαιης δίκης, του τεκμηρίου αθωότητας και των δικαιωμάτων υπεράσπισης.

Τα μέτρα επιβολής που προβλέπονται στην παρούσα παράγραφο δεν εφαρμόζονται σε φορείς δημόσιας διοίκησης που υπόκεινται στην παρούσα οδηγία.

6. Τα κράτη μέλη διασφαλίζουν ότι κάθε φυσικό πρόσωπο που είναι υπεύθυνο ή ενεργεί ως νόμιμος εκπρόσωπος βασικής οντότητας με βάση την εξουσία εκπροσώπησής της, την αρμοδιότητα να λαμβάνει αποφάσεις εξ ονόματός της ή να ασκεί τον έλεγχό της, έχει την εξουσία να διασφαλίζει τη συμμόρφωσή της με την παρούσα οδηγία. Τα κράτη μέλη μεριμνούν ώστε τα εν λόγω φυσικά πρόσωπα να μπορούν να θεωρηθούν υπεύθυνα για παράβαση των υποχρεώσεών τους, ώστε να εξασφαλίζεται η συμμόρφωση με την παρούσα οδηγία.

Η εφαρμογή της παρούσας παραγράφου δεν θίγει το εθνικό δίκαιο όσον αφορά τους κανόνες περί ευθύνης που ισχύουν για τους δημόσιους οργανισμούς, καθώς και την ευθύνη δημοσίων υπαλλήλων και αιρετών ή διορισμένων αξιωματούχων.

7. Όταν λαμβάνουν οποιοδήποτε από τα μέτρα επιβολής που αναφέρονται στην παράγραφο 4 ή 5, οι αρμόδιες αρχές σέβονται τα δικαιώματα υπεράσπισης και λαμβάνουν υπόψη τις περιστάσεις κάθε μεμονωμένης περίπτωσης και, τουλάχιστον, λαμβάνουν δεόντως υπόψη:

α) τη σοβαρότητα της παράβασης και τη σημασία των διατάξεων που παραβιάζονται, ενώ τα ακόλουθα, μεταξύ άλλων, θεωρούνται σοβαρές παραβάσεις σε κάθε περίπτωση:

i) οι επανειλημμένες παραβάσεις·

ii) η μη κοινοποίηση ή αποκατάσταση σημαντικών περιστατικών·

iii) η μη αποκατάσταση ελλείψεων σύμφωνα με δεσμευτικές οδηγίες των αρμόδιων αρχών·

iv) η παρεμπόδιση των ελέγχων ή των δραστηριοτήτων παρακολούθησης που διατάσσονται από την αρμόδια αρχή μετά τη διαπίστωση παράβασης·

v) η παροχή ψευδών ή κατάφωρα ανακριβών πληροφοριών σε σχέση με τα μέτρα διαχείρισης κινδύνου ή τις υποχρεώσεις υποβολής εκθέσεων που ορίζονται στα άρθρα 21 και 23·

β) τη διάρκεια της παράβασης·

γ) τυχόν σχετικές προηγούμενες παραβάσεις από την οικεία οντότητα·

δ) οποιαδήποτε υλική ή μη υλική ζημία που προκλήθηκε, συμπεριλαμβανομένης της χρηματοοικονομικής ή οικονομικής ζημίας, τις επιπτώσεις σε άλλες υπηρεσίες και τον αριθμό των θιγόμενων χρηστών·

ε) οποιαδήποτε πρόθεση ή αμέλεια εκ μέρους του δράστη της παράβασης·

στ) οποιαδήποτε μέτρα που λαμβάνει η οντότητα για την πρόληψη ή τον μετριασμό της υλικής ή μη υλικής ζημίας·

ζ) οποιαδήποτε τήρηση εγκεκριμένων κωδίκων δεοντολογίας ή εγκεκριμένων μηχανισμών πιστοποίησης·

η) τον βαθμό συνεργασίας των υπαίτιων φυσικών ή νομικών προσώπων με τις αρμόδιες αρχές.

8. Οι αρμόδιες αρχές αιτιολογούν λεπτομερώς τα μέτρα επιβολής τους. Πριν από τη λήψη των μέτρων αυτών, οι αρμόδιες αρχές κοινοποιούν στις ενδιαφερόμενες οντότητες τα προκαταρκτικά πορίσματά τους. Παρέχουν επίσης εύλογο χρονικό διάστημα στις οικείες οντότητες για να υποβάλουν παρατηρήσεις, εκτός από δεόντως αιτιολογημένες περιπτώσεις όπου διαφορετικά θα παρεμποδιζόταν η ανάληψη άμεσης δράσης για την πρόληψη ή την αντιμετώπιση περιστατικών.

9. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές τους δυνάμει της παρούσας οδηγίας ενημερώνουν τις σχετικές αρμόδιες αρχές εντός του ίδιου κράτους μέλους δυνάμει της οδηγίας (ΕΕ) 2022/2557 κατά την άσκηση των εποπτικών και εκτελεστικών εξουσιών τους με στόχο τη διασφάλιση της συμμόρφωσης μιας οντότητας που προσδιορίζεται ως κρίσιμη οντότητα βάσει της οδηγίας (ΕΕ) 2022/2557 με τις υποχρεώσεις της παρούσας οδηγίας. Κατά περίπτωση, οι αρμόδιες αρχές δυνάμει της οδηγίας (ΕΕ) 2022/2557 θα πρέπει να μπορούν να ζητούν από τις αρμόδιες αρχές δυνάμει της παρούσας οδηγίας να ασκούν τις εποπτικές και εκτελεστικές εξουσίες τους σε σχέση με οντότητα η οποία προσδιορίζεται ως κρίσιμη οντότητα δυνάμει της οδηγίας (ΕΕ) 2022/2557.

10. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές τους δυνάμει της παρούσας οδηγίας συνεργάζονται με τις σχετικές αρμόδιες αρχές του οικείου κράτους μέλους δυνάμει του κανονισμού (ΕΕ) 2022/2554 Ειδικότερα, τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές τους δυνάμει της παρούσας οδηγίας ενημερώνουν το φόρουμ εποπτείας που συστάθηκε σύμφωνα με το άρθρο 32 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554 κατά την άσκηση των εποπτικών και εκτελεστικών εξουσιών τους που αποσκοπούν στη διασφάλιση της συμμόρφωσης βασικής οντότητας που έχει οριστεί ως κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ σύμφωνα με το άρθρο 31 του κανονισμού (ΕΕ) 2022/2554 με τις υποχρεώσεις της παρούσας οδηγίας.

Άρθρο 33

Μέτρα εποπτείας και επιβολής όσον αφορά σημαντικές οντότητες

1. Όταν τους παρέχονται αποδεικτικά στοιχεία, ενδείξεις ή πληροφορίες ότι μια σημαντική οντότητα εικάζεται ότι δεν συμμορφώνεται με την παρούσα οδηγία, ιδίως τα άρθρα 21 και 23 αυτής, τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές λαμβάνουν μέτρα, εφόσον απαιτείται, μέσω κατασταλτικών εποπτικών μέτρων. Τα κράτη μέλη διασφαλίζουν ότι τα μέτρα αυτά είναι αποτελεσματικά, αναλογικά και αποτρεπτικά, λαμβάνοντας υπόψη τις περιστάσεις κάθε μεμονωμένης περίπτωσης.

2. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές, κατά την άσκηση των εξουσιών επιβολής σε σχέση με βασικές οντότητες, έχουν την εξουσία να υποβάλλουν τις εν λόγω οντότητες τουλάχιστον στα ακόλουθα:

α) επιτόπιες επιθεωρήσεις και κατασταλτική εποπτεία εκτός των εγκαταστάσεων, που διενεργούνται από καταρτισμένους επαγγελματίες·

β) στοχευμένους ελέγχους ασφάλειας που διενεργούνται από ανεξάρτητο όργανο ή αρμόδια αρχή·

γ) σαρώσεις ασφαλείας βάσει αντικειμενικών, αμερόληπτων, δίκαιων και διαφανών κριτηρίων αξιολόγησης του κινδύνου, όπου απαιτείται με τη συνεργασία της οικείας οντότητας·

δ) αιτήματα παροχής πληροφοριών αναγκαίων για την αξιολόγηση των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που λαμβάνει η οικεία οντότητα, συμπεριλαμβανομένων τεκμηριωμένων πολιτικών κυβερνοασφάλειας, καθώς και της συμμόρφωσης με την υποχρέωση διαβίβασης πληροφοριών στις αρμόδιες αρχές σύμφωνα με το άρθρο 27·

ε) αιτήματα για πρόσβαση σε δεδομένα, έγγραφα ή πληροφορίες που είναι αναγκαίες για την εκ μέρους τους εκτέλεση των εποπτικών καθηκόντων τους·

στ) αιτήματα για αποδεικτικά στοιχεία που αφορούν την εφαρμογή των πολιτικών κυβερνοασφάλειας, όπως τα αποτελέσματα των ελέγχων ασφάλειας που διενεργούνται από εξουσιοδοτημένο επιθεωρητή και τα αντίστοιχα υποκείμενα αποδεικτικά στοιχεία.

Οι στοχευμένοι έλεγχοι ασφάλειας που αναφέρονται στο πρώτο εδάφιο στοιχείο β) βασίζονται σε εκτιμήσεις κινδύνου που διενεργούνται από την αρμόδια αρχή ή την ελεγχόμενη οντότητα ή σε άλλες διαθέσιμες πληροφορίες σχετικά με κινδύνους.

Τα αποτελέσματα κάθε στοχευμένου ελέγχου ασφάλειας τίθενται στη διάθεση της αρμόδιας αρχής. Το κόστος του εν λόγω στοχευμένου ελέγχου ασφάλειας που διενεργείται από ανεξάρτητο όργανο καλύπτεται από την ελεγχόμενη οντότητα, εκτός από δεόντως αιτιολογημένες περιπτώσεις για τις οποίες η αρμόδια αρχή αποφασίζει διαφορετικά.

3. Κατά την άσκηση των εξουσιών τους δυνάμει της παραγράφου 2 στοιχείο δ), ε) ή στ), οι αρμόδιες αρχές δηλώνουν τον σκοπό του αιτήματος και προσδιορίζουν τις ζητούμενες πληροφορίες.

4. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές, κατά την άσκηση των εποπτικών καθηκόντων τους σε σχέση με σημαντικές οντότητες, έχουν την εξουσία τουλάχιστον για τα εξής:

α) να εκδίδουν προειδοποιήσεις σχετικά με τις παραβιάσεις της παρούσας οδηγίας από τις οικείες οντότητες·

β) να εκδίδουν δεσμευτικές οδηγίες ή διαταγή προς τις οικείες οντότητες να αποκαταστήσουν τις διαπιστωθείσες ελλείψεις ή την παράβαση των υποχρεώσεων της παρούσας οδηγίας·

γ) να εντέλλουν τις οικείες οντότητες να παύσουν συμπεριφορά που παραβιάζει την παρούσα οδηγία και να απέχουν από επανάληψη της εν λόγω συμπεριφοράς παραβίασης·

δ) να εντέλλουν τις οικείες οντότητες να διασφαλίσουν ότι τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας συμμορφώνονται με το άρθρο 21 ή να εκπληρώσουν τις υποχρεώσεις υποβολής εκθέσεων που ορίζονται στο άρθρο 23, με συγκεκριμένο τρόπο και εντός καθορισμένου χρονικού διαστήματος·

ε) να εντέλλουν τις οικείες οντότητες να ενημερώσουν τα φυσικά ή νομικά πρόσωπα σε σχέση με τα οποία παρέχουν υπηρεσίες ή ασκούν δραστηριότητες που ενδέχεται να επηρεαστούν από σημαντική κυβερνοαπειλή σχετικά με τη φύση της απειλής, καθώς και σχετικά με τυχόν μέτρα προστασίας ή αποκατάστασης που μπορούν να λάβουν τα εν λόγω φυσικά ή νομικά πρόσωπα για την αντιμετώπιση της εν λόγω απειλής·

στ) να δίνουν εντολή στις οικείες οντότητες να εφαρμόσουν τις συστάσεις που διατυπώθηκαν ως αποτέλεσμα ελέγχου ασφάλειας εντός εύλογης προθεσμίας·

ζ) να εντέλλουν τις οικείες οντότητες να δημοσιοποιούν πτυχές των παραβιάσεων της παρούσας οδηγίας με συγκεκριμένο τρόπο·

η) να επιβάλλουν, ή ζητούν την επιβολή από τα αρμόδια όργανα ή δικαστήρια, σύμφωνα με το εθνικό δίκαιο, διοικητικού προστίμου δυνάμει του άρθρου 34 επιπλέον οποιουδήποτε από τα μέτρα που αναφέρονται στα στοιχεία α) έως ζ) της παρούσας παραγράφου.

5. Το άρθρο 32 παράγραφοι 6, 7 και 8 εφαρμόζεται κατ' αναλογία στα μέτρα εποπτείας και επιβολής που προβλέπονται στο παρόν άρθρο για σημαντικές οντότητες.

6. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές τους δυνάμει της παρούσας οδηγίας συνεργάζονται με τις σχετικές αρμόδιες αρχές του οικείου κράτους μέλους δυνάμει του κανονισμού (ΕΕ) 2022/2554. Ειδικότερα, τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές τους δυνάμει της παρούσας οδηγίας ενημερώνουν το φόρουμ εποπτείας που συστάθηκε σύμφωνα με το άρθρο 32 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554 κατά την άσκηση των εποπτικών και εκτελεστικών εξουσιών τους που αποσκοπούν στη διασφάλιση της συμμόρφωσης σημαντικής οντότητας που έχει οριστεί ως κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ σύμφωνα με το άρθρο 31 του κανονισμού (ΕΕ) 2022/2554 με τις υποχρεώσεις της παρούσας οδηγίας.

Άρθρο 34

Γενικοί όροι για την επιβολή διοικητικών προστίμων σε βασικές και σημαντικές οντότητες

1. Τα κράτη μέλη διασφαλίζουν ότι τα μέτρα εποπτείας ή επιβολής που επιβάλλονται σε βασικές οντότητες σε σχέση με την παρούσα οδηγία είναι αποτελεσματικά, αναλογικά και αποτρεπτικά, λαμβάνοντας υπόψη τις περιστάσεις κάθε μεμονωμένης περίπτωσης.

2. Διοικητικά πρόστιμα επιβάλλονται επιπλέον οποιουδήποτε από τα μέτρα που αναφέρονται στο άρθρο 32 παράγραφος 4 στοιχεία α) έως η), στο άρθρο 32 παράγραφος 5 και στο άρθρο 33 παράγραφος 4 στοιχεία α) έως ζ).

3. Κατά τη λήψη απόφασης σχετικά με την επιβολή διοικητικού προστίμου και τη λήψη απόφασης σχετικά με το ύψος του σε κάθε μεμονωμένη περίπτωση, λαμβάνονται δεόντως υπόψη, κατ' ελάχιστον, τα στοιχεία που προβλέπονται στο άρθρο 32 παράγραφος 7.

4. Τα κράτη μέλη διασφαλίζουν ότι, όταν παραβιάζουν το άρθρο 21 ή το άρθρο 23, οι βασικές οντότητες υπόκεινται, σύμφωνα με τις παραγράφους 2 και 3 του παρόντος άρθρου, σε διοικητικά πρόστιμα ύψους κατ' ανώτατο όριο τουλάχιστον 10 000 000 EUR ή κατ' ανώτατο όριο τουλάχιστον 2 % του κατά το προηγούμενο οικονομικό έτος συνολικού παγκόσμιου ετήσιου κύκλου εργασιών της επιχείρησης στην οποία ανήκει η σημαντική οντότητα, ανάλογα με το ποιο είναι υψηλότερο.

5. Τα κράτη μέλη διασφαλίζουν ότι, όταν παραβιάζουν το άρθρο 21 ή 23, οι σημαντικές οντότητες υπόκεινται, σύμφωνα με τις παραγράφους 2 και 3 του παρόντος άρθρου, σε διοικητικά πρόστιμα ύψους κατ' ανώτατο όριο τουλάχιστον 7 000 000 EUR ή κατ' ανώτατο όριο τουλάχιστον 1,4 % του κατά το προηγούμενο οικονομικό έτος συνολικού παγκόσμιου ετήσιου κύκλου εργασιών της επιχείρησης στην οποία ανήκει η σημαντική οντότητα, ανάλογα με το ποιο είναι υψηλότερο.

6. Τα κράτη μέλη μπορούν να προβλέψουν τη δυνατότητα άσκησης εξουσίας επιβολής περιοδικών χρηματικών κυρώσεων προκειμένου να υποχρεώσουν βασική ή σημαντική οντότητα να παύσει μια παράβαση της παρούσας οδηγίας σύμφωνα με προηγούμενη απόφαση της αρμόδιας αρχής.

7. Με την επιφύλαξη των εξουσιών των αρμόδιων αρχών σύμφωνα με τα άρθρα 32 και 33, κάθε κράτος μέλος μπορεί να θεσπίζει κανόνες σχετικά με το εάν και σε ποιο βαθμό μπορούν να επιβληθούν διοικητικά πρόστιμα σε φορείς δημόσιας διοίκησης υποκείμενους στις υποχρεώσεις που ορίζονται στην παρούσα οδηγία.

8. Όταν το νομικό σύστημα κράτους μέλους δεν προβλέπει διοικητικά πρόστιμα, το εν λόγω κράτος μέλος διασφαλίζει ότι το παρόν άρθρο εφαρμόζεται κατά τρόπο ώστε το πρόστιμο να κινείται από την αρμόδια αρχή και να επιβάλλεται από τα αρμόδια εθνικά δικαστήρια, διασφαλίζοντας παράλληλα ότι τα εν λόγω ένδικα μέσα είναι αποτελεσματικά και έχουν ισοδύναμο αποτέλεσμα με τα διοικητικά πρόστιμα που επιβάλλονται από τις αρμόδιες αρχές. Σε κάθε περίπτωση, τα πρόστιμα που επιβάλλονται είναι αποτελεσματικά, αναλογικά και αποτρεπτικά. Το κράτος μέλος κοινοποιεί στην Επιτροπή τις διατάξεις των νόμων που θεσπίζει σύμφωνα με την παρούσα παράγραφο, έως τις 17 Οκτωβρίου 2024 και, χωρίς καθυστέρηση, κάθε επακολουθούντα τροποποιητικό νόμο ή τροποποίησή τους.

Άρθρο 35

Παραβάσεις που συνεπάγονται παραβίαση δεδομένων προσωπικού χαρακτήρα

1. Όταν οι αρμόδιες αρχές αντιληφθούν, στο πλαίσιο της εποπτείας ή της επιβολής, ότι η παράβαση από βασική ή σημαντική οντότητα των υποχρεώσεων που ορίζονται στα άρθρα 21 και 23 της παρούσας οδηγίας μπορεί να συνεπάγεται παραβίαση δεδομένων προσωπικού χαρακτήρα, όπως ορίζεται στο άρθρο 4 σημείο 12) του κανονισμού (ΕΕ) 2016/679, η οποία πρέπει να κοινοποιείται σύμφωνα με το άρθρο 33 του εν λόγω κανονισμού, ενημερώνουν χωρίς αδικαιολόγητη καθυστέρηση τις εποπτικές αρχές που αναφέρονται στο άρθρο 55 ή 56 του εν λόγω κανονισμού.

2. Όταν οι εποπτικές αρχές που αναφέρονται στο άρθρο 55 ή 56 του κανονισμού (ΕΕ) 2016/679 επιβάλλουν διοικητικό πρόστιμο σύμφωνα με το άρθρο 58 παράγραφος 2 στοιχείο θ) του εν λόγω κανονισμού, οι αρμόδιες αρχές δεν επιβάλλουν διοικητικό πρόστιμο σύμφωνα με το άρθρο 34 της παρούσας οδηγίας για παράβαση που αναφέρεται στην παράγραφο 1 του παρόντος άρθρου και η οποία απορρέει από την ίδια συμπεριφορά που αποτέλεσε αντικείμενο του διοικητικού προστίμου σύμφωνα με το άρθρο 58 παράγραφος 2 στοιχείο θ) του κανονισμού (ΕΕ) 2016/679. Οι αρμόδιες αρχές μπορούν, ωστόσο, να εφαρμόσουν τα μέτρα επιβολής που αναφέρονται στο άρθρο 32 παράγραφος 4 στοιχεία α) έως η), στο άρθρο 32 παράγραφος 5 και στο άρθρο 33 παράγραφος 4 στοιχεία α) έως ζ) της παρούσας οδηγίας.

3. Εάν η εποπτική αρχή που είναι αρμόδια δυνάμει του κανονισμού (ΕΕ) 2016/679 είναι εγκατεστημένη σε κράτος μέλος διαφορετικό από την αρμόδια αρχή, η αρμόδια αρχή ενημερώνει την εποπτική αρχή που είναι εγκατεστημένη στο ίδιο κράτος μέλος για την ενδεχόμενη παραβίαση των στοιχείων που αναφέρονται στην παράγραφο 1.

Άρθρο 36

Κυρώσεις

Τα κράτη μέλη καθορίζουν τους κανόνες για τις κυρώσεις που επιβάλλονται σε περίπτωση παραβιάσεων των εθνικών μέτρων που θεσπίζονται δυνάμει της παρούσας οδηγίας και λαμβάνουν τα αναγκαία μέτρα για να διασφαλίσουν την εφαρμογή τους. Οι προβλεπόμενες κυρώσεις είναι αποτελεσματικές, αναλογικές και αποτρεπτικές. Τα κράτη μέλη κοινοποιούν έως τις 17 Ιανουαρίου 2025 στην Επιτροπή τους εν λόγω κανόνες και τα εν λόγω μέτρα και την ενημερώνουν χωρίς αδικαιολόγητη καθυστέρηση σχετικά με κάθε μεταγενέστερη τροποποίησή τους.

Άρθρο 37

Αμοιβαία συνδρομή

1. Όταν μια οντότητα παρέχει υπηρεσίες σε περισσότερα του ενός κράτη μέλη ή παρέχει υπηρεσίες σε ένα ή περισσότερα κράτη μέλη και τα συστήματα δικτύου και πληροφοριών της βρίσκονται σε ένα ή περισσότερα άλλα κράτη μέλη, οι αρμόδιες αρχές των ενδιαφερόμενων κρατών μελών συνεργάζονται μεταξύ τους και παρέχουν αμοιβαία συνδρομή, ανάλογα με τις ανάγκες. Η συνεργασία αυτή συνεπάγεται, τουλάχιστον, ότι:

α) οι αρμόδιες αρχές που εφαρμόζουν μέτρα εποπτείας ή επιβολής σε ένα κράτος μέλος ενημερώνουν, μέσω του ενιαίου σημείου επαφής, και διαβουλεύονται με τις αρμόδιες αρχές των άλλων ενδιαφερόμενων κρατών μελών σχετικά με τα μέτρα εποπτείας και επιβολής που λαμβάνονται·

β) μια αρμόδια αρχή μπορεί να ζητήσει από άλλη αρμόδια αρχή να λάβει τα μέτρα εποπτείας ή επιβολής·

γ) μια αρμόδια αρχή, μόλις λάβει τεκμηριωμένο αίτημα από άλλη αρμόδια αρχή, παρέχει στην άλλη αρμόδια αρχή αμοιβαία συνδρομή ανάλογη προς τους πόρους που διαθέτει η ίδια, ώστε τα μέτρα εποπτείας ή επιβολής να μπορούν να εφαρμοστούν με αποτελεσματικό, αποδοτικό και συνεπή τρόπο.

Η αμοιβαία συνδρομή που αναφέρεται στο πρώτο εδάφιο στοιχείο γ) μπορεί να καλύπτει αιτήματα παροχής πληροφοριών και εποπτικά μέτρα, συμπεριλαμβανομένων αιτημάτων για τη διενέργεια επιτόπιων επιθεωρήσεων ή μη επιτόπιας εποπτείας ή στοχευμένων ελέγχων ασφάλειας. Η αρμόδια αρχή στην οποία απευθύνεται αίτημα συνδρομής δεν απορρίπτει την αίτηση αυτή, εκτός εάν διαπιστωθεί ότι δεν είναι αρμόδια να παράσχει τη ζητούμενη συνδρομή, ότι η ζητούμενη συνδρομή δεν είναι ανάλογη προς τα εποπτικά καθήκοντα της αρμόδιας αρχής ή ότι η αίτηση αφορά πληροφορίες ή συνεπάγεται δραστηριότητες οι οποίες, εάν κοινοποιηθούν ή εκτελεστούν, θα ήταν αντίθετες προς τα βασικά συμφέροντα εθνικής ασφάλειας, δημόσιας ασφάλειας ή άμυνας του κράτους μέλους. Πριν απορρίψει το εν λόγω αίτημα, η αρμόδια αρχή διαβουλεύεται με τις άλλες οικείες αρμόδιες αρχές, καθώς και, κατόπιν αιτήματος ενός από τα ενδιαφερόμενα κράτη μέλη, με την Επιτροπή και τον ENISA.

2. Κατά περίπτωση και με κοινή συμφωνία, οι αρμόδιες αρχές διαφόρων κρατών μελών μπορούν να αναλαμβάνουν κοινές εποπτικές ενέργειες.

ΚΕΦΑΛΑΙΟ VIII

ΚΑΤ' ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΚΑΙ ΕΚΤΕΛΕΣΤΙΚΕΣ ΠΡΑΞΕΙΣ

Άρθρο 38

Άσκηση της εξουσιοδότησης

1. Ανατίθεται στην Επιτροπή η εξουσία να εκδίδει κατ' εξουσιοδότηση πράξεις υπό τους όρους του παρόντος άρθρου.

2. Η προβλεπόμενη στο άρθρο 24 παράγραφος 2 εξουσία έκδοσης κατ' εξουσιοδότηση πράξεων ανατίθεται στην Επιτροπή για περίοδο πέντε ετών από τις 16 Ιανουαρίου 2023.

3. Η εξουσιοδότηση που προβλέπεται στο άρθρο 24 παράγραφος 2 μπορεί να ανακληθεί ανά πάσα στιγμή από το Ευρωπαϊκό Κοινοβούλιο ή το Συμβούλιο. Η απόφαση ανάκλησης περατώνει την εξουσιοδότηση που προσδιορίζεται στην εν λόγω απόφαση. Αρχίζει να ισχύει την επομένη της δημοσίευσης της απόφασης στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης* ή σε μεταγενέστερη ημερομηνία που ορίζεται σε αυτήν. Δεν θίγει το κύρος των κατ' εξουσιοδότηση πράξεων που ισχύουν ήδη.

4. Πριν από την έκδοση μιας κατ' εξουσιοδότηση πράξης, η Επιτροπή διεξάγει διαβουλεύσεις με εμπειρογνώμονες που ορίζουν τα κράτη μέλη σύμφωνα με τις αρχές της διοργανικής συμφωνίας της 13ης Απριλίου 2016 για τη βελτίωση του νομοθετικού έργου.

5. Μόλις εκδώσει μια κατ' εξουσιοδότηση πράξη, η Επιτροπή την κοινοποιεί ταυτόχρονα στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο.

6. Η κατ' εξουσιοδότηση πράξη που εκδίδεται δυνάμει του άρθρου 24 παράγραφος 2 τίθεται σε ισχύ εφόσον δεν έχει διατυπωθεί αντίρρηση από το Ευρωπαϊκό Κοινοβούλιο ή από το Συμβούλιο εντός δύο μηνών από την κοινοποίηση της εν λόγω πράξης στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο ή αν, πριν λήξει αυτή η περίοδος, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο ενημερώσουν αμφότερα την Επιτροπή ότι δεν θα προβάλουν αντιρρήσεις. Η προθεσμία αυτή παρατείνεται κατά δύο μήνες κατόπιν πρωτοβουλίας του Ευρωπαϊκού Κοινοβουλίου ή του Συμβουλίου.

Άρθρο 39

Διαδικασία επιτροπής

1. Η Επιτροπή επικουρείται από επιτροπή. Η εν λόγω επιτροπή αποτελεί επιτροπή κατά την έννοια του κανονισμού (ΕΕ) αριθ. 182/2011.

2. Όταν γίνεται παραπομπή στην παρούσα παράγραφο, εφαρμόζεται το άρθρο 5 του κανονισμού (ΕΕ) αριθ. 182/2011.

3. Αν η γνώμη της επιτροπής πρέπει να ληφθεί με γραπτή διαδικασία, η εν λόγω διαδικασία περατώνεται χωρίς αποτέλεσμα, εάν, εντός της προθεσμίας για την έκδοση γνώμης, το αποφασίσει ο πρόεδρος της επιτροπής ή το ζητήσει μέλος της επιτροπής.

ΚΕΦΑΛΑΙΟ IX

ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 40

Επανεξέταση

Έως τις 17 Οκτωβρίου 2027 και στη συνέχεια κάθε 36 μήνες, η Επιτροπή προβαίνει σε επανεξέταση της λειτουργίας της παρούσας οδηγίας και υποβάλλει έκθεση στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο. Η έκθεση αξιολογεί ιδίως τη σημασία του μεγέθους των οικείων οντοτήτων, και των τομέων, των υποτομέων και του είδους των οντοτήτων που αναφέρονται στα παραρτήματα I και II για τη λειτουργία της οικονομίας και της κοινωνίας σε σχέση με την κυβερνοασφάλεια. Για τον σκοπό αυτό και με στόχο την περαιτέρω προαγωγή της στρατηγικής και επιχειρησιακής συνεργασίας, η Επιτροπή λαμβάνει υπόψη τις εκθέσεις της Ομάδας Συνεργασίας και του δικτύου CSIRT σχετικά με την πείρα που έχει αποκτηθεί σε στρατηγικό και επιχειρησιακό επίπεδο. Η έκθεση συνοδεύεται, εφόσον είναι αναγκαίο, από νομοθετική πρόταση.

Άρθρο 41

Μεταφορά

1. Έως τις 17 Οκτωβρίου 2024, τα κράτη μέλη θεσπίζουν και δημοσιεύουν τα μέτρα που απαιτούνται προκειμένου να συμμορφωθούν προς την παρούσα οδηγία. Ενημερώνουν αμέσως την Επιτροπή σχετικά.

Εφαρμόζουν τα μέτρα αυτά από τις 18 Οκτωβρίου 2024.

2. Οι διατάξεις που αναφέρονται στην παράγραφο 1, όταν θεσπίζονται από τα κράτη μέλη, περιέχουν παραπομπή στην παρούσα οδηγία ή συνοδεύονται από την παραπομπή αυτή κατά την επίσημη δημοσίευσή τους. Ο τρόπος της παραπομπής αυτής καθορίζεται από τα κράτη μέλη.

Άρθρο 42

Τροποποιήσεις του κανονισμού (ΕΕ) αριθ. 910/2014

Στον κανονισμό (ΕΕ) αριθ. 910/2014, το άρθρο 19 απαλείφεται από τις 18 Οκτωβρίου 2024.

Άρθρο 43

Τροποποίηση της οδηγίας (ΕΕ) 2018/1972

Στην οδηγία (ΕΕ) 2018/1972, τα άρθρα 40 και 41 απαλείφονται από τις 18 Οκτωβρίου 2024.

Άρθρο 44

Κατάργηση

Η οδηγία (ΕΕ) 2016/1148 καταργείται από τις 18 Οκτωβρίου 2024.

Οι παραπομπές στην καταργούμενη οδηγία νοούνται ως παραπομπές στην παρούσα οδηγία σύμφωνα με τον πίνακα αντιστοιχίας που παρατίθεται στο παράρτημα III.

Άρθρο 45

Έναρξη ισχύος

Η παρούσα οδηγία αρχίζει να ισχύει την εικοστή ημέρα από τη δημοσίευσή της στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

Άρθρο 46

Αποδέκτες

Η παρούσα οδηγία απευθύνεται στα κράτη μέλη.

Στρασβούργο, 14 Δεκεμβρίου 2022.

Για το Ευρωπαϊκό Κοινοβούλιο	*Για το Συμβούλιο*
Η Πρόεδρος	*Ο Πρόεδρος*
R. METSOLA	M. BEK

ΠΑΡΑΡΤΗΜΑ Ι

ΤΟΜΕΙΣ ΥΨΗΛΗΣ ΚΡΙΣΙΜΟΤΗΤΑΣ

Τομέας	Υποτομέας	Είδος οντότητας
1. Ενέργεια	α) Ηλεκτρική ενέργεια	— Επιχειρήσεις ηλεκτρικής ενέργειας, όπως ορίζονται στο άρθρο 2 σημείο 57) της οδηγίας (ΕΕ) 2019/944 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([1]), οι οποίες ασκούν τη δραστηριότητα «προμήθεια», όπως ορίζεται στο άρθρο 2 σημείο 12) της εν λόγω οδηγίας
		— Διαχειριστές συστημάτων διανομής όπως ορίζονται στο άρθρο 2 σημείο 29) της οδηγίας (ΕΕ) 2019/944
		— Διαχειριστές συστημάτων μεταφοράς όπως ορίζονται στο άρθρο 2 σημείο 35) της οδηγίας (ΕΕ) 2019/944
		— Παραγωγοί όπως ορίζονται στο άρθρο 2 σημείο 38) της οδηγίας (ΕΕ) 2019/944
		— Ορισθέντες διαχειριστές αγοράς ηλεκτρικής ενέργειας, όπως ορίζονται στο άρθρο 2 σημείο 8) του κανονισμού (ΕΕ) 2019/943 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([2]) — Συμμετέχοντες στην αγορά, όπως ορίζονται στο άρθρο 2 σημείο 25) του κανονισμού (ΕΕ) 2019/943, οι οποίοι παρέχουν υπηρεσίες συγκέντρωσης, απόκρισης ζήτησης ή αποθήκευσης ενέργειας, όπως ορίζονται στο άρθρο 2 σημεία 18), 20) και 59) της οδηγίας (ΕΕ) 2019/944 — Διαχειριστές σημείου επαναφόρτισης που είναι υπεύθυνοι για τη διαχείριση και τη λειτουργία σημείου επαναφόρτισης, το οποίο παρέχει υπηρεσία επαναφόρτισης στους τελικούς χρήστες, μεταξύ άλλων εξ ονόματος και για λογαριασμό παρόχου υπηρεσιών κινητικότητας
	β) Τηλεθέρμανση και τηλεψύξη	— Διαχειριστές τηλεθέρμανσης ή τηλεψύξης, όπως ορίζονται στο άρθρο 2 σημείο 19) της οδηγίας (ΕΕ) 2018/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([3])
	γ) Πετρέλαιο	— Διαχειριστές αγωγών μεταφοράς πετρελαίου
		— Διαχειριστές παραγωγής πετρελαίου, εγκαταστάσεων διύλισης και επεξεργασίας, αποθήκευσης και μεταφοράς πετρελαίου
		— Κεντρικοί φορείς διατήρησης αποθεμάτων, όπως ορίζονται στο άρθρο 2 στοιχείο στ) της οδηγίας 2009/119/ΕΚ του Συμβουλίου ([4])
	δ) Αέριο	— Επιχειρήσεις προμήθειας όπως ορίζονται στο άρθρο 2 σημείο 8) της οδηγίας 2009/73/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([5])
		— Διαχειριστές συστημάτων διανομής όπως ορίζονται στο άρθρο 2 σημείο 6) της οδηγίας 2009/944/ΕΚ
		— Διαχειριστές συστημάτων μεταφοράς όπως ορίζονται στο άρθρο 2 σημείο 4) της οδηγίας 2009/73/ΕΚ
		— Διαχειριστές συστημάτων αποθήκευσης όπως ορίζονται στο άρθρο 2 σημείο 10) της οδηγίας 2009/73/ΕΚ
		— Διαχειριστές συστημάτων ΥΦΑ όπως ορίζονται στο άρθρο 2 σημείο 12) της οδηγίας 2009/73/ΕΚ
		— Επιχειρήσεις φυσικού αερίου όπως ορίζονται στο άρθρο 2 σημείο 1) της οδηγίας 2009/73/ΕΚ
		— Διαχειριστές εγκαταστάσεων διύλισης και επεξεργασίας φυσικού αερίου
	ε) Υδρογόνο	— Διαχειριστές παραγωγής, αποθήκευσης και μεταφοράς υδρογόνου

Τομέας	Υποτομέας	Είδος οντότητας
2. Μεταφορές	α) Εναέριες	— Αερομεταφορείς όπως ορίζονται στο άρθρο 3 σημείο 4) του κανονισμού (ΕΚ) αριθ. 300/2008, που χρησιμοποιούνται για εμπορικούς σκοπούς
		— Φορείς διαχείρισης αερολιμένα, όπως ορίζονται στο άρθρο 2 σημείο 2) της οδηγίας 2009/12/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([6]), αερολιμένες όπως ορίζονται στο άρθρο 2 σημείο 2) της εν λόγω οδηγίας, συμπεριλαμβανομένων των κεντρικών αερολιμένων που απαριθμούνται στο παράρτημα ΙΙ τμήμα 2 του κανονισμού (ΕΕ) αριθ. 1315/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([7]), και φορείς εκμετάλλευσης βοηθητικών εγκαταστάσεων που βρίσκονται εντός αερολιμένων
		— Φορείς εκμετάλλευσης ελέγχου διαχείρισης κυκλοφορίας που παρέχουν υπηρεσίες ελέγχου εναέριας κυκλοφορίας όπως ορίζονται στο άρθρο 2 σημείο 1) του κανονισμού (ΕΚ) αριθ. 549/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([8])
	β) Σιδηροδρομικές	— Διαχειριστές υποδομής όπως ορίζονται στο άρθρο 3 σημείο 2) της οδηγίας 2012/34/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([9])
		— Σιδηροδρομικές επιχειρήσεις, όπως ορίζονται στο άρθρο 3 σημείο 1) της οδηγίας 2012/34/ΕΕ, συμπεριλαμβανομένων των φορέων εκμετάλλευσης εγκαταστάσεων για την παροχή υπηρεσιών όπως ορίζονται στο άρθρο 3 σημείο 12) της εν λόγω οδηγίας
	γ) Πλωτές	— Εσωτερικές πλωτές, θαλάσσιες και ακτοπλοϊκές εταιρείες μεταφοράς επιβατών και εμπορευμάτων, όπως ορίζονται για τις θαλάσσιες μεταφορές στο παράρτημα Ι του κανονισμού (ΕΚ) αριθ. 725/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([10]), μη συμπεριλαμβανομένων των μεμονωμένων πλοίων που χρησιμοποιούνται από τις εταιρείες αυτές
		— Διαχειριστικοί φορείς των λιμένων, όπως ορίζονται στο άρθρο 3 σημείο 1) της οδηγίας 2005/65/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([11]), συμπεριλαμβανομένων των λιμενικών τους εγκαταστάσεων όπως ορίζονται στο άρθρο 2 σημείο 11) του κανονισμού (ΕΚ) αριθ. 725/2004, και φορείς εκμετάλλευσης έργων και εξοπλισμού που βρίσκονται εντός λιμένων
		— Φορείς εκμετάλλευσης υπηρεσιών εξυπηρέτησης κυκλοφορίας πλοίων (VTS), όπως ορίζονται στο άρθρο 3 στοιχείο ιε) της οδηγίας 2002/59/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([12])
	δ) Οδικές	— Οδικές αρχές, όπως ορίζονται στο άρθρο 2 σημείο 12) του κατ' εξουσιοδότηση κανονισμού (ΕΕ) 2015/962 της Επιτροπής ([13]), αρμόδιες για τον έλεγχο της διαχείρισης της κυκλοφορίας, εξαιρουμένων των δημόσιων φορέων για τους οποίους η διαχείριση της κυκλοφορίας ή η λειτουργία ευφυών συστημάτων μεταφορών αποτελεί μη ουσιώδες μέρος της γενικής δραστηριότητάς τους
		— Φορείς εκμετάλλευσης συστημάτων ευφυών μεταφορών (ITS), όπως ορίζονται στο άρθρο 4 σημείο 1) της οδηγίας 2010/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([14])
3. Τράπεζες		Πιστωτικά ιδρύματα όπως ορίζονται στο άρθρο 4 σημείο 1) του κανονισμού (ΕΕ) αριθ. 575/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([15])
4. Υποδομές χρηματοπιστωτικών αγορών		— Φορείς εκμετάλλευσης τόπων διαπραγμάτευσης, όπως ορίζονται στο άρθρο 4 σημείο 24) της οδηγίας 2014/65/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([16])
		— Κεντρικοί αντισυμβαλλόμενοι, όπως ορίζονται στο άρθρο 2 σημείο 1) του κανονισμού (ΕΕ) αριθ. 648/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([17])

Τομέας	Υποτομέας	Είδος οντότητας
5. Υγεία		— Πάροχοι υγειονομικής περίθαλψης, όπως ορίζονται στο άρθρο 3 στοιχείο ζ) της οδηγίας 2011/24/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([18])
		— Εργαστήρια αναφοράς της ΕΕ που αναφέρονται στο άρθρο 15 του κανονισμού (ΕΕ) 2022/2371 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([19])
		— Οντότητες που πραγματοποιούν δραστηριότητες έρευνας και ανάπτυξης για φάρμακα, που αναφέρονται στο άρθρο 1 σημείο 2) της οδηγίας 2001/83/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([20]) — Οντότητες που παρασκευάζουν βασικά φαρμακευτικά προϊόντα και φαρμακευτικά σκευάσματα που αναφέρονται στον τομέα Γ κλάδο 21 της NACE αναθ. 2 — Οντότητες που κατασκευάζουν ιατροτεχνολογικά προϊόντα που θεωρούνται κρίσιμης σημασίας κατά τη διάρκεια κατάστασης έκτακτης ανάγκης στον τομέα της δημόσιας υγείας (κατάλογος τεχνολογικών προϊόντων κρίσιμης σημασίας κατά τη διάρκεια κατάστασης έκτακτης ανάγκης στον τομέα της δημόσιας υγείας) κατά την έννοια του άρθρου 22 του κανονισμού (ΕΕ) 2022/123 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([21])
6. Πόσιμο νερό		Προμηθευτές και διανομείς νερού ανθρώπινης κατανάλωσης όπως ορίζονται στο άρθρο 2 σημείο 1) στοιχείο α) της οδηγίας (ΕΕ) 2020/2184 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([22]), εξαιρουμένων των διανομέων για τους οποίους η διανομή νερού ανθρώπινης κατανάλωσης αποτελεί επουσιώδες μέρος της γενικής τους δραστηριότητας διανομής λοιπών προϊόντων και αγαθών
7. Λύματα		Επιχειρήσεις συλλογής, διάθεσης ή επεξεργασίας αστικών, οικιακών ή βιομηχανικών λυμάτων που αναφέρονται στο άρθρο 2 σημεία 1), 2) και 3) της οδηγίας 91/271/ΕΟΚ του Συμβουλίου ([23]), εξαιρουμένων επιχειρήσεων για τις οποίες η συλλογή, η διάθεση ή η επεξεργασία αστικών, οικιακών ή βιομηχανικών λυμάτων αποτελεί επουσιώδες μέρος της γενικής τους δραστηριότητας.
8. Ψηφιακές υποδομές		— Πάροχοι σημείων ανταλλαγής κίνησης διαδικτύου
		— Πάροχοι υπηρεσιών συστήματος ονομάτων τομέα (DNS), εξαιρουμένων των διαχειριστών των εξυπηρετητών ονομάτων ρίζας
		— Μητρώα ονομάτων τομέα ανώτατου επιπέδου (TLD)
		— Πάροχοι υπηρεσιών υπολογιστικού νέφους
		— Πάροχοι υπηρεσιών κέντρου δεδομένων
		— Πάροχοι δικτύων διανομής περιεχομένου
		— Πάροχοι υπηρεσιών εμπιστοσύνης·
		— Πάροχοι δημόσιων δικτύων ηλεκτρονικών επικοινωνιών
		— Πάροχοι δημόσια διαθέσιμων υπηρεσιών ηλεκτρονικών επικοινωνιών
9. Διαχείριση υπηρεσιών ΤΠΕ (μεταξύ επιχειρήσεων)		— Πάροχοι διαχειριζόμενων υπηρεσιών — Πάροχοι διαχειριζόμενων υπηρεσιών ασφαλείας

Τομέας	Υποτομέας	Είδος οντότητας
10. Οντότητες δημόσιας διοίκησης		— Οντότητες δημόσιας διοίκησης της κυβέρνησης όπως ορίζονται από το κράτος μέλος σύμφωνα με το εθνικό δίκαιο
		— Οντότητες δημόσιας διοίκησης σε περιφερειακό επίπεδο όπως ορίζονται από το κράτος μέλος σύμφωνα με το εθνικό δίκαιο
11. Διάστημα		Φορείς εκμετάλλευσης επίγειας υποδομής, ιδιοκτησίας, διαχείρισης και εκμετάλλευσης από κράτη μέλη ή ιδιωτικούς φορείς, οι οποίοι υποστηρίζουν την παροχή διαστημικών υπηρεσιών, εξαιρουμένων των παρόχων δημόσιων δικτύων ηλεκτρονικών επικοινωνιών

(1) Οδηγία (ΕΕ) 2019/944 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 5ης Ιουνίου 2019, σχετικά με τους κοινούς κανόνες για την εσωτερική αγορά ηλεκτρικής ενέργειας και την τροποποίηση της οδηγίας 2012/27/ΕΕ (ΕΕ L 158 της 14.6.2019, σ. 125).

