AFGØRELSER

KOMMISSIONENS AFGØRELSE (EU, Euratom) 2017/46

af 10. januar 2017

om kommunikations- og informationssystemernes sikkerhed i Europa-Kommissionen

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 249,

under henvisning til traktaten om oprettelse af Det Europæiske Atomenergifællesskab,

ud fra følgende betragtninger:

(1) Kommissionens kommunikations- og informationssystemer (CIS'er) er en integreret del af Kommissionens funktionsmåde, og IT-sikkerhedshændelser kan have en alvorlig indvirkning på Kommissionens transaktioner samt på tredjemand, herunder enkeltpersoner, virksomheder og medlemsstater.

(2) Der er mange trusler, der kan skade fortroligheden, integriteten eller tilgængeligheden af Kommissionens kommunikations- og informationssystemer og de oplysninger, der behandles deri. Disse trusler omfatter ulykker, fejl, bevidste angreb og naturlige begivenheder og skal anerkendes som operationelle risici.

(3) Kommunikations- og informationssystemer skal leveres med et beskyttelsesniveau, der står mål med sandsynligheden for og indvirkningen og arten af de risici, som de udsættes for.

(4) Kommissionens IT-sikkerhed bør sikre, at Kommissionens CIS'er beskytter de oplysninger, de behandler, og at de fungerer, som de skal, når de skal, når de benyttes af legitime brugere.

(5) Kommissionens IT-sikkerhedspolitik bør gennemføres således, at den stemmer overens med Kommissionens politikker om sikkerhed.

(6) Sikkerhedsdirektoratet under Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed har det overordnede ansvar for sikkerheden i Kommissionen under det medlem af Kommissionen, som er ansvarlig for sikkerhed.

(7) Kommissionens tilgang bør være at tage hensyn til EU's politiske initiativer og lovgivning om net- og informationssikkerhed, branchestandarder og god praksis, overholde al relevant lovgivning og tillade interoperabilitet og kompatibilitet.

(8) Kommissionens tjenestegrene med ansvar for kommunikations- og informationssystemer bør træffe og gennemføre passende foranstaltninger, og i hele Kommissionen bør der træffes IT-sikkerhedsforanstaltninger til beskyttelse af kommunikations- og informationssystemer for at sikre effektivitet.

(9) Regler og procedurer for adgang til oplysninger i forbindelse med IT-sikkerhed, herunder håndtering af IT-sikkerhedshændelser, bør stå i forhold til den trussel, som Kommissionen eller dens personale er udsat for, og stemme overens med principperne i Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 ([1]) om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i unionsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger og under hensyntagen til princippet om tavshedspligt som fastlagt i artikel 339 i traktaten om Den Europæiske Unions funktionsmåde (TEUF).

([1]) Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger (EFT L 8 af 12.1.2001, s. 1).

(10) Politikker og regler for kommunikations- og informationssystemer, der behandler EU's klassificerede informationer (EUCI), følsomme, ikke-klassificerede informationer og uklassificerede informationer skal stemme fuldt ud overens med Kommissionens afgørelse (EU, Euratom) 2015/443 ([1]) og (EU, Euratom) 2015/444 ([2]).

(11) Kommissionen skal gennemgå og ajourføre bestemmelserne om sikkerheden af de kommunikations- og informationssystemer, som Kommissionen anvender.

(12) Kommissionens afgørelse C(2006) 3602 bør derfor ophæves —

VEDTAGET DENNE AFGØRELSE:

KAPITEL 1

ALMINDELIGE BESTEMMELSER

Artikel 1

Genstand og anvendelsesområde

1. Denne afgørelse gælder alle kommunikations- og informationssystemer (CIS'er), som ejes, indkøbes, styres eller anvendes af eller på vegne af Kommissionen og al Kommissionens brug af disse CIS'er.

2. I denne afgørelse fastlægges grundlæggende principper, mål, organisering og ansvar vedrørende sikkerheden af disse CIS'er og navnlig for de af Kommissionens tjenestegrene, der ejer, indkøber, styrer eller anvender CIS'er, herunder CIS'er, der leveres af en intern IT-leverandør. Når et CIS leveres, ejes, styres eller anvendes af en ekstern part på grundlag af en bilateral aftale eller kontrakt med Kommissionen, skal aftale- eller kontraktvilkårene stemme overens med denne afgørelse.

3. Denne afgørelse gælder alle Kommissionens tjenestegrene og forvaltningsorganer. Når et af Kommissionens CIS'er anvendes af andre organer og institutioner på grundlag af en bilateral aftale med Kommissionen, skal aftalevilkårene stemme overens med denne afgørelse.

4. Uanset eventuelle konkrete angivelser vedrørende særlige grupper af medarbejdere finder denne afgørelse anvendelse på medlemmerne af Kommissionen, på de af Kommissionens medarbejdere, der hører under anvendelsesområdet for vedtægten for tjenestemænd i Den Europæiske Union (»personalevedtægten«) og ansættelsesvilkårene for de øvrige ansatte i Den Europæiske Union (»AØAF«) ([3]), på udstationerede nationale eksperter i Kommissionen ([4]), på eksterne leverandører og deres personale, på praktikanter og på enkeltpersoner med adgang til CIS'er inden for denne afgørelses anvendelsesområde.