(2) Κανονισμός (ΕΕ) 2019/943 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 5ης Ιουνίου 2019, σχετικά με την εσωτερική αγορά ηλεκτρικής ενέργειας (ΕΕ L 158 της 14.6.2019, σ. 54).

(3) Οδηγία (ΕΕ) 2018/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Δεκεμβρίου 2018, για την προώθηση της χρήσης ενέργειας από ανανεώσιμες πηγές (ΕΕ L 328 της 21.12.2018, σ. 82).

(4) Οδηγία 2009/119/ΕΚ του Συμβουλίου, της 14ης Σεπτεμβρίου 2009, σχετικά με υποχρέωση διατήρησης ενός ελάχιστου επιπέδου αποθεμάτων αργού πετρελαίου ή/και προϊόντων πετρελαίου από τα κράτη μέλη (ΕΕ L 265 της 9.10.2009, σ. 9).

(5) Οδηγία 2009/73/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Ιουλίου 2009, σχετικά με τους κοινούς κανόνες για την εσωτερική αγορά φυσικού αερίου και την κατάργηση της οδηγίας 2003/55/ΕΚ (ΕΕ L 211 της 14.8.2009, σ. 94).

(6) Οδηγία 2009/12/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαρτίου 2009, για τα αερολιμενικά τέλη (ΕΕ L 70 της 14.3.2009, σ. 11).

(7) Κανονισμός (ΕΕ) αριθ. 1315/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Δεκεμβρίου 2013, περί των προσανατολισμών της Ένωσης για την ανάπτυξη του διευρωπαϊκού δικτύου μεταφορών και για την κατάργηση της απόφασης αριθ. 661/2010/ΕΕ (ΕΕ L 348 της 20.12.2013, σ. 1).

(8) Κανονισμός (ΕΚ) αριθ. 549/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 10ης Μαρτίου 2004, για τη χάραξη του πλαισίου για τη δημιουργία του Ενιαίου Ευρωπαϊκού Ουρανού (κανονισμός-πλαίσιο) (ΕΕ L 96 της 31.3.2004, σ. 1).

(9) Οδηγία 2012/34/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 21ης Νοεμβρίου 2012, για τη δημιουργία ενιαίου ευρωπαϊκού σιδηροδρομικού χώρου (ΕΕ L 343 της 14.12.2012, σ. 32).

(10) Κανονισμός (ΕΚ) αριθ. 725/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 31ης Μαρτίου 2004, για τη βελτίωση της ασφάλειας στα πλοία και στις λιμενικές εγκαταστάσεις (ΕΕ L 129 της 29.4.2004, σ. 6).

(11) Οδηγία 2005/65/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Οκτωβρίου 2005, σχετικά με την ενίσχυση της ασφαλείας των λιμένων (ΕΕ L 310 της 25.11.2005, σ. 28).

(12) Οδηγία 2002/59/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Ιουνίου 2002, για τη δημιουργία κοινοτικού συστήματος παρακολούθησης της κυκλοφορίας των πλοίων και ενημέρωσης και την κατάργηση της οδηγίας 93/75/ΕΟΚ του Συμβουλίου (ΕΕ L 208 της 5.8.2002, σ. 10).

(13) Κατ' εξουσιοδότηση κανονισμός (ΕΕ) 2015/962 της Επιτροπής, της 18ης Δεκεμβρίου 2014, για τη συμπλήρωση της οδηγίας 2010/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά την παροχή σε επίπεδο Ένωσης υπηρεσιών πληροφόρησης για την κυκλοφορία σε πραγματικό χρόνο (ΕΕ L 157 της 23.6.2015, σ. 21).

(14) Οδηγία 2010/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Ιουλίου 2010, περί πλαισίου ανάπτυξης των Συστημάτων Ευφυών Μεταφορών στον τομέα των οδικών μεταφορών και των διεπαφών με άλλους τρόπους μεταφοράς (ΕΕ L 207 της 6.8.2010, σ. 1).

(15) Κανονισμός (ΕΕ) αριθ. 575/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Ιουνίου 2013, σχετικά με τις απαιτήσεις προληπτικής εποπτείας για πιστωτικά ιδρύματα και για την τροποποίηση του κανονισμού (ΕΕ) αριθ. 648/2012 (ΕΕ L 176 της 27.6.2013, σ. 1).

(16) Οδηγία 2014/65/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαΐου 2014, για τις αγορές χρηματοπιστωτικών μέσων και την τροποποίηση της οδηγίας 2002/92/ΕΚ και της οδηγίας 2011/61/ΕΕ (ΕΕ L 173 της 12.6.2014, σ. 349).

(17) Κανονισμός (ΕΕ) αριθ. 648/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 4ης Ιουλίου 2012, για τα εξωχρηματιστηριακά παράγωγα, τους κεντρικούς αντισυμβαλλομένους και τα αρχεία καταγραφής συναλλαγών (ΕΕ L 201 της 27.7.2012, σ. 1).

(18) Οδηγία 2011/24/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Μαρτίου 2011, περί εφαρμογής των δικαιωμάτων των ασθενών στο πλαίσιο της διασυνοριακής υγειονομικής περίθαλψης (ΕΕ L 88 της 4.4.2011, σ. 45).

(19) Κανονισμός (ΕΕ) 2022/2371 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Νοεμβρίου 2022, σχετικά με σοβαρές διασυνοριακές απειλές κατά της υγείας και για την κατάργηση της απόφασης αριθ. 1082/2013/ΕΕ (ΕΕ L 314 της 6.12.2022, σ. 26).

(20) Οδηγία 2001/83/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Νοεμβρίου 2001, περί κοινοτικού κώδικος για τα φάρμακα που προορίζονται για ανθρώπινη χρήση (ΕΕ L 311 της 28.11.2001, σ. 67).

(21) Κανονισμός (ΕΕ) 2022/123 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 25ης Ιανουαρίου 2022 σχετικά με την ενίσχυση του ρόλου του Ευρωπαϊκού Οργανισμού Φαρμάκων όσον αφορά την ετοιμότητα έναντι κρίσεων και τη διαχείριση κρίσεων για τα φάρμακα και τα ιατροτεχνολογικά προϊόντα (ΕΕ L 20 της 31.1.2022, σ. 1).

(22) Οδηγία (ΕΕ) 2020/2184 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 16ης Δεκεμβρίου 2020, σχετικά με την ποιότητα του νερού ανθρώπινης κατανάλωσης (ΕΕ L 435 της 23.12.2020, σ. 1).

(23) Οδηγία 91/271/ΕΟΚ του Συμβουλίου, της 21ης Μαΐου 1991, για την επεξεργασία των αστικών λυμάτων (ΕΕ L 135 της 30.5.1991, σ. 40).

ΠΑΡΑΡΤΗΜΑ II

ΑΛΛΟΙ ΚΡΙΣΙΜΟΙ ΤΟΜΕΙΣ

Τομέας	Υποτομέας	Είδος οντότητας
1. Ταχυδρομικές υπηρεσίες και υπηρεσίες ταχυμεταφορών		Φορείς παροχής ταχυδρομικών υπηρεσιών όπως ορίζονται στο άρθρο 2 σημείο 1α) της οδηγίας 97/67/ΕΚ, συμπεριλαμβανομένων παρόχων υπηρεσιών ταχυμεταφορών
2. Διαχείριση αποβλήτων		Επιχειρήσεις διαχείρισης αποβλήτων όπως ορίζονται στο άρθρο 3 σημείο 9) της οδηγίας 2008/98/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([1]), με εξαίρεση τις επιχειρήσεις για τις οποίες η διαχείριση αποβλήτων δεν αποτελεί την κύρια οικονομική δραστηριότητα
3. Παρασκευή, παραγωγή και διανομή χημικών προϊόντων		Επιχειρήσεις που ασχολούνται με την παρασκευή ουσιών και τη διανομή ουσιών ή μειγμάτων, όπως αναφέρεται στο άρθρο 3 σημεία 9) και 14) του κανονισμού (ΕΚ) αριθ. 1907/2006 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([2]), και επιχειρήσεις που παράγουν αντικείμενα, όπως ορίζονται στο άρθρο 3 σημείο 3) του εν λόγω κανονισμού, από ουσίες ή μείγματα
4. Παραγωγή, μεταποίηση και διανομή τροφίμων		Επιχειρήσεις τροφίμων, όπως ορίζονται στο άρθρο 3 σημείο 2) του κανονισμού (ΕΚ) αριθ. 178/2002 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([3]), οι οποίες δραστηριοποιούνται στη χονδρική διανομή και τη βιομηχανική παραγωγή και μεταποίηση
5. Κατασκευαστικός τομέας	α) Κατασκευή ιατροτεχνολογικών προϊόντων και in vitro διαγνωστικών ιατροτεχνολογικών προϊόντων	Οντότητες που κατασκευάζουν ιατροτεχνολογικά προϊόντα, όπως ορίζονται στο άρθρο 2 σημείο 1) του κανονισμού (ΕΕ) 2017/745 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([4]), και οντότητες που κατασκευάζουν in vitro διαγνωστικά ιατροτεχνολογικά προϊόντα, όπως ορίζονται στο άρθρο 2 σημείο 2) του κανονισμού (ΕΕ) 2017/746 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([5]), εξαιρουμένων των οντοτήτων που κατασκευάζουν ιατροτεχνολογικά προϊόντα που αναφέρονται στο παράρτημα I σημείο 5 πέμπτη περίπτωση της παρούσας οδηγίας
	β) Κατασκευή προϊόντων υπολογιστών, ηλεκτρονικών και οπτικών προϊόντων	Επιχειρήσεις που ασκούν οικονομικές δραστηριότητες που αναφέρονται στον τομέα Γ κλάδο 26 της NACE αναθ. 2
	γ) Κατασκευή ηλεκτρολογικού εξοπλισμού	Επιχειρήσεις που ασκούν οικονομικές δραστηριότητες που αναφέρονται στον τομέα Γ κλάδο 27 της NACE αναθ. 2
	δ) Κατασκευή μηχανημάτων και εξοπλισμού π.δ.κ.α.	Επιχειρήσεις που ασκούν οικονομικές δραστηριότητες που αναφέρονται στον τομέα Γ κλάδο 28 της NACE αναθ. 2
	ε) Κατασκευή μηχανοκίνητων οχημάτων, ρυμουλκούμενων και ημιρυμουλκούμενων	Επιχειρήσεις που ασκούν οικονομικές δραστηριότητες που αναφέρονται στον τομέα Γ κλάδο 29 της NACE αναθ. 2
	στ) Κατασκευή άλλου εξοπλισμού μεταφορών	Επιχειρήσεις που ασκούν οικονομικές δραστηριότητες που αναφέρονται στον τομέα Γ κλάδο 30 της NACE αναθ. 2

Τομέας	Υποτομέας	Είδος οντότητας
6. Ψηφιακοί πάροχοι		— Πάροχοι επιγραμμικών αγορών
		— Πάροχοι επιγραμμικών μηχανών αναζήτησης
		— Πάροχοι πλατφόρμας υπηρεσιών κοινωνικής δικτύωσης
7. Έρευνα		Οργανισμοί έρευνας

(1) Οδηγία 2008/98/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 19ης Νοεμβρίου 2008, για τα απόβλητα και την κατάργηση ορισμένων οδηγιών (ΕΕ L 312 της 22.11.2008, σ. 3).

(2) Κανονισμός (ΕΚ) αριθ. 1907/2006 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Δεκεμβρίου 2006, για την καταχώριση, την αξιολόγηση, την αδειοδότηση και τους περιορισμούς των χημικών προϊόντων (REACH) και για την ίδρυση του Ευρωπαϊκού Οργανισμού Χημικών Προϊόντων καθώς και για την τροποποίηση της οδηγίας 1999/45/ΕΚ και για την κατάργηση του κανονισμού (ΕΟΚ) αριθ. 793/93 του Συμβουλίου και του κανονισμού (ΕΚ) αριθ. 1488/94 της Επιτροπής καθώς και της οδηγίας 76/769/ΕΟΚ του Συμβουλίου και των οδηγιών της Επιτροπής 91/155/ΕΟΚ, 93/67/ΕΟΚ, 93/105/ΕΚ και 2000/21/ΕΚ (ΕΕ L 396 της 30.12.2006, σ. 1).

(3) Κανονισμός (ΕΚ) αριθ. 178/2002 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 28ης Ιανουαρίου 2002, για τον καθορισμό των γενικών αρχών και απαιτήσεων της νομοθεσίας για τα τρόφιμα, για την ίδρυση της Ευρωπαϊκής Αρχής για την Ασφάλεια των Τροφίμων και τον καθορισμό διαδικασιών σε θέματα ασφαλείας των τροφίμων (ΕΕ L 31 της 1.2.2002, σ. 1).

(4) Κανονισμός (ΕΕ) 2017/745 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 5ης Απριλίου 2017, για τα ιατροτεχνολογικά προϊόντα, για την τροποποίηση της οδηγίας 2001/83/ΕΚ, του κανονισμού (ΕΚ) αριθ. 178/2002 και του κανονισμού (ΕΚ) αριθ. 1223/2009 και για την κατάργηση των οδηγιών του Συμβουλίου 90/385/ΕΟΚ και 93/42/ΕΟΚ (ΕΕ L 117 της 5.5.2017, σ. 1)

(5) Κανονισμός (ΕΕ) 2017/746 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 5ης Απριλίου 2017, για τα in vitro διαγνωστικά ιατροτεχνολογικά προϊόντα και για την κατάργηση της οδηγίας 98/79/ΕΚ και της απόφασης 2010/227/ΕΕ της Επιτροπής (ΕΕ L 117 της 5.5.2017, σ. 176).

ΠΑΡΑΡΤΗΜΑ III

ΠΙΝΑΚΑΣ ΑΝΤΙΣΤΟΙΧΙΑΣ

Οδηγία (ΕΕ) 2016/1148	Παρούσα οδηγία
Άρθρο 1 παράγραφος 1	Άρθρο 1 παράγραφος 1
Άρθρο 1 παράγραφος 2	Άρθρο 1 παράγραφος 2
Άρθρο 1 παράγραφος 3	-
Άρθρο 1 παράγραφος 4	Άρθρο 2 παράγραφος 12
Άρθρο 1 παράγραφος 5	Άρθρο 2 παράγραφος 13
Άρθρο 1 παράγραφος 6	Άρθρο 2 παράγραφοι 6 και 11
Άρθρο 1 παράγραφος 7	Άρθρο 4
Άρθρο 2	Άρθρο 2 παράγραφος 14
Άρθρο 3	Άρθρο 5
Άρθρο 4	Άρθρο 6
Άρθρο 5	-
Άρθρο 6	-
Άρθρο 7 παράγραφος 1	Άρθρο 7 παράγραφοι 1 και 2
Άρθρο 7 παράγραφος 2	Άρθρο 7 παράγραφος 4
Άρθρο 7 παράγραφος 3	Άρθρο 7 παράγραφος 3
Άρθρο 8 παράγραφοι 1 έως 5	Άρθρο 8 παράγραφοι 1 έως 5
Άρθρο 8 παράγραφος 6	Άρθρο 13 παράγραφος 4
Άρθρο 8 παράγραφος 7	Άρθρο 8 παράγραφος 6
Άρθρο 9 παράγραφοι 1, 2 και 3	Άρθρο 10 παράγραφοι 1, 2 και 3
Άρθρο 9 παράγραφος 4	Άρθρο 10 παράγραφος 9
Άρθρο 9 παράγραφος 5	Άρθρο 10 παράγραφος 10
Άρθρο 10 παράγραφοι 1, 2 και 3 πρώτο εδάφιο	Άρθρο 13 παράγραφοι 1, 2 και 3
Άρθρο 10 παράγραφος 3 δεύτερο εδάφιο	Άρθρο 23 παράγραφος 9
Άρθρο 11 παράγραφος 1	Άρθρο 14 παράγραφοι 1 και 2
Άρθρο 11 παράγραφος 2	Άρθρο 14 παράγραφος 3
Άρθρο 11 παράγραφος 3	Άρθρο 14 παράγραφος 4 πρώτο εδάφιο στοιχεία α) έως ιη) και παράγραφος 7
Άρθρο 11 παράγραφος 4	Άρθρο 14 παράγραφος 4 πρώτο εδάφιο στοιχείο ιη) και δεύτερο εδάφιο
Άρθρο 11 παράγραφος 5	Άρθρο 14 παράγραφος 8
Άρθρο 12 παράγραφοι 1 έως 5	Άρθρο 15 παράγραφοι 1 έως 5
Άρθρο 13	Άρθρο 17
Άρθρο 14 παράγραφοι 1 και 2	Άρθρο 21 παράγραφοι 1 έως 4
Άρθρο 14 παράγραφος 3	Άρθρο 23 παράγραφος 1
Άρθρο 14 παράγραφος 4	Άρθρο 23 παράγραφος 3
Άρθρο 14 παράγραφος 5	Άρθρο 23 παράγραφοι 5, 6 και 8

Οδηγία (ΕΕ) 2016/1148	Παρούσα οδηγία
Άρθρο 14 παράγραφος 6	Άρθρο 23 παράγραφος 7
Άρθρο 14 παράγραφος 7	Άρθρο 23 παράγραφος 11
Άρθρο 15 παράγραφος 1	Άρθρο 31 παράγραφος 1
Άρθρο 15 παράγραφος 2 πρώτο εδάφιο στοιχείο α)	Άρθρο 32 παράγραφος 2 στοιχείο ε)
Άρθρο 15 παράγραφος 2 πρώτο εδάφιο στοιχείο β)	Άρθρο 32 παράγραφος 2 στοιχείο ζ)
Άρθρο 15 παράγραφος 2 δεύτερο εδάφιο	Άρθρο 32 παράγραφος 3
Άρθρο 15 παράγραφος 3	Άρθρο 32 παράγραφος 4 στοιχείο β)
Άρθρο 15 παράγραφος 4	Άρθρο 31 παράγραφος 3
Άρθρο 16 παράγραφοι 1 και 2	Άρθρο 21 παράγραφοι 1 έως 4
Άρθρο 16 παράγραφος 3	Άρθρο 23 παράγραφος 1
Άρθρο 16 παράγραφος 4	Άρθρο 23 παράγραφος 3
Άρθρο 16 παράγραφος 5	-
Άρθρο 16 παράγραφος 6	Άρθρο 23 παράγραφος 6
Άρθρο 16 παράγραφος 7	Άρθρο 23 παράγραφος 7
Άρθρο 16 παράγραφοι 8 και 9	Άρθρο 21 παράγραφος 5 και άρθρο 23 παράγραφος 11
Άρθρο 16 παράγραφος 10	-
Άρθρο 16 παράγραφος 11	Άρθρο 2 παράγραφοι 1, 2 και 3
Άρθρο 17 παράγραφος 1	Άρθρο 33 παράγραφος 1
Άρθρο 17 παράγραφος 2 στοιχείο α)	Άρθρο 32 παράγραφος 2 στοιχείο ε)
Άρθρο 17 παράγραφος 2 στοιχείο β)	Άρθρο 32 παράγραφος 4 στοιχείο β)
Άρθρο 17 παράγραφος 3	Άρθρο 37 παράγραφος 1 στοιχεία α) και β)
Άρθρο 18 παράγραφος 1	Άρθρο 26 παράγραφος 1 στοιχείο β) και παράγραφος 2
Άρθρο 18 παράγραφος 2	Άρθρο 26 παράγραφος 3
Άρθρο 18 παράγραφος 3	Άρθρο 26 παράγραφος 4
Άρθρο 19	Άρθρο 25
Άρθρο 20	Άρθρο 30
Άρθρο 21	Άρθρο 36
Άρθρο 22	Άρθρο 39
Άρθρο 23	Άρθρο 40
Άρθρο 24	-
Άρθρο 25	Άρθρο 41
Άρθρο 26	Άρθρο 45
Άρθρο 27	Άρθρο 46
Παράρτημα 1 σημείο 1	Άρθρο 11 παράγραφος 1
Παράρτημα Ι σημείο 2 στοιχείο α) σημεία i) έως iv)	Άρθρο 11 παράγραφος 2 στοιχεία α) έως δ)

Οδηγία (ΕΕ) 2016/1148	Παρούσα οδηγία
Παράρτημα I σημείο 2 στοιχείο α) σημείο v)	Άρθρο 11 παράγραφος 2 στοιχείο στ)
Παράρτημα I σημείο 2 στοιχείο β)	Άρθρο 11 παράγραφος 4
Παράρτημα I σημείο 2 στοιχείο γ) σημεία i) και ii)	Άρθρο 11 παράγραφος 5 στοιχείο α)
Παράρτημα II	Παράρτημα I
Παράρτημα III σημεία 1 και 2	Παράρτημα II σημείο 6
Παράρτημα III σημείο 3	Παράρτημα I σημείο 8

ΟΔΗΓΙΑ (ΕΕ) 2022/2556 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

της 14ης Δεκεμβρίου 2022

για την τροποποίηση των οδηγιών 2009/65/ΕΚ, 2009/138/ΕΚ, 2011/61/ΕΕ, 2013/36/ΕΕ, 2014/59/ΕΕ, 2014/65/ΕΕ, (ΕΕ) 2015/2366 και (ΕΕ) 2016/2341 όσον αφορά την ψηφιακή επιχειρησιακή ανθεκτικότητα για τον χρηματοοικονομικό τομέα

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης, και ιδίως το άρθρο 53 παράγραφος 1 και το άρθρο 114,

Έχοντας υπόψη την πρόταση της Ευρωπαϊκής Επιτροπής,

Κατόπιν διαβίβασης του σχεδίου νομοθετικής πράξης στα εθνικά κοινοβούλια,

Έχοντας υπόψη τη γνώμη της Ευρωπαϊκής Κεντρικής Τράπεζας ([1]),

Έχοντας υπόψη τη γνωμοδότηση της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής ([2]),

Αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία ([3]),

Εκτιμώντας τα ακόλουθα:

(1) Η Ένωση χρειάζεται να αντιμετωπίσει με κατάλληλο και σφαιρικό τρόπο τους ψηφιακούς κινδύνους στους οποίους εκτίθενται όλες οι χρηματοοικονομικές οντότητες και οι οποίοι απορρέουν από την αυξημένη χρήση τεχνολογιών των πληροφοριών και των επικοινωνιών (ΤΠΕ) κατά την παροχή και την κατανάλωση χρηματοοικονομικών υπηρεσιών, προκειμένου να συμβάλει στην αξιοποίηση των δυνατοτήτων του ψηφιακού χρηματοοικονομικού τομέα όσον αφορά την ενίσχυση της καινοτομίας και την προώθηση του ανταγωνισμού σε ένα ασφαλές ψηφιακό περιβάλλον.

(2) Οι χρηματοοικονομικές οντότητες εξαρτώνται σε μεγάλο βαθμό από τη χρήση ψηφιακών τεχνολογιών στις καθημερινές δραστηριότητές τους. Είναι, συνεπώς, εξαιρετικά σημαντικό να διασφαλιστεί η επιχειρησιακή ανθεκτικότητα των ψηφιακών δραστηριοτήτων τους έναντι των κινδύνων ΤΠΕ. Η ανάγκη αυτή έχει καταστεί ακόμη πιο επιτακτική λόγω της ανάπτυξης πρωτοποριακών τεχνολογιών στην αγορά, ιδίως τεχνολογιών που επιτρέπουν τη μεταβίβαση και την ηλεκτρονική αποθήκευση ψηφιακών αναπαραστάσεων αξίας ή δικαιωμάτων, με τη χρήση τεχνολογίας κατανεμημένου καθολικού ή παρόμοιας τεχνολογίας (κρυπτοστοιχεία), και λόγω της ανάπτυξης υπηρεσιών που σχετίζονται με τα εν λόγω περιουσιακά στοιχεία.

([1]) ΕΕ C 343 της 26.8.2021, σ. 1.
([2]) ΕΕ C 155 της 30.4.2021, σ. 38.
([3]) Θέση του Ευρωπαϊκού Κοινοβουλίου της 10ης Νοεμβρίου 2022 (δεν έχει ακόμη δημοσιευθεί στην Επίσημη Εφημερίδα) και απόφαση του Συμβουλίου της 28ης Νοεμβρίου 2022.

(3) Σε επίπεδο Ένωσης, οι απαιτήσεις σχετικά με τη διαχείριση των κινδύνων ΤΠΕ στον χρηματοοικονομικό τομέα ορίζονται στις οδηγίες 2009/65/ΕΚ ([4]), 2009/138/ΕΚ ([5]), 2011/61/ΕΕ ([6]), 2013/36/ΕΕ ([7]), 2014/59/ΕΕ ([8]), 2014/65/ΕΕ ([9]), (ΕΕ) 2015/2366 ([10]) και (ΕΕ) 2016/2341 ([11]) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

Οι εν λόγω απαιτήσεις είναι ανομοιογενείς και ενίοτε ελλιπείς. Σε ορισμένες περιπτώσεις, οι κίνδυνοι ΤΠΕ έχουν αντιμετωπιστεί μόνο εμμέσως, στο πλαίσιο του λειτουργικού κινδύνου και σε άλλες περιπτώσεις δεν έχουν αντιμετωπιστεί καθόλου. Τα εν λόγω ζητήματα επανορθώνονται με την έκδοση του κανονισμού (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([12]). Οι εν λόγω οδηγίες θα πρέπει, συνεπώς, να τροποποιηθούν για να διασφαλιστεί συνέπεια με τον εν λόγω κανονισμό. Η παρούσα οδηγία θεσπίζει ένα σύνολο τροποποιήσεων που είναι απαραίτητες για να εξασφαλιστεί νομική σαφήνεια και συνοχή σε σχέση με την εφαρμογή, από τις χρηματοοικονομικές οντότητες που έχουν λάβει άδεια λειτουργίας και εποπτεύονται σύμφωνα με τις εν λόγω οδηγίες, διάφορων απαιτήσεων ψηφιακής επιχειρησιακής ανθεκτικότητας που είναι απαραίτητες για την άσκηση των δραστηριοτήτων τους και για την παροχή υπηρεσιών, διασφαλίζοντας με τον τρόπο αυτόν την ομαλή λειτουργία της εσωτερικής αγοράς. Είναι αναγκαίο να διασφαλιστεί η επάρκεια των εν λόγω απαιτήσεων σε σχέση με τις εξελίξεις της αγοράς και παράλληλα να ενθαρρυνθεί η αναλογικότητα ιδίως όσον αφορά το μέγεθος των χρηματοοικονομικών οντοτήτων και τα ειδικά καθεστώτα στα οποία υπάγονται, με στόχο τη μείωση του κόστους συμμόρφωσης.

(4) Στον τομέα των τραπεζικών υπηρεσιών, η οδηγία 2013/36/ΕΕ ορίζει, επί του παρόντος, μόνο γενικούς κανόνες εσωτερικής διακυβέρνησης και διατάξεις για τους λειτουργικούς κινδύνους που περιέχουν απαιτήσεις για σχέδια αντιμετώπισης επειγουσών καταστάσεων και επιχειρησιακής συνέχειας, τα οποία, εμμέσως, χρησιμεύουν ως βάση για την αντιμετώπιση των κινδύνων ΤΠΕ. Ωστόσο, προκειμένου να αντιμετωπίζονται ρητά και σαφώς οι κίνδυνοι ΤΠΕ, οι απαιτήσεις για σχέδια αντιμετώπισης επειγουσών καταστάσεων και επιχειρησιακής συνέχειας θα πρέπει να τροποποιηθούν ώστε να συμπεριλάβουν επίσης σχέδια επιχειρησιακής συνέχειας και σχέδια αντιμετώπισης και ανάκαμψης όσον αφορά τους κινδύνους ΤΠΕ, σύμφωνα με τις απαιτήσεις που ορίζονται στον κανονισμό (ΕΕ) 2022/2554 Επιπλέον, οι κίνδυνοι ΤΠΕ περιλαμβάνονται μόνο έμμεσα, ως μέρος των λειτουργικών κινδύνων, στη διαδικασία εποπτικού ελέγχου και αξιολόγησης (ΔΕΕΑ) που διενεργούν οι αρμόδιες αρχές και τα κριτήρια για την αξιολόγησή τους καθορίζονται επί του παρόντος στις κατευθυντήριες γραμμές σχετικά με την αξιολόγηση κινδύνων ΤΠΕ σύμφωνα με τη διαδικασία εποπτικού ελέγχου και αξιολόγησης (ΔΕΕΑ), που εκδόθηκαν από την Ευρωπαϊκή Εποπτική Αρχή (Ευρωπαϊκή Αρχή Τραπεζών) (ΕΑΤ), η οποία συγκροτήθηκε με τον κανονισμό (ΕΕ) αριθ. 1093/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([13]). Προκειμένου να εξασφαλιστεί νομική σαφήνεια και να διασφαλιστεί ότι οι εποπτικές αρχές των τραπεζών εντοπίζουν αποτελεσματικά τους κινδύνους ΤΠΕ

([4]) Οδηγία 2009/65/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Ιουλίου 2009, για τον συντονισμό των νομοθετικών, κανονιστικών και διοικητικών διατάξεων σχετικά με ορισμένους οργανισμούς συλλογικών επενδύσεων σε κινητές αξίες (ΟΣΕΚΑ) (ΕΕ L 302 της 17.11.2009, σ. 32).

([5]) Οδηγία 2009/138/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2009, σχετικά με την ανάληψη και την άσκηση δραστηριοτήτων ασφάλισης και αντασφάλισης (Φερεγγυότητα ΙΙ) (ΕΕ L 335 της 17.12.2009, σ. 1).

([6]) Οδηγία 2011/61/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 8ης Ιουνίου 2011, σχετικά με τους διαχειριστές οργανισμών εναλλακτικών επενδύσεων και για την τροποποίηση των οδηγιών 2003/41/ΕΚ και 2009/65/ΕΚ και των κανονισμών (ΕΚ) αριθ. 1060/2009 και (ΕΕ) αριθ. 1095/2010 (ΕΕ L 174 της 1.7.2011, σ. 1).

([7]) Οδηγία 2013/36/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Ιουνίου 2013, σχετικά με την πρόσβαση στη δραστηριότητα των πιστωτικών ιδρυμάτων και την προληπτική εποπτεία των πιστωτικών ιδρυμάτων, την τροποποίηση της οδηγίας 2002/87/ΕΚ και την κατάργηση των οδηγιών 2006/48/ΕΚ και 2006/49/ΕΚ (ΕΕ L 176 της 27.6.2013, σ. 338).

([8]) Οδηγία 2014/59/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαΐου 2014, για τη θέσπιση πλαισίου για την ανάκαμψη και την εξυγίανση πιστωτικών ιδρυμάτων και επιχειρήσεων επενδύσεων και για την τροποποίηση της οδηγίας 82/891/ΕΟΚ του Συμβουλίου, και των οδηγιών 2001/24/ΕΚ, 2002/47/ΕΚ, 2004/25/ΕΚ, 2005/56/ΕΚ, 2007/36/ΕΚ, 2011/35/ΕΕ, 2012/30/ΕΕ και 2013/36/ΕΕ, καθώς και των κανονισμών του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (ΕΕ) αριθ. 1093/2010 και (ΕΕ) αριθ. 648/2012 (ΕΕ L 173 της 12.6.2014, σ. 190).

([9]) Οδηγία 2014/65/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαΐου 2014, για τις αγορές χρηματοπιστωτικών μέσων και την τροποποίηση της οδηγίας 2002/92/ΕΚ και της οδηγίας 2011/61/ΕΕ (ΕΕ L 173 της 12.6.2014, σ. 349).

([10]) Οδηγία (ΕΕ) 2015/2366 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2015, σχετικά με υπηρεσίες πληρωμών στην εσωτερική αγορά, την τροποποίηση των οδηγιών 2002/65/ΕΚ, 2009/110/ΕΚ και 2013/36/ΕΕ και του κανονισμού (ΕΕ) αριθ. 1093/2010 και την κατάργηση της οδηγίας 2007/64/ΕΚ (ΕΕ L 337 της 23.12.2015, σ. 35).

([11]) Οδηγία (ΕΕ) 2016/2341 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2016, για τις δραστηριότητες και την εποπτεία των ιδρυμάτων επαγγελματικών συνταξιοδοτικών παροχών (ΙΕΣΠ) (ΕΕ L 354 της 23.12.2016, σ. 37).

([12]) Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (βλέπε σελίδα 1 της παρούσας Επίσημης Εφημερίδας).

([13]) Κανονισμός (ΕΕ) αριθ. 1093/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Νοεμβρίου 2010, σχετικά με τη σύσταση Ευρωπαϊκής Εποπτικής Αρχής (Ευρωπαϊκή Αρχή Τραπεζών), την τροποποίηση της απόφασης αριθ. 716/2009/ΕΚ και την κατάργηση της απόφασης 2009/78/ΕΚ της Επιτροπής (ΕΕ L 331 της 15.12.2010, σ. 12).

και παρακολουθούν τη διαχείρισή τους από τις χρηματοοικονομικές οντότητες, σύμφωνα με το νέο πλαίσιο για την ψηφιακή επιχειρησιακή ανθεκτικότητα, το πεδίο εφαρμογής της ΔΕΕΑ θα πρέπει επίσης να τροποποιηθεί ώστε να αναφέρει ρητά τις απαιτήσεις που ορίζονται στον κανονισμό (ΕΕ) 2022/2554 και να καλύπτει ιδίως τους κινδύνους που εντοπίζονται στις αναφορές σημαντικών συμβάντων που σχετίζονται με τις ΤΠΕ και στα αποτελέσματα των δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας που διενεργούνται από χρηματοοικονομικές οντότητες σύμφωνα με τον εν λόγω κανονισμό.

(5) Η ψηφιακή επιχειρησιακή ανθεκτικότητα είναι απαραίτητη για τη διατήρηση των κρίσιμων λειτουργιών και των βασικών επιχειρηματικών τομέων μιας χρηματοοικονομικής οντότητας σε περίπτωση εξυγίανσης και, ως εκ τούτου, για την αποφυγή διαταραχών στην πραγματική οικονομία και στο χρηματοοικονομικό σύστημα. Τα σημαντικά επιχειρησιακά συμβάντα μπορεί να παρεμποδίσουν την ικανότητα μιας χρηματοοικονομικής οντότητας να συνεχίσει τη λειτουργία της και μπορεί να θέσουν σε κίνδυνο τους στόχους της εξυγίανσης. Ορισμένες συμβατικές ρυθμίσεις για τη χρήση υπηρεσιών ΤΠΕ είναι απαραίτητες για τη διασφάλιση της επιχειρησιακής συνέχειας και για την παροχή των απαραίτητων δεδομένων σε περίπτωση εξυγίανσης. Προκειμένου να εξασφαλιστεί η ευθυγράμμιση προς τους στόχους του ενωσιακού πλαισίου για την επιχειρησιακή ανθεκτικότητα, η οδηγία 2014/59/ΕΕ θα πρέπει να τροποποιηθεί ανάλογα, ώστε να διασφαλίζεται ότι οι πληροφορίες σχετικά με την επιχειρησιακή ανθεκτικότητα λαμβάνονται υπόψη στο πλαίσιο του σχεδιασμού της εξυγίανσης και της αξιολόγησης της δυνατότητας εξυγίανσης των χρηματοοικονομικών οντοτήτων.

(6) Η οδηγία 2014/65/ΕΕ ορίζει αυστηρότερους κανόνες κινδύνων ΤΠΕ για τις επιχειρήσεις επενδύσεων και τους τόπους διαπραγμάτευσης που συμμετέχουν σε αλγοριθμικές συναλλαγές. Για τις υπηρεσίες αναφοράς δεδομένων και για τα αρχεία καταγραφής συναλλαγών ισχύουν λιγότερο λεπτομερείς απαιτήσεις. Επίσης, η οδηγία 2014/65/ΕΕ περιέχει μόνο περιορισμένες αναφορές σε μηχανισμούς ελέγχου και ασφάλειας των συστημάτων ηλεκτρονικής επεξεργασίας δεδομένων και στη χρήση κατάλληλων συστημάτων, πόρων και διαδικασιών για τη διασφάλιση της συνέχειας και της κανονικότητας των επιχειρηματικών υπηρεσιών. Επιπλέον, η εν λόγω οδηγία θα πρέπει να ευθυγραμμιστεί με τον κανονισμό (ΕΕ) 2022/2554 όσον αφορά τη συνεχή και τακτική παροχή επενδυτικών υπηρεσιών και την εκτέλεση επενδυτικών δραστηριοτήτων, την επιχειρησιακή ανθεκτικότητα, την ικανότητα των συστημάτων διαπραγμάτευσης και την αποτελεσματικότητα των ρυθμίσεων επιχειρησιακής συνέχειας και της διαχείρισης κινδύνων.

(7) Η οδηγία (ΕΕ) 2015/2366 ορίζει ειδικούς κανόνες για τους ελέγχους ασφάλειας των ΤΠΕ και στοιχεία μετριασμού για τους σκοπούς της απόκτησης άδειας παροχής υπηρεσιών πληρωμών. Οι εν λόγω κανόνες για τη χορήγηση άδειας θα πρέπει να τροποποιηθούν προκειμένου να ευθυγραμμιστούν με τον κανονισμό (ΕΕ) 2022/2554 Επιπλέον, προκειμένου να μειωθεί ο διοικητικός φόρτος και να αποφευχθούν η πολυπλοκότητα και οι αλληλεπικαλυπτόμενες απαιτήσεις υποβολής αναφορών, οι κανόνες αναφοράς συμβάντων που ορίζει η εν λόγω οδηγία θα πρέπει να παύσουν να εφαρμόζονται για τους παρόχους υπηρεσιών πληρωμών που ρυθμίζονται βάσει της εν λόγω οδηγίας και υπόκεινται επίσης στον κανονισμό (ΕΕ) 2022/2554, επιτρέποντας έτσι στους εν λόγω παρόχους υπηρεσιών πληρωμών να επωφελούνται από ενιαίο, πλήρως εναρμονισμένο μηχανισμό αναφοράς συμβάντων όσον αφορά όλα τα λειτουργικά συμβάντα ή συμβάντα ασφάλειας που σχετίζονται με πληρωμές, ανεξάρτητα αν τα εν λόγω συμβάντα σχετίζονται με τις ΤΠΕ.