5. Denne afgørelse finder anvendelse på Det Europæiske Kontor for Bekæmpelse af Svig (OLAF), i det omfang dette er foreneligt med EU-lovgivningen og Kommissionens afgørelse 1999/352/EF, EKSF, Euratom ([5]). Navnlig finder foranstaltningerne i denne afgørelse, herunder anvisninger, inspektioner, forespørgsler og tilsvarende foranstaltninger, muligvis ikke anvendelse på kontorets CIS'er, hvor dette ikke er foreneligt med kontorets uafhængige undersøgelsesfunktion og/eller fortroligheden af de oplysninger, som kontoret indhenter i forbindelse med udøvelsen af denne funktion.

Artikel 2

Definitioner

I denne afgørelse forstås ved:

1) »ansvarlig«: at være ansvarlig for handlinger, beslutninger og resultater

([1]) Kommissionens afgørelse (EU, Euratom) 2015/443 af 13. marts 2015 om sikkerhedsbeskyttelse i Kommissionen (EUT L 72 af 17.3.2015, s. 41).
([2]) Kommissionens afgørelse (EU, Euratom) 2015/444 af 13. marts 2015 om reglerne for sikkerhedsbeskyttelse af EU's klassificerede informationer (EUT L 72 af 17.3.2015, s. 53).
([3]) Fastlagt ved Rådets forordning (EØF, Euratom, EKSF) nr. 259/68 af 29. februar 1968 om vedtægten for tjenestemænd i De europæiske Fællesskaber og om ansættelsesvilkårene for de øvrige ansatte i disse Fællesskaber samt om særlige midlertidige foranstaltninger for tjenestemænd i Kommissionen (Vedtægten for tjenestemænd) (EFT L 56 af 4.3.1968, s. 1).
([4]) Kommissionens afgørelse af 12. november 2008 om ordningen for udstationering af nationale eksperter og for nationale eksperter under uddannelse i Kommissionen (C(2008) 6866 final).
([5]) Kommissionens afgørelse 1999/352/EF, EKSF, Euratom af 28. april 1999 om oprettelse af Det Europæiske Kontor for Bekæmpelse af Svig (OLAF) (EUT L 136 af 31.5.1999, s. 20).

2) »CERT-EU«: IT-beredskabsenheden for EU's institutioner og agenturer. Dens opgave er at støtte de europæiske institutioner, så de kan beskytte sig selv mod forsætlige og ondsindede angreb, der kan hæmme integriteten af deres IT-aktiver og skade EU's interesser. CERT-EU's aktiviteter omfatter forebyggelse, opdagelse, beredskab og genoprettelse

3) »Kommissionens tjenestegrene«: alle Kommissionens generaldirektorater eller tjenestegrene eller et medlem af Kommissionens kabinet

4) »Kommissionens sikkerhedsmyndighed«: den rolle, som er fastlagt i afgørelse (EU, Euratom) 2015/444

5) »kommunikations- og informationssystem« eller »CIS«: et system, der muliggør håndtering af informationer i elektronisk form, herunder alle aktiver, der kræves til dets drift, og den nødvendige infrastruktur, organisation, personale og informationskilder Denne definition omfatter også virksomhedsapplikationer, delte IT-tjenester, udliciterede systemer og slutbrugerenheder

6) »administrationsråd«: det højeste niveau af ledelsestilsyn vedrørende operationelle og administrative spørgsmål i Kommissionen

7) »dataejer«: den person, som er ansvarlig for at sikre beskyttelse og anvendelse af et specifikt datasæt, der håndteres af et CIS

8) »datasæt«: et sæt oplysninger, der fungerer som en konkret virksomhedsproces eller -aktivitet i Kommissionen

9) »hasteprocedure«: et foruddefineret sæt af metoder og ansvar, som anvendes til at reagere på akutte situationer for at forhindre en større indvirkning på Kommissionen

10) »informationssikkerhedspolitik«: et sæt informationssikkerhedsmål, som er etableret, gennemført og kontrolleret eller skal etableres, gennemføres og kontrolleres. Dette omfatter, men er ikke begrænset til, afgørelse (EU, Euratom) 2015/444 og (EU, Euratom) 2015/443

11) »styrelsesråd for informationssikkerhed«: det ledelsesorgan, der støtter administrationsrådet i dets IT-sikkerhedsrelaterede opgaver

12) »intern leverandør af IT-tjenester«: en af Kommissionens tjenestegrene, der leverer fælles IT-tjenester

13) »IT-sikkerhed« eller »sikkerhed af CIS«: bevarelse af fortrolighed, integritet og tilgængelighed af CIS'er og de datasæt, de behandler

14) »retningslinjer for IT-sikkerhed«: anbefalede, men frivillige foranstaltninger, der hjælper med at støtte IT-sikkerhedsstandarder eller fungerer som reference, når der ikke er fastsat gældende standarder

15) »IT-sikkerhedshændelse«: en hændelse, der kan påvirke fortroligheden, integriteten eller tilgængeligheden af et CIS negativt