(8) Οι οδηγίες 2009/138/ΕΚ και (ΕΕ) 2016/2341 αποτυπώνουν εν μέρει τους κινδύνους ΤΠΕ στις γενικές διατάξεις τους για τη διακυβέρνηση και τη διαχείριση κινδύνων, αφήνοντας ορισμένες απαιτήσεις να καθοριστούν με κατ' εξουσιοδότηση πράξεις με ή χωρίς ειδικές αναφορές στους κινδύνους ΤΠΕ. Ομοίως, για τους διαχειριστές οργανισμών εναλλακτικών επενδύσεων που υπόκεινται στην οδηγία 2011/61/ΕΕ και τις εταιρείες διαχείρισης που υπόκεινται στην οδηγία 2009/65/ΕΚ ισχύουν μόνο πολύ γενικοί κανόνες. Συνεπώς, οι εν λόγω οδηγίες θα πρέπει να ευθυγραμμιστούν με τις απαιτήσεις που ορίζονται στον κανονισμό (ΕΕ) 2022/2554 όσον αφορά τη διαχείριση συστημάτων και εργαλείων ΤΠΕ.

(9) Σε πολλές περιπτώσεις, έχουν ήδη θεσπιστεί περαιτέρω απαιτήσεις κινδύνων ΤΠΕ σε κατ' εξουσιοδότηση και εκτελεστικές πράξεις, που έχουν εκδοθεί βάσει σχεδίων ρυθμιστικών τεχνικών προτύπων και σχεδίων εκτελεστικών τεχνικών προτύπων που έχει καταρτίσει η αρμόδια Ευρωπαϊκή Εποπτική Αρχή. Καθώς οι διατάξεις του κανονισμού (ΕΕ) 2022/2554 συνιστούν στο εξής το νομικό πλαίσιο για τους κινδύνους ΤΠΕ στον χρηματοοικονομικό τομέα, ορισμένες εξουσιοδοτήσεις για την έκδοση κατ' εξουσιοδότηση και εκτελεστικών πράξεων στις οδηγίες 2009/65/ΕΚ, 2009/138/ΕΚ, 2011/61/ΕΕ και 2014/65/ΕΕ θα πρέπει να τροποποιηθούν, ώστε να αφαιρεθούν οι διατάξεις για τους κινδύνους ΤΠΕ από το πεδίο εφαρμογής των εν λόγω εξουσιοδοτήσεων.

(10) Προκειμένου να διασφαλιστεί η συνεπής εφαρμογή του νέου πλαισίου για την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα, τα κράτη μέλη θα πρέπει να εφαρμόσουν τις διατάξεις του εθνικού δικαίου που μεταφέρουν την παρούσα οδηγία στο εθνικό δίκαιο από την ημερομηνία εφαρμογής του κανονισμού (ΕΕ) 2022/2554

(11) Οι οδηγίες 2009/65/ΕΚ, 2009/138/ΕΚ, 2011/61/ΕΕ, 2013/36/ΕΕ, 2014/59/ΕΕ, 2014/65/ΕΕ, (ΕΕ) 2015/2366 και (ΕΕ) 2016/2341 έχουν εκδοθεί βάσει του άρθρου 53 παράγραφος 1 ή του άρθρου 114 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ) ή αμφοτέρων. Δεδομένου ότι το αντικείμενο και οι στόχοι των τροποποιήσεων είναι αλληλένδετα, οι τροποποιήσεις της παρούσας οδηγίας έχουν συμπεριληφθεί σε ενιαία νομοθετική πράξη. Επομένως, η παρούσα οδηγία θα πρέπει να εκδοθεί βάσει του άρθρου 53 παράγραφος 1 και του άρθρου 114 ΣΛΕΕ.

(12) Δεδομένου ότι οι στόχοι της παρούσας οδηγίας δεν μπορούν να επιτευχθούν ικανοποιητικά από τα κράτη μέλη, καθώς προϋποθέτουν την εναρμόνιση των απαιτήσεων που περιλαμβάνονται ήδη σε οδηγίες, μπορούν όμως, λόγω της κλίμακας και των επιπτώσεων της δράσης, να επιτευχθούν καλύτερα σε επίπεδο Ένωσης, η Ένωση δύναται να λάβει μέτρα, σύμφωνα με την αρχή της επικουρικότητας του άρθρου 5 της Συνθήκης για την Ευρωπαϊκή Ένωση. Σύμφωνα με την αρχή της αναλογικότητας, όπως διατυπώνεται στο ίδιο άρθρο, η παρούσα οδηγία δεν υπερβαίνει τα αναγκαία όρια για την επίτευξη των στόχων αυτών.

(13) Σύμφωνα με την κοινή πολιτική δήλωση, της 28ης Σεπτεμβρίου 2011, των κρατών μελών και της Επιτροπής σχετικά με τα επεξηγηματικά έγγραφα ([14]), τα κράτη μέλη δεσμεύτηκαν να επισυνάπτουν στην κοινοποίηση των εθνικών μέτρων μεταφοράς στο εθνικό δίκαιο, όταν δικαιολογείται, ένα ή περισσότερα έγγραφα που διευκρινίζουν τη σχέση ανάμεσα στα στοιχεία μιας οδηγίας και στα αντίστοιχα τμήματα των εθνικών πράξεων μεταφοράς. Για την παρούσα οδηγία, ο νομοθέτης εκτιμά ότι η διαβίβαση των εγγράφων αυτών είναι δικαιολογημένη,

ΕΞΕΔΩΣΑΝ ΤΗΝ ΠΑΡΟΥΣΑ ΟΔΗΓΙΑ:

Άρθρο 1

Τροποποιήσεις της οδηγίας 2009/65/ΕΚ

Το άρθρο 12 της οδηγίας 2009/65/ΕΚ τροποποιείται ως εξής:

1) Στην παράγραφο 1 δεύτερο εδάφιο, το στοιχείο α) αντικαθίσταται από το ακόλουθο κείμενο:

«α) να διαθέτει ορθές διοικητικές και λογιστικές διαδικασίες, ρυθμίσεις ελέγχου και ασφάλειας για την επεξεργασία των ηλεκτρονικών δεδομένων, μεταξύ άλλων όσων αφορά τα συστήματα δικτύου και πληροφοριών που έχουν δημιουργηθεί και τελούν υπό διαχείριση σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (*), καθώς και επαρκείς μηχανισμούς εσωτερικού ελέγχου, που περιλαμβάνουν, ιδίως, κανόνες για τις προσωπικές συναλλαγές των υπαλλήλων της ή για την κατοχή ή τη διαχείριση επενδύσεων σε χρηματοπιστωτικά μέσα με σκοπό την επένδυση για ίδιο λογαριασμό και που εξασφαλίζουν τουλάχιστον ότι για κάθε συναλλαγή στην οποία συμμετέχει ο ΟΣΕΚΑ είναι δυνατή η εξακρίβωση της προέλευσής της, των συναλλασσομένων, του χαρακτήρα της, καθώς και του τόπου και χρόνου πραγματοποίησής της, και ότι τα στοιχεία του ενεργητικού του ΟΣΕΚΑ που διαχειρίζεται η εταιρεία διαχείρισης επενδύονται σύμφωνα με τον κανονισμό του κεφαλαίου ή τα καταστατικά του έγγραφα, καθώς και τις ισχύουσες νομικές διατάξεις.

(*) Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (ΕΕ L 333 της 27.12.2022, σ. 1).».

2) Η παράγραφος 3 αντικαθίσταται από το ακόλουθο κείμενο:

«3. Με την επιφύλαξη του άρθρου 116, η Επιτροπή θεσπίζει, με κατ' εξουσιοδότηση πράξεις σύμφωνα με το άρθρο 112α, μέτρα που προσδιορίζουν:

α) τις διαδικασίες και τις ρυθμίσεις στις οποίες αναφέρεται η παράγραφος 1 δεύτερο εδάφιο στοιχείο α), πλην των διαδικασιών και ρυθμίσεων που αφορούν τα συστήματα δικτύου και πληροφοριών·

β) τις δομές και τις οργανωτικές ρυθμίσεις για την αποτροπή συγκρούσεων συμφερόντων κατά την παράγραφο 1 δεύτερο εδάφιο στοιχείο β).».

([14]) ΕΕ C 369 της 17.12.2011, σ. 14.

Άρθρο 2

Τροποποιήσεις της οδηγίας 2009/138/ΕΚ

Η οδηγία 2009/138/ΕΚ τροποποιείται ως εξής:

1) Στο άρθρο 41, η παράγραφος 4 αντικαθίσταται από το ακόλουθο κείμενο:

«4. Οι ασφαλιστικές και οι αντασφαλιστικές επιχειρήσεις λαμβάνουν εύλογα μέτρα προκειμένου να διασφαλίζουν τη συνέχεια και την κανονικότητα των δραστηριοτήτων τους, συμπεριλαμβανομένης της ανάπτυξης σχεδίων έκτακτης ανάγκης. Για τον σκοπό αυτό, οι επιχειρήσεις εφαρμόζουν και χρησιμοποιούν κατάλληλα και αναλογικά συστήματα, μέσα και διαδικασίες και ιδίως δημιουργούν και διαχειρίζονται συστήματα δικτύου και πληροφοριών σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (*).

_____

(*) Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (ΕΕ L 333 της 27.12.2022, σ. 1).».

2) Στο άρθρο 50 παράγραφος 1, τα στοιχεία α) και β) αντικαθίστανται από το ακόλουθο κείμενο:

«α) τα στοιχεία των συστημάτων που αναφέρονται στο άρθρο 41, στο άρθρο 44, ιδίως τα πεδία που απαριθμούνται στο άρθρο 44 παράγραφος 2, και στα άρθρα 46 και 47, πλην των στοιχείων που αφορούν τη διαχείριση των κινδύνων των τεχνολογιών των πληροφοριών και των επικοινωνιών·

β) τις λειτουργίες που αναφέρονται στα άρθρα 44, 46, 47 και 48, πλην των λειτουργιών που αφορούν τη διαχείριση των κινδύνων των τεχνολογιών των πληροφοριών και των επικοινωνιών.».

Άρθρο 3

Τροποποίηση της οδηγίας 2011/61/ΕΕ

Το άρθρο 18 της οδηγίας 2011/61/ΕΕ αντικαθίσταται από το ακόλουθο κείμενο:

«*Άρθρο 18*

Γενικές αρχές

1. Τα κράτη μέλη απαιτούν από τους ΔΟΕΕ να χρησιμοποιούν πάντα επαρκείς και κατάλληλους ανθρώπινους και τεχνικούς πόρους οι οποίοι είναι απαραίτητοι για την ορθή διαχείριση των ΟΕΕ.

Συγκεκριμένα, οι αρμόδιες αρχές του κράτους μέλους καταγωγής του ΔΟΕΕ, έχοντας επίσης υπόψη τη φύση των ΟΕΕ τους οποίους διαχειρίζεται ο ΔΟΕΕ, επιβάλλουν στον ΔΟΕΕ να διαθέτει ορθές διοικητικές και λογιστικές διαδικασίες, ρυθμίσεις ελέγχου και ασφάλειας για την επεξεργασία των ηλεκτρονικών δεδομένων, μεταξύ άλλων όσων αφορά τα συστήματα δικτύου και πληροφοριών που έχουν δημιουργηθεί και τελούν υπό διαχείριση σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (*), καθώς και κατάλληλους εσωτερικούς μηχανισμούς ελέγχου που περιλαμβάνουν, ιδίως, κανόνες για τις προσωπικές συναλλαγές των υπαλλήλων του ή για την κατοχή ή διαχείριση επενδύσεων με σκοπό την επένδυση για ίδιο λογαριασμό και που εξασφαλίζουν τουλάχιστον ότι για κάθε συναλλαγή στην οποία συμμετέχουν οι ΟΕΕ είναι δυνατή η εξακρίβωση της προέλευσής της, των συναλλασσομένων, του χαρακτήρα της, καθώς και του τόπου και χρόνου πραγματοποίησής της, και ότι τα στοιχεία του ενεργητικού των ΟΕΕ που διαχειρίζεται ο ΔΟΕΕ επενδύονται σύμφωνα με τον κανονισμό των ΟΕΕ ή τα καταστατικά τους έγγραφα, καθώς και με τις ισχύουσες νομικές διατάξεις.

2. Η Επιτροπή εκδίδει, με κατ' εξουσιοδότηση πράξεις σύμφωνα με το άρθρο 56 και υπό τις προϋποθέσεις των άρθρων 57 και 58, μέτρα που καθορίζουν τις διαδικασίες και τις ρυθμίσεις που αναφέρονται στην παράγραφο 1 του παρόντος άρθρου, πλην των διαδικασιών και ρυθμίσεων που αφορούν τα συστήματα δικτύου και πληροφοριών.

_____

(*) Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (ΕΕ L 333 της 27.12.2022, σ. 1).».

Άρθρο 4

Τροποποιήσεις της οδηγίας 2013/36/ΕΕ

Η οδηγία 2013/36/ΕΕ τροποποιείται ως εξής:

1) Στο άρθρο 65 παράγραφος 3, το στοιχείο α) σημείο vi) αντικαθίσταται από το ακόλουθο κείμενο:

«vi) τρίτους στους οποίους οι οντότητες που αναφέρονται στα σημεία i) έως iv) ανέθεσαν καθήκοντα ή δραστηριότητες, συμπεριλαμβανομένων των τρίτων παρόχων υπηρεσιών ΤΠΕ που αναφέρονται στο κεφάλαιο V του κανονισμού (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (*).

_____

(*) Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (ΕΕ L L 333 της 27.12.2022, σ.1).».

2) Στο άρθρο 74 παράγραφος 1, το πρώτο εδάφιο αντικαθίσταται από το ακόλουθο κείμενο:

«Τα ιδρύματα θεσπίζουν άρτιες ρυθμίσεις διακυβέρνησης, οι οποίες περιλαμβάνουν σαφή οργανωτική διάρθρωση με σαφώς καθορισμένες, διαφανείς και συνεπείς γραμμές ευθύνης, αποτελεσματικές διαδικασίες εντοπισμού, διαχείρισης, παρακολούθησης και αναφοράς των κινδύνων τους οποίους αναλαμβάνουν ή ενδέχεται να αναλάβουν, επαρκείς μηχανισμούς εσωτερικού ελέγχου, περιλαμβανομένων των κατάλληλων διοικητικών και λογιστικών διαδικασιών, συστήματα δικτύου και πληροφοριών που έχουν δημιουργηθεί και τελούν υπό διαχείριση σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554, καθώς και πολιτικές και πρακτικές αποδοχών που συνάδουν προς τις αρχές της ορθής και αποτελεσματικής διαχείρισης κινδύνων και τις προωθούν.».

3) Στο άρθρο 85, η παράγραφος 2 αντικαθίσταται από το ακόλουθο κείμενο:

«2. Οι αρμόδιες αρχές διασφαλίζουν ότι τα ιδρύματα καταρτίζουν πολιτικές και σχέδια αντιμετώπισης επειγουσών καταστάσεων και επιχειρησιακής συνέχειας, συμπεριλαμβανομένων των πολιτικών και των σχεδίων επιχειρησιακής συνέχειας των ΤΠΕ και των σχεδίων αντιμετώπισης και ανάκαμψης των ΤΠΕ όσον αφορά την τεχνολογία που χρησιμοποιούν για την κοινοποίηση πληροφοριών, και ότι τα εν λόγω σχέδια καταρτίζονται, τελούν υπό διαχείριση και υποβάλλονται σε δοκιμές σύμφωνα με το άρθρο 11 του κανονισμού (ΕΕ) 2022/2554, ώστε τα ιδρύματα να έχουν τη δυνατότητα να συνεχίσουν τη λειτουργία τους σε περίπτωση σοβαρής διαταραχής της δραστηριότητάς τους και να περιορίσουν τις ζημίες που προκαλούνται ως συνέπεια της διαταραχής αυτής.».

4) Στο άρθρο 97 παράγραφος 1, προστίθεται το ακόλουθο στοιχείο:

«δ) κινδύνους που εντοπίζονται με δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας σύμφωνα με το κεφάλαιο IV του κανονισμού (ΕΕ) 2022/2554.».

Άρθρο 5

Τροποποιήσεις της οδηγίας 2014/59/ΕΕ

Η οδηγία 2014/59/ΕΕ τροποποιείται ως εξής:

1) το άρθρο 10 τροποποιείται ως εξής:

α) στην παράγραφο 7, το στοιχείο γ) αντικαθίσταται από το ακόλουθο κείμενο:

«γ) παρουσίαση του τρόπου με τον οποίο θα μπορούσαν να διαχωριστούν νομικά και οικονομικά οι κρίσιμες λειτουργίες και οι βασικοί επιχειρηματικοί τομείς, στον αναγκαίο βαθμό, από άλλες λειτουργίες, ούτως ώστε να διασφαλιστεί η συνέχεια και η ψηφιακή επιχειρησιακή ανθεκτικότητα σε περίπτωση πτώχευσης του ιδρύματος·»·

β) στην παράγραφο 7, το στοιχείο ιζ) αντικαθίσταται από το ακόλουθο κείμενο:

«ιζ) περιγραφή των βασικών λειτουργιών και συστημάτων για τη διατήρηση της συνεχούς λειτουργίας των επιχειρησιακών διαδικασιών του ιδρύματος, συμπεριλαμβανομένων των συστημάτων δικτύου και πληροφοριών που δημιουργούνται σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (*)·

_____

(*) Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (ΕΕ L 333 της 27.12.2022, σ. 1).»·

γ) στην παράγραφο 9, προστίθεται το ακόλουθο εδάφιο:

«Σύμφωνα με το άρθρο 10 του κανονισμού (ΕΕ) αριθ. 1093/2010, η ΕΑΤ επανεξετάζει και, εάν κρίνεται σκόπιμο, επικαιροποιεί τα ρυθμιστικά τεχνικά πρότυπα, προκειμένου, μεταξύ άλλων, να λαμβάνει υπόψη τις διατάξεις του κεφαλαίου ΙΙ του κανονισμού (ΕΕ) 2022/2554.».

2) Το παράρτημα τροποποιείται ως εξής:

α) στο τμήμα Α, το σημείο 16 αντικαθίσταται από το ακόλουθο κείμενο:

«16. ρυθμίσεις και μέτρα που είναι αναγκαία για τη διατήρηση της συνεχούς λειτουργίας των επιχειρησιακών διαδικασιών του ιδρύματος, συμπεριλαμβανομένων των συστημάτων δικτύου και πληροφοριών που έχουν δημιουργηθεί και τελούν υπό διαχείριση σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554·»·

β) το τμήμα Β τροποποιείται ως εξής:

i) το σημείο 14 αντικαθίσταται από το ακόλουθο κείμενο:

«14. στοιχεία των κατόχων των συστημάτων που προσδιορίζονται στο σημείο 13, τις συμφωνίες για το επίπεδο των υπηρεσιών που σχετίζονται με αυτά, και κάθε λογισμικό και συστήματα ή άδειες, συμπεριλαμβανομένης της καταγραφής τους στις νομικές οντότητες, τις κρίσιμες λειτουργίες και βασικούς επιχειρηματικούς τομείς του ιδρύματος, καθώς και τα στοιχεία των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ όπως ορίζονται στο άρθρο 3 σημείο 23) του κανονισμού (ΕΕ) 2022/2554·»·

ii) παρεμβάλλεται το ακόλουθο σημείο:

«14α. τα αποτελέσματα των δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας των ιδρυμάτων σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554·»·

γ) το τμήμα Γ τροποποιείται ως εξής:

i) το σημείο 4 αντικαθίσταται από το ακόλουθο κείμενο:

«4. τον βαθμό στον οποίο οι συμφωνίες παροχής υπηρεσιών, συμπεριλαμβανομένων των συμβατικών ρυθμίσεων για τη χρήση υπηρεσιών ΤΠΕ, που διατηρεί το ίδρυμα είναι άρτιες και πλήρως εκτελεστές σε περίπτωση εξυγίανσης του ιδρύματος·»·

ii) παρεμβάλλεται το ακόλουθο σημείο:

«4α. την ψηφιακή επιχειρησιακή ανθεκτικότητα των συστημάτων δικτύου και πληροφοριών που υποστηρίζουν τις κρίσιμες λειτουργίες και τους βασικούς επιχειρηματικούς τομείς του ιδρύματος, λαμβάνοντας υπόψη τις αναφορές σημαντικών συμβάντων που σχετίζονται με τις ΤΠΕ και τα αποτελέσματα των δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας βάσει του κανονισμού (ΕΕ) 2022/2554·».

Άρθρο 6

Τροποποιήσεις της οδηγίας 2014/65/ΕΕ

Η οδηγία 2014/65/ΕΕ τροποποιείται ως εξής:

1) Το άρθρο 16 τροποποιείται ως εξής:

α) η παράγραφος 4 αντικαθίσταται από το ακόλουθο κείμενο:

«4. Η επιχείρηση επενδύσεων ενεργεί τα ευλόγως πρακτέα για να εξασφαλίζεται η συνεχής και τακτική εκτέλεση των επενδυτικών υπηρεσιών και δραστηριοτήτων. Για τον σκοπό αυτό, η επιχείρηση επενδύσεων χρησιμοποιεί κατάλληλα και αναλογικά συστήματα, συμπεριλαμβανομένων των συστημάτων τεχνολογιών των πληροφοριών και των επικοινωνιών («ΤΠΕ») που έχουν δημιουργηθεί και τελούν υπό διαχείριση σύμφωνα με το άρθρο 7 του κανονισμού (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (*), καθώς και κατάλληλα και αναλογικά μέσα και διαδικασίες.

(*) Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (ΕΕ L 333 της 27.12.2022, σ. 1).»·

β) στην παράγραφο 5, το δεύτερο και το τρίτο εδάφιο αντικαθίστανται από το ακόλουθο κείμενο:

«Η επιχείρηση επενδύσεων οφείλει να έχει υγιείς διοικητικές και λογιστικές διαδικασίες, μηχανισμούς εσωτερικού ελέγχου και αποτελεσματικές διαδικασίες εκτίμησης των κινδύνων.

Με την επιφύλαξη του δικαιώματος των αρμόδιων αρχών να απαιτούν πρόσβαση στις επικοινωνίες δυνάμει της παρούσας οδηγίας και του κανονισμού (ΕΕ) αριθ. 600/2014, μια επιχείρηση επενδύσεων διαθέτει ισχυρούς μηχανισμούς ασφαλείας, σύμφωνα με τις απαιτήσεις που ορίζει ο κανονισμός (ΕΕ) 2022/2554, για τη διασφάλιση και την εξακρίβωση της γνησιότητας των μέσων διαβίβασης των πληροφοριών, την ελαχιστοποίηση του κινδύνου καταστροφής των δεδομένων και πρόσβασης χωρίς άδεια και την αποφυγή της διαρροής των πληροφοριών, ώστε να τηρείται πάντοτε το απόρρητο των δεδομένων.».

2) Το άρθρο 17 τροποποιείται ως εξής:

α) η παράγραφος 1 αντικαθίσταται από το ακόλουθο κείμενο:

«1. Μια επιχείρηση επενδύσεων που δραστηριοποιείται μέσω αλγοριθμικών συναλλαγών χρησιμοποιεί αποτελεσματικά συστήματα και ελέγχους κινδύνου, κατάλληλους για τις εργασίες που διεκπεραιώνει, προκειμένου να διασφαλίζει ότι τα συστήματα συναλλαγών της είναι ανθεκτικά και διαθέτουν επαρκή χωρητικότητα σύμφωνα με τις απαιτήσεις που ορίζει το κεφάλαιο II του κανονισμού0 (ΕΕ) 2022/2554, υπόκεινται σε κατάλληλα κατώτατα και ανώτατα όρια συναλλαγών και αποτρέπουν την αποστολή εσφαλμένων εντολών ή τη λειτουργία των συστημάτων κατά τρόπο που ενδέχεται να οδηγήσει ή να συμβάλει στη μη εύρυθμη λειτουργία της αγοράς.

Μια τέτοια επιχείρηση χρησιμοποιεί επίσης αποτελεσματικά συστήματα και ελέγχους κινδύνου προκειμένου να διασφαλίζεται ότι τα συστήματα συναλλαγών δεν δύνανται να χρησιμοποιούνται για σκοπό που είναι αντίθετος στον κανονισμό (ΕΕ) αριθ. 596/2014 ή στους κανόνες ενός τόπου διαπραγμάτευσης με τον οποίο αυτή συνδέεται.

Η επιχείρηση επενδύσεων διαθέτει αποτελεσματικές ρυθμίσεις επιχειρησιακής συνέχειας για την αντιμετώπιση κάθε αστοχίας στα συστήματα συναλλαγών της, συμπεριλαμβανομένων των πολιτικών και των σχεδίων επιχειρησιακής συνέχειας των ΤΠΕ και των σχεδίων αντιμετώπισης και ανάκαμψης των ΤΠΕ τα οποία έχουν καταρτιστεί σύμφωνα με το άρθρο 11 του κανονισμού (ΕΕ) 2022/2554, και διασφαλίζει ότι τα συστήματά της έχουν υποβληθεί σε πλήρεις δοκιμές και παρακολουθούνται κατάλληλα, ώστε να διασφαλίζεται ότι πληρούν τις γενικές απαιτήσεις της παρούσας παραγράφου και τυχόν ειδικές απαιτήσεις που ορίζονται στα κεφάλαια II και IV του κανονισμού (ΕΕ) 2022/2554.»·

β) στην παράγραφο 7, το στοιχείο α) αντικαθίσταται από το ακόλουθο κείμενο:

«α) τις λεπτομέρειες των οργανωτικών απαιτήσεων που ορίζονται στις παραγράφους 1 έως 6, πλην όσων σχετίζονται με τη διαχείριση των κινδύνων ΤΠΕ, και οι οποίες θα επιβληθούν στις επιχειρήσεις επενδύσεων που παρέχουν διαφορετικές επενδυτικές υπηρεσίες, επενδυτικές δραστηριότητες, παρεπόμενες υπηρεσίες ή συνδυασμούς αυτών, όπου οι διευκρινίσεις που αφορούν τις οργανωτικές απαιτήσεις που ορίζονται στην παράγραφο 5 προσδιορίζουν συγκεκριμένες απαιτήσεις για την άμεση πρόσβαση στην αγορά και για την κατευθείαν πρόσβαση στην αγορά, ούτως ώστε να εξασφαλίζεται ότι οι έλεγχοι που εφαρμόζονται για την κατευθείαν πρόσβαση στην αγορά είναι τουλάχιστον ισότιμοι με εκείνους που εφαρμόζονται για την άμεση πρόσβαση στην αγορά,».

3) Στο άρθρο 47, η παράγραφος 1 τροποποιείται ως εξής:

α) το στοιχείο β) αντικαθίσταται από το ακόλουθο κείμενο:

«β) να έχει κατάλληλα μέσα που να της επιτρέπουν να διαχειρίζεται τους κινδύνους στους οποίους είναι εκτεθειμένη, συμπεριλαμβανομένης της διαχείρισης κινδύνων ΤΠΕ σύμφωνα με το κεφάλαιο II του κανονισμού (ΕΕ) 2022/2554, να εφαρμόζει κατάλληλους μηχανισμούς και συστήματα για τον εντοπισμό σημαντικών κινδύνων για τη λειτουργία της, και να έχει λάβει αποτελεσματικά μέτρα για τον περιορισμό αυτών των κινδύνων,»·

β) το στοιχείο γ) διαγράφεται.

4) Το άρθρο 48 τροποποιείται ως εξής:

α) η παράγραφος 1 αντικαθίσταται από το ακόλουθο κείμενο:

«1. Τα κράτη μέλη απαιτούν μια ρυθμιζόμενη αγορά να αναπτύσσει και να διατηρεί την επιχειρησιακή ανθεκτικότητά της σύμφωνα με τις απαιτήσεις που ορίζονται στο κεφάλαιο II του κανονισμού (ΕΕ) 2022/2554, προκειμένου να διασφαλίζει ότι τα συστήματα συναλλαγών της είναι ανθεκτικά, έχουν επαρκή χωρητικότητα για την εξυπηρέτηση μεγάλων όγκων εντολών και μηνυμάτων, μπορούν να διασφαλίσουν την εύρυθμη διεξαγωγή συναλλαγών υπό ακραίες συνθήκες πίεσης στην αγορά, ελέγχονται πλήρως για τη διασφάλιση της εκπλήρωσης των όρων αυτών και διαθέτουν αποτελεσματικές ρυθμίσεις επιχειρησιακής συνέχειας, συμπεριλαμβανομένων των πολιτικών και των σχεδίων επιχειρησιακής συνέχειας των ΤΠΕ και των σχεδίων αντιμετώπισης και ανάκαμψης των ΤΠΕ τα οποία έχουν καταρτιστεί σύμφωνα με το άρθρο 11 του κανονισμού (ΕΕ) 2022/2554, που διασφαλίζουν τη συνέχιση των υπηρεσιών της σε περίπτωση αστοχίας των συστημάτων συναλλαγών.»·

β) η παράγραφος 6 αντικαθίσταται από το ακόλουθο κείμενο:

«6. Τα κράτη μέλη απαιτούν μια ρυθμιζόμενη αγορά να διαθέτει αποτελεσματικά συστήματα, διαδικασίες και ρυθμίσεις, που περιλαμβάνουν την απαίτηση από τα μέλη ή τους συμμετέχοντες να εφαρμόζουν τις κατάλληλες διαδικασίες δοκιμαστικής λειτουργίας των αλγορίθμων και την παροχή περιβάλλοντος για τη διευκόλυνση της πραγματοποίησης των δοκιμών αυτών σύμφωνα με τις απαιτήσεις που ορίζονται στα κεφάλαια II και IV του κανονισμού (ΕΕ) 2022/2554, οι οποίες να εξασφαλίζουν ότι τα συστήματα αλγοριθμικών συναλλαγών δεν μπορούν να δημιουργήσουν ή να συμβάλουν στη διαμόρφωση συνθηκών μη εύρυθμης διεξαγωγής συναλλαγών στην αγορά και να διαχειρίζονται τις συνθήκες μη εύρυθμης διεξαγωγής συναλλαγών που ανακύπτουν από αυτά τα συστήματα κατάρτισης αλγοριθμικών συναλλαγών, συμπεριλαμβανομένων συστημάτων για τον περιορισμό της αναλογίας ανεκτέλεστων εντολών που μπορούν να εισαχθούν στο σύστημα από μέλος ή συμμετέχοντα προς τις συναλλαγές, συστημάτων για την επιβράδυνση της ροής των εντολών αν υπάρχει κίνδυνος για εξάντληση της χωρητικότητας του συστήματος και συστημάτων για τον περιορισμό και την επιβολή του ελάχιστου βήματος τιμής στο οποίο μπορούν να εκτελεστούν οι συναλλαγές στην αγορά.»·

γ) η παράγραφος 12 τροποποιείται ως εξής:

i) το στοιχείο α) αντικαθίσταται από το ακόλουθο κείμενο:

«α) τις απαιτήσεις για τη διασφάλιση της ανθεκτικότητας και της επαρκούς χωρητικότητας των συστημάτων συναλλαγών των ρυθμιζόμενων αγορών, με εξαίρεση τις απαιτήσεις που αφορούν την ψηφιακή επιχειρησιακή ανθεκτικότητα·»·

ii) το στοιχείο ζ) αντικαθίσταται από το ακόλουθο κείμενο:

«ζ) τις απαιτήσεις για την εξασφάλιση της εφαρμογής κατάλληλων διαδικασιών δοκιμαστικής λειτουργίας, πλην των δοκιμών για την ψηφιακή επιχειρησιακή ανθεκτικότητα, ώστε να διασφαλίζεται ότι τα συστήματα αλγοριθμικών συναλλαγών, συμπεριλαμβανομένων των συστημάτων αλγοριθμικών συναλλαγών σε υψηλή συχνότητα, δεν μπορούν να προκαλέσουν ή να συμβάλουν σε συνθήκες μη εύρυθμης διεξαγωγής συναλλαγών στην αγορά.».

Άρθρο 7

Τροποποιήσεις της οδηγίας (ΕΕ) 2015/2366

Η οδηγία (ΕΕ) 2015/2366 τροποποιείται ως εξής:

1) Στο άρθρο 3, το στοιχείο ι) αντικαθίσταται από το ακόλουθο κείμενο:

«ι) στις υπηρεσίες παρόχων τεχνικών υπηρεσιών, οι οποίες υποστηρίζουν την παροχή υπηρεσιών πληρωμών, χωρίς ποτέ να περιέρχονται στην κατοχή τους τα υπό μεταφορά χρηματικά ποσά· στις υπηρεσίες αυτές περιλαμβάνονται η επεξεργασία και αποθήκευση δεδομένων, οι υπηρεσίες εμπιστοσύνης και προστασίας της ιδιωτικής ζωής, η εξακρίβωση δεδομένων και οντοτήτων, η παροχή τεχνολογιών των πληροφοριών και των επικοινωνιών (ΤΠΕ) και δικτύου επικοινωνιών, καθώς και η παροχή και συντήρηση τερματικών και συσκευών που χρησιμοποιούνται για υπηρεσίες πληρωμών, με εξαίρεση τις υπηρεσίες εκκίνησης πληρωμών και τις υπηρεσίες παροχής πληροφοριών λογαριασμού·».

2) Το άρθρο 5 παράγραφος 1 τροποποιείται ως εξής:

α) το πρώτο εδάφιο τροποποιείται ως εξής:

i) το στοιχείο ε) αντικαθίσταται από το ακόλουθο κείμενο:

«ε) περιγραφή του οργανωτικού πλαισίου διακυβέρνησης και των μηχανισμών εσωτερικού ελέγχου του αιτούντος, συμπεριλαμβανομένης της διοικητικής και λογιστικής οργάνωσης και της διαχείρισης κινδύνου, καθώς και ρυθμίσεων για τη χρήση υπηρεσιών ΤΠΕ σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (*), η οποία να καταδεικνύει ότι το εν λόγω οργανωτικό πλαίσιο διακυβέρνησης και οι μηχανισμοί εσωτερικού ελέγχου είναι αναλογικοί, κατάλληλοι, ορθοί και επαρκείς·

(*) Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (ΕΕ L 333 της 27.12.2022, σ. 1).»·

ii) το στοιχείο στ) αντικαθίσταται από το ακόλουθο κείμενο:

«στ) περιγραφή της υφιστάμενης διαδικασίας ελέγχου, διαχείρισης και παρακολούθησης ενός περιστατικού ασφαλείας, καθώς και των παραπόνων των πελατών για ζητήματα σχετικά με την ασφάλεια, συμπεριλαμβανομένου ενός μηχανισμού αναφοράς συμβάντων που να λαμβάνει υπόψη τις υποχρεώσεις κοινοποίησης του ιδρύματος πληρωμών που καθορίζονται στο κεφάλαιο III του κανονισμού (ΕΕ) 2022/2554·»·

iii) το στοιχείο η) αντικαθίσταται από το ακόλουθο κείμενο:

«η) περιγραφή των ρυθμίσεων επιχειρησιακής συνέχειας που περιλαμβάνουν σαφή προσδιορισμό των κρίσιμων λειτουργιών, αποτελεσματικών πολιτικών και σχεδίων επιχειρησιακής συνέχειας των ΤΠΕ και σχεδίων αντιμετώπισης και ανάκαμψης των ΤΠΕ και μιας διαδικασίας για την τακτική δοκιμή και επανεξέταση της επάρκειας και της αποτελεσματικότητας των εν λόγω σχεδίων σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554·»·

β) το τρίτο εδάφιο αντικαθίσταται από το ακόλουθο κείμενο:

«Ο έλεγχος ασφάλειας και τα μέτρα μείωσης κινδύνων που αναφέρονται στο πρώτο εδάφιο στοιχείο ι) υποδεικνύουν τον τρόπο διασφάλισης υψηλού επιπέδου ψηφιακής επιχειρησιακής ανθεκτικότητας σύμφωνα με το κεφάλαιο ΙΙ του κανονισμού (ΕΕ) 2022/2554, ιδίως σε σχέση με την τεχνική ασφάλεια και την προστασία των δεδομένων, συμπεριλαμβανομένου του λογισμικού και των συστημάτων ΤΠΕ που χρησιμοποιούνται από τον αιτούντα ή τις επιχειρήσεις στις οποίες αναθέτει το σύνολο ή μέρος των δραστηριοτήτων του. Τα εν λόγω μέτρα περιλαμβάνουν επίσης τα μέτρα ασφαλείας που προβλέπονται στο άρθρο 95 παράγραφος 1 της παρούσας οδηγίας. Τα εν λόγω μέτρα λαμβάνουν υπόψη τις επικείμενες κατευθυντήριες γραμμές για τα μέτρα ασφαλείας της ΕΑΤ που αναφέρονται στο άρθρο 95 παράγραφος 3 της παρούσας οδηγίας.».

3) Στο άρθρο 19 παράγραφος 6, το δεύτερο εδάφιο αντικαθίσταται από το ακόλουθο κείμενο:

«Η ανάθεση σημαντικών λειτουργικών δραστηριοτήτων σε εξωτερικούς φορείς, περιλαμβανομένων των συστημάτων ΤΠΕ, δεν γίνεται με τρόπο που βλάπτει ουσιαστικά την ποιότητα των εσωτερικών ελέγχων του ιδρύματος πληρωμών και την ικανότητα των αρμόδιων αρχών να παρακολουθούν και να εξακριβώνουν τη συμμόρφωση του ιδρύματος πληρωμών με όλες τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία.».

4) Στο άρθρο 95 παράγραφος 1, προστίθεται το ακόλουθο εδάφιο:

«Το πρώτο εδάφιο δεν θίγει την εφαρμογή του κεφαλαίου ΙΙ του κανονισμού (ΕΕ) 2022/2554:

α) στους παρόχους υπηρεσιών πληρωμών που αναφέρονται στο άρθρο 1 παράγραφος 1 στοιχεία α), β) και δ) της παρούσας οδηγίας·

β) στους παρόχους υπηρεσιών πληροφοριών λογαριασμού που αναφέρονται στο άρθρο 33 παράγραφος 1 της παρούσας οδηγίας·

γ) στα ιδρύματα πληρωμών που εξαιρούνται δυνάμει του άρθρου 32 παράγραφος 1 της παρούσας οδηγίας· και

δ) στα ιδρύματα ηλεκτρονικού χρήματος που δικαιούνται απαλλαγής όπως αναφέρεται στο άρθρο 9 παράγραφος 1 της οδηγίας 2009/110/ΕΚ·».

5) Στο άρθρο 96, προστίθεται η ακόλουθη παράγραφος:

«7. Τα κράτη μέλη διασφαλίζουν ότι οι παράγραφοι 1 έως 5 του παρόντος άρθρου δεν εφαρμόζονται:

α) στους παρόχους υπηρεσιών πληρωμών που αναφέρονται στο άρθρο 1 παράγραφος 1 στοιχεία α), β) και δ) της παρούσας οδηγίας·

β) στους παρόχους υπηρεσιών πληροφοριών λογαριασμού που αναφέρονται στο άρθρο 33 παράγραφος 1 της παρούσας οδηγίας·

γ) στα ιδρύματα πληρωμών που εξαιρούνται δυνάμει του άρθρου 32 παράγραφος 1 της παρούσας οδηγίας· και

δ) στα ιδρύματα ηλεκτρονικού χρήματος που δικαιούνται απαλλαγής όπως αναφέρεται στο άρθρο 9 παράγραφος 1 της οδηγίας 2009/110/ΕΚ.».

6) Στο άρθρο 98, η παράγραφος 5 αντικαθίσταται από το ακόλουθο κείμενο:

«5. Σύμφωνα με το άρθρο 10 του κανονισμού (ΕΕ) αριθ. 1093/2010, η ΕΑΤ επανεξετάζει και, εάν κρίνεται σκόπιμο, επικαιροποιεί τα ρυθμιστικά τεχνικά πρότυπα σε τακτική βάση, προκειμένου, μεταξύ άλλων, να λαμβάνει υπόψη την καινοτομία και τις τεχνολογικές εξελίξεις και τις διατάξεις του κεφαλαίου ΙΙ του κανονισμού (ΕΕ) 2022/2554».

Άρθρο 8

Τροποποίηση της οδηγίας (ΕΕ) 2016/2341

Το άρθρο 21 παράγραφος 5 της οδηγίας (ΕΕ) 2016/2341 αντικαθίσταται από το ακόλουθο κείμενο:

«5. Τα κράτη μέλη διασφαλίζουν ότι τα ΙΕΣΠ λαμβάνουν εύλογα μέτρα προκειμένου να εξασφαλίζουν τη συνέχεια και την κανονικότητα της άσκησης των δραστηριοτήτων τους, συμπεριλαμβανομένης της κατάρτισης σχεδίων έκτακτης ανάγκης. Για

τον σκοπό αυτό, τα ΙΕΣΠ χρησιμοποιούν κατάλληλα και αναλογικά συστήματα, πόρους και διαδικασίες και, ιδίως, δημιουργούν και διαχειρίζονται συστήματα δικτύου και πληροφοριών κατ' εφαρμογή του κανονισμού (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (*), κατά περίπτωση.

_____

(*) Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (ΕΕ L 333 της 27.12.2022, σ. 1).».

Άρθρο 9

Μεταφορά στο εθνικό δίκαιο

1. Έως τις 17 Ιανουαρίου 2025, τα κράτη μέλη εκδίδουν και δημοσιεύουν τα μέτρα που είναι αναγκαία για τη συμμόρφωση με την παρούσα οδηγία. Ενημερώνουν αμέσως σχετικά την Επιτροπή.

Εφαρμόζουν τα εν λόγω μέτρα από τις 17 Ιανουαρίου 2025.

Τα εν λόγω μέτρα, όταν θεσπίζονται από τα κράτη μέλη, περιέχουν παραπομπή στην παρούσα οδηγία ή συνοδεύονται από την παραπομπή αυτή κατά την επίσημη δημοσίευσή τους. Ο τρόπος της παραπομπής αυτής καθορίζεται από τα κράτη μέλη.

2. Τα κράτη μέλη ανακοινώνουν στην Επιτροπή το κείμενο των ουσιωδών μέτρων εθνικού δικαίου τα οποία θεσπίζουν στον τομέα που διέπεται από την παρούσα οδηγία.

Άρθρο 10

Έναρξη ισχύος

Η παρούσα οδηγία αρχίζει να ισχύει την εικοστή ημέρα από τη δημοσίευσή της στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

Άρθρο 11

Αποδέκτες

Η παρούσα οδηγία απευθύνεται στα κράτη μέλη.

Στρασβούργο, 14 Δεκεμβρίου 2022.

Για το Ευρωπαϊκό Κοινοβούλιο	*Για το Συμβούλιο*
Η Πρόεδρος	*Ο Πρόεδρος*
R. METSOLA	M. BEK

ΟΔΗΓΙΑ (ΕΕ) 2022/2557 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

της 14ης Δεκεμβρίου 2022

για την ανθεκτικότητα των κρίσιμων οντοτήτων και την κατάργηση της οδηγίας 2008/114/ΕΚ του Συμβουλίου

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης, και ιδίως το άρθρο 114,

Έχοντας υπόψη την πρόταση της Ευρωπαϊκής Επιτροπής,

Κατόπιν διαβίβασης του σχεδίου νομοθετικής πράξης στα εθνικά κοινοβούλια,

Έχοντας υπόψη τη γνώμη της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής ([1]),

Έχοντας υπόψη τη γνώμη της Επιτροπής των Περιφερειών ([2]),

Αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία ([3]),

Εκτιμώντας τα ακόλουθα:

(1) Οι κρίσιμες οντότητες, ως πάροχοι βασικών υπηρεσιών, διαδραματίζουν θεμελιώδη ρόλο στη διατήρηση ζωτικών κοινωνικών λειτουργιών ή οικονομικών δραστηριοτήτων στην εσωτερική αγορά σε μια ολοένα και πιο αλληλεξαρτώμενη οικονομία της Ένωσης. Ως εκ τούτου, είναι σημαντικό να καθοριστεί ένα ενωσιακό πλαίσιο με σκοπό τόσο την ενίσχυση της ανθεκτικότητας των κρίσιμων οντοτήτων στην εσωτερική αγορά με τον καθορισμό εναρμονισμένων ελάχιστων κανόνων όσο και την παροχή συνδρομής σε αυτές μέσω συνεκτικών και ειδικών μέτρων στήριξης και εποπτείας.

(2) Η οδηγία 2008/114/ΕΚ του Συμβουλίου ([4]) καθορίζει διαδικασία για τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας στους τομείς της ενέργειας και των μεταφορών, των οποίων η διακοπή λειτουργίας ή η καταστροφή θα είχε σημαντικό διασυνοριακό αντίκτυπο σε τουλάχιστον δύο κράτη μέλη. Η εν λόγω οδηγία εστιάζει αποκλειστικά στην προστασία τέτοιων υποδομών. Ωστόσο, η αξιολόγηση της οδηγίας 2008/114/ΕΚ, η οποία διενεργήθηκε το 2019, κατέδειξε ότι λόγω του ολοένα και πιο διασυνδεδεμένου και διασυνοριακού χαρακτήρα των λειτουργιών που χρησιμοποιούν υποδομές ζωτικής σημασίας, τα μέτρα προστασίας που αφορούν μόνο επιμέρους περιουσιακά στοιχεία δεν επαρκούν για την πρόληψη όλων των πιθανών διαταραχών. Ως εκ τούτου, είναι αναγκαίο να μετατοπιστεί η προσέγγιση προς τη διασφάλιση ότι οι κίνδυνοι λαμβάνονται καλύτερα υπόψη, ότι ο ρόλος και τα καθήκοντα των κρίσιμων οντοτήτων ως παρόχων υπηρεσιών που είναι απαραίτητες για τη λειτουργία της εσωτερικής αγοράς καθορίζονται καλύτερα και με

([1]) ΕΕ C 286 της 16.7.2021, σ. 170.
([2]) ΕΕ C 440 της 29.10.2021, σ. 99.
([3]) Θέση του Ευρωπαϊκού Κοινοβουλίου της 22ας Νοεμβρίου 2022 (δεν έχει ακόμη δημοσιευθεί στην Επίσημη Εφημερίδα) και απόφαση του Συμβουλίου της 8ης Δεκεμβρίου 2022 .
([4]) Οδηγία 2008/114/ΕΚ του Συμβουλίου, της 8ης Δεκεμβρίου 2008, σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας, και σχετικά με την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους (ΕΕ L 345 της 23.12.2008, σ. 75).

συνέπεια, και ότι θεσπίζονται ενωσιακοί κανόνες για την ενίσχυση της ανθεκτικότητας των κρίσιμων οντοτήτων. Οι κρίσιμες οντότητες θα πρέπει να είναι σε θέση να ενισχύουν την ικανότητά τους να προλαμβάνουν, να προστατεύουν, να αντιδρούν, να αντιστέκονται, να μετριάζουν, να απορροφούν, να προσαρμόζονται και να ανακάμπτουν από περιστατικά που ενδέχεται να διαταράξουν την παροχή βασικών υπηρεσιών.

(3) Μολονότι ορισμένα μέτρα σε ενωσιακό επίπεδο, όπως το Ευρωπαϊκό Πρόγραμμα για την Προστασία των Υποδομών Ζωτικής Σημασίας, και σε εθνικό επίπεδο αποσκοπούν στην υποστήριξη της προστασίας των υποδομών ζωτικής σημασίας στην Ένωση, θα πρέπει να γίνουν περισσότερα ώστε οι οντότητες που διαχειρίζονται τέτοιες υποδομές να είναι καλύτερα εξοπλισμένες με σκοπό την αντιμετώπιση των κινδύνων που απειλούν τη λειτουργία τους και θα μπορούσαν να οδηγήσουν σε διαταραχές στην παροχή βασικών υπηρεσιών. Θα πρέπει επίσης να γίνουν περισσότερα για τον καλύτερο εξοπλισμό αυτών των οντοτήτων, διότι υπάρχει ένα δυναμικό τοπίο απειλών, που περιλαμβάνει τις εξελισσόμενες υβριδικές και τρομοκρατικές απειλές, και τις αυξανόμενες αλληλεξαρτήσεις μεταξύ υποδομών και τομέων. Επιπλέον, υπάρχουν αυξανόμενοι φυσικοί κίνδυνοι λόγω φυσικών καταστροφών και της κλιματικής αλλαγής, η οποία εντείνει τη συχνότητα και την κλίμακα των συμβάντων που οφείλονται σε ακραία καιρικά φαινόμενα και επιφέρει μακροπρόθεσμες αλλαγές στις μέσες κλιματικές συνθήκες οι οποίες μπορούν να μειώσουν την ικανότητα, την αποδοτικότητα και τη διάρκεια ζωής ορισμένων ειδών υποδομών, αν δεν έχουν ληφθεί μέτρα προσαρμογής στην κλιματική αλλαγή. Επιπλέον, η εσωτερική αγορά χαρακτηρίζεται από κατακερματισμό όσον αφορά τον προσδιορισμό των κρίσιμων οντοτήτων, διότι οι συναφείς τομείς και κατηγορίες οντοτήτων δεν αναγνωρίζονται με συνεπή τρόπο ως κρίσιμες οντότητες σε όλα τα κράτη μέλη. Ως εκ τούτου, η παρούσα οδηγία θα πρέπει να επιτύχει ένα αξιόπιστο επίπεδο εναρμόνισης όσον αφορά τους τομείς και τις κατηγορίες οντοτήτων που εμπίπτουν στο πεδίο εφαρμογής της.

(4) Αν και ορισμένοι τομείς της οικονομίας, οι τομείς της ενέργειας και των μεταφορών, ρυθμίζονται ήδη από ειδικές τομεακές νομοθετικές πράξεις της Ένωσης, οι εν λόγω νομοθετικές πράξεις περιλαμβάνουν διατάξεις που αφορούν μόνον ορισμένες πτυχές της ανθεκτικότητας των οντοτήτων που δραστηριοποιούνται στους εν λόγω τομείς. Προκειμένου να καλυφθεί με ολοκληρωμένο τρόπο η ανθεκτικότητα των οντοτήτων που είναι κρίσιμες για την ορθή λειτουργία της εσωτερικής αγοράς, η παρούσα οδηγία δημιουργεί ένα γενικό πλαίσιο για την ανθεκτικότητα των κρίσιμων οντοτήτων έναντι όλων των κινδύνων, είτε φυσικών είτε ανθρωπογενών, τυχαίων ή εκούσιων.

(5) Οι αυξανόμενες αλληλεξαρτήσεις μεταξύ υποδομών και τομέων είναι το αποτέλεσμα ενός ολοένα και πιο διασυνοριακού και αλληλεξαρτώμενου δικτύου παροχής υπηρεσιών που χρησιμοποιεί βασικές υποδομές σε ολόκληρη την Ένωση στους τομείς της ενέργειας, των μεταφορών, των τραπεζών, του πόσιμου νερού, των λυμάτων, της παραγωγής, μεταποίησης και διανομής τροφίμων, της υγείας, του διαστήματος, των υποδομών χρηματοπιστωτικών αγορών και ορισμένων πτυχών της δημόσιας διοίκησης. Ο τομέας του διαστήματος εμπίπτει στο πεδίο εφαρμογής της παρούσας οδηγίας όσον αφορά την παροχή ορισμένων υπηρεσιών που εξαρτάται από επίγειες υποδομές των οποίων η κυριότητα, η διαχείριση και η λειτουργία ανήκει είτε σε κράτη μέλη είτε σε ιδιώτες. Ως εκ τούτου, υποδομές των οποίων η κυριότητα, η διαχείριση ή η λειτουργία ανήκει στην Ένωση ή γίνεται εξ ονόματός της στο πλαίσιο του διαστημικού προγράμματός της δεν εμπίπτει στο πεδίο εφαρμογής της παρούσας οδηγίας.

Όσον αφορά τον τομέα της ενέργειας και, ειδικότερα, τις μεθόδους παραγωγής και διανομής ηλεκτρικής ενέργειας (σε σχέση με την παροχή ηλεκτρικής ενέργειας), γίνεται κατανοητό ότι, όπου κρίνεται αναγκαίο, στην παραγωγή ηλεκτρικής ενέργειας δύνανται να περιλαμβάνονται τα μέρη μετάδοσης της ηλεκτρικής ενέργειας των πυρηνικών σταθμών παραγωγής ενέργειας, αλλά εξαιρούνται τα αμιγώς πυρηνικά τμήματα που καλύπτονται από συνθήκες και το ενωσιακό δίκαιο, συμπεριλαμβανομένων σχετικών νομικών πράξεων της Ένωσης σχετικά με την πυρηνική ενέργεια. Η διαδικασία προσδιορισμού των κρίσιμων οντοτήτων στον τομέα των τροφίμων θα πρέπει να αντικατοπτρίζει καταλλήλως τη φύση της εσωτερικής αγοράς στον εν λόγω τομέα και τους εκτενείς ενωσιακούς κανόνες που σχετίζονται με τις γενικές αρχές και απαιτήσεις της νομοθεσίας για τα τρόφιμα και της ασφάλειας των τροφίμων. Ως εκ τούτου, προκειμένου να διασφαλιστεί η ύπαρξη μιας αναλογικής προσέγγισης και να αποτυπωθεί καταλλήλως ο ρόλος και η σημασία των οντοτήτων αυτών σε εθνικό επίπεδο, οι κρίσιμες οντότητες θα πρέπει να προσδιορίζονται μόνο μεταξύ επιχειρήσεων τροφίμων, κερδοσκοπικών ή μη, δημόσιων ή ιδιωτικών, οι οποίες δραστηριοποιούνται αποκλειστικά στην εφοδιαστική, χονδρική διανομή, και στη βιομηχανική παραγωγή και μεταποίηση μεγάλης κλίμακας με σημαντικό μερίδιο αγοράς, όπως παρατηρείται σε εθνικό επίπεδο. Ως συνέπεια των εν λόγω αλληλεξαρτήσεων, οποιαδήποτε διαταραχή στην παροχή βασικών υπηρεσιών, ακόμη και αν αρχικά περιορίζεται σε μία οντότητα ή έναν τομέα, μπορεί να προκαλέσει ευρύτερες αλυσιδωτές επιπτώσεις και ενδεχομένως να οδηγήσει σε εκτεταμένες και μακροπρόθεσμες αρνητικές επιπτώσεις στην παροχή υπηρεσιών σε ολόκληρη την εσωτερική αγορά. Μείζονες κρίσεις, όπως η πανδημία της COVID-19, κατέδειξαν την ευπάθεια των ολοένα και πιο αλληλεξαρτώμενων κοινωνιών μας απέναντι σε κινδύνους μικρής πιθανότητας με μεγάλο αντίκτυπο.

(6) Οι οντότητες που συμμετέχουν στην παροχή βασικών υπηρεσιών υπόκεινται ολοένα και περισσότερο σε αποκλίνουσες απαιτήσεις, που επιβάλλονται από το εθνικό δίκαιο. Το γεγονός ότι ορισμένα κράτη μέλη επιβάλλουν λιγότερο αυστηρές απαιτήσεις ασφάλειας στις εν λόγω οντότητες όχι μόνο οδηγεί σε ποικίλα επίπεδα ανθεκτικότητας, αλλά και ενέχει τον κίνδυνο να επηρεάσει αρνητικά τη διατήρηση ζωτικών κοινωνικών λειτουργιών ή οικονομικών δραστηριοτήτων σε ολόκληρη την Ένωση, και προκαλεί εμπόδια στην ορθή λειτουργία της εσωτερικής αγοράς. Οι επενδυτές και οι εταιρείες μπορούν να βασίζονται στις ανθεκτικές κρίσιμες οντότητες και να τις εμπιστεύονται, αφού η αξιοπιστία και η εμπιστοσύνη αποτελούν τους ακρογωνιαίους λίθους μιας εύρυθμης εσωτερικής αγοράς. Παρόμοια είδη οντοτήτων θεωρούνται κρίσιμα σε ορισμένα κράτη μέλη αλλά όχι σε άλλα, ενώ και οι οντότητες που έχουν προσδιοριστεί ως κρίσιμες υπόκεινται σε αποκλίνουσες απαιτήσεις σε διαφορετικά κράτη μέλη. Η κατάσταση αυτή οδηγεί σε πρόσθετες και περιττές διοικητικές επιβαρύνσεις για τις εταιρείες που δραστηριοποιούνται σε διασυνοριακό επίπεδο, κυρίως για τις εταιρείες που δραστηριοποιούνται σε κράτη μέλη με αυστηρότερες απαιτήσεις. Επομένως, ένα ενωσιακό πλαίσιο θα είχε επίσης ως αποτέλεσμα την εξασφάλιση ισότιμων όρων ανταγωνισμού για τις κρίσιμες οντότητες σε ολόκληρη την Ένωση.

(7) Είναι αναγκαίο να καθοριστούν εναρμονισμένοι ελάχιστοι κανόνες για τη διασφάλιση της παροχής βασικών υπηρεσιών στην εσωτερική αγορά, την ενίσχυση της ανθεκτικότητας των κρίσιμων οντοτήτων και τη βελτίωση της διασυνοριακής συνεργασίας μεταξύ των αρμόδιων αρχών. Είναι σημαντικό οι κανόνες αυτοί να είναι διαχρονικοί ως προς τον σχεδιασμό και την εφαρμογή τους, και παράλληλα να εξασφαλίζουν την αναγκαία ευελιξία. Επίσης, έχει ζωτική σημασία να βελτιωθεί η ικανότητα των κρίσιμων οντοτήτων να παρέχουν βασικές υπηρεσίες έναντι ποικίλων κινδύνων.

(8) Για την επίτευξη υψηλού επιπέδου ανθεκτικότητας, τα κράτη μέλη θα πρέπει να προσδιορίσουν τις κρίσιμες οντότητες που θα υπόκεινται σε ειδικές απαιτήσεις και εποπτεία και θα λαμβάνουν ιδιαίτερη στήριξη και καθοδήγηση έναντι όλων των συναφών κινδύνων.

(9) Δεδομένης της σημασίας της κυβερνοασφάλειας για την ανθεκτικότητα των κρίσιμων οντοτήτων και για λόγους συνοχής, θα πρέπει να διασφαλιστεί, όπου είναι δυνατόν, συνοχή μεταξύ των προσεγγίσεων της παρούσας οδηγίας και της οδηγίας (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([5]). Υπό το φως της μεγαλύτερης συχνότητας και των ιδιαίτερων χαρακτηριστικών των κινδύνων στον κυβερνοχώρο, η οδηγία (ΕΕ) 2022/2555 επιβάλλει ολοκληρωμένες απαιτήσεις σε ένα ευρύ σύνολο οντοτήτων με στόχο τη διασφάλιση της κυβερνοασφάλειάς τους. Δεδομένου ότι η κυβερνοασφάλεια αντιμετωπίζεται επαρκώς από την οδηγία (ΕΕ) 2022/2555, τα ζητήματα που καλύπτονται από την εν λόγω οδηγία θα πρέπει να εξαιρεθούν από το πεδίο εφαρμογής της παρούσας οδηγίας, χωρίς να θίγεται το ειδικό καθεστώς των οντοτήτων του τομέα των ψηφιακών υποδομών.

(10) Όταν διατάξεις τομεακών νομοθετικών πράξεων της Ένωσης απαιτούν από κρίσιμες οντότητες να λάβουν μέτρα για την ενίσχυση της ανθεκτικότητάς τους και όταν οι εν λόγω απαιτήσεις αναγνωρίζονται από τα κράτη μέλη, ως τουλάχιστον ισοδύναμες με τις αντίστοιχες υποχρεώσεις που καθορίζονται στην παρούσα οδηγία, οι σχετικές διατάξεις της παρούσας οδηγίας δεν θα πρέπει να εφαρμόζονται, ώστε να αποφεύγονται οι αλληλεπικαλύψεις και οι περιττές επιβαρύνσεις. Στην περίπτωση αυτή, θα πρέπει να εφαρμόζονται οι σχετικές διατάξεις αυτών των νομοθετικών πράξεων της Ένωσης. Όταν δεν εφαρμόζονται οι σχετικές διατάξεις της παρούσας οδηγίας, δεν θα πρέπει να εφαρμόζονται ούτε οι διατάξεις περί εποπτείας και επιβολής που θεσπίζονται στην παρούσα οδηγία.

(11) Η παρούσα οδηγία δεν θίγει τις αρμοδιότητες των κρατών μελών και των αρχών τους όσον αφορά τη διοικητική αυτονομία, ή την ευθύνη τους για τη διαφύλαξη της εθνικής ασφάλειας και άμυνας ή την εξουσία τους να διαφυλάσσουν άλλες ουσιώδεις λειτουργίες του κράτους, ιδίως όσον αφορά τη δημόσια ασφάλεια, την εδαφική ακεραιότητα και τη διατήρηση της δημόσιας τάξης. Η εξαίρεση των φορέων δημόσιας διοίκησης από το πεδίο εφαρμογής της παρούσας οδηγίας θα πρέπει να ισχύει για τους φορείς των οποίων οι δραστηριότητες ασκούνται κατά κύριο λόγο στους τομείς της εθνικής ασφάλειας, της δημόσιας ασφάλειας, της άμυνας ή της επιβολής του νόμου, συμπεριλαμβανομένης της διερεύνησης, ανίχνευσης και δίωξης ποινικών αδικημάτων. Εν τούτοις, οι φορείς δημόσιας διοίκησης των οποίων οι δραστηριότητες σχετίζονται μόνον οριακά με τους εν λόγω τομείς θα πρέπει να εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας. Για τους σκοπούς της παρούσας οδηγίας, οι φορείς που διαθέτουν κανονιστικές αρμοδιότητες δεν θεωρείται ότι ασκούν δραστηριότητες στον τομέα της επιβολής του νόμου και, ως εκ τούτου, δεν εξαιρούνται για τους λόγους αυτούς από το πεδίο εφαρμογής της παρούσας οδηγίας. Οι φορείς δημόσιας διοίκησης που ιδρύονται από κοινού με τρίτη χώρα δυνάμει διεθνούς συμφωνίας, εξαιρούνται από το πεδίο εφαρμογής της παρούσας οδηγίας. Η παρούσα οδηγία δεν εφαρμόζεται στις διπλωματικές και προξενικές αποστολές των κρατών μελών σε τρίτες χώρες.

([5]) Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, για την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972 και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2) (βλέπε σελίδα 80 της παρούσας Επίσημης Εφημερίδας).

Ορισμένες κρίσιμες οντότητες ασκούν δραστηριότητες στους τομείς της εθνικής ασφάλειας, της δημόσιας ασφάλειας, της άμυνας ή της επιβολής του νόμου, συμπεριλαμβανομένης της διερεύνησης, του εντοπισμού και της δίωξης ποινικών αδικημάτων, ή παρέχουν υπηρεσίες αποκλειστικά σε φορείς δημόσιας διοίκησης οι οποίοι ασκούν δραστηριότητες κατά κύριο λόγο στους εν λόγω τομείς. Δεδομένης της ευθύνης που υπέχουν για τη διαφύλαξη της εθνικής ασφάλειας και άμυνας, τα κράτη μέλη θα πρέπει να μπορούν να αποφασίσουν ότι οι υποχρεώσεις των κρίσιμων οντοτήτων που θεσπίζονται στην παρούσα οδηγία δεν ισχύουν, εν όλω ή εν μέρει, για τις εν λόγω κρίσιμες οντότητες, εάν οι υπηρεσίες που παρέχουν ή οι δραστηριότητες που ασκούν σχετίζονται κατά κύριο λόγο με τους τομείς της εθνικής ασφάλειας, της δημόσιας ασφάλειας, της άμυνας ή της επιβολής του νόμου συμπεριλαμβανομένης της διερεύνησης, του εντοπισμού και της δίωξης ποινικών αδικημάτων. Οι κρίσιμες οντότητες των οποίων οι υπηρεσίες ή οι δραστηριότητες σχετίζονται μόνον οριακά με τους εν λόγω τομείς θα πρέπει να εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας. Κανένα κράτος μέλος δεν θα πρέπει να υποχρεούται να παρέχει πληροφορίες, η γνωστοποίηση των οποίων θα ήταν αντίθετη προς τα ουσιώδη συμφέροντα της εθνικής του ασφάλειας. Οι ενωσιακοί ή εθνικοί κανόνες για την προστασία διαβαθμισμένων πληροφοριών και οι συμφωνίες εμπιστευτικότητας είναι σημαντικές εν προκειμένω.

(12) Προκειμένου να μην τίθεται σε κίνδυνο η εθνική ασφάλεια ή η ασφάλεια και τα εμπορικά συμφέροντα των κρίσιμων οντοτήτων, οι ευαίσθητες πληροφορίες θα πρέπει να προσεγγίζονται, να ανταλλάσσονται και να τυγχάνουν χειρισμού με σύνεση και ιδιαίτερη προσοχή στους διαύλους διαβίβασης και τις ικανότητες αποθήκευσης που χρησιμοποιούνται.

(13) Για να διασφαλιστεί μια ολοκληρωμένη προσέγγιση όσον αφορά την ανθεκτικότητα των κρίσιμων οντοτήτων, κάθε κράτος μέλος θα πρέπει να έχει θεσπίσει στρατηγική για την ενίσχυση της ανθεκτικότητας των κρίσιμων οντοτήτων («στρατηγική»). Η στρατηγική θα πρέπει να καθορίζει τους στρατηγικούς στόχους και τα μέτρα πολιτικής που πρέπει να εφαρμοστούν. Για λόγους συνοχής και αποτελεσματικότητας, η στρατηγική θα πρέπει να σχεδιαστεί έτσι ώστε να ενσωματώνουν απρόσκοπτα τις υφιστάμενες πολιτικές, αξιοποιώντας, όπου είναι δυνατόν, τις σχετικές υφιστάμενες εθνικές και τομεακές στρατηγικές, σχέδια ή παρόμοια έγγραφα. Για να επιτευχθεί ολοκληρωμένη προσέγγιση, τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι οι στρατηγικές τους παρέχουν ένα πλαίσιο πολιτικής για ενισχυμένο συντονισμό μεταξύ των αρμόδιων αρχών βάσει της παρούσας οδηγίας και των αρμόδιων αρχών βάσει της οδηγίας (ΕΕ) 2022/2555 όσον αφορά την ανταλλαγή πληροφοριών σχετικά με τους κινδύνους κυβερνοασφάλειας, τις απειλές και τα περιστατικά στον κυβερνοχώρο και τους κινδύνους, τις απειλές και τα περιστατικά εκτός κυβερνοχώρου καθώς και στο πλαίσιο της άσκησης εποπτικών καθηκόντων. Όταν τα κράτη μέλη θεσπίζουν τις στρατηγικές τους, θα πρέπει να λαμβάνουν δεόντως υπόψη τον υβριδικό χαρακτήρα των απειλών κατά των κρίσιμων οντοτήτων.

(14) Τα κράτη μέλη θα πρέπει να κοινοποιούν στην Επιτροπή τις στρατηγικές τους και τις ουσιώδεις επικαιροποιήσεις τους, ιδίως για να μπορεί η Επιτροπή να αξιολογεί την ορθή εφαρμογή της παρούσας οδηγίας όσον αφορά τις προσεγγίσεις πολιτικής για την ανθεκτικότητα των κρίσιμων οντοτήτων σε εθνικό επίπεδο. Εάν χρειάζεται, οι στρατηγικές θα μπορούν να κοινοποιούνται ως διαβαθμισμένες πληροφορίες.. Η Επιτροπή θα πρέπει να καταρτίσει συνοπτική έκθεση των στρατηγικών που κοινοποιούνται από τα κράτη μέλη, η οποία θα χρησιμεύσει ως βάση για ανταλλαγές με σκοπό τον εντοπισμό βέλτιστων πρακτικών και ζητημάτων κοινού ενδιαφέροντος στο πλαίσιο της ομάδας για την ανθεκτικότητα των κρίσιμων οντοτήτων. Λόγω του ευαίσθητου χαρακτήρα των συγκεντρωτικών πληροφοριών, διαβαθμισμένων και μη, που περιλαμβάνονται στη συνοπτική έκθεση η Επιτροπή θα πρέπει να διαχειρίζεται τη συνοπτική έκθεση με τον δέοντα βαθμό επίγνωσης όσον αφορά την ασφάλεια των κρίσιμων οντοτήτων, των κρατών μελών και της Ένωσης. Η συνοπτική έκθεση και οι στρατηγικές θα πρέπει να προστατεύονται από παράνομες ή κακόβουλες ενέργειες και θα πρέπει να είναι προσβάσιμες μόνον από εξουσιοδοτημένα πρόσωπα για την εκπλήρωση των στόχων της παρούσας οδηγίας. Η κοινοποίηση των στρατηγικών και των ουσιωδών επικαιροποιήσεών τους θα πρέπει επίσης να βοηθήσει την Επιτροπή στην κατανόηση των εξελίξεων όσον αφορά τις προσεγγίσεις για την ανθεκτικότητα των κρίσιμων οντοτήτων και θα τροφοδοτεί την παρακολούθηση του αντικτύπου και της προστιθέμενης αξίας της παρούσας οδηγίας, την οποία η Επιτροπή θα επανεξετάζει τακτικά.

(15) Οι δράσεις των κρατών μελών για τον προσδιορισμό και την υποστήριξη της διασφάλισης της ανθεκτικότητας των κρίσιμων οντοτήτων θα πρέπει να ακολουθούν μια προσέγγιση βάσει κινδύνων, η οποία θα εστιάζει στις οντότητες με τη μεγαλύτερη σημασία για τη διεξαγωγή ζωτικών κοινωνικών λειτουργιών ή οικονομικών δραστηριοτήτων. Για τη διασφάλιση μιας τέτοιας στοχευμένης προσέγγισης, κάθε κράτος μέλος θα πρέπει να διενεργεί, εντός εναρμονισμένου πλαισίου, εκτίμηση των σχετικών φυσικών και ανθρωπογενών κινδύνων, συμπεριλαμβανομένων των κινδύνων διατομεακής ή διασυνοριακής φύσης, που ενδέχεται να επηρεάσουν την παροχή βασικών υπηρεσιών, στους οποίους περιλαμβάνονται, μεταξύ άλλων, ατυχήματα, φυσικές καταστροφές, καταστάσεις έκτακτης ανάγκης στον τομέα της δημόσιας υγείας –όπως οι πανδημίες και, οι υβριδικές απειλές ή άλλες ανταγωνιστικές απειλές, συμπεριλαμβανομένων των τρομοκρατικών εγκλημάτων, της διείσδυσης εγκληματικών στοιχείων και της δολιοφθοράς («εκτίμηση κινδύνου από τα κράτη μέλη»). Κατά τη διενέργεια των εκτιμήσεων κινδύνων από τα κράτη μέλη, τα κράτη μέλη θα πρέπει να λαμβάνουν υπόψη τους άλλες γενικές ή ειδικές τομεακές εκτιμήσεις κινδύνων που έχουν διενεργηθεί βάσει άλλων νομοθετικών πράξεων της Ένωσης, και θα πρέπει να εξετάζουν τον βαθμό στον οποίο οι τομείς εξαρτώνται ο ένας από τον άλλον, συμπεριλαμβανομένων των τομέων σε άλλα κράτη μέλη και τρίτες χώρες. Το αποτέλεσμα των εκτιμήσεων κινδύνων από τα κράτη μέλη μπορεί να χρησιμοποιηθεί για

τους σκοπούς προσδιορισμού των κρίσιμων οντοτήτων και για την υποστήριξη των εν λόγω οντοτήτων προκειμένου να εκπληρώσουν τις απαιτήσεις τους περί ανθεκτικότητας. Η παρούσα οδηγία εφαρμόζεται μόνο στα κράτη μέλη και στις κρίσιμες οντότητες που δραστηριοποιούνται εντός της Ένωσης. Ωστόσο, η εμπειρογνωσία και οι γνώσεις που παράγονται από τις αρμόδιες αρχές, ιδίως μέσω εκτιμήσεων κινδύνων, και από την Επιτροπή, ιδίως μέσω διαφόρων μορφών στήριξης και συνεργασίας, θα μπορούσαν να χρησιμοποιηθούν, κατά περίπτωση και σύμφωνα με τις ισχύουσες νομικές πράξεις, προς όφελος τρίτων χωρών, ιδίως στην άμεση γειτονία της Ένωσης, τροφοδοτώντας την υφιστάμενη συνεργασία για την ανθεκτικότητα.

(16) Προκειμένου να διασφαλιστεί ότι όλες οι συναφείς οντότητες υπόκεινται στις απαιτήσεις περί ανθεκτικότητας της παρούσας οδηγίας και για να μειωθούν οι αποκλίσεις εν προκειμένω, είναι σημαντικό να θεσπιστούν εναρμονισμένοι κανόνες που να καθιστούν δυνατό τον προσδιορισμό των κρίσιμων οντοτήτων με τρόπο συνεπή σε ολόκληρη την Ένωση και, παράλληλα, να δίνουν στα κράτη μέλη τη δυνατότητα να αποτυπώνουν καταλλήλως τον ρόλο και τη σημασία των οντοτήτων αυτών σε εθνικό επίπεδο. Όταν εφαρμόζει τα κριτήρια που καθορίζονται στην παρούσα οδηγία, κάθε κράτος μέλος θα πρέπει να προσδιορίζει τις οντότητες οι οποίες παρέχουν μία ή περισσότερες βασικές υπηρεσίες και δραστηριοποιούνται και διαθέτουν υποδομή ζωτικής σημασίας στο έδαφός του. Μια οντότητα θα πρέπει να θεωρείται ότι δραστηριοποιείται στο έδαφος του κράτους μέλους στο οποίο ασκεί δραστηριότητες που είναι αναγκαίες για την εν λόγω βασική υπηρεσία ή υπηρεσίες, και στο οποίο βρίσκεται η υποδομή ζωτικής σημασίας της εν λόγω οντότητας, η οποία χρησιμοποιείται για την παροχή της εν λόγω υπηρεσίας ή υπηρεσιών. Εάν σε κράτος μέλος δεν υπάρχει οντότητα που να πληροί αυτά τα κριτήρια, το κράτος μέλος δεν θα πρέπει να υποχρεούται να προσδιορίσει κρίσιμη οντότητα στον αντίστοιχο τομέα ή υποτομέα. Για λόγους αποτελεσματικότητας, αποδοτικότητας, συνέπειας και ασφάλειας δικαίου, θα πρέπει να θεσπιστούν κατάλληλοι κανόνες για την ενημέρωση των οντοτήτων ότι έχουν χαρακτηριστεί ως κρίσιμες οντότητες.

(17) Τα κράτη μέλη θα πρέπει να υποβάλλουν στην Επιτροπή, κατά τρόπο που να πληροί τους στόχους της παρούσας οδηγίας, κατάλογο των βασικών υπηρεσιών, τον αριθμό των κρίσιμων οντοτήτων που έχουν προσδιοριστεί για καθέναν από τους τομείς και υποτομείς που αναφέρονται στο παράρτημα και για τη βασική υπηρεσία ή υπηρεσίες που παρέχει κάθε οντότητα και, εφόσον εφαρμόζονται, τα κατώτατα όρια. Θα πρέπει να είναι δυνατόν να παρουσιάζονται τα κατώτατα όρια ως έχουν ή σε συγκεντρωτική μορφή, πράγμα που σημαίνει ότι οι πληροφορίες μπορούν να υπολογίζονται κατά μέσο όρο ανά γεωγραφική περιοχή, ανά έτος, ανά τομέα, ανά υποτομέα ή με άλλα μέσα, και μπορούν να περιλαμβάνουν στοιχεία σχετικά με το εύρος των παρεχόμενων δεικτών.

(18) Θα πρέπει να καθοριστούν κριτήρια προκειμένου να προσδιορίζεται πόσο σημαντική είναι η διαταραχή που προκαλείται από ένα περιστατικό. Τα εν λόγω κριτήρια θα πρέπει να βασίζονται στα κριτήρια που προβλέπονται στην οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([6]) ώστε να αξιοποιηθούν οι προσπάθειες που έχουν καταβληθεί από τα κράτη μέλη για τον προσδιορισμό των φορέων εκμετάλλευσης βασικών υπηρεσιών, όπως ορίζονται στην εν λόγω οδηγία και η εμπειρία που έχει αποκτηθεί συναφώς. Μείζονες κρίσεις, όπως η πανδημία της COVID-19, κατέδειξαν πόσο σημαντική είναι η εγγύηση της ασφάλειας της αλυσίδας εφοδιασμού και πώς η διατάραξη της λειτουργίας της μπορεί να έχει αρνητικές οικονομικές και κοινωνικές επιπτώσεις σε πολλούς τομείς και σε διασυνοριακό επίπεδο. Συνεπώς, τα κράτη μέλη θα πρέπει επίσης να εξετάζουν τις επιπτώσεις στην αλυσίδα εφοδιασμού, στο μέτρο του δυνατού, κατά τον καθορισμό του βαθμού στον οποίο άλλοι τομείς και υποτομείς εξαρτώνται από την απαραίτητη υπηρεσία που παρέχεται από μια κρίσιμη οντότητα.

(19) Σύμφωνα με την ισχύουσα ενωσιακή και εθνική νομοθεσία, συμπεριλαμβανομένου του κανονισμού (ΕΕ) 2019/452 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([7]), ο οποίος θεσπίζει ένα πλαίσιο για τον έλεγχο των άμεσων ξένων επενδύσεων στην Ένωση, η πιθανή απειλή που δημιουργεί η ξένη ιδιοκτησία κρίσιμων υποδομών εντός της Ένωσης πρέπει να αναγνωριστεί, διότι οι υπηρεσίες, η οικονομία και η ελεύθερη κυκλοφορία και η ασφάλεια των πολιτών της Ένωσης εξαρτώνται από την ορθή λειτουργία κρίσιμων υποδομών.

(20) Η οδηγία (ΕΕ) 2022/2555 απαιτεί από τις οντότητες που ανήκουν στον τομέα των ψηφιακών υποδομών, οι οποίες ενδέχεται να χαρακτηριστούν κρίσιμες οντότητες βάσει της παρούσας οδηγίας, να λαμβάνουν κατάλληλα και αναλογικά τεχνικά, επιχειρησιακά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων που απειλούν την ασφάλεια των συστημάτων δικτύου και πληροφοριών και για την κοινοποίηση σημαντικών περιστατικών και κυβερνοαπειλών. Δεδομένου ότι οι απειλές για την ασφάλεια των συστημάτων δικτύου και πληροφοριών μπορεί να έχουν διαφορετικές προελεύσεις, η οδηγία (ΕΕ) 2022/2555 εφαρμόζει μια προσέγγιση «έναντι όλων των κινδύνων» που περιλαμβάνει την ανθεκτικότητα των συστημάτων δικτύου και πληροφοριών, καθώς και των υλικών συστατικών στοιχείων και του περιβάλλοντος των εν λόγω συστημάτων.

([6]) Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση (ΕΕ L 194 της 19.7.2016, σ. 1).

([7]) Κανονισμός (ΕΕ) 2019/452 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 19ης Μαρτίου 2019, για τη θέσπιση πλαισίου για τον έλεγχο των άμεσων ξένων επενδύσεων στην Ένωση (ΕΕ L 79 I της 21.3.2019, σ. 1).

Δεδομένου ότι οι απαιτήσεις που καθορίζονται στην οδηγία (ΕΕ) 2022/2555 εν προκειμένω είναι τουλάχιστον ισοδύναμες με τις αντίστοιχες υποχρεώσεις που καθορίζονται στην παρούσα οδηγία, οι υποχρεώσεις που καθορίζονται στο άρθρο 11 και τα κεφάλαια III, IV και VI της παρούσας οδηγίας δεν θα πρέπει να εφαρμόζονται σε οντότητες που ανήκουν στον τομέα των ψηφιακών υποδομών ώστε να αποφεύγονται οι αλληλεπικαλύψεις και η περιττή διοικητική επιβάρυνση. Ωστόσο, λαμβανομένης υπόψη της σημασίας των υπηρεσιών που παρέχονται από οντότητες που ανήκουν στον τομέα των ψηφιακών υποδομών σε κρίσιμες οντότητες που ανήκουν σε όλους τους άλλους τομείς, τα κράτη μέλη θα πρέπει να προσδιορίζουν, με βάση τα κριτήρια και με τη διαδικασία που προβλέπεται στην παρούσα οδηγία οντότητες που ανήκουν στον τομέα των ψηφιακών υποδομών ως κρίσιμες οντότητες. Κατά συνέπεια, θα πρέπει να εφαρμόζονται οι στρατηγικές, οι εκτιμήσεις κινδύνων από τα κράτη μέλη και τα μέτρα στήριξης που καθορίζονται στο κεφάλαιο II της παρούσας οδηγίας. Τα κράτη μέλη θα πρέπει να μπορούν να θεσπίζουν ή να διατηρούν διατάξεις του εθνικού δικαίου για την επίτευξη υψηλότερου επιπέδου ανθεκτικότητας για τις εν λόγω κρίσιμες οντότητες, υπό την προϋπόθεση ότι οι εν λόγω διατάξεις συνάδουν με το εφαρμοστέο ενωσιακό δίκαιο.