16) »IT-sikkerhedsforanstaltning«: en teknisk eller organisatorisk foranstaltning til afbødning af IT-sikkerhedsrisici

17) »IT-sikkerhedsbehov«: en præcis og entydig definition af niveauet af fortrolighed, integritet og tilgængelighed i forbindelse med en oplysning eller et IT-system med henblik på at fastslå det påkrævede beskyttelsesniveau

18) »IT-sikkerhedsmål«: en hensigtserklæring til imødegåelse af konkrete trusler og eller til opfyldelse af konkrete organisatoriske sikkerhedskrav eller -forudsætninger

19) »IT-sikkerhedsplan«: dokumentationen for de IT-sikkerhedsforanstaltninger, som er påkrævet for at opfylde IT-sikkerhedsbehovene i et CIS

20) »IT-sikkerhedspolitik«: et sæt IT-sikkerhedsmål, som er etableret, gennemført og kontrolleret, eller som skal etableres, gennemføres og kontrolleres. Det omfatter denne afgørelse og dens gennemførelsesbestemmelser

21) »IT-sikkerhedskrav«: et formaliseret IT-sikkerhedsbehov i en foruddefineret proces

22) »IT-sikkerhedsrisiko«: en virkning, som en IT-sikkerhedstrussel kan påføre et CIS ved at udnytte en sårbarhed. En IT-sikkerhedsrisiko er således kendetegnet af to faktorer: 1) usikkerhed, dvs. sandsynligheden for, at en IT-sikkerhedstrussel forårsager en uønsket hændelse, og 2) indvirkning, dvs. de konsekvenser, som en sådan uønsket hændelse kan have på et CIS

23) »IT-sikkerhedsstandarder«: konkrete obligatoriske IT-sikkerhedsforanstaltninger, der hjælper med at håndhæve og støtte IT-sikkerhedspolitikken

24) »IT-sikkerhedsstrategi«: et sæt projekter og aktiviteter, som har til formål at nå Kommissionens mål, og som skal etableres, gennemføres og kontrolleres

25) »IT-sikkerhedstrussel«: en faktor, der potentielt kan føre til en uønsket begivenhed, som kan medføre skade på et CIS. Sådanne trusler kan være uagtsomme eller forsætlige og karakteriseres ved trusselselementer, potentielle mål og angrebsmetoder

26) »lokal IT-sikkerhedsansvarlig« eller »LISO«: den person, som er ansvarlig for IT-sikkerheden i en af Kommissionens tjenestegrene

27) »personoplysninger«, »behandling af personoplysninger«, »den registeransvarlige« og »register med personoplysninger«: samme betydning som i forordning (EF) nr. 45/2001 og navnlig artikel 2

28) »behandling af oplysninger«: alle funktioner i et CIS med hensyn til datasæt, herunder oprettelse, ændring, visning, lagring, transmission, sletning og arkivering af oplysninger. Behandling af oplysninger kan ske i et CIS som et sæt af funktioner til brugerne og som IT-tjenester til andre CIS'er

29) »tavshedspligt«: beskyttelse af virksomhedsoplysninger af den slags, som er omfattet af tavshedspligt, navnlig oplysninger om virksomheder og om deres forretningsforbindelser eller omkostningsforhold som fastlagt i artikel 339 i TEUF

30) »ansvarlig«: være forpligtet til at handle og træffe beslutninger for at opnå det ønskede resultat

31) »sikkerhedsbeskyttelse i Kommissionen«: sikkerhedsbeskyttelse af personer, aktiver og information i Kommissionen og navnlig fysisk beskyttelse af personer og aktiver, integriteten, fortroligheden og tilgængeligheden af informationer og kommunikations- og informationssystemer, samt et uhindret forløb af Kommissionens aktiviteter

32) »fælles IT-tjeneste«: den tjeneste, et CIS yder andre CIS'er i forbindelse med behandling af oplysninger

33) »systemejer«: den ansvarlige person for overordnet indkøb, udvikling, integration, ændring, drift, vedligeholdelse og tilbagetrækning af et CIS

34) »bruger«: enhver person, der bruger en funktionalitet fra et CIS, enten i eller uden for Kommissionen.

Artikel 3

Principper for IT-sikkerhed i Kommissionen

1. IT-sikkerhed i Kommissionen skal baseres på legalitetsprincippet, proportionalitetsprincippet, princippet om gennemsigtighed og princippet om ansvarlighed.

2. IT-sikkerhedsspørgsmål skal tages i betragtning fra starten af udviklingen og gennemførelsen af Kommissionens CIS'er. For at gøre dette skal Generaldirektoratet for Informationsteknologi og Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed inddrages i deres respektive ansvarsområder.