(21) Το δίκαιο της Ένωσης στον τομέα των χρηματοπιστωτικών υπηρεσιών επιβάλλει στις χρηματοπιστωτικές οντότητες ολοκληρωμένες υποχρεώσεις να διαχειρίζονται όλους τους κινδύνους τους οποίους αντιμετωπίζουν, συμπεριλαμβανομένων των λειτουργικών κινδύνων, και να διασφαλίζουν την επιχειρησιακή συνέχεια. Στο εν λόγω δίκαιο περιλαμβάνονται οι κανονισμοί (ΕΕ) αριθ. 648/2012 ([8]), (ΕΕ) αριθ. 575/2013 ([9]) και (ΕΕ) αριθ. 600/2014 ([10]) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και οι οδηγίες 2013/36/ΕΕ ([11]) και 2014/65/ΕΕ ([12]) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου. Το νομικό πλαίσιο αυτό συμπληρώνεται με τον κανονισμό (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([13]), ο οποίος θεσπίζει υποχρεώσεις που ισχύουν για τις χρηματοπιστωτικές επιχειρήσεις όσον αφορά τη διαχείριση των κινδύνων από την τεχνολογία πληροφοριών και επικοινωνιών (ΤΠΕ), μεταξύ άλλων και σχετικά με την προστασία των υλικών υποδομών ΤΠΕ. Δεδομένου, επομένως, ότι η ανθεκτικότητα των εν λόγω οντοτήτων καλύπτεται λεπτομερώς, το άρθρο 11 και τα κεφάλαια III, IV και VI της παρούσας οδηγίας δεν θα πρέπει να εφαρμόζονται στις εν λόγω οντότητες, ώστε να αποφεύγονται οι αλληλεπικαλύψεις και η περιττή διοικητική επιβάρυνση.

Ωστόσο, λαμβανομένης υπόψη της σημασίας των υπηρεσιών που παρέχονται από οντότητες του χρηματοπιστωτικού τομέα σε κρίσιμες οντότητες που ανήκουν σε όλους τους άλλους τομείς, τα κράτη μέλη θα πρέπει να προσδιορίζουν, με βάση τα κριτήρια και με τη διαδικασία που προβλέπεται στην παρούσα οδηγία, οντότητες των χρηματοπιστωτικών τομέων ως κρίσιμες οντότητες. Κατά συνέπεια, θα πρέπει να εφαρμόζονται οι στρατηγικές, οι εκτιμήσεις κινδύνων από τα κράτη μέλη και τα μέτρα στήριξης που καθορίζονται στο κεφάλαιο II της παρούσας οδηγίας. Τα κράτη μέλη θα πρέπει να μπορούν να θεσπίζουν ή να διατηρούν διατάξεις του εθνικού δικαίου για την επίτευξη υψηλότερου επιπέδου ανθεκτικότητας για τις εν λόγω κρίσιμες οντότητες, υπό την προϋπόθεση ότι αυτές οι διατάξεις συνάδουν με το εφαρμοστέο ενωσιακό δίκαιο.

(22) Τα κράτη μέλη θα πρέπει να ορίσουν ή να συστήσουν αρχές αρμόδιες για την εποπτεία της εφαρμογής, και, όταν είναι απαραίτητο, την επιβολή των κανόνων της παρούσας οδηγίας και να διασφαλίζουν ότι οι εν λόγω αρχές διαθέτουν κατάλληλες εξουσίες και πόρους. Δεδομένων των διαφορών μεταξύ των εθνικών δομών διακυβέρνησης, προκειμένου να μην υπονομευθούν ήδη υφιστάμενες τομεακές ρυθμίσεις ή εποπτικοί και ρυθμιστικοί φορείς της Ένωσης, και προς αποφυγή αλληλεπικαλύψεων, τα κράτη μέλη θα πρέπει να έχουν τη δυνατότητα να ορίσουν ή να συστήσουν περισσότερες από μία αρμόδιες αρχές. Όταν τα κράτη μέλη ορίσουν ή συστήσουν περισσότερες από μία αρμόδιες αρχές θα πρέπει να οριοθετήσουν σαφώς τα αντίστοιχα καθήκοντα των εκάστοτε αρχών και να διασφαλίσουν ότι αυτές συνεργάζονται απρόσκοπτα και αποτελεσματικά. Όλες οι αρμόδιες αρχές θα πρέπει επίσης να συνεργάζονται γενικότερα με άλλες σχετικές αρχές, τόσο σε ενωσιακό όσο και σε εθνικό επίπεδο.

([8]) Κανονισμός (ΕΕ) αριθ. 648/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 4ης Ιουλίου 2012, για τα εξωχρηματιστηριακά παράγωγα, τους κεντρικούς αντισυμβαλλομένους και τα αρχεία καταγραφής συναλλαγών (ΕΕ L 201 της 27.7.2012, σ. 1).

([9]) Κανονισμός (ΕΕ) αριθ. 575/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Ιουνίου 2013, σχετικά με τις απαιτήσεις προληπτικής εποπτείας για πιστωτικά ιδρύματα και την τροποποίηση του κανονισμού (ΕΕ) αριθ. 648/201 (ΕΕ L 176 της 27.6.2013, σ. 1).

([10]) Κανονισμός (ΕΕ) αριθ. 600/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαΐου 2014, για τις αγορές χρηματοπιστωτικών μέσων και για την τροποποίηση του κανονισμού (ΕΕ) αριθ. 648/2012 (ΕΕ L 173 της 12.6.2014, σ. 84).

([11]) Οδηγία 2013/36/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Ιουνίου 2013, σχετικά με την πρόσβαση στη δραστηριότητα πιστωτικών ιδρυμάτων και την προληπτική εποπτεία πιστωτικών ιδρυμάτων και επιχειρήσεων επενδύσεων, για την τροποποίηση της οδηγίας 2002/87/ΕΚ και για την κατάργηση των οδηγιών 2006/48/ΕΚ και 2006/49/ΕΚ (ΕΕ L 176 της 27.6.2013, σ. 338).

([12]) Οδηγία 2014/65/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαΐου 2014, για τις αγορές χρηματοπιστωτικών μέσων και την τροποποίηση της οδηγίας 2002/92/ΕΚ και της οδηγίας 2011/61/ΕΕ (ΕΕ L 173 της 12.6.2014, σ. 349).

([13]) Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (βλέπε σελίδα 1 της παρούσας Επίσημης Εφημερίδας).

(23) Προκειμένου να διευκολύνεται η διασυνοριακή συνεργασία και επικοινωνία και να είναι δυνατή η αποτελεσματική εφαρμογή της παρούσας οδηγίας, κάθε κράτος μέλος θα πρέπει, με την επιφύλαξη των απαιτήσεων των τομεακών νομικών πράξεων της Ένωσης, να ορίσει ένα ενιαίο σημείο επαφής υπεύθυνο για τον συντονισμό των ζητημάτων που άπτονται της ανθεκτικότητας των κρίσιμων οντοτήτων και της σχετικής διασυνοριακής συνεργασίας σε ενωσιακό επίπεδο («ενιαίο σημείο επαφής»), κατά περίπτωση εντός αρμόδιας αρχής. Κάθε ενιαίο σημείο επαφής θα πρέπει να λειτουργεί ως σύνδεσμος και να συντονίζει την επικοινωνία, κατά περίπτωση, με τις αρμόδιες αρχές του κράτους μέλους του, με τα ενιαία σημεία επαφής άλλων κρατών μελών και με την ομάδα για την ανθεκτικότητα των κρίσιμων οντοτήτων.

(24) Οι αρμόδιες αρχές σύμφωνα με την παρούσα οδηγία και οι αρμόδιες αρχές σύμφωνα με την οδηγία (ΕΕ) 2022/2555 θα πρέπει να συνεργάζονται και να ανταλλάσσουν πληροφορίες όσον αφορά τους κινδύνους κυβερνοασφάλειας, τις απειλές και τα περιστατικά στον κυβερνοχώρο και τους κινδύνους, τις απειλές και τα περιστατικά εκτός κυβερνοχώρου που επηρεάζουν κρίσιμες οντότητες, καθώς και σε σχέση με τα οικεία μέτρα που λαμβάνονται από τις αρμόδιες αρχές σύμφωνα με την παρούσα οδηγία και τις αρμόδιες αρχές σύμφωνα με την οδηγία (ΕΕ) 2022/2555. Είναι σημαντικό τα κράτη μέλη να διασφαλίζουν ότι οι απαιτήσεις που προβλέπονται στην παρούσα οδηγία και στην οδηγία (ΕΕ) 2022/2555 εφαρμόζονται συμπληρωματικά και ότι οι κρίσιμες οντότητες δεν υπόκεινται σε διοικητική επιβάρυνση πέραν της αναγκαίας για την επίτευξη των στόχων της παρούσας οδηγίας και της εν λόγω οδηγίας.

(25) Τα κράτη μέλη θα πρέπει να υποστηρίζουν τις κρίσιμες οντότητες, μεταξύ άλλων τις χαρακτηριζόμενες ως μικρές ή μεσαίες επιχειρήσεις, για την ενίσχυση της ανθεκτικότητάς τους, σύμφωνα με τις υποχρεώσεις του κράτους μέλους οι οποίες καθορίζονται στην παρούσα οδηγία, χωρίς να θίγεται η ιδία νομική ευθύνη των κρίσιμων οντοτήτων να διασφαλίζουν τη σχετική συμμόρφωσή τους, και στο πλαίσιο αυτό να αποφεύγουν την υπερβολική διοικητική επιβάρυνση. Ειδικότερα, τα κράτη μέλη θα μπορούσαν να αναπτύξουν υλικό καθοδήγησης και μεθοδολογίες, να υποστηρίξουν τη διοργάνωση ασκήσεων για τον έλεγχο της ανθεκτικότητας των κρίσιμων οντοτήτων και να παρέχουν συμβουλές και κατάρτιση στο προσωπικό των κρίσιμων οντοτήτων. Όταν είναι αναγκαίο και αιτιολογημένο για λόγους δημοσίου συμφέροντος, τα κράτη μέλη θα μπορούσαν να παρέχουν χρηματοδοτικούς πόρους και θα πρέπει να διευκολύνουν την οικειοθελή ανταλλαγή πληροφοριών και ορθών πρακτικών μεταξύ κρίσιμων οντοτήτων, με την επιφύλαξη της εφαρμογής των κανόνων ανταγωνισμού που ορίζονται στη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ).

(26) Με στόχο την ενίσχυση της ανθεκτικότητας των κρίσιμων οντοτήτων που προσδιορίζονται από τα κράτη μέλη και τη μείωση της διοικητικής επιβάρυνσης για τις εν λόγω κρίσιμες οντότητες, οι αρμόδιες αρχές θα πρέπει να διαβουλεύονται μεταξύ τους, όποτε κρίνεται σκόπιμο, για να εξασφαλιστεί η συνεπής εφαρμογή της παρούσας οδηγίας. Οι διαβουλεύσεις θα πρέπει να πραγματοποιούνται κατόπιν αιτήματος οποιασδήποτε ενδιαφερόμενης αρμόδιας αρχής και θα πρέπει να επικεντρώνονται στη διασφάλιση συγκλίνουσας προσέγγισης όσον αφορά τις διασυνδεδεμένες κρίσιμες οντότητες που χρησιμοποιούν υποδομές ζωτικής σημασίας οι οποίες συνδέονται φυσικά μεταξύ δύο ή περισσότερων κρατών μελών, ανήκουν στους ίδιους ομίλους ή εταιρικές δομές ή έχουν προσδιοριστεί σε ένα κράτος μέλος και παρέχουν βασικές υπηρεσίες προς άλλα κράτη μέλη ή εντός αυτών.

(27) Όταν διατάξεις του ενωσιακού ή του εθνικού δικαίου απαιτούν από τις κρίσιμες οντότητες να διενεργούν εκτίμηση των κινδύνων που σχετίζονται με τους σκοπούς της παρούσας οδηγίας και να λαμβάνουν μέτρα για τη διασφάλιση της ανθεκτικότητάς τους, οι εν λόγω απαιτήσεις θα πρέπει να λαμβάνονται καταλλήλως υπόψη για τον σκοπό της εποπτείας της συμμόρφωσης των κρίσιμων οντοτήτων με τις διατάξεις της παρούσας οδηγίας.

(28) Οι κρίσιμες οντότητες θα πρέπει να έχουν ολοκληρωμένη επίγνωση των συναφών κινδύνων στους οποίους εκτίθενται και υποχρέωση να διενεργούν σχετική ανάλυση κινδύνων. Για τον σκοπό αυτόν, θα πρέπει να διενεργούν εκτιμήσεις κινδύνων κάθε φορά που κρίνεται αναγκαίο υπό το πρίσμα των ιδιαίτερων συνθηκών τους και της εξέλιξης των εκάστοτε κινδύνων, και σε κάθε περίπτωση ανά τετραετία, προκειμένου να αξιολογήσουν όλους τους σχετικούς κινδύνους που θα μπορούσαν να διαταράξουν την παροχή των βασικών υπηρεσιών τους («αξιολόγηση κινδύνου κρίσιμης οντότητας»). Όταν οι κρίσιμες οντότητες έχουν προβεί σε άλλες εκτιμήσεις κινδύνων ή έχουν καταρτίσει έγγραφα σύμφωνα με υποχρεώσεις που προβλέπονται σε άλλες νομοθετικές πράξεις και σχετίζονται με την οικεία εκτίμηση κινδύνων κρίσιμων οντοτήτων, θα πρέπει να μπορούν να χρησιμοποιούν τις εν λόγω εκτιμήσεις και τα εν λόγω έγγραφα προκειμένου να συμμορφωθούν με τις απαιτήσεις που ορίζονται στην παρούσα οδηγία σχετικά με τις εκτιμήσεις κινδύνου κρίσιμων οντοτήτων. Μια αρμόδια αρχή θα πρέπει να μπορεί να δηλώσει ότι μια υφιστάμενη εκτίμηση κινδύνων που διενεργήθηκε από μια κρίσιμη οντότητα και αφορά τους σχετικούς κινδύνους και τη σχετική έκταση της εξάρτησης συμμορφώνεται, εν όλω ή εν μέρει, με τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία.

(29) Οι κρίσιμες οντότητες θα πρέπει να λαμβάνουν τεχνικά και οργανωτικά μέτρα και μέτρα ασφάλειας που είναι κατάλληλα και αναλογικά προς τους κινδύνους που αντιμετωπίζουν ώστε να προλαμβάνουν, να προστατεύουν, να αντιδρούν, να αντιστέκονται, να μετριάζουν, να απορροφούν, να προσαρμόζονται και να ανακάμπτουν από περιστατικά. Μολονότι οι κρίσιμες οντότητες θα πρέπει να λαμβάνουν τα εν λόγω μέτρα σύμφωνα με την παρούσα οδηγία, οι λεπτομέρειες και η έκταση τέτοιων μέτρων θα πρέπει να αντικατοπτρίζουν τους διαφορετικούς κινδύνους που η κάθε κρίσιμη οντότητα έχει προσδιορίσει στο πλαίσιο της εκτίμησης κινδύνων κρίσιμης οντότητάς της και τις ιδιαιτερότητες της εκάστοτε οντότητας, με κατάλληλο και αναλογικό τρόπο. Για την προώθηση μιας συνεκτικής προσέγγισης σε επίπεδο Ένωσης, η Επιτροπή θα πρέπει, κατόπιν διαβούλευσης με την ομάδα για την ανθεκτικότητα των κρίσιμων οντοτήτων, να εγκρίνει μη δεσμευτικές κατευθυντήριες γραμμές για τον περαιτέρω προσδιορισμό των εν λόγω τεχνικών μέτρων, μέτρων ασφάλειας και οργανωτικών μέτρων. Τα κράτη μέλη θα πρέπει να εξασφαλίζουν ότι κάθε κρίσιμη οντότητα ορίζει έναν αξιωματικό σύνδεσμο ή ισοδύναμο υπάλληλο ως σημείο επαφής με τις αρμόδιες αρχές.

(30) Για λόγους αποτελεσματικότητας και λογοδοσίας, οι κρίσιμες οντότητες θα πρέπει να περιγράφουν τα μέτρα που λαμβάνουν, με βαθμό λεπτομέρειας που επιτυγχάνει επαρκώς τους στόχους αποτελεσματικότητας και λογοδοσίας, λαμβανομένων υπόψη των κινδύνων που έχουν προσδιοριστεί, σε σχέδιο ανθεκτικότητας ή σε ισοδύναμο έγγραφο ή έγγραφα, και να εφαρμόζουν το σχέδιο αυτό στην πράξη. Όταν μια κρίσιμη οντότητα έχει ήδη λάβει τεχνικά και οργανωτικά μέτρα και μέτρα ασφάλειας και έχει καταρτίσει έγγραφα σύμφωνα με άλλες νομοθετικές πράξεις που αφορούν μέτρα ενίσχυσης της ανθεκτικότητας βάσει της παρούσας οδηγίας, θα πρέπει να είναι εφικτό, προς αποφυγή αλληλεπικάλυψης, να μπορεί να χρησιμοποιεί τα εν λόγω μέτρα και έγγραφα για την εκπλήρωση των απαιτήσεων όσον αφορά τα μέτρα ανθεκτικότητας σύμφωνα με την παρούσα οδηγία. Προκειμένου να αποφευχθεί η αλληλοεπικάλυψη, μια αρμόδια αρχή θα πρέπει να μπορεί να δηλώσει ότι τα υφιστάμενα μέτρα ανθεκτικότητας που έχει λάβει μια κρίσιμη οντότητα τα οποία ανταποκρίνονται στην υποχρέωσή της να λαμβάνει τεχνικά, και οργανωτικά μέτρα και μέτρα ασφαλείας σύμφωνα με την παρούσα οδηγία συμμορφώνονται, εν όλω ή εν μέρει, με τις απαιτήσεις της παρούσας οδηγίας.

(31) Οι κανονισμοί (ΕΚ) αριθ. 725/2004 ([14]) και (ΕΚ) αριθ. 300/2008 ([15]) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και η οδηγία 2005/65/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([16]) θεσπίζουν απαιτήσεις που εφαρμόζονται στις οντότητες των τομέων των αεροπορικών και θαλάσσιων μεταφορών με σκοπό την πρόληψη περιστατικών που οφείλονται σε παράνομες πράξεις και την αντιμετώπιση και τον μετριασμό των συνεπειών τέτοιων περιστατικών. Μολονότι τα μέτρα που απαιτούνται βάσει της παρούσας οδηγίας είναι ευρύτερα όσον αφορά τους κινδύνους που καλύπτουν και τα είδη των μέτρων που πρέπει να λαμβάνονται, οι κρίσιμες οντότητες στους εν λόγω τομείς θα πρέπει να αποτυπώνουν στο σχέδιο ανθεκτικότητας ή στα ισοδύναμα έγγραφά τους τα μέτρα που έχουν λάβει σύμφωνα με αυτές τις άλλες νομικές πράξεις της Ένωσης. Οι κρίσιμες οντότητες πρέπει επίσης να λάβουν υπόψη την οδηγία 2008/96/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([17]), η οποία καθιερώνει αξιολόγηση ολόκληρου του οδικού δικτύου για τη χαρτογράφηση του κινδύνου ατυχημάτων και στοχευμένη επιθεώρηση οδικής ασφάλειας για τον εντοπισμό επικίνδυνων συνθηκών, ελαττωμάτων και προβλημάτων που αυξάνουν τον κίνδυνο ατυχημάτων και τραυματισμών, με βάση επιτόπιες επισκέψεις σε υφιστάμενες οδούς ή τμήματα οδών. Η διασφάλιση της προστασίας και της ανθεκτικότητας των κρίσιμων οντοτήτων είναι υψίστης σημασίας για τον σιδηροδρομικό τομέα και, όταν οι κρίσιμες οντότητες εφαρμόζουν μέτρα ανθεκτικότητας βάσει της παρούσας οδηγίας, παροτρύνονται να αναφέρονται σε μη δεσμευτικές κατευθυντήριες γραμμές και έγγραφα ορθών πρακτικών που έχουν αναπτυχθεί στο πλαίσιο τομεακών αξόνων εργασιών, όπως η πλατφόρμα της ΕΕ για την ασφάλεια των επιβατών σιδηροδρομικών μεταφορών που συστάθηκε με την απόφαση 2018/C/ 232/03 της Επιτροπής ([18]).

(32) Για παράδειγμα, ο κίνδυνος κατάχρησης των δικαιωμάτων τους πρόσβασης εντός της οντότητας με σκοπό την πρόκληση βλάβης και ζημίας από υπαλλήλους κρίσιμων οντοτήτων ή τους υπεργολάβους τους εγείρει ολοένα και περισσότερες ανησυχίες. Τα κράτη μέλη θα πρέπει συνεπώς να καθορίζουν τις προϋποθέσεις σύμφωνα με τις οποίες επιτρέπεται στις κρίσιμες οντότητες, σε δεόντως αιτιολογημένες περιπτώσεις και λαμβανομένων υπόψη των εκτιμήσεων κινδύνων από τα κράτη μέλη, να υποβάλλουν αιτήματα για ελέγχους ιστορικού των προσώπων που εμπίπτουν σε συγκεκριμένες κατηγορίες του προσωπικού τους. Πρέπει να διασφαλίζεται ότι οι αρμόδιες αρχές αξιολογούν τα αιτήματα αυτά εντός εύλογης προθεσμίας και ότι η επεξεργασία τους γίνεται σύμφωνα με το εθνικό δίκαιο και τις εθνικές διαδικασίες και τη σχετική εφαρμοστέα ενωσιακή νομοθεσία, μεταξύ άλλων όσον αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα. Προκειμένου να επιβεβαιώνεται η ταυτότητα προσώπου το οποίο υποβάλλεται σε έλεγχο ιστορικού, είναι σκόπιμο τα κράτη μέλη να απαιτούν αποδεικτικό ταυτότητας, όπως διαβατήριο, εθνικό δελτίο ταυτότητας ή ψηφιακή μορφή ταυτοποίησης, σύμφωνα με το εφαρμοστέο δίκαιο.

([14]) Κανονισμός (ΕΚ) αριθ. 725/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 31ης Μαρτίου 2004, για τη βελτίωση της ασφάλειας στα πλοία και στις λιμενικές εγκαταστάσεις (ΕΕ L 129 της 29.4.2004, σ. 6).

([15]) Κανονισμός (ΕΚ) αριθ. 300/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαρτίου 2008, για τη θέσπιση κοινών κανόνων στο πεδίο της ασφάλειας της πολιτικής αεροπορίας και την κατάργηση του κανονισμού (ΕΚ) αριθ. 2320/2002 (ΕΕ L 97 της 9.4.2008, σ. 72).

([16]) Οδηγία 2005/65/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Οκτωβρίου 2005, σχετικά με την ενίσχυση της ασφαλείας των λιμένων (ΕΕ L 310 της 25.11.2005, σ. 28).

([17]) Οδηγία 2008/96/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 19ης Νοεμβρίου 2008, για τη διαχείριση της ασφάλειας των οδικών υποδομών (ΕΕ L 319 της 29.11.2008, σ. 59).

([18]) Απόφαση της Επιτροπής, της 29ης Ιουνίου 2018, για τη σύσταση της πλατφόρμας της ΕΕ για την ασφάλεια των επιβατών σιδηροδρομικών μεταφορών από έκνομες ενέργειες 20018/C 232/03 (ΕΕ C 232 της 3.7.2018, σ. 10).

Οι έλεγχοι ιστορικού θα πρέπει να περιλαμβάνουν έλεγχο του ποινικού μητρώου του προσώπου ενδιαφέροντος. Τα κράτη μέλη θα πρέπει να χρησιμοποιούν το Ευρωπαϊκό Σύστημα Πληροφοριών Ποινικού Μητρώου, σύμφωνα με τις διαδικασίες που ορίζονται στην απόφαση-πλαίσιο 2009/315/ΔΕΥ ([19]) του Συμβουλίου και, κατά περίπτωση και εφόσον κρίνεται σκόπιμο, στον κανονισμό (ΕΕ) 2019/816 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([20]), προκειμένου να λαμβάνουν πληροφορίες από τα ποινικά μητρώα που τηρούνται σε άλλα κράτη μέλη. Τα κράτη μέλη μπορούν επίσης, κατά περίπτωση και εφόσον κρίνεται σκόπιμο, να βασίζονται σε πληροφορίες του Συστήματος Πληροφοριών Σένγκεν δεύτερης γενιάς (SIS II) το οποίο συστάθηκε με τον κανονισμό (ΕΕ) 2018/1862 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([21]), σε πληροφορίες ασφάλειας και σε κάθε άλλη διαθέσιμη αντικειμενική πληροφορία που ενδέχεται να είναι αναγκαία για να διαπιστωθεί η καταλληλότητα του προσώπου ενδιαφέροντος να εργαστεί στη θέση για την οποία η κρίσιμη οντότητα έχει ζητήσει έλεγχο ιστορικού.

(33) Θα πρέπει να θεσπιστεί μηχανισμός για την κοινοποίηση ορισμένων περιστατικών, ο οποίος θα δίνει στις αρμόδιες αρχές τη δυνατότητα να ανταποκρίνονται σε περιστατικά με ταχύ και κατάλληλο τρόπο και να έχουν ολοκληρωμένη εποπτεία των επιπτώσεων, της φύσης, της αιτίας και των πιθανών συνεπειών περιστατικών που αντιμετωπίζουν οι κρίσιμες οντότητες. Οι κρίσιμες οντότητες θα πρέπει να κοινοποιούν αμελλητί στις αρμόδιες αρχές τα περιστατικά που προκαλούν ή έχουν τη δυνατότητα να προκαλέσουν σημαντική διαταραχή στην παροχή βασικών υπηρεσιών. Οι κρίσιμες οντότητες θα πρέπει να υποβάλουν αρχική κοινοποίηση το αργότερο εντός 24 ωρών από τη στιγμή που λαμβάνουν γνώση ενός περιστατικού, εκτός εάν δεν υπάρχει η σχετική επιχειρησιακή δυνατότητα. Η αρχική κοινοποίηση θα πρέπει να περιλαμβάνει μόνο τις πληροφορίες που είναι απολύτως αναγκαίες για να ενημερωθεί η αρμόδια αρχή σχετικά με το περιστατικό και να δοθεί η δυνατότητα στην κρίσιμη οντότητα να ζητήσει συνδρομή, αν απαιτείται. Στην κοινοποίηση θα πρέπει να αναφέρεται, ει δυνατόν, η εικαζόμενη αιτία του περιστατικού. Τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι η απαίτηση υποβολής αυτής της αρχικής κοινοποίησης δεν εκτρέπει τους πόρους της αναφέρουσας κρίσιμης οντότητας από δραστηριότητες που σχετίζονται με τον χειρισμό περιστατικών, στις οποίες θα πρέπει να δίνεται προτεραιότητα. Η αρχική κοινοποίηση θα πρέπει να ακολουθείται, κατά περίπτωση, από λεπτομερή έκθεση το αργότερο έναν μήνα μετά το περιστατικό. Η λεπτομερής έκθεση θα πρέπει να συμπληρώνει την αρχική κοινοποίηση και να παρέχει πληρέστερη επισκόπηση του περιστατικού.

(34) Η τυποποίηση θα πρέπει να παραμείνει πρωτίστως διαδικασία καθοδηγούμενη από την αγορά. Ωστόσο, ενδέχεται να υπάρχουν ακόμη περιπτώσεις στις οποίες είναι σκόπιμο να απαιτείται συμμόρφωση με συγκεκριμένα πρότυπα. Τα κράτη μέλη θα πρέπει, όταν κρίνεται χρήσιμο, να ενθαρρύνουν τη χρήση ευρωπαϊκών και διεθνών προτύπων και τεχνικών προδιαγραφών σχετικών με τα μέτρα ασφάλειας και ανθεκτικότητας που εφαρμόζονται σε κρίσιμες οντότητες.

(35) Ενώ οι κρίσιμες οντότητες γενικά λειτουργούν ως μέρος ενός ολοένα και πιο διασυνδεδεμένου δικτύου παροχής υπηρεσιών και υποδομών και συχνά παρέχουν βασικές υπηρεσίες σε περισσότερα από ένα κράτη μέλη, ορισμένες από αυτές τις κρίσιμες οντότητες είναι ιδιαίτερου ενδιαφέροντος για την Ένωση και την εσωτερική αγορά της διότι παρέχουν βασικές υπηρεσίες προς ή εντός έξι ή περισσοτέρων κρατών μελών και, ως εκ τούτου, θα μπορούσαν να επωφεληθούν από ειδική στήριξη σε επίπεδο Ένωσης. Επομένως, θα πρέπει να θεσπιστούν κανόνες σχετικά με τις συμβουλευτικές αποστολές όσον αφορά τέτοιες κρίσιμες οντότητες ιδιαίτερου ευρωπαϊκού ενδιαφέροντος. Οι κανόνες αυτοί δεν θίγουν τους κανόνες περί εποπτείας και επιβολής που προβλέπονται στην παρούσα οδηγία.

(36) Κατόπιν αιτιολογημένου αιτήματος από την Επιτροπή ή από ένα ή περισσότερα κράτη μέλη προς τα οποία ή εντός των οποίων παρέχεται η βασική υπηρεσία όταν απαιτούνται πρόσθετες πληροφορίες για να υπάρχει δυνατότητα παροχής συμβουλών σε κρίσιμη οντότητα προκειμένου αυτή να εκπληρώσει τις υποχρεώσεις της δυνάμει της παρούσας οδηγίας ή για να αξιολογηθεί η συμμόρφωση κρίσιμης οντότητας ιδιαίτερου ευρωπαϊκού ενδιαφέροντος με τις εν λόγω υποχρεώσεις, το κράτος μέλος που έχει προσδιορίσει κρίσιμη οντότητα ιδιαίτερου ευρωπαϊκού ενδιαφέροντος ως κρίσιμη οντότητα θα πρέπει να παρέχει στην Επιτροπή ορισμένες πληροφορίες όπως ορίζονται στην παρούσα οδηγία. Σε συμφωνία με το κράτος μέλος που έχει προσδιορίσει την κρίσιμη οντότητα ιδιαίτερου ευρωπαϊκού ενδιαφέροντος ως κρίσιμη οντότητα, η Επιτροπή θα πρέπει να είναι σε θέση να οργανώσει συμβουλευτική αποστολή για την αξιολόγηση των μέτρων που έχει λάβει η εκάστοτε οντότητα. Για τη διασφάλιση της ορθής διεξαγωγής των εν λόγω συμβουλευτικών αποστολών, θα πρέπει να θεσπιστούν συμπληρωματικοί κανόνες, ιδίως σχετικά με την οργάνωση και τη διεξαγωγή των συμβουλευτικών αποστολών, τις ενέργειες παρακολούθησης που πρέπει να αναληφθούν και τις υποχρεώσεις των εκάστοτε κρίσιμων οντοτήτων

([19]) Απόφαση-πλαίσιο 2009/315/ΔΕΥ του Συμβουλίου, της 26ης Φεβρουαρίου 2009, σχετικά με τη διοργάνωση και το περιεχόμενο της ανταλλαγής πληροφοριών που προέρχονται από το ποινικό μητρώο μεταξύ των κρατών μελών (ΕΕ L 93 της 7.4.2009, σ. 23).

([20]) Κανονισμός (ΕΕ) 2019/816 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, για τη θέσπιση κεντρικού συστήματος εντοπισμού των κρατών μελών που διαθέτουν πληροφορίες σχετικά με καταδικαστικές αποφάσεις εις βάρος υπηκόων τρίτων χωρών και ανιθαγενών (ECRIS-TCN), με σκοπό τη συμπλήρωση του Ευρωπαϊκού Συστήματος Πληροφοριών Ποινικού Μητρώου, και για την τροποποίηση του κανονισμού (ΕΕ) 2018/1726 (ΕΕ L 135 της 22.5.2019, σ. 1).

([21]) Κανονισμός (ΕΕ) 2018/1862 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 28ης Νοεμβρίου 2018, σχετικά με την εγκατάσταση, τη λειτουργία και τη χρήση του συστήματος πληροφοριών Σένγκεν (SIS) στον τομέα της αστυνομικής συνεργασίας και της δικαστικής συνεργασίας σε ποινικές υποθέσεις, την τροποποίηση και κατάργηση της απόφασης 2007/533/ΔΕΥ του Συμβουλίου και την κατάργηση του κανονισμού (ΕΚ) αριθ. 1986/2006 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και της απόφασης 2010/261/ΕΕ της Επιτροπής (ΕΕ L 312 της 7.12.2018, σ. 56).

ιδιαίτερου ευρωπαϊκού ενδιαφέροντος. Με την επιφύλαξη της ανάγκης συμμόρφωσης του κράτους μέλους στο οποίο πραγματοποιείται η συμβουλευτική αποστολή και της εκάστοτε κρίσιμης οντότητας με τους κανόνες που ορίζονται στην παρούσα οδηγία, οι συμβουλευτικές αποστολές θα πρέπει να διεξάγονται σύμφωνα με τους λεπτομερείς κανόνες της νομοθεσίας του εν λόγω κράτους μέλους, για παράδειγμα τους κανόνες σχετικά με τις ακριβείς προϋποθέσεις που πρέπει να πληρούνται για την απόκτηση πρόσβασης στους οικείους χώρους ή σε έγγραφα, καθώς και σχετικά με τις δυνατότητες δικαστικής προσφυγής. Η ειδική εμπειρογνωσία που απαιτείται για τις συμβουλευτικές αποστολές αυτού του είδους θα μπορούσε, κατά περίπτωση, να ζητείται μέσω του Κέντρου Συντονισμού Αντιμετώπισης Εκτάκτων Αναγκών που συστάθηκε με την απόφαση αριθ. 1313/2013/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([22]).

(37) Για την υποστήριξη της Επιτροπής και τη διευκόλυνση της συνεργασίας μεταξύ των κρατών μελών και της ανταλλαγής πληροφοριών, συμπεριλαμβανομένων βέλτιστων πρακτικών, σχετικά με τα ζητήματα που άπτονται της παρούσας οδηγίας, θα πρέπει να συσταθεί ομάδα για την ανθεκτικότητα των κρίσιμων οντοτήτων ως ομάδα εμπειρογνωμόνων της Επιτροπής. Τα κράτη μέλη θα πρέπει να επιδιώκουν να διασφαλίζουν την αποτελεσματική και αποδοτική συνεργασία μεταξύ των ορισθέντων εκπροσώπων των αρμόδιων αρχών τους στο πλαίσιο της ομάδας για την ανθεκτικότητα των κρίσιμων οντοτήτων, μεταξύ άλλων ορίζοντας εκπροσώπους που διαθέτουν εξουσιοδότηση ασφαλείας, κατά περίπτωση. Η ομάδα για την ανθεκτικότητα των κρίσιμων οντοτήτων θα πρέπει να αρχίσει να ασκεί τα καθήκοντά της το συντομότερο δυνατό, ούτως ώστε να αποτελέσει ένα επιπλέον μέσο κατάλληλης συνεργασίας κατά την περίοδο μεταφοράς της παρούσας οδηγίας στο εθνικό δίκαιο. Η ομάδα για την ανθεκτικότητα των κρίσιμων οντοτήτων θα πρέπει να αλληλεπιδρά με σχετικές ομάδες εργασίας εμπειρογνωμόνων άλλων τομέων.

(38) Η ομάδα για την ανθεκτικότητα των κρίσιμων οντοτήτων θα πρέπει να συνεργάζεται με την ομάδα συνεργασίας που συστάθηκε δυνάμει της οδηγίας (ΕΕ) 2022/2555 με σκοπό την υποστήριξη ενός ολοκληρωμένου πλαισίου για την ανθεκτικότητα των κρίσιμων οντοτήτων εντός και εκτός κυβερνοχώρου. Η ομάδα για την ανθεκτικότητα των κρίσιμων οντοτήτων και η ομάδα συνεργασίας που συστάθηκε δυνάμει της οδηγίας (ΕΕ) 2022/2555 θα πρέπει να συμμετέχουν σε τακτικό διάλογο για την προώθηση της συνεργασίας μεταξύ των αρμόδιων αρχών βάσει της παρούσας οδηγίας και των αρμόδιων αρχών βάσει της οδηγίας (ΕΕ) 2022/2555 και για τη διευκόλυνση της ανταλλαγής πληροφοριών, ιδίως για θέματα που ενδιαφέρουν και τις δύο ομάδες.

(39) Για την επίτευξη των στόχων της παρούσας οδηγίας και χωρίς να θίγεται η νομική ευθύνη των κρατών μελών και των κρίσιμων οντοτήτων να διασφαλίζουν τη συμμόρφωσή τους με τις αντίστοιχες υποχρεώσεις τους που προβλέπονται σε αυτήν, η Επιτροπή θα πρέπει, όταν το κρίνει σκόπιμο, να στηρίζει τις αρμόδιες αρχές και τις κρίσιμες οντότητες με στόχο τη διευκόλυνση της συμμόρφωσής τους με τις αντίστοιχες υποχρεώσεις τους. Η Επιτροπή, όταν υποστηρίζει τα κράτη μέλη και τις κρίσιμες οντότητες στην εκπλήρωση των υποχρεώσεών τους βάσει της παρούσας οδηγίας, θα πρέπει να αξιοποιεί τις υφιστάμενες δομές και εργαλεία, όπως αυτά που προβλέπονται στο πλαίσιο του μηχανισμού πολιτικής προστασίας της Ένωσης, που συστάθηκε με την απόφαση αριθ. 1313/2013/ΕΕ, και του ευρωπαϊκού δικτύου αναφοράς για την προστασία των υποδομών ζωτικής σημασίας. Επιπλέον, θα πρέπει να ενημερώνει τα κράτη μέλη σχετικά με τους πόρους που διατίθενται σε επίπεδο Ένωσης, όπως στο πλαίσιο του Ταμείου Εσωτερικής Ασφάλειας, που θεσπίστηκε με τον κανονισμό (ΕΕ) 2021/1149 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([23]), του προγράμματος «Ορίζων Ευρώπη», που θεσπίστηκε με τον κανονισμό (ΕΕ) 2021/695 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([24]), ή σε άλλα μέσα που αφορούν την ανθεκτικότητα των κρίσιμων οντοτήτων.

(40) Τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι οι αρμόδιες αρχές τους διαθέτουν ορισμένες ειδικές εξουσίες για την ορθή εφαρμογή και επιβολή της παρούσας οδηγίας όσον αφορά τις κρίσιμες οντότητες, όταν οι εν λόγω οντότητες υπάγονται στη δικαιοδοσία τους όπως ορίζεται στην παρούσα οδηγία. Στις εν λόγω εξουσίες θα πρέπει να συμπεριλαμβάνονται, ιδίως, η εξουσία να διενεργούν επιθεωρήσεις και ελέγχους, η εξουσία να εποπτεύουν, η εξουσία να ζητούν από τις κρίσιμες οντότητες πληροφορίες και αποδεικτικά στοιχεία σχετικά με τα μέτρα που έχουν λάβει προκειμένου να συμμορφωθούν με τις υποχρεώσεις τους και, όταν είναι αναγκαίο, η εξουσία να εκδίδουν εντολές για την αποκατάσταση των παραβάσεων που εντοπίστηκαν. Τα κράτη μέλη, όταν εκδίδουν τέτοιες εντολές, δεν θα πρέπει να απαιτούν μέτρα που υπερβαίνουν τα αναγκαία και αναλογικά όρια για να επιτευχθεί η συμμόρφωση της εκάστοτε κρίσιμης οντότητας, λαμβανομένων ιδίως υπόψη της σοβαρότητας της παράβασης και των οικονομικών δυνατοτήτων της οικείας κρίσιμης οντότητας. Γενικότερα, οι εξουσίες αυτές θα πρέπει να συνοδεύονται από κατάλληλες και αποτελεσματικές διασφαλίσεις που θα ορίζονται στο εθνικό

([22]) Απόφαση αριθ. 1313/2013/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Δεκεμβρίου 2013, περί μηχανισμού πολιτικής προστασίας της Ένωσης (ΕΕ L 347 της 20.12.2013, σ. 924).

([23]) Κανονισμός (ΕΕ) 2021/1149 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 7ης Ιουλίου 2021 για τη θέσπιση του Ταμείου Εσωτερικής Ασφάλειας (ΕΕ L 251 της 15.7.2021, σ. 94).

([24]) Κανονισμός (ΕΕ) 2021/695 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 28ης Απριλίου 2021 για τη θέσπιση του προγράμματος-πλαισίου έρευνας και καινοτομίας «Ορίζων Ευρώπη», τον καθορισμό των κανόνων συμμετοχής και διάδοσής του, και για την κατάργηση των κανονισμών (ΕΕ) αριθ. 1290/2013 και (ΕΕ) αριθ. 1291/2013 (ΕΕ L 170 της 12.5.2021, σ. 1).

δίκαιο σύμφωνα με το Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης. Κατά την αξιολόγηση της συμμόρφωσης κρίσιμης οντότητας με τις υποχρεώσεις της που προβλέπονται στην παρούσα οδηγία, οι αρμόδιες αρχές βάσει της παρούσας οδηγίας θα πρέπει να μπορούν να ζητούν από τις αρμόδιες αρχές βάσει της οδηγίας (ΕΕ) 2022/2555 να ασκούν τις εξουσίες εποπτείας και επιβολής που διαθέτουν σε σχέση με οντότητα βάσει της εν λόγω οδηγίας[+], η οποία έχει προσδιοριστεί επίσης ως κρίσιμη οντότητα βάσει της παρούσας οδηγίας. Οι αρμόδιες αρχές βάσει της παρούσας οδηγίας και οι αρμόδιες αρχές βάσει της οδηγίας (ΕΕ) 2022/2555 θα πρέπει να συνεργάζονται και να ανταλλάσσουν πληροφορίες για τον σκοπό αυτόν.

(41) Για την αποτελεσματική και συνεπή εφαρμογή της παρούσας οδηγίας, θα πρέπει να ανατεθεί στην Επιτροπή η εξουσία έκδοσης πράξεων σύμφωνα με το άρθρο 290 ΣΛΕΕ, ώστε να συμπληρώνει την παρούσα οδηγία καταρτίζοντας κατάλογο βασικών υπηρεσιών. Ο εν λόγω κατάλογος θα πρέπει να χρησιμοποιείται από τις αρμόδιες αρχές με σκοπό τη διενέργεια εκτιμήσεων κινδύνων από τα κράτη μέλη και για τον προσδιορισμό των κρίσιμων οντοτήτων δυνάμει της παρούσας οδηγίας. Υπό το πρίσμα της προσέγγισης ελάχιστης εναρμόνισης της παρούσας οδηγίας, ο εν λόγω κατάλογος δεν είναι εξαντλητικός και τα κράτη μέλη θα μπορούν να τον συμπληρώσουν με πρόσθετες βασικές υπηρεσίες σε εθνικό επίπεδο, ώστε να λαμβάνονται υπόψη οι εθνικές ιδιαιτερότητες ως προς την παροχή βασικών υπηρεσιών. Είναι ιδιαίτερα σημαντικό η Επιτροπή να διεξάγει, κατά τις προπαρασκευαστικές της εργασίες, τις κατάλληλες διαβουλεύσεις, μεταξύ άλλων σε επίπεδο εμπειρογνωμόνων, οι οποίες να πραγματοποιούνται σύμφωνα με τις αρχές που ορίζονται στη διοργανική συμφωνία της 13ης Απριλίου 2016 για τη βελτίωση του νομοθετικού έργου ([25]). Πιο συγκεκριμένα, προκειμένου να διασφαλιστεί η ίση συμμετοχή στην προετοιμασία των κατ' εξουσιοδότηση πράξεων, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο λαμβάνουν όλα τα έγγραφα κατά τον ίδιο χρόνο με τους εμπειρογνώμονες των κρατών μελών, και οι εμπειρογνώμονές τους έχουν συστηματικά πρόσβαση στις συνεδριάσεις των ομάδων εμπειρογνωμόνων της Επιτροπής που ασχολούνται με την προετοιμασία κατ' εξουσιοδότηση πράξεων.

(42) Προκειμένου να διασφαλιστούν ενιαίες προϋποθέσεις για την εφαρμογή της παρούσας οδηγίας, θα πρέπει να ανατεθούν στην Επιτροπή εκτελεστικές αρμοδιότητες. Οι εν λόγω αρμοδιότητες θα πρέπει να ασκούνται σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 182/2011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([26]).

(43) Δεδομένου ότι οι στόχοι της παρούσας οδηγίας, δηλαδή η διασφάλιση ότι οι υπηρεσίες που είναι βασικές για τη διατήρηση ζωτικών κοινωνικών λειτουργιών ή οικονομικών δραστηριοτήτων παρέχονται απρόσκοπτα στην εσωτερική αγορά και η ενίσχυση της ανθεκτικότητας των κρίσιμων οντοτήτων που παρέχουν τις εν λόγω υπηρεσίες, δεν μπορούν να επιτευχθούν ικανοποιητικά από τα κράτη μέλη, μπορούν όμως, λόγω των αποτελεσμάτων της δράσης, να επιτευχθούν καλύτερα σε επίπεδο Ένωσης, η Ένωση δύναται να λάβει μέτρα, σύμφωνα με την αρχή της επικουρικότητας του άρθρου 5 της Συνθήκης για την Ευρωπαϊκή Ένωση. Σύμφωνα με την αρχή της αναλογικότητας όπως διατυπώνεται στο ίδιο άρθρο, η παρούσα οδηγία δεν υπερβαίνει τα αναγκαία όρια για την επίτευξη των στόχων αυτών.

(44) Σύμφωνα με το άρθρο 42 παράγραφος 1 του κανονισμού (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([27]), ζητήθηκε η γνώμη του Ευρωπαίου Επόπτη Προστασίας Δεδομένων, ο οποίος γνωμοδότησε στις 11 Αυγούστου 2021.

(45) Επομένως, η οδηγία 2008/114/ΕΚ θα πρέπει να καταργηθεί,

([25]) ΕΕ L 123 της 12.5.2016, σ. 1.

([26]) Κανονισμός (ΕΕ) αριθ. 182/2011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 16ης Φεβρουαρίου 2011, για τη θέσπιση κανόνων και γενικών αρχών σχετικά με τους τρόπους ελέγχου από τα κράτη μέλη της άσκησης των εκτελεστικών αρμοδιοτήτων από την Επιτροπή (ΕΕ L 55 της 28.2.2011, σ. 13).

([27]) Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2018, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ (ΕΕ L 295 της 21.11.2018, σ. 39).

ΕΞΕΔΩΣΑΝ ΤΗΝ ΠΑΡΟΥΣΑ ΟΔΗΓΙΑ:

ΚΕΦΆΛΑΙΟ I

ΓΕΝΙΚΈΣ ΔΙΑΤΆΞΕΙΣ

Άρθρο 1

Αντικείμενο και πεδίο εφαρμογής

1. Η παρούσα οδηγία:

α) θεσπίζει υποχρεώσεις στα κράτη μέλη για λήψη ειδικών μέτρων με στόχο τη διασφάλιση της απρόσκοπτης παροχής υπηρεσιών οι οποίες είναι βασικές για τη διατήρηση ζωτικών κοινωνικών λειτουργιών ή οικονομικών δραστηριοτήτων, εντός του πεδίου εφαρμογής του άρθρου 114 ΣΛΕΕ, ιδίως υποχρεώσεις για τον προσδιορισμό κρίσιμων οντοτήτων και τη στήριξη κρίσιμων οντοτήτων για την εκπλήρωση των υποχρεώσεων που τους επιβάλλονται·

β) θεσπίζει υποχρεώσεις των κρίσιμων οντοτήτων με στόχο την ενίσχυση της ανθεκτικότητάς τους και της ικανότητάς τους να παρέχουν τις αναφερόμενες στο στοιχείο α) υπηρεσίες στην εσωτερική αγορά·

γ) θεσπίζει κανόνες:

i) σχετικά με την εποπτεία των κρίσιμων οντοτήτων·

ii) σχετικά με την επιβολή της νομοθεσίας·

iii) για τον προσδιορισμό των κρίσιμων οντοτήτων ιδιαίτερου ευρωπαϊκού ενδιαφέροντος και σχετικά με συμβουλευτικές αποστολές για την αξιολόγηση των μέτρων που έχουν θεσπίσει οι εν λόγω οντότητες για την εκπλήρωση των υποχρεώσεών τους βάσει του κεφαλαίου III·

δ) θεσπίζει κοινές διαδικασίες συνεργασίας και υποβολής εκθέσεων για την εφαρμογή της παρούσας οδηγίας·

ε) θεσπίζει μέτρα με σκοπό την επίτευξη υψηλού επιπέδου ανθεκτικότητας των κρίσιμων οντοτήτων, προκειμένου να διασφαλιστεί η παροχή βασικών υπηρεσιών εντός της Ένωσης και να βελτιωθεί η λειτουργία της εσωτερικής αγοράς.

2. Η παρούσα οδηγία δεν εφαρμόζεται σε ζητήματα που διέπονται από την οδηγία (ΕΕ) 2022/2555, με την επιφύλαξη του άρθρου 8 της παρούσας οδηγίας. Δεδομένης της σχέσης μεταξύ της υλικής ασφάλειας και της ασφάλειας στον κυβερνοχώρο των κρίσιμων οντοτήτων, τα κράτη μέλη μεριμνούν ώστε η παρούσα οδηγία και η οδηγία (ΕΕ) 2022/2555 να εφαρμόζονται με συντονισμένο τρόπο.

3. Όταν διατάξεις ειδικών τομεακών νομικών πράξεων της Ένωσης επιβάλλουν στις κρίσιμες οντότητες την υποχρέωση λήψης μέτρων για την ενίσχυση της ανθεκτικότητάς τους, και εφόσον οι εν λόγω απαιτήσεις αναγνωρίζονται από τα κράτη μέλη ως τουλάχιστον ισοδύναμες με τις αντίστοιχες υποχρεώσεις που καθορίζονται στην παρούσα οδηγία, οι σχετικές διατάξεις της παρούσας οδηγίας, συμπεριλαμβανομένων των διατάξεων του κεφαλαίου VI περί εποπτείας και επιβολής, δεν εφαρμόζονται.

4. Με την επιφύλαξη του άρθρου 346 της ΣΛΕΕ, πληροφορίες που είναι απόρρητες σύμφωνα με ενωσιακούς ή εθνικούς κανόνες, όπως κανόνες περί επιχειρηματικού απορρήτου, ανταλλάσσονται με την Επιτροπή και άλλες αρμόδιες αρχές σύμφωνα με την παρούσα οδηγία μόνον όταν η ανταλλαγή είναι αναγκαία για την εφαρμογή της παρούσας οδηγίας. Οι ανταλλασσόμενες πληροφορίες περιορίζονται σε ό,τι είναι συναφές και αναλογικό προς τον σκοπό της εκάστοτε ανταλλαγής. Η ανταλλαγή πληροφοριών διαφυλάσσει το απόρρητο αυτών των πληροφοριών και τα συμφέροντα ασφάλειας και τα εμπορικά συμφέροντα των κρίσιμων οντοτήτων, μεριμνώντας ταυτόχρονα για την ασφάλεια των κρατών μελών.

5. Η παρούσα οδηγία δεν θίγει την ευθύνη των κρατών μελών να διαφυλάσσουν την εθνική ασφάλεια και άμυνα και την εξουσία τους να διαφυλάσσουν άλλες βασικές λειτουργίες του κράτους, περιλαμβανομένης της διασφάλισης της εδαφικής ακεραιότητας του κράτους και της τήρησης της δημόσιας τάξης.

6. Η παρούσα οδηγία δεν εφαρμόζεται σε φορείς δημόσιας διοίκησης που ασκούν τις δραστηριότητές τους στους τομείς της εθνικής ασφάλειας, της δημόσιας ασφάλειας, της άμυνας, ή της επιβολής του νόμου, συμπεριλαμβανομένων της διερεύνησης, ανίχνευσης και δίωξης ποινικών αδικημάτων.

7. Τα κράτη μέλη μπορούν να αποφασίζουν ότι το άρθρο 11 και τα κεφάλαια III έως VI, εν όλω ή εν μέρει, δεν εφαρμόζονται σε συγκεκριμένες κρίσιμες οντότητες οι οποίες ασκούν δραστηριότητες στους τομείς της εθνικής ασφάλειας, της δημόσιας ασφάλειας, της άμυνας, ή της επιβολής του νόμου, συμπεριλαμβανομένων των δραστηριοτήτων που σχετίζονται με τη διερεύνηση, ανίχνευση και δίωξη ποινικών αδικημάτων, ή οι οποίες παρέχουν υπηρεσίες αποκλειστικά στους φορείς δημόσιας διοίκησης που αναφέρονται στην παράγραφο 6 του παρόντος άρθρου.

8. Οι υποχρεώσεις που προβλέπονται στην παρούσα οδηγία δεν συνεπάγονται την παροχή πληροφοριών, η γνωστοποίηση των οποίων θα ήταν αντίθετη προς τα βασικά συμφέροντα εθνικής ασφάλειας των κρατών μελών, δημόσιας ασφάλειας ή άμυνας των κρατών μελών.

9. Η παρούσα οδηγία δεν θίγει το ενωσιακό δίκαιο περί προστασίας των δεδομένων προσωπικού χαρακτήρα, ειδικότερα τον κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([28]) και την οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([29]).

Άρθρο 2

Ορισμοί

Για τους σκοπούς της παρούσας οδηγίας, ισχύουν οι ακόλουθοι ορισμοί:

1) «κρίσιμη οντότητα»: δημόσια ή ιδιωτική οντότητα η οποία έχει προσδιοριστεί από κράτος μέλος σύμφωνα με το άρθρο 6 ότι ανήκει σε μία από τις κατηγορίες που ορίζονται στην τρίτη στήλη του πίνακα του παραρτήματος·

2) «ανθεκτικότητα»: η ικανότητα κρίσιμης οντότητας να προλαμβάνει, να προστατεύει, να αντιδρά, να αντιστέκεται, να μετριάζει, να απορροφά, να προσαρμόζεται και να ανακάμπτει από περιστατικό ·

3) «περιστατικό»: κάθε συμβάν που έχει τη δυνατότητα να διαταράξει σημαντικά ή που διαταράσσει την παροχή βασικής υπηρεσίας, μεταξύ άλλων όταν επηρεάζει τα εθνικά συστήματα που διαφυλάσσουν το κράτος δικαίου·

4) «υποδομή ζωτικής σημασίας»: περιουσιακό στοιχείο, εγκατάσταση, εξοπλισμός, δίκτυο ή σύστημα ή μέρος ενός περιουσιακού στοιχείου, μιας εγκατάστασης, ενός εξοπλισμού, ενός δικτύου ή ενός συστήματος, το οποίο είναι απαραίτητο για την παροχή βασικής υπηρεσίας·

5) «βασική υπηρεσία»: υπηρεσία η οποία είναι κρίσιμης σημασίας για τη διατήρηση ζωτικών κοινωνικών λειτουργιών, οικονομικών δραστηριοτήτων, της δημόσιας υγείας και ασφάλειας ή του περιβάλλοντος·

6) «κίνδυνος»: η πιθανότητα απώλειας ή διαταραχής που προκαλείται από περιστατικό και εκφράζεται ως συνδυασμός της έκτασης της εν λόγω απώλειας ή διαταραχής και της πιθανότητας επέλευσης του περιστατικού·

7) «εκτίμηση κινδύνων»: η συνολική διαδικασία για τον προσδιορισμό της φύσης και της έκτασης ενός κινδύνου μέσω εντοπισμού και ανάλυσης πιθανών σχετικών απειλών, τρωτών σημείων και κινδύνων που θα μπορούσαν να οδηγήσουν σε περιστατικό και μέσω αξιολόγησης της δυνητικής απώλειας ή διαταραχής της παροχής βασικής υπηρεσίας που προκαλείται από το εν λόγω περιστατικό.

8) «πρότυπο»: πρότυπο όπως ορίζεται στο άρθρο 2 σημείο 1) του κανονισμού (ΕΕ) αριθ. 1025/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([30])·

([28]) Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (ΕΕ L 119 της 4.5.2016, σ. 1).

([29]) Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) (ΕΕ L 201 της 31.7.2002, σ. 37).

([30]) Κανονισμός (ΕΕ) αριθ. 1025/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Οκτωβρίου 2012, σχετικά με την ευρωπαϊκή τυποποίηση, την τροποποίηση των οδηγιών του Συμβουλίου 89/686/ΕΟΚ και 93/15/ΕΟΚ και των οδηγιών του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου 94/9/ΕΚ, 94/25/ΕΚ, 95/16/ΕΚ, 97/23/ΕΚ, 98/34/ΕΚ, 2004/22/ΕΚ, 2007/23/ΕΚ, 2009/23/ΕΚ και 2009/105/ΕΚ και την κατάργηση της απόφασης 87/95/ΕΟΚ του Συμβουλίου και της απόφασης αριθ. 1673/2006/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (ΕΕ L 316 της 14.11.2012, σ. 12).

9) «τεχνική προδιαγραφή»: τεχνική προδιαγραφή όπως ορίζεται στο άρθρο 2 σημείο 4) του κανονισμού (ΕΕ) αριθ. 1025/2012·

10) «φορέας δημόσιας διοίκησης»: οντότητα που αναγνωρίζεται ως τέτοια σε ένα κράτος μέλος σύμφωνα με το εθνικό δίκαιο, εξαιρουμένων των δικαστικών αρχών, των κοινοβουλίων ή των κεντρικών τραπεζών, η οποία πληροί τα ακόλουθα κριτήρια:

α) έχει συσταθεί με σκοπό την κάλυψη αναγκών γενικού συμφέροντος και δεν έχει βιομηχανικό ή εμπορικό χαρακτήρα·

β) έχει νομική προσωπικότητα ή δικαιούται εκ του νόμου να ενεργεί για λογαριασμό άλλης οντότητας με νομική προσωπικότητα·

γ) χρηματοδοτείται κατά το μεγαλύτερο μέρος από τις κρατικές αρχές ή από άλλους κεντρικούς οργανισμούς δημοσίου δικαίου, η διαχείρισή του υπόκειται στην εποπτεία των ανωτέρω αρχών ή οργανισμών, ή έχει διοικητικό, διευθυντικό ή εποπτικό συμβούλιο, του οποίου περισσότερα από τα μισά μέλη διορίζονται από τις κρατικές αρχές ή από άλλους κεντρικούς οργανισμούς δημοσίου δικαίου·

δ) έχει την εξουσία να εκδίδει διοικητικές ή κανονιστικές αποφάσεις που απευθύνονται σε φυσικά ή νομικά πρόσωπα και επηρεάζουν τα δικαιώματά τους όσον αφορά τη διασυνοριακή κυκλοφορία προσώπων, εμπορευμάτων, υπηρεσιών ή κεφαλαίων.

Άρθρο 3

Ελάχιστη εναρμόνιση

Η παρούσα οδηγία δεν εμποδίζει τα κράτη μέλη να θεσπίζουν ή να διατηρούν διατάξεις εθνικού δικαίου με στόχο την επίτευξη υψηλότερου επιπέδου ανθεκτικότητας των κρίσιμων οντοτήτων, υπό την προϋπόθεση ότι οι διατάξεις αυτές συνάδουν με τις υποχρεώσεις των κρατών μελών που καθορίζονται στο ενωσιακό δίκαιο.

ΚΕΦΆΛΑΙΟ II

ΕΘΝΙΚΆ ΠΛΑΊΣΙΑ ΓΙΑ ΤΗΝ ΑΝΘΕΚΤΙΚΌΤΗΤΑ ΤΩΝ ΚΡΊΣΙΜΩΝ ΟΝΤΟΤΉΤΩΝ

Άρθρο 4

Στρατηγική για την ανθεκτικότητα των κρίσιμων οντοτήτων

1. Κατόπιν διαβούλευσης ανοικτής, στο μέτρο του δυνατού, στους σχετικούς ενδιαφερομένους, κάθε κράτος μέλος εγκρίνει, έως τις 17 Ιανουαρίου 2026, στρατηγική για την ενίσχυση της ανθεκτικότητας των κρίσιμων οντοτήτων («στρατηγική»). Η στρατηγική καθορίζει στρατηγικούς στόχους και μέτρα πολιτικής, αξιοποιώντας σχετικές υφιστάμενες εθνικές και τομεακές στρατηγικές, σχέδια ή παρόμοια έγγραφα, με σκοπό την επίτευξη και τη διατήρηση υψηλού επιπέδου ανθεκτικότητας από μέρους των κρίσιμων οντοτήτων, τουλάχιστον στους τομείς που ορίζονται στο παράρτημα.

2. Κάθε στρατηγική περιέχει τουλάχιστον τα ακόλουθα στοιχεία:

α) στρατηγικούς στόχους και προτεραιότητες με σκοπό την ενίσχυση της συνολικής ανθεκτικότητας των κρίσιμων οντοτήτων, λαμβανομένων υπόψη των διασυνοριακών και διατομεακών εξαρτήσεων και αλληλεξαρτήσεων·

β) πλαίσιο διακυβέρνησης για την επίτευξη των στρατηγικών στόχων και προτεραιοτήτων, συμπεριλαμβανομένης περιγραφής των ρόλων και των αρμοδιοτήτων των διαφόρων αρχών, κρίσιμων οντοτήτων και άλλων μερών που συμμετέχουν στην υλοποίηση της στρατηγικής·

γ) περιγραφή των μέτρων που είναι απαραίτητα για την ενίσχυση της συνολικής ανθεκτικότητας των κρίσιμων οντοτήτων, συμπεριλαμβανομένης περιγραφής της εκτίμησης κινδύνων που αναφέρεται στο άρθρο 5·

δ) περιγραφή της διαδικασίας με την οποία προσδιορίζονται οι κρίσιμες οντότητες·

ε) περιγραφή της διαδικασίας στήριξης των κρίσιμων οντοτήτων σύμφωνα με το παρόν κεφάλαιο, συμπεριλαμβανομένων μέτρων για την ενίσχυση της συνεργασίας μεταξύ του δημόσιου τομέα, αφενός, και του ιδιωτικού τομέα και των δημόσιων και ιδιωτικών οντοτήτων, αφετέρου·

στ) κατάλογο των κύριων αρχών και των σχετικών ενδιαφερομένων, εκτός των κρίσιμων οντοτήτων, που συμμετέχουν στην υλοποίηση της στρατηγικής·

ζ) πλαίσιο πολιτικής για συντονισμό μεταξύ των αρμόδιων αρχών σύμφωνα με την παρούσα οδηγία («αρμόδιες αρχές») και των αρμόδιων αρχών σύμφωνα με την οδηγία (ΕΕ) 2022/2555 για τον σκοπό της ανταλλαγής πληροφοριών σχετικά με κινδύνους κυβερνοασφάλειας, απειλές και περιστατικά στον κυβερνοχώρο, και κινδύνους, εκτός κυβερνοχώρου, απειλές και περιστατικά και για τον σκοπό της άσκησης εποπτικών καθηκόντων·

η) περιγραφή των ήδη θεσπισμένων μέτρων που αποσκοπούν στη διευκόλυνση της εφαρμογής των υποχρεώσεων σύμφωνα με το κεφάλαιο III της παρούσας οδηγίας από τις μικρές και μεσαίες επιχειρήσεις κατά την έννοια του παραρτήματος της σύστασης 2003/361/ΕΚ της Επιτροπής ([31]), τις οποίες το εν λόγω κράτος μέλος έχει προσδιορίσει ως κρίσιμες οντότητες.

Κατόπιν διαβούλευσης η οποία είναι, στο μέτρο του πρακτικά δυνατού, ανοικτή στους σχετικούς ενδιαφερομένους, τα κράτη μέλη επικαιροποιούν τη στρατηγική τους τουλάχιστον ανά τετραετία.

3. Τα κράτη μέλη κοινοποιούν στην Επιτροπή τις στρατηγικές τους και τις ουσιώδεις επικαιροποιήσεις τους εντός τριών μηνών από την έγκρισή τους.

Άρθρο 5

Εκτίμηση κινδύνων από τα κράτη μέλη

1. Ανατίθεται στην Επιτροπή η εξουσία να εκδώσει κατ' εξουσιοδότηση πράξη, σύμφωνα με το άρθρο 23, έως τις 17 Νοεμβρίου 2023 με σκοπό τη συμπλήρωση της παρούσας οδηγίας με την κατάρτιση μη εξαντλητικού καταλόγου βασικών υπηρεσιών στους τομείς και υποτομείς που ορίζονται στο παράρτημα. Οι αρμόδιες αρχές χρησιμοποιούν τον εν λόγω κατάλογο βασικών υπηρεσιών με σκοπό τη διενέργεια εκτίμησης κινδύνων («εκτίμηση κινδύνων από τα κράτη μέλη») έως τις 17 Ιανουαρίου 2026, όποτε είναι απαραίτητο στη συνέχεια και τουλάχιστον ανά τετραετία. Οι αρμόδιες αρχές χρησιμοποιούν τις εκτιμήσεις κινδύνων από τα κράτη μέλη με σκοπό να προσδιορίσουν τις κρίσιμες οντότητες σύμφωνα με το άρθρο 6 και να συνδράμουν τις εν λόγω κρίσιμες οντότητες στη λήψη μέτρων σύμφωνα με το άρθρο 13.

Οι εκτιμήσεις κινδύνων από τα κράτη μέλη λαμβάνουν υπόψη τους συναφείς φυσικούς και ανθρωπογενείς κινδύνους, στους οποίους περιλαμβάνονται, μεταξύ άλλων, οι κίνδυνοι διατομεακού ή διασυνοριακού χαρακτήρα, τα ατυχήματα, οι φυσικές καταστροφές, οι καταστάσεις έκτακτης ανάγκης στη δημόσια υγεία και οι υβριδικές απειλές ή άλλες ανταγωνιστικές απειλές, συμπεριλαμβανομένων των τρομοκρατικών εγκλημάτων όπως προβλέπεται στην οδηγία (ΕΕ) 2017/541 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([32]).

2. Κατά τη διενέργεια της εκτίμησης κινδύνων από τα κράτη μέλη, τα κράτη μέλη λαμβάνουν υπόψη τουλάχιστον τα ακόλουθα:

α) τη γενική εκτίμηση κινδύνων που έχει διενεργηθεί σύμφωνα με το άρθρο 6 παράγραφος 1 της απόφασης αριθ. 1313/2013/ΕΕ·

β) άλλες συναφείς εκτιμήσεις κινδύνων που έχουν διενεργηθεί σύμφωνα με τις απαιτήσεις των σχετικών ειδικών τομεακών νομικών πράξεων της Ένωσης, συμπεριλαμβανομένων των κανονισμών (ΕΕ) 2017/1938 ([33]) και (ΕΕ) 2019/941 ([34]) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και των οδηγιών 2007/60/ΕΚ ([35]) και 2012/18/ΕΕ ([36]) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου·

([31]) Σύσταση 2003/361/ΕΚ της Επιτροπής, της 6ης Μαΐου 2003, σχετικά με τον ορισμό των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων (ΕΕ L 124 της 20.5.2003, σ. 36).

([32]) Οδηγία (ΕΕ) 2017/541 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαρτίου 2017, για την καταπολέμηση της τρομοκρατίας και την αντικατάσταση της απόφασης-πλαισίου 2002/475/ΔΕΥ του Συμβουλίου και για την τροποποίηση της απόφασης 2005/671/ΔΕΥ του Συμβουλίου (ΕΕ L 88 της 31.3.2017, σ. 6).

([33]) Κανονισμός (ΕΕ) 2017/1938 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Οκτωβρίου 2017, σχετικά με τα μέτρα κατοχύρωσης της ασφάλειας εφοδιασμού με φυσικό αέριο και με την κατάργηση του κανονισμού (ΕΕ) αριθ. 994/2010 (ΕΕ L 280 της 28.10.2017, σ. 1).

([34]) Κανονισμός (ΕΕ) 2019/941 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 5ης Ιουνίου 2019, σχετικά με την ετοιμότητα αντιμετώπισης κινδύνων στον τομέα της ηλεκτρικής ενέργειας και με την κατάργηση της οδηγίας 2005/89/ΕΚ (ΕΕ L 158 της 14.6.2019, σ. 1).

([35]) Οδηγία 2007/60/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2007, για την αξιολόγηση και τη διαχείριση των κινδύνων πλημμύρας (ΕΕ L 288 της 6.11.2007, σ. 27).

([36]) Οδηγία 2012/18/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 4ης Ιουλίου 2012, για την αντιμετώπιση των κινδύνων μεγάλων ατυχημάτων σχετιζόμενων με επικίνδυνες ουσίες και για την τροποποίηση και στη συνέχεια την κατάργηση της οδηγίας 96/82/ΕΚ του Συμβουλίου (ΕΕ L 197 της 24.7.2012, σ. 1).

γ) τους σχετικούς κινδύνους που απορρέουν από το βαθμό στον οποίο οι τομείς που ορίζονται στο παράρτημα εξαρτώνται μεταξύ τους, συμπεριλαμβανομένου του βαθμού στον οποίο εξαρτώνται από οντότητες που βρίσκονται σε άλλα κράτη μέλη και τρίτες χώρες, καθώς και τον αντίκτυπο που μια σημαντική διαταραχή σε έναν τομέα ενδέχεται να έχει σε άλλους τομείς, συμπεριλαμβανομένων τυχόν σημαντικών κινδύνων για τους πολίτες και την εσωτερική αγορά·

δ) τις τυχόν πληροφορίες για περιστατικά που έχουν κοινοποιηθεί σύμφωνα με το άρθρο 15.

Για τους σκοπούς του πρώτου εδαφίου στοιχείο γ), τα κράτη μέλη συνεργάζονται, κατά περίπτωση, με τις αρμόδιες αρχές άλλων κρατών μελών και τις αρμόδιες αρχές τρίτων χωρών.

3. Τα κράτη μέλη καθιστούν τα σχετικά στοιχεία των εκτιμήσεων κινδύνων από τα κράτη μέλη διαθέσιμα, κατά περίπτωση μέσω των ενιαίων σημείων επαφής τους, στις κρίσιμες οντότητες που έχουν προσδιορίσει σύμφωνα με το άρθρο 6. Τα κράτη μέλη εξασφαλίζουν ότι οι πληροφορίες που παρέχονται στις κρίσιμες οντότητες τις βοηθούν στη διενέργεια της δικής τους εκτίμησης κινδύνων σύμφωνα με το άρθρο 12 και στη λήψη μέτρων για τη διασφάλιση της ανθεκτικότητάς τους σύμφωνα με το άρθρο 13.

4. Εντός τριών μηνών από τη διενέργεια εκτίμησης κινδύνου από τα κράτη μέλη, ένα κράτος μέλος υποβάλλει στην Επιτροπή σχετικές πληροφορίες σχετικά με τα είδη των κινδύνων που προσδιορίστηκαν από την εκτίμηση κινδύνου από το εν λόγω κράτος μέλος και τα αποτελέσματα της εκτίμησης κινδύνου από το εν λόγω κράτος μέλος, ανά τομέα και υποτομέα που ορίζονται στο παράρτημα.

5. Η Επιτροπή, σε συνεργασία με τα κράτη μέλη, αναπτύσσει προαιρετικό κοινό υπόδειγμα υποβολής στοιχείων για τους σκοπούς της συμμόρφωσης με την παράγραφο 4.

Άρθρο 6

Προσδιορισμός των κρίσιμων οντοτήτων

1. Έως τις 17 Ιουλίου 2026 κάθε κράτος μέλος προσδιορίζει τις κρίσιμες οντότητες για τους τομείς και τους υποτομείς που αναφέρονται στο παράρτημα.

2. Όταν ένα κράτος μέλος προσδιορίζει τις κρίσιμες οντότητες δυνάμει της παραγράφου 1, λαμβάνει υπόψη τα αποτελέσματα της δικής του εκτίμησης κινδύνου από τα κράτη μέλη και τη στρατηγική και εφαρμόζει όλα τα ακόλουθα κριτήρια:

α) η οντότητα παρέχει μία ή περισσότερες βασικές υπηρεσίες·

β) η οντότητα δραστηριοποιείται και η υποδομή ζωτικής σημασίας που διαθέτει βρίσκεται στο έδαφος του εν λόγω κράτους μέλους· και

γ) τυχόν περιστατικό θα προκαλούσε σημαντική διαταραχή, κατά την έννοια του άρθρου 7 παράγραφος 1, στην παροχή από την οντότητα μίας ή περισσότερων βασικών υπηρεσιών ή στην παροχή άλλων βασικών υπηρεσιών στους τομείς που ορίζονται στο παράρτημα οι οποίες εξαρτώνται από την εν λόγω ή τις εν λόγω βασικές υπηρεσίες.

3. Κάθε κράτος μέλος καταρτίζει κατάλογο των κρίσιμων οντοτήτων που έχει προσδιορίσει δυνάμει της παραγράφου 2 και διασφαλίζει ότι οι εν λόγω κρίσιμες οντότητες ειδοποιούνται ότι έχουν προσδιοριστεί ως κρίσιμες οντότητες εντός ενός μηνός από τον εν λόγω προσδιορισμό. Τα κράτη μέλη ενημερώνουν τις εν λόγω κρίσιμες οντότητες για τις υποχρεώσεις τους βάσει των κεφαλαίων III και IV και για την ημερομηνία κατά την οποία οι εν λόγω υποχρεώσεις αρχίζουν να εφαρμόζονται σε αυτές, με την επιφύλαξη του άρθρου 8. Τα κράτη μέλη ενημερώνουν τις κρίσιμες οντότητες στους τομείς που καθορίζονται στα σημεία 3, 4 και 8 του πίνακα του παραρτήματος ότι δεν υπέχουν υποχρεώσεις βάσει των κεφαλαίων III και IV, εκτός εάν προβλέπεται διαφορετικά στα εθνικά μέτρα.

Για τις οικείες κρίσιμες οντότητες, το κεφάλαιο III αρχίζει να εφαρμόζεται δέκα μήνες μετά την ημερομηνία της ειδοποίησης που αναφέρεται στο πρώτο εδάφιο της παρούσας παραγράφου.

4. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές τους βάσει της παρούσας οδηγίας κοινοποιούν στις αρμόδιες αρχές σύμφωνα με την οδηγία (ΕΕ) 2022/2555 την ταυτότητα των κρίσιμων οντοτήτων που έχουν προσδιορίσει βάσει του παρόντος άρθρου εντός ενός μηνός από τον εν λόγω προσδιορισμό. Με την κοινοποίηση αυτή διευκρινίζεται, κατά περίπτωση, ότι οι οικείες κρίσιμες οντότητες αποτελούν οντότητες στους τομείς που καθορίζονται στα σημεία 3, 4 και 8 του πίνακα του παραρτήματος της παρούσας οδηγίας και δεν υπέχουν υποχρεώσεις βάσει των κεφαλαίων της III και IV.

5. Τα κράτη μέλη, όποτε είναι απαραίτητο και σε κάθε περίπτωση τουλάχιστον ανά τετραετία, επανεξετάζουν και, αν συντρέχει περίπτωση, επικαιροποιούν τον κατάλογο των προσδιορισμένων κρίσιμων οντοτήτων που αναφέρονται στην παράγραφο 3. Όταν οι εν λόγω επικαιροποιήσεις έχουν ως αποτέλεσμα τον προσδιορισμό επιπρόσθετων κρίσιμων οντοτήτων, εφαρμόζονται οι παράγραφοι 3 και 4 στις εν λόγω πρόσθετες κρίσιμες οντότητες. Επιπλέον, τα κράτη μέλη διασφαλίζουν ότι οι οντότητες που δεν προσδιορίζονται πλέον ως κρίσιμες οντότητες κατόπιν τέτοιας επικαιροποίησης λαμβάνουν ειδοποίηση εγκαίρως για το γεγονός αυτό και για το γεγονός ότι δεν υπέχουν πλέον τις υποχρεώσεις του κεφαλαίου ΙΙΙ από την ημερομηνία παραλαβής της εν λόγω ειδοποίησης.

6. Η Επιτροπή, σε συνεργασία με τα κράτη μέλη, καταρτίζει συστάσεις και μη δεσμευτικές κατευθυντήριες γραμμές για να στηρίξει τα κράτη μέλη κατά τον προσδιορισμό κρίσιμων οντοτήτων.

Άρθρο 7

Σημαντική διαταραχή

1. Για να καθοριστεί πόσο σημαντική είναι μια διαταραχή κατά το άρθρο 6 παράγραφος 2 στοιχείο γ), τα κράτη μέλη λαμβάνουν υπόψη τα ακόλουθα κριτήρια:

α) τον αριθμό των χρηστών που εξαρτώνται από τη βασική υπηρεσία που παρέχεται από την εν λόγω οντότητα·

β) τον βαθμό στον οποίο άλλοι τομείς και υποτομείς όπως ορίζονται στο παράρτημα εξαρτώνται από την εν λόγω βασική υπηρεσία·

γ) τον αντίκτυπο που θα μπορούσαν να έχουν τα περιστατικά, από πλευράς μεγέθους και διάρκειας, σε οικονομικές και κοινωνικές δραστηριότητες, στο περιβάλλον, στη δημόσια ασφάλεια ή την προστασία, και στην υγεία του πληθυσμού·

δ) το μερίδιο αγοράς της οντότητας στην αγορά παροχής της συγκεκριμένης βασικής υπηρεσίας ή των οικείων βασικών υπηρεσιών·

ε) τη γεωγραφική περιοχή που θα μπορούσε να επηρεαστεί από ένα περιστατικό, συμπεριλαμβανομένων τυχόν διασυνοριακών επιπτώσεων, λαμβανομένης υπόψη της τρωτότητας που συνδέεται με τον βαθμό απομόνωσης ορισμένων τύπων γεωγραφικών περιοχών, όπως είναι οι νησιωτικές, οι απομακρυσμένες ή οι ορεινές περιοχές·

στ) τη σημασία της οντότητας για τη διατήρηση επαρκούς επιπέδου της βασικής υπηρεσίας, λαμβανομένων υπόψη των διαθέσιμων εναλλακτικών μέσων για την παροχή της εν λόγω βασικής υπηρεσίας.

2. Μετά τον προσδιορισμό των κρίσιμων οντοτήτων βάσει του άρθρου 6 παράγραφος 1, κάθε κράτος μέλος υποβάλλει στην Επιτροπή τις ακόλουθες πληροφορίες χωρίς άσκοπη καθυστέρηση:

α) κατάλογο των βασικών υπηρεσιών σε αυτό το κράτος μέλος όταν υπάρχουν πρόσθετες βασικές υπηρεσίες σε σύγκριση με τον κατάλογο των βασικών υπηρεσιών που αναφέρονται στο άρθρο 5 παράγραφος 1·

β) τον αριθμό των κρίσιμων οντοτήτων που έχουν προσδιοριστεί για κάθε τομέα και υποτομέα που καθορίζεται στο παράρτημα και για κάθε βασική υπηρεσία·

γ) τα τυχόν κατώτατα όρια που εφαρμόζονται για τον προσδιορισμό ενός ή περισσότερων από τα κριτήρια της παραγράφου 1.

Τα κατώτατα όρια που αναφέρονται στο πρώτο εδάφιο στοιχείο γ) μπορούν να παρουσιάζονται ως έχουν ή σε συγκεντρωτική μορφή.

Τα κράτη μέλη στη συνέχεια υποβάλλουν τις πληροφορίες που αναφέρονται στο πρώτο εδάφιο όποτε είναι απαραίτητο και τουλάχιστον ανά τετραετία.

3. Η Επιτροπή, αφού ζητήσει τη γνώμη της ομάδας για την ανθεκτικότητα των κρίσιμων οντοτήτων που αναφέρεται στο άρθρο 19, εκδίδει μη δεσμευτικές κατευθυντήριες γραμμές για τη διευκόλυνση της εφαρμογής των κριτηρίων της παραγράφου 1 του παρόντος άρθρου, λαμβάνοντας υπόψη τις πληροφορίες της παραγράφου 2 του παρόντος άρθρου.

Άρθρο 8

Κρίσιμες οντότητες στον τραπεζικό τομέα, στον τομέα των υποδομών των χρηματοπιστωτικών αγορών και στον τομέα των ψηφιακών υποδομών

Τα κράτη μέλη διασφαλίζουν ότι το άρθρο 11 και τα κεφάλαια III, IV και VI δεν εφαρμόζονται για τις κρίσιμες οντότητες που έχουν προσδιοριστεί στους τομείς που καθορίζονται στα σημεία 3, 4 και 8 του πίνακα του παραρτήματος. Τα κράτη μέλη μπορούν να θεσπίζουν ή να διατηρούν διατάξεις του εθνικού δικαίου για την επίτευξη υψηλότερου επιπέδου ανθεκτικότητας για τις εν λόγω κρίσιμες οντότητες, υπό την προϋπόθεση ότι αυτές οι διατάξεις συνάδουν με το εφαρμοστέο ενωσιακό δίκαιο.

Άρθρο 9

Αρμόδιες αρχές και ενιαίο σημείο επαφής

1. Κάθε κράτος μέλος ορίζει ή θεσπίζει μία ή περισσότερες αρμόδιες αρχές ως υπεύθυνες για την ορθή εφαρμογή και, όταν είναι απαραίτητο, την επιβολή των κανόνων που καθορίζονται στην παρούσα οδηγία σε εθνικό επίπεδο.

Όσον αφορά τις κρίσιμες οντότητες στους τομείς που καθορίζονται στα σημεία 3 και 4 του πίνακα του παραρτήματος της παρούσας οδηγίας, οι αρμόδιες αρχές είναι, καταρχήν, οι αρμόδιες αρχές που αναφέρονται στο άρθρο 46 του κανονισμού (ΕΕ) 2022/2554. Όσον αφορά τις κρίσιμες οντότητες του τομέα που καθορίζεται στο σημείο 8 του πίνακα του παραρτήματος της παρούσας οδηγίας, οι αρμόδιες αρχές είναι, καταρχήν, οι αρμόδιες αρχές βάσει της οδηγίας (ΕΕ) 2022/2555. Τα κράτη μέλη μπορούν να ορίσουν διαφορετική αρμόδια αρχή για τους τομείς που καθορίζονται στα σημεία 3, 4 και 8 του καταλόγου του παραρτήματος της παρούσας οδηγίας σύμφωνα με τα υφιστάμενα εθνικά πλαίσια.

Όταν τα κράτη μέλη ορίζουν ή θεσπίζουν περισσότερες από μία αρμόδιες αρχές, καθορίζουν σαφώς τα καθήκοντα κάθε μίας από τις οικείες αρχές και διασφαλίζουν ότι αυτές συνεργάζονται αποτελεσματικά για την εκπλήρωση των καθηκόντων τους βάσει της παρούσας οδηγίας, μεταξύ άλλων όσον αφορά τον ορισμό και τις δραστηριότητες του ενιαίου σημείου επαφής της παραγράφου 2.

2. Κάθε κράτος μέλος ορίζει ή θεσπίζει ένα ενιαίο σημείο επαφής το οποίο ασκεί καθήκοντα συνδέσμου για τον σκοπό της διασφάλισης της διασυνοριακής συνεργασίας με τα ενιαία σημεία επαφής των άλλων κρατών μελών και την ομάδα για την ανθεκτικότητα των κρίσιμων οντοτήτων του άρθρου 19 («ενιαίο σημείο επαφής»). Κατά περίπτωση, ένα κράτος μέλος ορίζει το ενιαίο σημείο επαφής του εντός της αρμόδιας αρχής. Κατά περίπτωση, ένα κράτος μέλος μπορεί να ορίσει ότι το ενιαίο σημείο επαφής του λειτουργεί επίσης ως σύνδεσμος με την Επιτροπή και εξασφαλίζει τη συνεργασία με τρίτες χώρες.