3. Effektiv IT-sikkerhed skal sikre et passende niveau af:

a) autenticitet: sikkerhed for, at informationer er ægte og fra bona fide-kilder

b) tilgængelighed: det forhold, at informationer er tilgængelige og kan anvendes på anmodning af en autoriseret enhed

c) fortrolighed: det forhold, at informationer ikke videregives til uautoriserede personer, enheder eller processer

d) integritet: sikkerhed for, at informationerne og aktiverne er korrekte og fuldstændige

e) uafviselighed: evnen til at bevise, at en handling eller begivenhed har fundet sted, så denne handling eller begivenhed ikke senere kan benægtes

f) beskyttelse af personoplysninger: passende sikkerhedsforanstaltninger med hensyn til personoplysninger i fuld overensstemmelse med forordning (EF) nr. 45/2001

g) tavshedspligt: beskyttelse af oplysninger af den slags, som er omfattet af tavshedspligt, navnlig oplysninger om virksomheder og om deres forretningsforbindelser eller omkostningsforhold som fastlagt i artikel 339 i TEUF.

4. IT-sikkerhed skal baseres på en risikostyringsproces. Denne proces har til formål at fastlægge niveauet for IT-sikkerhedsrisici og definere sikkerhedsforanstaltninger for at reducere sådanne risici til et passende niveau og med forholdsmæssige omkostninger.

5. Alle CIS'er skal identificeres, knyttes til en systemejer og registreres i en fortegnelse.

6. Sikkerhedskravene for alle CIS'er skal fastlægges på grundlag af deres sikkerhedsbehov og sikkerhedsbehovene for de oplysninger, de behandler. CIS'er, der leverer tjenester til andre CIS'er, kan udformes således, at de understøtter bestemte niveauer af sikkerhedsbehov.

7. IT-sikkerhedsplaner og IT-sikkerhedsforanstaltninger skal stå i forhold til CIS'ets sikkerhedsbehov.

Processerne i forbindelse med disse principper og aktiviteter beskrives nærmere i gennemførelsesbestemmelserne.

KAPITEL 2

ORGANISATION OG ANSVARSOMRÅDER

Artikel 4

Administrationsrådet

Administrationsrådet har det overordnede ansvar for styring af IT-sikkerhed som helhed i Kommissionen.

Artikel 5

Styrelsesrådet for informationssikkerhed

1. Styrelsesrådet for informationssikkerhed ledes af vicegeneralsekretæren med ansvar for Kommissionens IT-sikkerhedsstyring. Medlemmerne repræsenterer virksomheders interesser og teknologi- og sikkerhedsinteresser i Kommissionens tjenestegrene og omfatter repræsentanter for Generaldirektoratet for Informationsteknologi, Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed, Generaldirektoratet for Budget og, i en toårig rotationsordning, repræsentanter for fire andre af Kommissionens tjenestegrene, hvor IT-sikkerhed er et vigtigt spørgsmål for deres drift. Medlemskab er på øverste ledelsesniveau.

2. Styrelsesrådet for informationssikkerhed støtter administrationsrådet i dets IT-sikkerhedsrelaterede opgaver. Styrelsesrådet for informationssikkerhed påtager sig det driftsmæssige ansvar for styringen af IT-sikkerheden som helhed i Kommissionen.

3. Styrelsesrådet for informationssikkerhed anbefaler, at Kommissionen vedtager Kommissionens IT-sikkerhedspolitik.

4. Styrelsesrådet for informationssikkerhed foretager gennemgange af og rapporterer halvårligt til administrationsrådet om ledelsesmæssige forhold samt om IT-sikkerhedsrelaterede spørgsmål, herunder alvorlige IT-sikkerhedshændelser.

5. Styrelsesrådet for informationssikkerhed overvåger og gennemgår den overordnede gennemførelse af denne afgørelse og rapporterer derom til administrationsrådet.

6. På forslag fra Generaldirektoratet for Informationsteknologi gennemgår, godkender og overvåger styrelsesrådet for informationssikkerhed gennemførelsen af den rullende IT-sikkerhedsstrategi. Styrelsesrådet for informationssikkerhed rapporterer derom til administrationsrådet.

7. Styrelsesrådet for informationssikkerhed overvåger, evaluerer og kontrollerer landskabet for risikohåndtering af virksomhedsoplysninger og har beføjelse til at udstede formelle krav til forbedringer, hvor dette er nødvendigt.

Processerne i forbindelse med disse ansvarsområder og aktiviteter beskrives nærmere i gennemførelsesbestemmelserne.

Artikel 6

Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed

I forhold til IT-sikkerhed har Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed følgende ansvarsområder: Det skal:

1) sikre overensstemmelse mellem IT-sikkerhedspolitikken og Kommissionens informationssikkerhedspolitik

2) etablere en ramme for godkendelse af brugen af krypteringsteknologier til lagring og formidling af information i CIS'er

3) informere Generaldirektoratet for Informationsteknologi om konkrete trusler, som kan have en betydelig indvirkning på sikkerheden af CIS'er og de datasæt, de behandler

4) gennemføre IT-sikkerhedsinspektioner for at vurdere, om Kommissionens CIS'er overholder sikkerhedspolitikken, og rapportere resultaterne til styrelsesrådet for informationssikkerhed

5) etablere en ramme for godkendelse af adgang og de tilhørende passende sikkerhedsregler til Kommissionens CIS'er fra eksterne netværk og udvikle de tilhørende IT-sikkerhedsstandarder og retningslinjer i tæt samarbejde med Generaldirektoratet for Informationsteknologi

6) foreslå principper og regler for udlicitering af CIS'er for at opretholde en passende kontrol med informationssikkerheden

7) udvikle relevante IT-sikkerhedsstandarder og retningslinjer i forbindelse med artikel 6 i tæt samarbejde med Generaldirektoratet for Informationsteknologi.