3. Έως τις 17 Ιουλίου 2028 και ανά δύο έτη στη συνέχεια, τα ενιαία σημεία επαφής υποβάλλουν συνοπτική έκθεση στην Επιτροπή και την ομάδα για την ανθεκτικότητα των κρίσιμων οντοτήτων που αναφέρονται στο άρθρο 19 σχετικά με τις κοινοποιήσεις που έχουν λάβει, συμπεριλαμβανομένων του αριθμού των κοινοποιήσεων, της φύσης των κοινοποιημένων περιστατικών και των μέτρων που λήφθηκαν σύμφωνα με το άρθρο 15 παράγραφος 3.

Η Επιτροπή, σε συνεργασία με την ομάδα για την ανθεκτικότητα των κρίσιμων οντοτήτων, καταρτίζει κοινό υπόδειγμα υποβολής εκθέσεων. Οι αρμόδιες αρχές μπορούν να χρησιμοποιούν, σε εθελοντική βάση, το εν λόγω κοινό υπόδειγμα υποβολής εκθέσεων για τον σκοπό της υποβολής των συνοπτικών εκθέσεων που αναφέρονται στο πρώτο εδάφιο.

4. Κάθε κράτος μέλος διασφαλίζει ότι η αρμόδια αρχή του και το ενιαίο σημείο επαφής του διαθέτουν τις εξουσίες και επαρκείς οικονομικούς, ανθρώπινους και τεχνικούς πόρους για να εκτελούν, με αποτελεσματικό και αποδοτικό τρόπο, τα καθήκοντα που τους ανατίθενται.

5. Κάθε κράτος μέλος διασφαλίζει ότι η αρμόδια αρχή του, όταν συντρέχει σχετική περίπτωση και σύμφωνα με το ενωσιακό και το εθνικό δίκαιο, διαβουλεύεται και συνεργάζεται με τις λοιπές σχετικές εθνικές αρχές, μεταξύ των οποίων εκείνες που είναι αρμόδιες για την πολιτική προστασία, την επιβολή του νόμου και την προστασία των δεδομένων προσωπικού χαρακτήρα και με τις κρίσιμες οντότητες και συναφή ενδιαφερόμενα μέρη.

6. Κάθε κράτος μέλος διασφαλίζει ότι η αρμόδια αρχή του βάσει της παρούσας οδηγίας συνεργάζεται και ανταλλάσσει πληροφορίες με τις αρμόδιες αρχές βάσει της οδηγίας (ΕΕ) 2022/2555 όσον αφορά τους κινδύνους κυβερνοασφάλειας, τις απειλές και τα περιστατικά στον κυβερνοχώρο και τους κινδύνους, τις απειλές και τα περιστατικά εκτός κυβερνοχώρου που επηρεάζουν κρίσιμες οντότητες, συμπεριλαμβανομένων όσον αφορά σχετικά μέτρα που έχουν λάβει οι αρμόδιες αρχές του και οι αρμόδιες αρχές βάσει της οδηγίας (ΕΕ) 2022/2555.

7. Εντός τριών μηνών από τον ορισμό ή τη σύσταση της αρμόδιας αρχής και του ενιαίου σημείου επαφής, κάθε κράτος μέλος κοινοποιεί στην Επιτροπή την ταυτότητά τους και τα καθήκοντά και τις αρμοδιότητές τους βάσει της παρούσας οδηγίας, τα στοιχεία επικοινωνίας τους και κάθε μεταγενέστερη μεταβολή τους. Τα κράτη μέλη ενημερώνουν την Επιτροπή σε περίπτωση που αποφασίσουν να ορίσουν άλλες αρχές από εκείνες που αναφέρονται στην παράγραφο 1 δεύτερο εδάφιο ως τις αρμόδιες αρχές όσον αφορά τις κρίσιμες οντότητες στους τομείς που ορίζονται στα σημεία 3, 4 και 8 του πίνακα του παραρτήματος. Κάθε κράτος μέλος δημοσιοποιεί την ταυτότητα της αρμόδιας αρχής του και του ενιαίου σημείου επαφής.

8. Η Επιτροπή δημοσιοποιεί κατάλογο των ενιαίων σημείων επαφής.

Άρθρο 10

Υποστήριξη των κρίσιμων οντοτήτων από τα κράτη μέλη

1. Τα κράτη μέλη υποστηρίζουν τις κρίσιμες οντότητες για την ενίσχυση της ανθεκτικότητάς τους. Η εν λόγω υποστήριξη μπορεί να συμπεριλαμβάνει την ανάπτυξη υλικού καθοδήγησης και μεθοδολογιών, την υποστήριξη της διοργάνωσης ασκήσεων για τον έλεγχο της ανθεκτικότητας και την παροχή συμβουλών και κατάρτισης στο προσωπικό των κρίσιμων οντοτήτων. Με την επιφύλαξη των εφαρμοστέων κανόνων για τις κρατικές ενισχύσεις, τα κράτη μέλη δύνανται να παρέχουν χρηματοδοτικούς πόρους σε κρίσιμες οντότητες όταν αυτό είναι αναγκαίο και δικαιολογείται από στόχους δημόσιου συμφέροντος.

2. Κάθε κράτος μέλος διασφαλίζει ότι η αρμόδια αρχή του συνεργάζεται και ανταλλάσσει πληροφορίες και ορθές πρακτικές με τις κρίσιμες οντότητες των τομέων που ορίζονται στο παράρτημα.

3. Τα κράτη μέλη διευκολύνουν την οικειοθελή ανταλλαγή πληροφοριών μεταξύ κρίσιμων οντοτήτων σχετικά με ζητήματα που καλύπτονται από την παρούσα οδηγία, σύμφωνα με την ενωσιακή και την εθνική νομοθεσία, ιδίως στους τομείς των διαβαθμισμένων και ευαίσθητων πληροφοριών, του ανταγωνισμού και της προστασίας των δεδομένων προσωπικού χαρακτήρα.

Άρθρο 11

Συνεργασία μεταξύ των κρατών μελών

1. Όποτε κρίνεται σκόπιμο τα κράτη μέλη διαβουλεύονται μεταξύ τους σχετικά με τις κρίσιμες οντότητες με σκοπό να διασφαλίσουν ότι η παρούσα οδηγία εφαρμόζεται με συνέπεια. Οι εν λόγω διαβουλεύσεις πραγματοποιούνται ιδίως όσον αφορά τις κρίσιμες οντότητες που:

α) χρησιμοποιούν υποδομές ζωτικής σημασίας που συνδέονται φυσικά μεταξύ δύο ή περισσότερων κρατών μελών·

β) αποτελούν μέρος εταιρικών δομών που συνδέονται με κρίσιμες οντότητες σε άλλα κράτη μέλη ή έχουν σχέση με αυτές·

γ) έχουν προσδιοριστεί ως κρίσιμες οντότητες σε ένα κράτος μέλος και παρέχουν βασικές υπηρεσίες προς άλλα κράτη μέλη ή εντός αυτών.

2. Οι διαβουλεύσεις που αναφέρονται στην παράγραφο 1 αποσκοπούν στην ενίσχυση της ανθεκτικότητας των κρίσιμων οντοτήτων και, όπου είναι δυνατόν, στη μείωση του διοικητικού φόρτου για αυτές.

ΚΕΦΆΛΑΙΟ III

ΑΝΘΕΚΤΙΚ'ΟΤΗΤΑ ΤΩΝ ΚΡ'ΙΣΙΜΩΝ ΟΝΤΟΤ'ΗΤΩΝ

Άρθρο 12

Εκτίμηση κινδύνων από τις κρίσιμες οντότητες

1. Με την επιφύλαξη της προθεσμίας που ορίζεται στο άρθρο 6 παράγραφος 3 δεύτερο εδάφιο, τα κράτη μέλη διασφαλίζουν ότι οι κρίσιμες οντότητες διενεργούν εκτίμηση κινδύνων, εντός εννέα μηνών από τη λήψη της ειδοποίησης που αναφέρεται στο άρθρο 6 παράγραφος 3, όποτε είναι απαραίτητο στη συνέχεια και τουλάχιστον ανά τετραετία, με βάση τις εκτιμήσεις κινδύνων των κρατών μελών και άλλες συναφείς πηγές πληροφοριών, ώστε να εκτιμηθούν όλοι οι συναφείς κίνδυνοι που θα μπορούσαν να διαταράξουν την παροχή των βασικών υπηρεσιών («εκτίμηση κινδύνου κρίσιμης οντότητας»).

2. Οι εκτιμήσεις κινδύνων των κρίσιμων οντοτήτων καλύπτουν όλους τους συναφείς φυσικούς και ανθρωπογενείς κινδύνους οι οποίοι θα μπορούσαν να προκαλέσουν περιστατικό, συμπεριλαμβανομένων των κινδύνων διατομεακού ή διασυνοριακού χαρακτήρα, των ατυχημάτων, των φυσικών καταστροφών, των καταστάσεων έκτακτης ανάγκης για τη δημόσια υγεία και των υβριδικών απειλών και άλλων ανταγωνιστικών απειλών, συμπεριλαμβανομένων των εγκλημάτων τρομοκρατίας, όπως προβλέπεται στην οδηγία (ΕΕ) 2017/541. Η εκτίμηση κινδύνου μιας κρίσιμης οντότητας λαμβάνει υπόψη τον βαθμό στον οποίο άλλοι τομείς, όπως ορίζονται στο παράρτημα, εξαρτώνται από τη βασική υπηρεσία που παρέχει η κρίσιμη οντότητα και τον βαθμό στον οποίο η εν λόγω κρίσιμη οντότητα εξαρτάται από βασικές υπηρεσίες που παρέχονται από άλλες οντότητες σε άλλους τέτοιους τομείς, συμπεριλαμβανομένων, κατά περίπτωση, γειτονικών κρατών μελών και τρίτων χωρών.

Όταν μία κρίσιμη οντότητα έχει διενεργήσει άλλες εκτιμήσεις κινδύνου ή έχει συντάξει έγγραφα σύμφωνα με υποχρεώσεις που προβλέπονται σε άλλες νομοθετικές πράξεις που σχετίζονται με την εκτίμηση κινδύνου της κρίσιμης οντότητάς τους, μπορεί να χρησιμοποιεί τις εν λόγω εκτιμήσεις και τα εν λόγω έγγραφα προκειμένου να συμμορφωθεί με τις απαιτήσεις που ορίζονται στο παρόν άρθρο. Κατά την άσκηση των εποπτικών καθηκόντων της, η αρμόδια αρχή μπορεί να δηλώσει ότι υφιστάμενη εκτίμηση κινδύνου που διενεργήθηκε από μια κρίσιμη οντότητα και περιλαμβάνει τους κινδύνους και την έκταση της εξάρτησης που αναφέρεται στο πρώτο εδάφιο της παρούσας παραγράφου συμμορφώνεται εν μέρει ή εν όλω, με τις υποχρεώσεις που απορρέουν από το παρόν άρθρο.

Άρθρο 13

Μέτρα ανθεκτικότητας των κρίσιμων οντοτήτων

1. Τα κράτη μέλη διασφαλίζουν ότι οι κρίσιμες οντότητες λαμβάνουν κατάλληλα και αναλογικά τεχνικά μέτρα, μέτρα ασφάλειας και οργανωτικά μέτρα για τη διασφάλιση της ανθεκτικότητάς τους, βάσει των σχετικών πληροφοριών που παρέχουν τα κράτη μέλη σχετικά με την εκτίμηση κινδύνων από τα κράτη μέλη και τα αποτελέσματα της εκτίμησης κινδύνων της κρίσιμης οντότητας, συμπεριλαμβανομένων των μέτρων που είναι αναγκαία για:

α) την πρόληψη της επέλευσης περιστατικών, με δέουσα εξέταση των μέτρων μείωσης του κινδύνου καταστροφών και προσαρμογής στην κλιματική αλλαγή·

β) τη διασφάλιση επαρκούς φυσικής προστασίας των εγκαταστάσεών τους και των υποδομών ζωτικής σημασίας, εξετάζοντας δεόντως, για παράδειγμα,τις περιφράξεις, τα εμπόδια, τα εργαλεία και τις διαδικασίες επιτήρησης περιμέτρου τον εξοπλισμό ανίχνευσης και τους ελέγχους πρόσβασης·

γ) την ανταπόκριση στις συνέπειες των περιστατικών, την αντίσταση σε αυτές και τον μετριασμό τους, με δέουσα εξέταση της εφαρμογής διαδικασιών και πρωτοκόλλων διαχείρισης κινδύνων και κρίσεων, καθώς και διαδικασιών έγκαιρης προειδοποίησης·

δ) την ανάκαμψη από περιστατικά, με δέουσα εξέταση μέτρων επιχειρησιακής συνέχειας και του προσδιορισμού εναλλακτικών αλυσίδων εφοδιασμού προκειμένου να αποκατασταθεί η παροχή της βασικής υπηρεσίας·

ε) τη διασφάλιση της κατάλληλης διαχείρισης ασφάλειας των εργαζομένων, με δέουσα εξέταση μέτρων όπως ο ορισμός κατηγοριών προσωπικού που επιτελεί κρίσιμες λειτουργίες, η θέσπιση δικαιωμάτων πρόσβασης σε εγκαταστάσεις, υποδομές ζωτικής σημασίας και ευαίσθητες πληροφορίες, η θέσπιση διαδικασιών ελέγχου ιστορικού σύμφωνα με το άρθρο 14, και ο καθορισμός των κατηγοριών των προσώπων που απαιτούνται για τη διενέργεια τέτοιων ελέγχων ιστορικού, και ο καθορισμός των κατάλληλων απαιτήσεων όσον αφορά την κατάρτιση και τα επαγγελματικά προσόντα·

στ) την ευαισθητοποίηση του οικείου προσωπικού για τα μέτρα των στοιχείων α) έως ε), με δέουσα εξέταση εκπαιδευτικών μαθημάτων, ενημερωτικού υλικού και ασκήσεων.

Για τους σκοπούς του πρώτου εδαφίου στοιχείο ε), τα κράτη μέλη διασφαλίζουν ότι οι κρίσιμες οντότητες λαμβάνουν υπόψη το προσωπικό των εξωτερικών παρόχων υπηρεσιών κατά τον καθορισμό των κατηγοριών του προσωπικού που ασκεί κρίσιμες λειτουργίες.

2. Τα κράτη μέλη διασφαλίζουν ότι οι κρίσιμες οντότητες διαθέτουν και εφαρμόζουν σχέδιο ανθεκτικότητας ή ισοδύναμο έγγραφο ή έγγραφα όπου περιγράφονται τα μέτρα που έχουν ληφθεί δυνάμει της παραγράφου 1. Όταν οι κρίσιμες οντότητες έχουν καταρτίσει έγγραφα ή λάβει μέτρα σε εκπλήρωση υποχρεώσεων από άλλες νομικές πράξεις που εμφανίζουν συνάφεια με τα μέτρα της παραγράφου 1, μπορούν να χρησιμοποιούν τα εν λόγω έγγραφα και μέτρα προκειμένου να συμμορφωθούν με τις απαιτήσεις που ορίζονται στο παρόν άρθρο. Κατά την άσκηση των εποπτικών καθηκόντων της, η αρμόδια αρχή μπορεί να δηλώσει ότι υφιστάμενα μέτρα ενίσχυσης της ανθεκτικότητας που έχει λάβει μια κρίσιμη οντότητα, τα οποία περιλαμβάνουν με κατάλληλο και αναλογικό τρόπο τα τεχνικά μέτρα, μέτρα ασφάλειας και οργανωτικά μέτρα που αναφέρονται στην παράγραφο 1, συμμορφώνονται εν μέρει ή εν όλω με τις υποχρεώσεις που απορρέουν από το παρόν άρθρο.

3. Τα κράτη μέλη διασφαλίζουν ότι κάθε κρίσιμη οντότητα ορίζει έναν αξιωματικό σύνδεσμο ή ισοδύναμο υπάλληλο ως σημείο επαφής με τις αρμόδιες αρχές.

4. Κατόπιν αιτήματος του κράτους μέλους που έχει προσδιορίσει την κρίσιμη οντότητα και με τη σύμφωνη γνώμη της εκάστοτε κρίσιμης οντότητας, η Επιτροπή διοργανώνει συμβουλευτικές αποστολές, σύμφωνα με τις ρυθμίσεις του άρθρου 18 παράγραφοι 6, 8 και 9, για την παροχή συμβουλών στην οικεία κρίσιμη οντότητα όσον αφορά την εκπλήρωση των υποχρεώσεών της βάσει του κεφαλαίου III. Η συμβουλευτική αποστολή υποβάλλει έκθεση με τα πορίσματά της στην Επιτροπή, το εν λόγω κράτος μέλος και την οικεία κρίσιμη οντότητα.

5. Η Επιτροπή, κατόπιν διαβούλευσης με την ομάδα για την ανθεκτικότητα των κρίσιμων οντοτήτων που αναφέρεται στο άρθρο 19, εκδίδει μη δεσμευτικές κατευθυντήριες γραμμές για την περαιτέρω διευκρίνιση των τεχνικών μέτρων, των μέτρων ασφάλειας και των οργανωτικών μέτρων που μπορούν να ληφθούν σύμφωνα με την παράγραφο 1 του παρόντος άρθρου.

6. Η Επιτροπή εκδίδει εκτελεστικές πράξεις για τον καθορισμό των απαραίτητων τεχνικών και μεθοδολογικών προδιαγραφών σχετικά με την εφαρμογή των μέτρων της παραγράφου 1 του παρόντος άρθρου. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης στην οποία παραπέμπει το άρθρο 24 παράγραφος 2.

Άρθρο 14

Έλεγχοι ιστορικού

1. Τα κράτη μέλη καθορίζουν τις προϋποθέσεις υπό τις οποίες επιτρέπεται σε κρίσιμη οντότητα, σε δεόντως αιτιολογημένες περιπτώσεις και λαμβανομένης υπόψη της εκτίμησης κινδύνων από τα κράτη μέλη, να υποβάλλουν αιτήματα για ελέγχους ιστορικού όσον αφορά τα πρόσωπα που:

α) κατέχουν ευαίσθητους ρόλους εντός της κρίσιμης οντότητας ή προς όφελος αυτής, ιδίως όσον αφορά την ανθεκτικότητα της κρίσιμης οντότητας·

β) είναι εξουσιοδοτημένα να έχουν άμεση ή εξ αποστάσεως πρόσβαση στις εγκαταστάσεις, στα συστήματα πληροφοριών ή ελέγχου αυτής, μεταξύ άλλων και σε σχέση με την ασφάλεια της κρίσιμης οντότητας·

γ) είναι υπό εξέταση για πρόσληψη σε θέσεις που εμπίπτουν στα κριτήρια που καθορίζονται στο στοιχείο α) ή β).

2. Αιτήματα που αναφέρονται στην παράγραφο 1 του παρόντος άρθρου αξιολογούνται εντός εύλογου χρονικού διαστήματος και υπόκεινται σε επεξεργασία σύμφωνα με το εθνικό δίκαιο και διαδικασίες και το σχετικό και εφαρμοστέο ενωσιακό δίκαιο, συμπεριλαμβανομένων του κανονισμού (ΕΕ) 2016/679 και της οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([37]). Οι έλεγχοι ιστορικού είναι αναλογικοί και περιορίζονται αυστηρά στα όρια του αναγκαίου. Διενεργούνται με αποκλειστικό σκοπό την αξιολόγηση δυνητικού κινδύνου για την ασφάλεια της οικείας κρίσιμης οντότητας.

3. Ο έλεγχος ιστορικού που αναφέρεται στην παράγραφο 1, τουλάχιστον:

α) επιβεβαιώνει την ταυτότητα του προσώπου που αποτελεί αντικείμενο του ελέγχου ιστορικού·

β) ελέγχει το ποινικό μητρώο του εν λόγω προσώπου όσον αφορά εγκλήματα που θα μπορούσαν να είναι συναφή με συγκεκριμένη θέση.

Κατά τη διενέργεια ελέγχων ιστορικού, τα κράτη μέλη χρησιμοποιούν το Ευρωπαϊκό Σύστημα Πληροφοριών Ποινικού Μητρώου, σύμφωνα με τις διαδικασίες που ορίζονται στην απόφαση-πλαίσιο 2009/315/ΔΕΥ και, κατά περίπτωση και εφόσον κρίνεται σκόπιμο, στον κανονισμό (ΕΕ) 2019/816 με σκοπό την απόκτηση πληροφοριών από ποινικά μητρώα που τηρούνται από άλλα κράτη μέλη. Οι κεντρικές αρχές που αναφέρονται στο άρθρο 3 παράγραφος 1 της απόφασης-πλαισίου 2009/315/ΔΕΥ και στο άρθρο 3 σημείο 5) του κανονισμού (ΕΕ) 2019/816 απαντούν σε αιτήματα τέτοιων πληροφοριών εντός 10 εργάσιμων ημερών από την ημερομηνία λήψης του αιτήματος, σύμφωνα με το άρθρο 8 παράγραφος 1 της απόφασης-πλαισίου 2009/315/ΔΕΥ.

([37]) Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου (ΕΕ L 119 της 4.5.2016, σ. 89).

Άρθρο 15

Κοινοποίηση περιστατικών

1. Τα κράτη μέλη διασφαλίζουν ότι οι κρίσιμες οντότητες κοινοποιούν στην αρμόδια αρχή, χωρίς αδικαιολόγητη καθυστέρηση, τα περιστατικά τα οποία διαταράσσουν σημαντικά ή έχουν τη δυνατότητα να διαταράξουν σημαντικά την παροχή βασικών υπηρεσιών. Τα κράτη μέλη διασφαλίζουν ότι, εκτός και αν δεν υπάρχει η σχετική επιχειρησιακή δυνατότητα, οι κρίσιμες οντότητες υποβάλλουν αρχική κοινοποίηση το αργότερο 24 ώρες αφότου λάβουν γνώση περιστατικού, και ακολουθείται, κατά περίπτωση, από λεπτομερή έκθεση το αργότερο έναν μήνα μετά. Προκειμένου να καθοριστεί πόσο σημαντική είναι μια διαταραχή, λαμβάνονται ιδίως υπόψη οι ακόλουθες παράμετροι:

α) ο αριθμός και η αναλογία των χρηστών που επηρεάζονται από τη διαταραχή·

β) η διάρκεια της διαταραχής·

γ) η γεωγραφική περιοχή που επηρεάζεται από τη διαταραχή, αφού ληφθεί υπόψη αν η εν λόγω περιοχή είναι γεωγραφικά απομονωμένη.

Όταν ένα περιστατικό έχει ή ενδέχεται να έχει σημαντικό αντίκτυπο στη συνέχεια της παροχής βασικών υπηρεσιών σε έξι ή περισσότερα κράτη μέλη, οι αρμόδιες αρχές των κρατών μελών που επηρεάζονται από το περιστατικό κοινοποιούν στην Επιτροπή το εν λόγω περιστατικό.

2. Οι κοινοποιήσεις όπως αναφέρονται στην παράγραφο 1 πρώτο εδάφιο, περιλαμβάνουν όλες τις διαθέσιμες πληροφορίες που είναι απαραίτητες προκειμένου να δοθεί στην αρμόδια αρχή η δυνατότητα να κατανοήσει τη φύση, την αιτία και τις πιθανές συνέπειες του περιστατικού, συμπεριλαμβανομένων όλων των διαθέσιμων πληροφοριών που είναι αναγκαίες για τον προσδιορισμό ενδεχόμενου διασυνοριακού αντικτύπου του περιστατικού. Οι κοινοποιήσεις αυτές δεν συνεπάγονται αυξημένη ευθύνη για τις κρίσιμες οντότητες.

3. Με βάση τις πληροφορίες που παρέχονται από την κρίσιμη οντότητα σε κοινοποίηση όπως αναφέρεται στην παράγραφο 1, η οικεία αρμόδια αρχή, μέσω του ενιαίου σημείου επαφής, ενημερώνει το ενιαίο σημείο επαφής των άλλων επηρεαζόμενων κρατών μελών, αν το περιστατικό έχει ή ενδέχεται να έχει σημαντικό αντίκτυπο σε κρίσιμες οντότητες και στη συνέχεια της παροχής βασικών υπηρεσιών προς ή εντός ενός ή περισσοτέρων άλλων κρατών μελών.

Τα ενιαία σημεία επαφής που αποστέλλουν και λαμβάνουν πληροφορίες δυνάμει του πρώτου εδαφίου, χειρίζονται, σύμφωνα με το ενωσιακό ή το εθνικό δίκαιο,τις πληροφορίες αυτές με τρόπο που σέβεται την εμπιστευτικότητά τους και προστατεύει τα συμφέροντα ασφάλειας και τα εμπορικά συμφέροντα της εκάστοτε κρίσιμης οντότητας.

4. Το συντομότερο δυνατόν μετά την κοινοποίηση όπως αναφέρεται στην παράγραφο 1, η οικεία αρμόδια αρχή παρέχει στην οικεία κρίσιμη οντότητα σχετικές πληροφορίες για τη συνέχεια που δόθηκε, συμπεριλαμβανομένων πληροφοριών που θα μπορούσαν να υποστηρίξουν την αποτελεσματική αντιμετώπιση του περιστατικού αυτού από την εν λόγω κρίσιμη οντότητα. Τα κράτη μέλη ενημερώνουν το κοινό, όταν κρίνουν ότι αυτό θα είναι προς το δημόσιο συμφέρον.

Άρθρο 16

Πρότυπα

Προκειμένου να προωθηθεί η συγκλίνουσα εφαρμογή της παρούσας οδηγίας, τα κράτη μέλη, χωρίς να επιβάλλουν ή να εισάγουν διακρίσεις υπέρ της χρήσης συγκεκριμένου είδους τεχνολογίας, ενθαρρύνουν, όπου αυτό είναι χρήσιμο, τη χρήση ευρωπαϊκών και διεθνών προτύπων και τεχνικών προδιαγραφών σχετικών με τα μέτρα ασφάλειας και ανθεκτικότητας που εφαρμόζονται στις κρίσιμες οντότητες.

ΚΕΦΆΛΑΙΟ IV

ΚΡΊΣΙΜΕΣ ΟΝΤΌΤΗΤΕΣ ΙΔΙΑΊΤΕΡΟΥ ΕΥΡΩΠΑΪΚΟΎ ΕΝΔΙΑΦΈΡΟΝΤΟΣ

Άρθρο 17

Προσδιορισμός των κρίσιμων οντοτήτων ιδιαίτερου ευρωπαϊκού ενδιαφέροντος

1. Οντότητα θεωρείται κρίσιμη οντότητα ιδιαίτερου ευρωπαϊκού ενδιαφέροντος όταν:

α) έχει προσδιοριστεί ως κρίσιμη οντότητα σύμφωνα με το άρθρο 6 παράγραφος 1·

β) παρέχει τις ίδιες ή παρεμφερείς βασικές υπηρεσίες προς ή εντός έξι ή περισσότερων κρατών μελών· και

γ) έχει ειδοποιηθεί σύμφωνα με την παράγραφο 3 του παρόντος άρθρου.

2. Τα κράτη μέλη διασφαλίζουν ότι μια κρίσιμη οντότητα, μετά την κοινοποίηση που αναφέρεται στο άρθρο 6 παράγραφος 3, ενημερώνει την αρμόδια αρχή της όταν παρέχει βασικές υπηρεσίες προς ή εντός έξι ή περισσότερων κρατών μελών. Στην περίπτωση αυτή, τα κράτη μέλη διασφαλίζουν ότι η κρίσιμη οντότητα ενημερώνει την αρμόδια αρχή της για τις βασικές υπηρεσίες που παρέχει σε ή εντός των εν λόγω κρατών μελών και για τα κράτη μέλη προς τα οποία ή εντός των οποίων παρέχει τέτοιες βασικές υπηρεσίες. Τα κράτη μέλη κοινοποιούν στην Επιτροπή, χωρίς αδικαιολόγητη καθυστέρηση, την ταυτότητα των εν λόγω κρίσιμων οντοτήτων και τα στοιχεία που παρέχουν σύμφωνα με την παρούσα παράγραφο.

Η Επιτροπή διαβουλεύεται με την αρμόδια αρχή του κράτους μέλους που προσδιόρισε μια κρίσιμη οντότητα όπως αναφέρεται στο πρώτο εδάφιο, την αρμόδια αρχή άλλων ενδιαφερόμενων κρατών μελών και την συγκεκριμένη κρίσιμη οντότητα. Κατά τη διάρκεια των εν λόγω διαβουλεύσεων, κάθε κράτος μέλος ενημερώνει την Επιτροπή εάν κρίνει ότι οι υπηρεσίες που παρέχονται στο εν λόγω κράτος μέλος από την κρίσιμη οντότητα είναι βασικές υπηρεσίες.

3. Εάν η Επιτροπή αποφασίσει, με βάση τις διαβουλεύσεις που αναφέρονται στην παράγραφο 2 του παρόντος άρθρου, ότι η οικεία κρίσιμη οντότητα παρέχει βασικές υπηρεσίες προς ή εντός έξι ή περισσότερων κρατών μελών, η Επιτροπή κοινοποιεί στην εν λόγω κρίσιμη οντότητα, μέσω της αρμόδιας αρχής της, ότι θεωρείται κρίσιμη οντότητα ιδιαίτερου ευρωπαϊκού ενδιαφέροντος και πληροφορεί την εν λόγω κρίσιμη οντότητα για τις υποχρεώσεις της βάσει του παρόντος κεφαλαίου και για την ημερομηνία από την οποία ισχύουν για αυτήν οι εν λόγω υποχρεώσεις. Μόλις η Επιτροπή ενημερώσει την αρμόδια αρχή για την απόφασή της να θεωρήσει μια κρίσιμη οντότητα ως κρίσιμη οντότητα ιδιαίτερου ευρωπαϊκού ενδιαφέροντος, η αρμόδια αρχή προωθεί την εν λόγω κοινοποίηση στην εν λόγω κρίσιμη οντότητα χωρίς αδικαιολόγητη καθυστέρηση.

4. Το παρόν κεφάλαιο εφαρμόζεται στην εκάστοτε κρίσιμη οντότητα ιδιαίτερου ευρωπαϊκού ενδιαφέροντος από την ημερομηνία παραλαβής της ειδοποίησης που αναφέρεται στην παράγραφο 3 του παρόντος άρθρου.

Άρθρο 18

Συμβουλευτικές αποστολές

1. Κατόπιν αιτήματος του κράτους μέλους το οποίο έχει προσδιορίσει μια κρίσιμη οντότητα ιδιαίτερου ευρωπαϊκού ενδιαφέροντος ως κρίσιμη οντότητα δυνάμει του άρθρου 6 παράγραφος 1, η Επιτροπή οργανώνει συμβουλευτική αποστολή για την αξιολόγηση των μέτρων που εφαρμόζει η εν λόγω κρίσιμη οντότητα για την εκπλήρωση των υποχρεώσεών της βάσει του κεφαλαίου III.

2. Με δική της πρωτοβουλία ή κατόπιν αιτήματος ενός ή περισσότερων κρατών μελών προς τα οποία ή εντός των οποίων παρέχεται η βασική υπηρεσία, και υπό την προϋπόθεση ότι το κράτος μέλος που έχει προσδιορίσει κρίσιμη οντότητα ιδιαίτερου ευρωπαϊκού ενδιαφέροντος ως κρίσιμη οντότητα δυνάμει του άρθρου 6 παράγραφος 1 συμφωνεί, η Επιτροπή οργανώνει συμβουλευτική αποστολή όπως αναφέρεται στην παράγραφο 1 του παρόντος άρθρου,

3. Κατόπιν αιτιολογημένου αιτήματος από την Επιτροπή ή από ένα ή περισσότερα κράτη μέλη προς τα οποία ή εντός των οποίων παρέχεται η βασική υπηρεσία, το κράτος μέλος που προσδιόρισε κρίσιμη οντότητα ιδιαίτερου ευρωπαϊκού ενδιαφέροντος ως κρίσιμη οντότητα δυνάμει του άρθρου 6 παράγραφος 1 παρέχει στην Επιτροπή τα ακόλουθα:

α) τα σχετικά σημεία της εκτίμησης κινδύνων της κρίσιμης οντότητας·

β) κατάλογο των σχετικών μέτρων που λαμβάνονται σύμφωνα με το άρθρο 13·

γ) τα εποπτικά μέτρα ή μέτρα επιβολής, συμπεριλαμβανομένων αξιολογήσεων της συμμόρφωσης ή εντολών που εκδόθηκαν, στα οποία προέβη η αρμόδια αρχή της σύμφωνα με τα άρθρα 21 και 22 όσον αφορά την εν λόγω κρίσιμη οντότητα.

4. Η συμβουλευτική αποστολή υποβάλλει έκθεση με τα πορίσματά της στην Επιτροπή, στο κράτος μέλος που προσδιόρισε κρίσιμη οντότητα ιδιαίτερου ευρωπαϊκού ενδιαφέροντος ως κρίσιμη οντότητα δυνάμει του άρθρου 6 παράγραφος 1, στα κράτη μέλη προς τα οποία ή εντός των οποίων παρέχεται η βασική υπηρεσία και στην οικεία κρίσιμη οντότητα εντός τριών μηνών από την ολοκλήρωση της συμβουλευτικής αποστολής.

Τα κράτη μέλη προς τα οποία ή εντός των οποίων παρέχεται η βασική υπηρεσία αναλύουν την έκθεση που αναφέρεται στο πρώτο εδάφιο και, αν είναι απαραίτητο, υποβάλλουν στην Επιτροπή τη γνώμη τους σχετικά με το κατά πόσον η οικεία κρίσιμη οντότητα ιδιαίτερου ευρωπαϊκού ενδιαφέροντος συμμορφώνεται με τις υποχρεώσεις της βάσει του κεφαλαίου III και, κατά περίπτωση, ποια μέτρα θα μπορούσαν να ληφθούν για να βελτιωθεί η ανθεκτικότητα της εν λόγω κρίσιμης οντότητας.

Η Επιτροπή, βάσει της γνώμης που αναφέρεται στο δεύτερο εδάφιο της παρούσας παραγράφου, κοινοποιεί τη δική της γνώμη στο κράτος μέλος το οποίο έχει προσδιορίσει κρίσιμη οντότητα ιδιαίτερου ευρωπαϊκού ενδιαφέροντος ως κρίσιμη οντότητα δυνάμει του άρθρου 6 παράγραφος 1, στα κράτη μέλη προς τα οποία ή εντός των οποίων παρέχεται η βασική υπηρεσία και στην εν λόγω κρίσιμη οντότητα το κατά πόσον η εν λόγω κρίσιμη οντότητα συμμορφώνεται με τις υποχρεώσεις της βάσει του κεφαλαίου III και, κατά περίπτωση, ποια μέτρα θα μπορούσαν να ληφθούν για να βελτιωθεί η ανθεκτικότητα της εν λόγω κρίσιμης οντότητας.

Το κράτος μέλος το οποίο έχει προσδιορίσει κρίσιμη οντότητα ιδιαίτερου ευρωπαϊκού ενδιαφέροντος ως κρίσιμη οντότητα δυνάμει του άρθρου 6 παράγραφος 1 διασφαλίζει ότι η αρμόδια αρχή του και η οικεία κρίσιμη οντότητα λαμβάνουν υπόψη τη γνώμη που αναφέρεται στο τρίτο εδάφιο της παρούσας παραγράφου και παρέχει πληροφορίες στην Επιτροπή και στα κράτη μέλη προς τα οποία ή εντός των οποίων παρέχεται η βασική υπηρεσία σχετικά με τα μέτρα που έχει λάβει σύμφωνα με τη γνώμη αυτή.

5. Κάθε συμβουλευτική αποστολή απαρτίζεται από εμπειρογνώμονες από το κράτος μέλος στο οποίο βρίσκεται η κρίσιμη οντότητα ιδιαίτερου ευρωπαϊκού ενδιαφέροντος, εμπειρογνώμονες από τα κράτη μέλη προς τα οποία ή εντός των οποίων παρέχεται η βασική υπηρεσία και από εκπροσώπους της Επιτροπής. Τα εν λόγω κράτη μέλη μπορούν να προτείνουν υποψηφίους για να συμμετάσχουν σε συμβουλευτική αποστολή. Η Επιτροπή, κατόπιν διαβούλευσης με το κράτος μέλος που έχει προσδιορίσει κρίσιμη οντότητα ιδιαίτερου ευρωπαϊκού ενδιαφέροντος ως κρίσιμη οντότητα δυνάμει του άρθρου 6 παράγραφος 1, επιλέγει και διορίζει τα μέλη κάθε συμβουλευτικής αποστολής σύμφωνα με την επαγγελματική ιδιότητά τους, διασφαλίζοντας, όπου είναι δυνατόν, γεωγραφικά ισορροπημένη εκπροσώπηση όλων αυτών των κρατών μελών. Όταν είναι αναγκαίο, τα μέλη της συμβουλευτικής αποστολής διαθέτουν έγκυρη και κατάλληλη εξουσιοδότηση ασφαλείας. Η Επιτροπή βαρύνεται με τις δαπάνες συμμετοχής στη συμβουλευτική αποστολή.

Η Επιτροπή οργανώνει το πρόγραμμα κάθε συμβουλευτικής αποστολής, σε συνεννόηση με τα μέλη της συγκεκριμένης συμβουλευτικής αποστολής και σε συμφωνία με το κράτος μέλος που έχει προσδιορίσει κρίσιμη οντότητα ιδιαίτερου ευρωπαϊκού ενδιαφέροντος ως κρίσιμη οντότητα δυνάμει του άρθρου 6 παράγραφος 1.

6. Η Επιτροπή εκδίδει εκτελεστική πράξη για τη θέσπιση κανόνων σχετικά με τις διαδικαστικές ρυθμίσεις για αιτήματα διοργάνωσης συμβουλευτικών αποστολών, για τη διεκπεραίωση τέτοιων αιτημάτων, για τη διεξαγωγή των συμβουλευτικών αποστολών και την υποβολή των σχετικών εκθέσεων και για τον χειρισμό της επικοινωνίας σχετικά με τη γνώμη της Επιτροπής που αναφέρεται στην παράγραφο 4 τρίτο εδάφιο του παρόντος άρθρου και τα μέτρα που λήφθηκαν, λαμβάνοντας δεόντως υπόψη το απόρρητο και τον εμπορικά ευαίσθητο χαρακτήρα των οικείων πληροφοριών. Η εν λόγω εκτελεστική πράξη εκδίδεται σύμφωνα με τη διαδικασία εξέτασης στην οποία παραπέμπει το άρθρο 24 παράγραφος 2.

7. Τα κράτη μέλη διασφαλίζουν ότι οι κρίσιμες οντότητες ιδιαίτερου ευρωπαϊκού ενδιαφέροντος παρέχουν στις συμβουλευτικές αποστολές πρόσβαση στις πληροφορίες, τα συστήματα και τις εγκαταστάσεις που σχετίζονται με την παροχή των βασικών υπηρεσιών τους που είναι αναγκαίες για τη διεξαγωγή της οικείας συμβουλευτικής αποστολής.

8. Οι συμβουλευτικές αποστολές διεξάγονται σύμφωνα με το εφαρμοστέο εθνικό δίκαιο του κράτους μέλους στο οποίο πραγματοποιούνται, με σεβασμό της ευθύνης του εν λόγω κράτους μέλους όσον αφορά την εθνική ασφάλεια και την προστασία των συμφερόντων ασφαλείας του.

9. Κατά τη διοργάνωση των συμβουλευτικών αποστολών, η Επιτροπή λαμβάνει υπόψη τις τυχόν εκθέσεις που έχουν καταρτιστεί στο πλαίσιο επιθεωρήσεων που διεξήγαγε η Επιτροπή σύμφωνα με τους κανονισμούς (ΕΚ) αριθ. 725/2004 και (ΕΚ) αριθ. 300/2008 και τις τυχόν εκθέσεις που έχουν καταρτιστεί στο πλαίσιο παρακολούθησης που διενήργησε η Επιτροπή σύμφωνα με την οδηγία 2005/65/ΕΚ όσον αφορά την οικεία κρίσιμη οντότητα.

10. Η Επιτροπή ενημερώνει την ομάδα για την ανθεκτικότητα των κρίσιμων οντοτήτων που αναφέρεται στο άρθρο 19 κάθε φορά που οργανώνεται συμβουλευτική αποστολή. Το κράτος μέλος στο οποίο πραγματοποιήθηκε η συμβουλευτική αποστολή και η Επιτροπή ενημερώνουν επίσης την ομάδα για την ανθεκτικότητα των κρίσιμων οντοτήτων σχετικά με τα κυριότερα ευρήματα της συμβουλευτικής αποστολής και τα διδάγματα που αντλήθηκαν με σκοπό την προώθηση της αμοιβαίας μάθησης.

ΚΕΦΆΛΑΙΟ V

ΣΥΝΕΡΓΑΣΊΑ ΚΑΙ ΥΠΟΒΟΛΉ ΕΚΘΈΣΕΩΝ

Άρθρο 19

Ομάδα για την ανθεκτικότητα των κρίσιμων οντοτήτων

1. Συστήνεται ομάδα για την ανθεκτικότητα των κρίσιμων οντοτήτων. Η ομάδα για την ανθεκτικότητα των κρίσιμων οντοτήτων υποστηρίζει την Επιτροπή και διευκολύνει τη συνεργασία μεταξύ των κρατών μελών και την ανταλλαγή πληροφοριών σε ζητήματα σχετικά με την παρούσα οδηγία.

2. Η ομάδα για την ανθεκτικότητα των κρίσιμων οντοτήτων απαρτίζεται από εκπροσώπους των κρατών μελών και της Επιτροπής που διαθέτουν εξουσιοδότηση ασφαλείας, κατά περίπτωση. Όταν είναι σκόπιμο για την εκτέλεση των καθηκόντων της, η ομάδα για την ανθεκτικότητα των κρίσιμων οντοτήτων μπορεί να προσκαλεί σχετικούς ενδιαφερόμενους να συμμετάσχουν στις εργασίες της. Εάν ζητηθεί από το Ευρωπαϊκό Κοινοβούλιο, η Επιτροπή μπορεί να προσκαλέσει εμπειρογνώμονες από το Ευρωπαϊκό Κοινοβούλιο να παραστούν στις συνεδριάσεις της ομάδας για την ανθεκτικότητα των κρίσιμων οντοτήτων.

Ο εκπρόσωπος της Επιτροπής προεδρεύει της ομάδας για την ανθεκτικότητα των κρίσιμων οντοτήτων.

3. Η ομάδα για την ανθεκτικότητα των κρίσιμων οντοτήτων έχει τα ακόλουθα καθήκοντα:

α) υποστηρίζει την Επιτροπή κατά την παροχή συνδρομής στα κράτη μέλη με σκοπό την ενίσχυση της ικανότητάς τους να συμβάλλουν στη διασφάλιση της ανθεκτικότητας των κρίσιμων οντοτήτων σύμφωνα με την παρούσα οδηγία·

β) αναλύει τις στρατηγικές προκειμένου να προσδιορίσει βέλτιστες πρακτικές όσον αφορά τις στρατηγικές·

γ) διευκολύνει την ανταλλαγή βέλτιστων πρακτικών όσον αφορά τον προσδιορισμό των κρίσιμων οντοτήτων από τα κράτη μέλη δυνάμει του άρθρου 6 παράγραφος 1, μεταξύ άλλων σε σχέση με τις διασυνοριακές και διατομεακές εξαρτήσεις και όσον αφορά κινδύνους και περιστατικά·

δ) κατά περίπτωση, συμβάλλει όσον αφορά θέματα που σχετίζονται με την παρούσα οδηγία σε έγγραφα σχετικά με την ανθεκτικότητα σε επίπεδο Ένωσης·

ε) συμβάλλει στην κατάρτιση των κατευθυντήριων γραμμών που αναφέρονται στο άρθρο 7 παράγραφος 3 και στο άρθρο 13 παράγραφος 5 και, κατόπιν αιτήματος, οποιωνδήποτε κατ' εξουσιοδότηση ή εκτελεστικών πράξεων που εκδίδονται δυνάμει της παρούσας οδηγίας ·

στ) αναλύει τις συνοπτικές εκθέσεις που αναφέρονται στο άρθρο 9 παράγραφος 3 με σκοπό την προώθηση της ανταλλαγής βέλτιστων πρακτικών σχετικά με τα μέτρα που λαμβάνονται σύμφωνα με το άρθρο 15 παράγραφος 3·

ζ) ανταλλάσσει βέλτιστες πρακτικές όσον αφορά την κοινοποίηση περιστατικών κατά το άρθρο 15·

η) συζητάει τις συνοπτικές εκθέσεις των συμβουλευτικών αποστολών και τα διδάγματα που αντλήθηκαν σύμφωνα με το άρθρο 18 παράγραφος 10·

θ) ανταλλάσσει πληροφορίες και βέλτιστες πρακτικές για την καινοτομία, την έρευνα και την ανάπτυξη σχετικά με την ανθεκτικότητα των κρίσιμων οντοτήτων σύμφωνα με την παρούσα οδηγία·

ι) κατά περίπτωση, ανταλλάσσει πληροφορίες για ζητήματα ανθεκτικότητας των κρίσιμων οντοτήτων με τα αρμόδια θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης.

4. Έως τις 17 Ιανουαρίου 2025 και στη συνέχεια ανά διετία, η ομάδα για την ανθεκτικότητα των κρίσιμων οντοτήτων καταρτίζει πρόγραμμα εργασιών, σύμφωνο προς τις απαιτήσεις και τους στόχους της. Το εν λόγω πρόγραμμα εργασιών συνάδει με τις απαιτήσεις και τους στόχους της παρούσας οδηγίας.

5. Η ομάδα για την ανθεκτικότητα των κρίσιμων οντοτήτων συνεδριάζει σε τακτική βάση και σε κάθε περίπτωση τουλάχιστον μία φορά ετησίως με την ομάδα συνεργασίας που έχει συσταθεί βάσει της οδηγίας (ΕΕ) 2022/2555 για την προώθηση και διευκόλυνση της συνεργασίας και της ανταλλαγής πληροφοριών.

6. Η Επιτροπή μπορεί να εκδίδει εκτελεστικές πράξεις που καθορίζουν τις διαδικαστικές ρυθμίσεις που είναι αναγκαίες για τη λειτουργία της ομάδας για την ανθεκτικότητα των κρίσιμων οντοτήτων, τηρώντας το άρθρο 1 παράγραφος 4. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης στην οποία παραπέμπει το άρθρο 24 παράγραφος 2.

7. Η Επιτροπή διαβιβάζει στην ομάδα για την ανθεκτικότητα των κρίσιμων οντοτήτων συνοπτική έκθεση σχετικά με τις πληροφορίες που παρέχουν τα κράτη μέλη σύμφωνα με το άρθρο 4 παράγραφος 3 και το άρθρο 5 παράγραφος 4 έως τις 17 Ιανουαρίου 2027 και, στη συνέχεια, όποτε είναι απαραίτητο και τουλάχιστον ανά τετραετία.

Άρθρο 20

Παροχή υποστήριξης στις αρμόδιες αρχές και τις κρίσιμες οντότητες από την Επιτροπή

1. Η Επιτροπή υποστηρίζει, κατά περίπτωση, τα κράτη μέλη και τις κρίσιμες οντότητες όσον αφορά τη συμμόρφωσή τους με τις υποχρεώσεις τους βάσει της παρούσας οδηγίας. Η Επιτροπή εκπονεί ενωσιακού επιπέδου επισκόπηση των διασυνοριακών και διατομεακών κινδύνων για την παροχή βασικών υπηρεσιών, οργανώνει τις συμβουλευτικές αποστολές που αναφέρονται στο άρθρο 13 παράγραφος 4 και στο άρθρο 18 και διευκολύνει την ανταλλαγή πληροφοριών μεταξύ κρατών μελών και εμπειρογνωμόνων σε ολόκληρη την Ένωση.

2. Η Επιτροπή συμπληρώνει τις δραστηριότητες των κρατών μελών όπως αναφέρονται στο άρθρο 10 μέσω της ανάπτυξης βέλτιστων πρακτικών, υλικού καθοδήγησης και μεθοδολογιών, και διασυνοριακών δραστηριοτήτων κατάρτισης και ασκήσεων δοκιμής της ανθεκτικότητας κρίσιμων οντοτήτων.

3. Η Επιτροπή ενημερώνει τα κράτη μέλη σχετικά με τους χρηματοδοτικούς πόρους που διατίθενται στα κράτη μέλη σε επίπεδο Ένωσης για την ενίσχυση της ανθεκτικότητας των κρίσιμων οντοτήτων.

ΚΕΦΆΛΑΙΟ VI

ΕΠΟΠΤΕΊΑ ΚΑΙ ΕΠΙΒΟΛΉ

Άρθρο 21

Εποπτεία και επιβολή

1. Για την αξιολόγηση της συμμόρφωσης με τις υποχρεώσεις βάσει της παρούσας οδηγίας των οντοτήτων που τα κράτη μέλη έχουν προσδιορίσει ως κρίσιμες οντότητες δυνάμει του άρθρου 6 παράγραφος 1, τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές τους έχουν τις εξουσίες και τα μέσα για να:

α) διεξάγουν επιτόπιες επιθεωρήσεις των υποδομών ζωτικής σημασίας και των εγκαταστάσεων που η κρίσιμη οντότητα χρησιμοποιεί για την παροχή των βασικών υπηρεσιών της, και μη επιτόπια εποπτεία των μέτρων που λαμβάνουν οι κρίσιμες οντότητες σύμφωνα με το άρθρο 13·

β) διενεργούν ή δίνουν εντολή για ελέγχους αναφορικά με τις κρίσιμες οντότητες.

2. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές έχουν τις εξουσίες και τα μέσα για να απαιτούν, όταν είναι αναγκαίο για την εκτέλεση των καθηκόντων τους σύμφωνα με την παρούσα οδηγία, οι οντότητες βάσει της οδηγίας (ΕΕ) 2022/2555 που τα κράτη μέλη έχουν επίσης προσδιορίσει ως κρίσιμες οντότητες βάσει της παρούσας οδηγίας, να παρέχουν εντός εύλογου χρονικού διαστήματος που καθορίζουν οι εν λόγω αρχές:

α) τις πληροφορίες που είναι αναγκαίες για την αξιολόγηση του κατά πόσον τα μέτρα που οι εν λόγω οντότητες έλαβαν για τη διασφάλιση της ανθεκτικότητάς τους πληρούν τις απαιτήσεις που ορίζονται στο άρθρο 13·

β) στοιχεία που να αποδεικνύουν την πραγματική εφαρμογή των εν λόγω μέτρων, συμπεριλαμβανομένων των αποτελεσμάτων ελέγχου που έχει διενεργηθεί από ανεξάρτητο και αναγνωρισμένο ελεγκτή, επιλεγμένο από την εν λόγω οντότητα, με δαπάνες αυτής.

Όταν οι αρμόδιες αρχές ζητούν τις εν λόγω πληροφορίες, δηλώνουν τον σκοπό για τον οποίο τις ζητούν και προσδιορίζουν τις πληροφορίες που ζητούνται.

3. Χωρίς να θίγεται η δυνατότητα επιβολής κυρώσεων σύμφωνα με το άρθρο 22, οι αρμόδιες αρχές μπορούν, μετά τα μέτρα εποπτείας που αναφέρονται στην παράγραφο 1 του παρόντος άρθρου ή την αξιολόγηση των πληροφοριών που αναφέρονται στην παράγραφο 2 του παρόντος άρθρου, να δίνουν στις οικείες κρίσιμες οντότητες εντολή για τη λήψη των αναγκαίων και αναλογικών μέτρων για την αποκατάσταση κάθε εντοπισθείσας παράβασης της παρούσας οδηγίας, εντός εύλογης προθεσμίας που καθορίζεται από τις εν λόγω αρχές, και για την υποβολή πληροφοριών στις εν λόγω αρχές σχετικά με τα μέτρα που έλαβαν. Οι εν λόγω εντολές λαμβάνουν υπόψη ιδίως τη σοβαρότητα της παράβασης.

4. Τα κράτη μέλη διασφαλίζουν ότι οι εξουσίες που προβλέπονται στις παραγράφους 1, 2 και 3 μπορούν να ασκούνται μόνο υπό κατάλληλες διασφαλίσεις. Οι εν λόγω διασφαλίσεις εγγυώνται, ιδίως, ότι η άσκηση των εξουσιών αυτών πραγματοποιείται με αντικειμενικό, διαφανή και αναλογικό τρόπο και ότι διασφαλίζονται δεόντως τα δικαιώματα και τα έννομα συμφέροντα των επηρεαζόμενων κρίσιμων οντοτήτων, όπως η προστασία του εμπορικού και του επιχειρηματικού απορρήτου, συμπεριλαμβανομένου του δικαιώματος ακρόασης, του δικαιώματος υπεράσπισης και του δικαιώματος πραγματικής προσφυγής σε ανεξάρτητο δικαστήριο.

5. Τα κράτη μέλη διασφαλίζουν ότι, όταν αρμόδια αρχή βάσει της παρούσας οδηγίας αξιολογεί τη συμμόρφωση κρίσιμης οντότητας δυνάμει του παρόντος άρθρου, η εν λόγω κρίσιμη οντότητα ενημερώνει τις αρμόδιες αρχές του οικείου κράτους μέλους βάσει της οδηγίας (ΕΕ) 2022/2555. Για τον σκοπό αυτό, τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές βάσει της παρούσας οδηγίας μπορούν να ζητήσουν από τις αρμόδιες αρχές βάσει της οδηγίας (ΕΕ) 2022/2555 να ασκήσουν τις εποπτικές και εκτελεστικές τους εξουσίες σε σχέση με οντότητα βάσει της εν λόγω οδηγίας που έχει προσδιοριστεί ως κρίσιμη οντότητα βάσει της παρούσας οδηγίας. Για τον σκοπό αυτόν, τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές βάσει της παρούσας οδηγίας συνεργάζονται και ανταλλάσσουν πληροφορίες με τις αρμόδιες αρχές βάσει της οδηγίας (ΕΕ) 2022/2555.

Άρθρο 22

Κυρώσεις

Τα κράτη μέλη καθορίζουν τους κανόνες για τις κυρώσεις που επιβάλλονται σε περίπτωση παραβάσεων των εθνικών μέτρων που θεσπίζονται δυνάμει της παρούσας οδηγίας και λαμβάνουν όλα τα αναγκαία μέτρα για να διασφαλίσουν την εφαρμογή τους. Οι προβλεπόμενες κυρώσεις είναι αποτελεσματικές, αναλογικές και αποτρεπτικές. Τα κράτη μέλη γνωστοποιούν στην Επιτροπή, έως τις 17 Οκτωβρίου 2024, τους κανόνες και τα μέτρα αυτά και την ενημερώνουν αμελλητί σχετικά με κάθε μεταγενέστερη τροποποίησή τους.

ΚΕΦΆΛΑΙΟ VII

ΚΑΤ' ΕΞΟΥΣΙΟΔ'ΟΤΗΣΗ ΚΑΙ ΕΚΤΕΛΕΣΤΙΚΈΣ ΠΡΆΞΕΙΣ

Άρθρο 23

Άσκηση της εξουσιοδότησης

1. Ανατίθεται στην Επιτροπή η εξουσία να εκδίδει κατ' εξουσιοδότηση πράξεις υπό τους όρους του παρόντος άρθρου.

2. Η προβλεπόμενη στο άρθρο 5 παράγραφος 1 εξουσία έκδοσης κατ' εξουσιοδότηση πράξεων ανατίθεται στην Επιτροπή για περίοδο πέντε ετών από τις 16 Ιανουαρίου 2023.

3. Η εξουσιοδότηση που προβλέπεται στο άρθρο 5 παράγραφος 1 μπορεί να ανακληθεί ανά πάσα στιγμή από το Ευρωπαϊκό Κοινοβούλιο ή το Συμβούλιο. Η απόφαση ανάκλησης περατώνει την εξουσιοδότηση που προσδιορίζεται στην εν λόγω απόφαση. Αρχίζει να ισχύει την επομένη της δημοσίευσης της απόφασης στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης* ή σε μεταγενέστερη ημερομηνία που ορίζεται σε αυτήν. Δεν θίγει το κύρος των κατ' εξουσιοδότηση πράξεων που ισχύουν ήδη.

4. Προτού εκδώσει κατ' εξουσιοδότηση πράξη, η Επιτροπή διεξάγει διαβουλεύσεις με εμπειρογνώμονες που ορίζουν τα κράτη μέλη σύμφωνα με τις αρχές της διοργανικής συμφωνίας της 13ης Απριλίου 2016 για τη βελτίωση του νομοθετικού έργου.

5. Μόλις εκδώσει κατ' εξουσιοδότηση πράξη, η Επιτροπή την κοινοποιεί ταυτόχρονα στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο.

6. Η κατ' εξουσιοδότηση πράξη που εκδίδεται δυνάμει του άρθρου 5 παράγραφος 1 τίθεται σε ισχύ μόνο αν δεν διατυπωθεί αντίρρηση από το Ευρωπαϊκό Κοινοβούλιο ή το Συμβούλιο εντός δύο μηνών από την ημέρα κοινοποίησης της πράξης στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο ή αν, πριν λήξει αυτή η προθεσμία, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο ενημερώσουν αμφότερα την Επιτροπή ότι δεν θα προβάλουν αντιρρήσεις. Η προθεσμία αυτή παρατείνεται κατά δύο μήνες κατόπιν πρωτοβουλίας του Ευρωπαϊκού Κοινοβουλίου ή του Συμβουλίου.

Άρθρο 24

Διαδικασία επιτροπής

1. Η Επιτροπή επικουρείται από επιτροπή. Πρόκειται για επιτροπή κατά την έννοια του κανονισμού (ΕΕ) αριθ. 182/2011.

2. Όταν γίνεται παραπομπή στην παρούσα παράγραφο, εφαρμόζεται το άρθρο 5 του κανονισμού (ΕΕ) αριθ. 182/2011.

ΚΕΦΆΛΑΙΟ VIII

ΤΕΛΙΚΈΣ ΔΙΑΤΆΞΕΙΣ

Άρθρο 25

Υποβολή εκθέσεων και επανεξέταση

Έως τις 17 Ιουλίου 2027, η Επιτροπή υποβάλλει προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο έκθεση στην οποία αξιολογεί τον βαθμό στον οποίο κάθε κράτος μέλος έχει λάβει τα αναγκαία μέτρα προκειμένου να συμμορφωθεί με την παρούσα οδηγία.

Η Επιτροπή προβαίνει σε περιοδική επανεξέταση της λειτουργίας της παρούσας οδηγίας και υποβάλλει έκθεση στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο. Στην εν λόγω έκθεση αξιολογούνται, ιδίως, η προστιθέμενη αξία της παρούσας οδηγίας, ο αντίκτυπός της όσον αφορά τη διασφάλιση της ανθεκτικότητας των κρίσιμων οντοτήτων και το κατά πόσον το παράρτημα της παρούσας οδηγίας θα πρέπει να τροποποιηθεί. Η Επιτροπή υποβάλλει την πρώτη αυτή έκθεση έως τις 17 Ιουνίου 2029. Για τον σκοπό υποβολής εκθέσεων σύμφωνα με το παρόν άρθρο, η Επιτροπή λαμβάνει υπόψη σχετικά έγγραφα της ομάδας για την ανθεκτικότητα των κρίσιμων οντοτήτων.

Άρθρο 26

Μεταφορά στο εθνικό δίκαιο

1. Έως τις 17 Οκτωβρίου 2024, τα κράτη μέλη θεσπίζουν και δημοσιεύουν τα αναγκαία μέτρα για να συμμορφωθούν με την παρούσα οδηγία. Ενημερώνουν αμέσως την Επιτροπή σχετικά.

Εφαρμόζουν τα εν λόγω μέτρα από τις 18 Οκτωβρίου 2024.

2. Όταν τα κράτη μέλη θεσπίζουν τα μέτρα που αναφέρονται στην παράγραφο 1, περιέχουν παραπομπή στην παρούσα οδηγία ή συνοδεύονται από την παραπομπή αυτή κατά την επίσημη δημοσίευσή τους. Οι μέθοδοι της παραπομπής αυτής καθορίζονται από τα κράτη μέλη.

Άρθρο 27

Κατάργηση της οδηγίας 2008/114/ΕΚ

Η οδηγία 2008/114/ΕΚ καταργείται από τις 18 Οκτωβρίου 2024.

Οι παραπομπές στην καταργούμενη οδηγία νοούνται ως παραπομπές στην παρούσα οδηγία.

Άρθρο 28

Έναρξη ισχύος

Η παρούσα οδηγία αρχίζει να ισχύει την εικοστή ημέρα από τη δημοσίευσή της στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

Άρθρο 29

Αποδέκτες

Η παρούσα οδηγία απευθύνεται στα κράτη μέλη.

Στρασβούργο, 14 Δεκεμβρίου 2022.

Για το Ευρωπαϊκό Κοινοβούλιο	*Για το Συμβούλιο*
Η Πρόεδρος	*Ο Πρόεδρος*
R. METSOLA	M. BEK

ΠΑΡΑΡΤΗΜΑ

Τομείς, υποτομείς και κατηγορίες οντοτήτων

Τομείς	Υποτομείς	Κατηγορίες οντοτήτων
1. Ενέργεια	α) Ηλεκτρική ενέργεια	— Επιχειρήσεις ηλεκτρικής ενέργειας όπως καθορίζονται στο άρθρο 2 σημείο 57) της οδηγίας (ΕΕ) 2019/944 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([1]), οι οποίες ασκούν τη δραστηριότητα «προμήθειας» όπως καθορίζεται στο άρθρο 2 σημείο 12) της εν λόγω οδηγίας
		— Διαχειριστές συστήματος διανομής όπως καθορίζονται στο άρθρο 2 σημείο 29) της οδηγίας (ΕΕ) 2019/944
		— Διαχειριστές συστήματος μεταφοράς όπως καθορίζονται στο άρθρο 2 σημείο 35) της οδηγίας (ΕΕ) 2019/944
		— Παραγωγοί όπως καθορίζονται στο άρθρο 2 σημείο 38) της οδηγίας (ΕΕ) 2019/944
		— Ορισθέντες διαχειριστές αγοράς ηλεκτρικής ενέργειας όπως καθορίζονται στο άρθρο 2 σημείο 8) του κανονισμού (ΕΕ) 2019/943 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([2])
		— Συμμετέχοντες στην αγορά όπως καθορίζονται στο άρθρο 2 σημείο 25) του κανονισμού (ΕΕ) 2019/943, οι οποίοι παρέχουν υπηρεσίες σωρευτικής εκπροσώπησης, απόκρισης ζήτησης ή αποθήκευσης ενέργειας όπως καθορίζονται στο άρθρο 2 σημεία 18, 20 και 59 της οδηγίας (ΕΕ) 2019/944
	β) Τηλεθέρμανση και τηλεψύξη	— Διαχειριστές τηλεθέρμανσης ή τηλεψύξης όπως καθορίζονται στο άρθρο 2 σημείο 19) της οδηγίας (ΕΕ) 2018/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([3])
	γ) Πετρέλαιο	— Διαχειριστές αγωγών μεταφοράς πετρελαίου
		— Διαχειριστές παραγωγής πετρελαίου, εγκαταστάσεων διύλισης και επεξεργασίας, αποθήκευσης και μεταφοράς πετρελαίου
		— Κεντρικοί φορείς διατήρησης αποθεμάτων όπως καθορίζονται στο άρθρο 2 στοιχείο στ) της οδηγίας 2009/119/ΕΚ του Συμβουλίου ([4])

Τομείς	Υποτομείς	Κατηγορίες οντοτήτων
	δ) Αέριο	— Επιχειρήσεις προμήθειας όπως καθορίζονται στο άρθρο 2 σημείο 8) της οδηγίας 2009/73/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([5])
		— Διαχειριστές συστήματος διανομής όπως καθορίζονται στο άρθρο 2 σημείο 6) της οδηγίας 2009/73/ΕΚ
		— Διαχειριστές συστήματος μεταφοράς όπως καθορίζονται στο άρθρο 2 σημείο 4) της οδηγίας 2009/73/ΕΚ
		— Διαχειριστές συστήματος αποθήκευσης όπως καθορίζονται στο άρθρο 2 σημείο 10) της οδηγίας 2009/73/ΕΚ
		— Διαχειριστές συστήματος ΥΦΑ όπως καθορίζονται στο άρθρο 2 σημείο 12) της οδηγίας 2009/73/ΕΚ
		— Επιχειρήσεις φυσικού αερίου όπως καθορίζονται στο άρθρο 2 σημείο 1) της οδηγίας 2009/73/ΕΚ
		— Διαχειριστές εγκαταστάσεων διύλισης και επεξεργασίας φυσικού αερίου
	ε) Υδρογόνο	— Διαχειριστές παραγωγής, αποθήκευσης και μεταφοράς υδρογόνου
2. Μεταφορές	α) Αεροπορικές	— Αερομεταφορείς όπως καθορίζονται στο άρθρο 3 σημείο 4) του κανονισμού (ΕΚ) αριθ. 300/2008, οι οποίοι χρησιμοποιούνται για εμπορικούς σκοπούς
		— Φορείς διαχείρισης αερολιμένα όπως καθορίζονται στο άρθρο 2 σημείο 2) της οδηγίας 2009/12/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([6]), αερολιμένες όπως καθορίζονται στο άρθρο 2 σημείο 1) της ίδιας οδηγίας, συμπεριλαμβανομένων των κεντρικών αερολιμένων που απαριθμούνται στο παράρτημα ΙΙ τμήμα 2 του κανονισμού (ΕΕ) αριθ. 1315/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([7]), και φορείς εκμετάλλευσης βοηθητικών εγκαταστάσεων που βρίσκονται εντός των αερολιμένων
		— Φορείς εκμετάλλευσης ελέγχου διαχείρισης κυκλοφορίας που παρέχουν υπηρεσίες ελέγχου εναέριας κυκλοφορίας όπως καθορίζονται στο άρθρο 2 σημείο 1) του κανονισμού (ΕΚ) αριθ. 549/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([8])

Τομείς	Υποτομείς	Κατηγορίες οντοτήτων
	β) Σιδηροδρομικές	— Διαχειριστές υποδομής όπως καθορίζονται στο άρθρο 3 σημείο 2) της οδηγίας 2012/34/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([9])
		— Σιδηροδρομικές επιχειρήσεις όπως καθορίζονται στο άρθρο 3 σημείο 1) της οδηγίας 2012/34/ΕΕ και φορείς εκμετάλλευσης εγκαταστάσεων για την παροχή υπηρεσιών όπως καθορίζονται στο άρθρο 3 σημείο 12) της εν λόγω οδηγίας
	γ) Πλωτές	— Εταιρείες εσωτερικής πλωτής, θαλάσσιας και ακτοπλοϊκής μεταφοράς επιβατών και εμπορευμάτων όπως καθορίζονται για τις θαλάσσιες μεταφορές στο παράρτημα I του κανονισμού (ΕΚ) αριθ. 725/2004, μη συμπεριλαμβανομένων των μεμονωμένων πλοίων που χρησιμοποιούνται από τις εταιρείες αυτές
		— Διαχειριστικοί φορείς των λιμένων όπως καθορίζονται στο άρθρο 3 σημείο 1) της οδηγίας 2005/65/ΕΚ, συμπεριλαμβανομένων των λιμενικών τους εγκαταστάσεων όπως καθορίζονται στο άρθρο 2 σημείο 11) του κανονισμού (ΕΚ) αριθ. 725/2004, και φορείς εκμετάλλευσης έργων και εξοπλισμού που βρίσκονται εντός των λιμένων
		— Φορείς εκμετάλλευσης υπηρεσιών εξυπηρέτησης κυκλοφορίας πλοίων (VTS) όπως καθορίζονται στο άρθρο 3 στοιχείο ιε) της οδηγίας 2002/59/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([10])
	δ) Οδικές	— Οδικές αρχές όπως καθορίζονται στο άρθρο 2 σημείο 12) του κατ' εξουσιοδότηση κανονισμού (ΕΕ) 2015/962 της Επιτροπής ([11]) που είναι υπεύθυνες για τον έλεγχο διαχείρισης της κυκλοφορίας, με εξαίρεση τους δημόσιους φορείς για τους οποίους η διαχείριση της κυκλοφορίας ή η λειτουργία συστημάτων ευφυών μεταφορών αποτελεί επουσιώδες μέρος της γενικής τους δραστηριότητας
		— Διαχειριστές Συστημάτων Ευφυών Μεταφορών όπως καθορίζονται στο άρθρο 4 σημείο 1) της οδηγίας 2010/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([12])
	ε) Δημόσιες μεταφορές	— Φορείς δημόσιας υπηρεσίας μεταφορών όπως καθορίζονται στο άρθρο 2 στοιχείο δ) του κανονισμού (ΕΚ) αριθ. 1370/2007 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([13])
3. Τραπεζικός κλάδος		— Πιστωτικά ιδρύματα όπως καθορίζονται στο άρθρο 4 σημείο 1) του κανονισμού (ΕΕ) αριθ. 575/2013
4. Υποδομές χρηματοπιστωτικών αγορών		— Διαχειριστές τόπων διαπραγμάτευσης όπως καθορίζονται στο άρθρο 4 σημείο 24) της οδηγίας 2014/65/ΕΕ
		— Κεντρικοί αντισυμβαλλόμενοι (CCP) όπως καθορίζονται στο άρθρο 2 σημείο 1) του κανονισμού (ΕΕ) αριθ. 648/2012

Τομείς	Υποτομείς	Κατηγορίες οντοτήτων
5. Υγεία		— Πάροχοι υγειονομικής περίθαλψης όπως καθορίζονται στο άρθρο 3 στοιχείο ζ) της οδηγίας 2011/24/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([14])
		— Εργαστήρια αναφοράς της ΕΕ που αναφέρονται στο άρθρο 15 του κανονισμού (ΕΕ) 2022/2371 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([15])
		— Οντότητες που διεξάγουν δραστηριότητες έρευνας και ανάπτυξης φαρμάκων όπως καθορίζονται στο άρθρο 1 σημείο 2) της οδηγίας 2001/83/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([16])
		— Οντότητες που κατασκευάζουν βασικά φαρμακευτικά προϊόντα και φαρμακευτικά παρασκευάσματα που αναφέρονται στον κλάδο 21 τομέας Γ της NACE αναθ. 2
		— Οντότητες που κατασκευάζουν ιατροτεχνολογικά προϊόντα τα οποία θεωρούνται κρίσιμης σημασίας κατά τη διάρκεια κατάστασης έκτακτης ανάγκης στον τομέα της δημόσιας υγείας («κατάλογος προϊόντων κρίσιμης σημασίας κατά τη διάρκεια κατάστασης έκτακτης ανάγκης για τη δημόσια υγεία») κατά την έννοια του άρθρου 22 του κανονισμού (ΕΕ) 2022/123 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([17])
		— Οντότητες που κατέχουν άδεια χονδρικής πώλησης όπως αναφέρεται στο άρθρο 79 της οδηγίας 2001/83/ΕΚ
6. Πόσιμο νερό		— Προμηθευτές και διανομείς νερού ανθρώπινης κατανάλωσης όπως καθορίζονται στο άρθρο 2 σημείο 1) στοιχείο α) της οδηγίας (ΕΕ) 2020/2184 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([18]), εξαιρουμένων των διανομέων για τους οποίους η διανομή νερού ανθρώπινης κατανάλωσης αποτελεί επουσιώδες μέρος της γενικής τους δραστηριότητας διανομής λοιπών προϊόντων και αγαθών
7. Λύματα		— Επιχειρήσεις συλλογής, διάθεσης ή επεξεργασίας αστικών λυμάτων, οικιακών λυμάτων ή βιομηχανικών λυμάτων όπως καθορίζονται στο άρθρο 2 σημεία 1), 2) και 3) της οδηγίας 91/271/ΕΟΚ του Συμβουλίου ([19]), εξαιρουμένων επιχειρήσεων για τις οποίες η συλλογή, η διάθεση ή η επεξεργασία αστικών λυμάτων, οικιακών λυμάτων ή βιομηχανικών λυμάτων αποτελεί επουσιώδες μέρος της γενικής τους δραστηριότητας

Τομείς	Υποτομείς	Κατηγορίες οντοτήτων
8. Ψηφιακές υποδομές		— Πάροχοι σημείου ανταλλαγής κίνησης διαδικτύου όπως καθορίζονται στο άρθρο 6 σημείο 18) της οδηγίας (ΕΕ) 2022/2555
		— Πάροχοι υπηρεσιών συστήματος ονομάτων τομέα όπως καθορίζονται στο άρθρο 6 σημείο 20) της οδηγίας (ΕΕ) 2022/2555, εξαιρουμένων των διαχειριστών των εξυπηρετητών ονομάτων ρίζας
		— Μητρώα ονομάτων τομέα ανώτατου επιπέδου όπως καθορίζονται στο άρθρο 6 σημείο 21) της οδηγίας (ΕΕ) 2022/2555
		— Πάροχοι υπηρεσίας νεφοϋπολογιστικής όπως καθορίζονται στο άρθρο 6 σημείο 30) της οδηγίας (ΕΕ) 2022/2555
		— Πάροχοι υπηρεσίας κέντρου δεδομένων όπως καθορίζονται στο άρθρο 6 σημείο 31) της οδηγίας (ΕΕ) 2022/2555
		— Πάροχοι δικτύου διανομής περιεχομένου όπως καθορίζονται στο άρθρο 6 σημείο 32) της οδηγίας (ΕΕ) 2022/2555
		— Πάροχοι υπηρεσιών εμπιστοσύνης όπως καθορίζονται στο άρθρο 3 σημείο 19) του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([20])
		— Πάροχοι δημόσιου δικτύου ηλεκτρονικών επικοινωνιών όπως καθορίζονται στο άρθρο 2 σημείο 8) της οδηγίας (ΕΕ) 2018/1972 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([21])
		— Πάροχοι υπηρεσιών ηλεκτρονικών επικοινωνιών όπως καθορίζονται στο άρθρο 2 σημείο 4) της οδηγίας (ΕΕ) 2018/1972, εφόσον οι υπηρεσίες τους είναι δημόσια διαθέσιμες
9. Δημόσια διοίκηση		— Φορείς δημόσιας διοίκησης εθνικών κυβερνήσεων όπως καθορίζονται από τα κράτη μέλη σύμφωνα με το εθνικό δίκαιο
10. Διάστημα		— Διαχειριστές επίγειων υποδομών των οποίων η κυριότητα, η διαχείριση και η λειτουργία ανήκει σε κράτη μέλη ή ιδιώτες και οι οποίες υποστηρίζουν την παροχή διαστημικών υπηρεσιών, με εξαίρεση τους παρόχους δημόσιων δικτύων ηλεκτρονικών επικοινωνιών όπως καθορίζονται στο άρθρο 2 σημείο 8) της οδηγίας (ΕΕ) 2018/1972

Τομείς	Υποτομείς	Κατηγορίες οντοτήτων
11. Παραγωγή, μεταποίηση και διανομή τροφίμων		— Επιχειρήσεις τροφίμων όπως καθορίζονται στο άρθρο 3 σημείο 2) του κανονισμού (ΕΚ) αριθ. 178/2002 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([22]), οι οποίες ασχολούνται αποκλειστικά με την εφοδιαστική, τη χονδρική πώληση και τη βιομηχανική παραγωγή και μεταποίηση μεγάλης κλίμακας

([1]) Οδηγία (ΕΕ) 2019/944 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 5ης Ιουνίου 2019, σχετικά με τους κοινούς κανόνες για την εσωτερική αγορά ηλεκτρικής ενέργειας και την τροποποίηση της οδηγίας 2012/27/ΕΕ (ΕΕ L 158 της 14.6.2019, σ. 125).

([2]) Κανονισμός (ΕΕ) 2019/943 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 5ης Ιουνίου 2019, σχετικά με την εσωτερική αγορά ηλεκτρικής ενέργειας (ΕΕ L 158 της 14.6.2019, σ. 54).

([3]) Οδηγία (ΕΕ) 2018/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Δεκεμβρίου 2018, για την προώθηση της χρήσης ενέργειας από ανανεώσιμες πηγές (ΕΕ L 328 της 21.12.2018, σ. 82).

([4]) Οδηγία 2009/119/ΕΚ του Συμβουλίου, της 14ης Σεπτεμβρίου 2009, σχετικά με υποχρέωση διατήρησης ενός ελάχιστου επιπέδου αποθεμάτων αργού πετρελαίου ή/και προϊόντων πετρελαίου από τα κράτη μέλη (ΕΕ L 265 της 9.10.2009, σ. 9).

([5]) Οδηγία 2009/73/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Ιουλίου 2009, σχετικά με τους κοινούς κανόνες για την εσωτερική αγορά φυσικού αερίου και την κατάργηση της οδηγίας 2003/55/ΕΚ (ΕΕ L 211 της 14.8.2009, σ. 94).

([6]) Οδηγία 2009/12/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαρτίου 2009, για τα αερολιμενικά τέλη (ΕΕ L 70 της 14.3.2009, σ. 11).

([7]) Κανονισμός (ΕΕ) αριθ. 1315/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Δεκεμβρίου 2013, περί των προσανατολισμών της Ένωσης για την ανάπτυξη του διευρωπαϊκού δικτύου μεταφορών και για την κατάργηση της απόφασης αριθ. 661/2010/ΕΕ (ΕΕ L 348 της 20.12.2013, σ. 1).

([8]) Κανονισμός (ΕΚ) αριθ. 549/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 10ης Μαρτίου 2004, για τη χάραξη του πλαισίου για τη δημιουργία του Ενιαίου Ευρωπαϊκού Ουρανού («κανονισμός-πλαίσιο») (ΕΕ L 96 της 31.3.2004, σ. 1).

([9]) Οδηγία 2012/34/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 21ης Νοεμβρίου 2012, για τη δημιουργία ενιαίου ευρωπαϊκού σιδηροδρομικού χώρου (ΕΕ L 343 της 14.12.2012, σ. 32).

([10]) Οδηγία 2002/59/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Ιουνίου 2002, για τη δημιουργία κοινοτικού συστήματος παρακολούθησης της κυκλοφορίας των πλοίων και ενημέρωσης και την κατάργηση της οδηγίας 93/75/ΕΟΚ του Συμβουλίου (ΕΕ L 208 της 5.8.2002, σ. 10).

([11]) Κατ' εξουσιοδότηση κανονισμός (ΕΕ) 2015/962 της Επιτροπής, της 18ης Δεκεμβρίου 2014, για τη συμπλήρωση της οδηγίας 2010/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά την παροχή σε επίπεδο Ένωσης υπηρεσιών πληροφόρησης για την κυκλοφορία σε πραγματικό χρόνο (ΕΕ L 157 της 23.6.2015, σ. 21).

([12]) Οδηγία 2010/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Ιουλίου 2010, περί πλαισίου ανάπτυξης των Συστημάτων Ευφυών Μεταφορών στον τομέα των οδικών μεταφορών και των διεπαφών με άλλους τρόπους μεταφοράς (ΕΕ L 207 της 6.8.2010, σ. 1).

([13]) Κανονισμός (ΕΚ) αριθ. 1370/2007 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2007, για τις δημόσιες επιβατικές σιδηροδρομικές και οδικές μεταφορές και την κατάργηση των κανονισμών του Συμβουλίου (ΕΟΚ) αριθ. 1191/69 και (ΕΟΚ) αριθ. 1107/70 (ΕΕ L 315 της 3.12.2007, σ. 1).

([14]) Οδηγία 2011/24/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Μαρτίου 2011, περί εφαρμογής των δικαιωμάτων των ασθενών στο πλαίσιο της διασυνοριακής υγειονομικής περίθαλψης (ΕΕ L 88 της 4.4.2011, σ. 45).

([15]) Κανονισμός (ΕΕ) 2022/2371 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Νοεμβρίου 2022, σχετικά με σοβαρές διασυνοριακές απειλές κατά της υγείας και την κατάργηση της απόφασης αριθ. 1082/2013/ΕΕ (ΕΕ L 314 της 6.12.2022, σ. 26).

([16]) Οδηγία 2001/83/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Νοεμβρίου 2001, περί κοινοτικού κώδικος για τα φάρμακα που προορίζονται για ανθρώπινη χρήση (ΕΕ L 311 της 28.11.2001, σ. 67).

([17]) Κανονισμός (ΕΕ) 2022/123 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Ιανουαρίου 2022, σχετικά με την ενίσχυση του ρόλου του Ευρωπαϊκού Οργανισμού Φαρμάκων όσον αφορά την ετοιμότητα έναντι κρίσεων και τη διαχείριση κρίσεων για τα φάρμακα και τα ιατροτεχνολογικά προϊόντα (ΕΕ L 20 της 31.1.2022, σ. 1).

([18]) Οδηγία (ΕΕ) 2020/2184 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 16ης Δεκεμβρίου 2020, σχετικά με την ποιότητα του νερού ανθρώπινης κατανάλωσης (ΕΕ L 435 της 23.12.2020, σ. 1).

([19]) Οδηγία 91/271/ΕΟΚ του Συμβουλίου, της 21ης Μαΐου 1991, για την επεξεργασία των αστικών λυμάτων (ΕΕ L 135 της 30.5.1991, σ. 40).

([20]) Κανονισμός (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Ιουλίου 2014, σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ (ΕΕ L 257 της 28.8.2014, σ. 73).

([21]) Οδηγία (ΕΕ) 2018/1972 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Δεκεμβρίου 2018, για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών (ΕΕ L 321 της 17.12.2018, σ. 36).

([22]) Κανονισμός (ΕΚ) αριθ. 178/2002 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 28ης Ιανουαρίου 2002, για τον καθορισμό των γενικών αρχών και απαιτήσεων της νομοθεσίας για τα τρόφιμα, για την ίδρυση της Ευρωπαϊκής Αρχής για την Ασφάλεια των Τροφίμων και τον καθορισμό διαδικασιών σε θέματα ασφαλείας των τροφίμων (ΕΕ L 31 της 1.2.2002, σ. 1).

ISSN 1977-0669 (ηλεκτρονική έκδοση)
ISSN 1725-2547 (έντυπη έκδοση)

Υπηρεσία Εκδόσεων
της Ευρωπαϊκής Ένωσης
L-2985 Λουξεμβούργο
ΛΟΥΞΕΜΒΟΥΡΓΟ

EL