Processerne i forbindelse med disse ansvarsområder og aktiviteter beskrives nærmere i gennemførelsesbestemmelserne.

Artikel 7

Generaldirektoratet for Informationsteknologi

I forbindelse med Kommissionens overordnede IT-sikkerhed har Generaldirektoratet for Informationsteknologi følgende ansvarsområder: Det skal:

1) udvikle IT-sikkerhedsstandarder og -retningslinjer undtagen som fastsat i artikel 6 i tæt samarbejde med Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed for at sikre sammenhæng mellem IT-sikkerhedspolitikken og Kommissionens informationssikkerhedspolitik og foreslå dem til styrelsesrådet for informationssikkerhed

2) vurdere risikostyringsmetoder for IT-sikkerhed, processer og resultater for alle Kommissionens tjenestegrene og regelmæssigt rapportere om dette til styrelsesrådet for informationssikkerhed

3) foreslå en rullende IT-sikkerhedsstrategi, som styrelsesrådet for informationssikkerhed skal revidere og godkende, og som videre skal godkendes af administrationsrådet, og foreslå et program, herunder planlægning af projekter og aktiviteter til gennemførelse af IT-sikkerhedsstrategien

4) overvåge gennemførelsen af Kommissionens IT-sikkerhedsstrategi og regelmæssigt underrette styrelsesrådet for informationssikkerhed derom

5) overvåge IT-sikkerhedsrisici og IT-sikkerhedsforanstaltninger, som er gennemført i CIS'er, og regelmæssigt underrette styrelsesrådet for informationssikkerhed derom

6) regelmæssigt underrette styrelsesrådet for informationssikkerhed om den overordnede gennemførelse og overholdelse af denne afgørelse

7) efter at have rådført sig med Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed anmode systemejerne om at træffe konkrete IT-sikkerhedsforanstaltninger for at afbøde IT-sikkerhedsrisici for Kommissionens CIS'er

8) sikre, at der er et tilstrækkeligt tilgængeligt katalog over Generaldirektoratet for Informationsteknologis IT-sikkerhedstjenester for system- og dataejerne, så de kan påtage sig deres ansvar for IT-sikkerhed og opfylde IT-sikkerhedspolitik og -standarder.

9) give system- og dataejere tilstrækkelig dokumentation og rådføre sig med dem, hvor det er relevant, om de gennemførte IT-sikkerhedsforanstaltninger for deres tjenester for at gøre det lettere at overholde IT-sikkerhedspolitikken og støtte systemejerne i IT-risikostyringen

10) afholde regelmæssige møder i LISO's netværk og støtte LISO'er i udførelsen af deres opgaver

11) definere uddannelsesbehov og koordinere uddannelsesprogrammer om IT-sikkerhed i samarbejde med Kommissionens tjenestegrene samt udvikle, gennemføre og koordinere oplysningskampagner om IT-sikkerhed i tæt samarbejde med Generaldirektoratet for Menneskelige Ressourcer

12) sikre, at systemejere, dataejere og andre roller med IT-sikkerhedsansvar i Kommissionens tjenestegrene bliver gjort opmærksomme på IT-sikkerhedspolitikken

13) informere Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed om konkrete IT-sikkerhedstrusler, hændelser og undtagelser fra Kommissionens IT-sikkerhedspolitik, som systemejerne har anmeldt, og som kan have en betydelig indvirkning på sikkerheden i Kommissionen

14) med hensyn til rollen som intern leverandør af IT-tjenester give Kommissionen et katalog over fælles IT-tjenester med definerede sikkerhedsniveauer. Dette skal ske ved systematisk at vurdere, styre og overvåge IT-sikkerhedsrisici for at gennemføre sikkerhedsforanstaltningerne og nå det definerede sikkerhedsniveau.

De dermed forbundne processer og mere detaljerede ansvarsområder defineres nærmere i gennemførelsesbestemmelserne.

Artikel 8

Kommissionens tjenestegrene

Med hensyn til IT-sikkerheden i de enkelte tjenestegrene skal lederne af Kommissionens tjenestegrene:

1) formelt udpege en systemejer, som er en tjenestemand eller en midlertidigt ansat, til hvert CIS, som er ansvarlig for IT-sikkerheden i det pågældende CIS, og formelt udpege en dataejer for hvert datasæt, der behandles i et CIS, som skal tilhøre den administrative enhed, som er registeransvarlig for datasæt i henhold til forordning (EF) nr. 45/2001

2) formelt udpege en lokal IT-sikkerhedsansvarlig (LISO), som kan påtage sig ansvaret uafhængigt af systemejere og dataejere. En LISO kan udpeges for en eller flere af Kommissionens tjenestegrene

3) sikre, at der er udformet og gennemført passende risikovurderinger af IT-sikkerheden og IT-sikkerhedsplaner

4) sikre, at der regelmæssigt indberettes et sammendrag af IT-sikkerhedsrisici og -foranstaltninger til Generaldirektoratet for Informationsteknologi

5) med støtte fra Generaldirektoratet for Informationsteknologi sikre, at der er indført passende processer, procedurer og løsninger for at sikre effektiv opdagelse, rapportering og løsning af IT-sikkerhedshændelser vedrørende deres CIS'er

6) iværksætte en hasteprocedure i tilfælde af hastende IT-sikkerhedshændelser

7) påtage sig det ultimative ansvar for IT-sikkerheden, herunder systemejerens og dataejerens ansvarsområder

8) eje risiciene i forbindelse med deres CIS'er og datasæt

9) løse eventuelle uoverensstemmelser mellem dataejere og systemejere og i tilfælde af fortsat uenighed indbringe spørgsmålet for styrelsesrådet for informationssikkerhed

10) sikre, at IT-sikkerhedsplaner og IT-sikkerhedsforanstaltninger gennemføres, og at risiciene er tilstrækkeligt dækket.

Processerne i forbindelse med disse ansvarsområder og aktiviteter beskrives nærmere i gennemførelsesbestemmelserne.

Artikel 9

Systemejere

1. Systemejeren er ansvarlig for CIS'ets IT-sikkerhed og rapporterer til lederen af Kommissionens tjenestegren.

2. Med hensyn til IT-sikkerhed skal systemejeren:

a) sikre, at CIS'et overholder IT-sikkerhedspolitikken

b) sikre, at CIS'et er korrekt registreret i det relevante lager

c) vurdere IT-sikkerhedsrisici og bestemme IT-sikkerhedsbehovene for hver enkelt CIS i samarbejde med dataejerne og i samråd med Generaldirektoratet for Informationsteknologi

d) udarbejde en sikkerhedsplan, herunder, hvor det er relevant, detaljerede oplysninger om vurderede risici og eventuelle supplerende påkrævede sikkerhedsforanstaltninger

e) gennemføre passende IT-sikkerhedsforanstaltninger, som står i forhold til de identificerede IT-risici, og følge de anbefalinger, som styrelsesrådet for informationssikkerhed har godkendt

f) identificere eventuel afhængighed af andre CIS'er eller fælles IT-tjenester og gennemføre relevante sikkerhedsforanstaltninger baseret på det sikkerhedsniveau, som disse CIS'er eller delte IT-tjenester har foreslået

g) styre og overvåge IT-sikkerhedsrisici

h) regelmæssigt underrette lederen af Kommissionens tjenestegren om risikoprofilen for CIS'ets IT-sikkerhed og underrette Generaldirektoratet for Informationsteknologi om dermed forbundne risici, risikostyringsaktiviteter og trufne sikkerhedsforanstaltninger

i) høre LISO'en for Kommissionens relevante tjenestegrene om IT-sikkerhedsmæssige aspekter

j) udstede anvisninger til brugere om brug af CIS og dermed forbundne data samt om brugernes ansvar i forbindelse med CIS.

k) anmode om godkendelse fra Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed på vegne af krypteringsmyndigheden af ethvert CIS, der anvender krypteringsteknologi

l) på forhånd høre Kommissionens sikkerhedsmyndighed om ethvert system, der behandler EU's klassificerede informationer

m) sikre, at der gemmes sikkerhedskopier af alle krypteringsnøgler på en spærret konto. Genoprettelse af krypterede oplysninger må kun ske med godkendelse efter de rammer, som Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed har defineret

n) overholde alle anvisninger fra relevante registeransvarlige vedrørende beskyttelse af personoplysninger og anvendelse af databeskyttelsesregler om sikker behandling

o) underrette Generaldirektoratet for Informationsteknologi om eventuelle undtagelser fra Kommissionens IT-sikkerhedspolitik, herunder relevante begrundelser

p) indberette eventuelle uløselige uoverensstemmelser mellem dataejeren og systemejeren til lederen af Kommissionens tjenestegren, formidle IT-sikkerhedshændelser til de relevante aktører rettidigt, hvor det er relevant, alt efter hvor alvorlige de er, som fastlagt i artikel 15

q) for udliciterede systemer sikre, at der indgår passende IT-sikkerhedsbestemmelser i udliciteringskontrakterne, og at IT-sikkerhedshændelser, der forekommer i det udliciterede CIS, indberettes i overensstemmelse med artikel 15

r) for CIS'er, der leverer delte IT-tjenester sikre, at der leveres et defineret og tydeligt dokumenteret sikkerhedsniveau, og at der er gennemført sikkerhedsforanstaltninger for CIS'et for at nå det definerede sikkerhedsniveau.

3. Systemejere kan formelt uddelegere nogle af eller alle deres IT-sikkerhedsopgaver, men de er fortsat ansvarlige for IT-sikkerheden af deres CIS.

Processerne i forbindelse med disse ansvarsområder og aktiviteter beskrives nærmere i gennemførelsesbestemmelserne.

Artikel 10

Dataejere

1. Dataejeren er ansvarlig for IT-sikkerheden for et bestemt datasæt over for lederen af Kommissionens tjenestegren og er ansvarlig for datasættes fortrolighed, integritet og tilgængelighed.

2. I forhold til dette datasæt skal dataejeren:

a) sikre, at alle datasæt, som denne er ansvarlig for, klassificeres korrekt i overensstemmelse med afgørelse (EU, Euratom) 2015/443 og (EU, Euratom) 2015/444

b) definere informationssikkerhedsbehov og informere de relevante systemejere om dette behov

c) deltage i CIS-risikovurderingen

d) indberette alle uløselige uoverensstemmelser mellem dataejeren og systemejeren til lederen af Kommissionens tjenestegren

e) formidle IT-sikkerhedshændelser som fastsat i artikel 15.

3. Dataejere kan formelt uddelegere nogle af eller alle deres IT-sikkerhedsopgaver, men de bibeholder deres ansvar som fastsat i denne artikel.

Processerne i forbindelse med disse ansvarsområder og aktiviteter beskrives nærmere i gennemførelsesbestemmelserne.

Artikel 11

Lokale IT-sikkerhedsansvarlige (LISO'er)

I forhold til IT-sikkerhed skal LISO'en:

a) proaktivt identificere og informere systemejere, dataejere og andre roller med IT-sikkerhedsansvar i Kommissionens tjenestegrene om IT-sikkerhedspolitikken

b) samarbejde om IT-sikkerhedsrelaterede spørgsmål i Kommissionens tjenestegren(e) med Generaldirektoratet for Informationsteknologi som led i LISO-netværket

c) deltage i regelmæssige LISO-møder

d) vedligeholde en oversigt over risikostyringsprocessen for informationssikkerhed og over udviklingen og gennemførelsen af sikkerhedsplaner for informationssikkerhed

e) underrette dataejere, systemejere og ledere af Kommissionens tjenestegrene om IT-sikkerhedsrelaterede spørgsmål

f) samarbejde med Generaldirektoratet for Informationsteknologi om at udbrede god IT-sikkerhedspraksis og foreslå særlige oplysnings- og uddannelsesprogrammer

g) indberette IT-sikkerhed og identificere mangler og forbedringer til lederen af Kommissionens tjenestegren(e).

Processerne i forbindelse med disse ansvarsområder og aktiviteter beskrives nærmere i gennemførelsesbestemmelserne.

Artikel 12

Brugere

1. I forhold til IT-sikkerhed skal brugere:

a) overholde IT-sikkerhedspolitikken og anvisningerne fra systemejeren om brug af de enkelte CIS'er

b) formidle IT-sikkerhedshændelser som fastsat i artikel 15.

2. Brug af Kommissionens CIS i strid med IT-sikkerhedspolitikken eller anvisninger fra systemejeren kan give anledning til disciplinærsager.

Processerne i forbindelse med disse ansvarsområder og aktiviteter fastlægges yderligere i gennemførelsesbestemmelser.

KAPITEL 3

SIKKERHEDSKRAV OG -FORPLIGTELSER

Artikel 13

Gennemførelse af denne afgørelse

1. Vedtagelsen af gennemførelsesbestemmelser til artikel 6 og af de dermed forbundne standarder og retningslinjer vil være underlagt en bemyndigelsesprocedure i Kommissionen til fordel for de medlemmer af Kommissionen, som er ansvarlige for sikkerhedsspørgsmål.

2. Vedtagelsen af alle andre gennemførelsesbestemmelser i forbindelse med denne afgørelse og af de dermed forbundne IT-sikkerhedsstandarder og -retningslinjer vil være underlagt en bemyndigelsesprocedure i Kommissionen til fordel for de medlemmer af Kommissionen, som er ansvarlige for informationsteknologi.

3. Styrelsesrådet for informationssikkerhed godkender de i stk. 1 og 2 ovenfor anførte gennemførelsesbestemmelser, standarder og retningslinjer, inden de vedtages.

Artikel 14

Overholdelsesforpligtelse

1. Det er obligatorisk at overholde bestemmelserne i IT-sikkerhedspolitikken og -standarderne.

2. Manglende overholdelse af IT-sikkerhedspolitikken og -standarderne kan give anledning til disciplinærsager i overensstemmelse med traktaterne, personalevedtægten og AØAF, til kontraktlige sanktioner og/eller til retlige skridt i medfør af nationale love og forskrifter.

3. Generaldirektoratet for Informationsteknologi skal underrettes om eventuelle undtagelser fra IT-sikkerhedspolitikken.

4. Såfremt styrelsesrådet for informationssikkerhed beslutter, at der er en vedvarende uacceptabel risiko for en af Kommissionens CIS'er, foreslår Generaldirektoratet for Informatik i samarbejde med systemejeren afbødende foranstaltninger, som styrelsesrådet for informationssikkerhed skal godkende. Disse foranstaltninger kan bl.a. omfatte øget overvågning og rapportering, begrænsede tjenester og frakobling.

5. Styrelsesrådet for informationssikkerhed gennemfører ovennævnte afbødende foranstaltninger, når det er nødvendigt. Styrelsesrådet for informationssikkerhed kan også anbefale generaldirektøren for Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed at indlede en administrativ undersøgelse. Generaldirektoratet for Informationsteknologi underretter styrelsesrådet for informationssikkerhed om enhver situation, hvor der træffes afbødende foranstaltninger.

Processerne i forbindelse med disse ansvarsområder og aktiviteter fastlægges yderligere i gennemførelsesbestemmelser.

Artikel 15

Håndtering af IT-sikkerhedshændelser

1. Generaldirektoratet for Informationsteknologi er ansvarlig for at levere det vigtigste operationelle beredskab ved IT-sikkerhedshændelser i Kommissionen.

2. Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed skal som bidragende aktører til beredskabet ved IT-sikkerhedshændelser:

a) have ret til adgang til kortfattede oplysninger om alle hændelsesregistreringer og på anmodning fulde oplysninger

b) deltage i krisestyringsgrupper om IT-sikkerhedshændelser og hasteprocedurer for IT-sikkerhed

c) være ansvarlig for forbindelser med politi- og efterretningstjenester

d) foretage kriminaltekniske undersøgelser vedrørende cybersikkerhed i overensstemmelse med artikel 11 i afgørelse (EU, Euratom) 2015/443

e) træffe beslutning om behovet for at indlede en formel undersøgelse

f) underrette Generaldirektoratet for Informationsteknologi om IT-sikkerhedshændelser, der kan udgøre en risiko for andre CIS'er.

3. Generaldirektoratet for Informationsteknologi og Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed kommunikerer løbende for at udveksle oplysninger og koordinere håndteringen af sikkerhedshændelser, navnlig IT-sikkerhedshændelser, der kan kræve en formel undersøgelse.

4. Hændelseskoordineringstjenesten i IT-beredskabsenheden for EU's institutioner og agenturer (»CERT-EU«) kan anvendes til at støtte hændelseshåndteringsprocessen, når det er relevant, og til at dele viden med andre EU-institutioner og agenturer, som kan være påvirket.

5. Systemejere, som er involveret i en IT-sikkerhedshændelse, skal:

a) straks underrette lederen af Kommissionens tjenestegren, Generaldirektoratet for Informationsteknologi, Generaldirektoratet for Menneskelige Ressourcer, LISO'en og, hvor det er relevant, dataejeren af en større IT-sikkerhedshændelse, navnlig hvis den omfatter brud på datafortrolighed

b) samarbejde og følge anvisningerne fra Kommissionens myndigheder om kommunikation, beredskab og udbedring i forbindelse med hændelser.

6. Brugere skal rettidigt indberette alle faktiske eller formodede IT-sikkerhedshændelser til den relevante IT-helpdesk.

7. Dataejere skal rettidigt indberette alle faktiske eller formodede IT-sikkerhedshændelser til den relevante beredskabsgruppe for IT-sikkerhedshændelser.

8. Generaldirektoratet for Informationsteknologi er med støtte fra de øvrige medvirkende aktører ansvarlig for at håndtere alle IT-sikkerhedshændelser i forbindelse med Kommissionens CIS'er, der ikke er udliciterede systemer.

9. Generaldirektoratet for Informationsteknologi underretter de af Kommissionens tjenestegrene, som er berørte, om IT-sikkerhedshændelser, de relevante LISO'er og, hvor det er relevant, CERT-EU efter behov.

10. Generaldirektoratet for Informationsteknologi indberetter regelmæssigt større IT-sikkerhedshændelser, der påvirker Kommissionens CIS, til styrelsesrådet for informationssikkerhed.

11. Den relevante LISO har, på anmodning, adgang til fortegnelser over IT-sikkerhedshændelser vedrørende CIS'et i Kommissionens tjenestegren.

12. I tilfælde af en større IT-sikkerhedshændelse er Generaldirektoratet for Informationsteknologi kontaktpunkt for styring af krisesituationer og koordinerer krisestyringsgrupper for IT-sikkerhedshændelser.

13. I nødstilfælde kan generaldirektøren for Generaldirektoratet for Informationsteknologi beslutte at lancere en hasteprocedure for IT-sikkerhed. Generaldirektoratet for Informationsteknologi udarbejder hasteprocedurer, som skal godkendes af styrelsesrådet for informationssikkerhed.

14. Generaldirektoratet for Informationsteknologi rapporter om gennemførelsen af hasteprocedurerne til styrelsesrådet for informationssikkerhed og lederne af Kommissionens tjenestegrene.

Processerne i forbindelse med disse ansvarsområder og aktiviteter beskrives nærmere i gennemførelsesbestemmelserne.

KAPITEL 4

AFSLUTTENDE BESTEMMELSER

Artikel 16

Gennemsigtighed

Denne afgørelse bekendtgøres for Kommissionens personale og alle personer, som den gælder for, og offentliggøres i *Den Europæiske Unions Tidende*.

Artikel 17

Tilknytning til andre retsakter

Bestemmelserne i denne afgørelse berører ikke afgørelse (EU, Euratom) 2015/443, afgørelse (EU, Euratom) 2015/444, forordning (EF) nr. 45/2001, Europa-Parlamentets og Rådets forordning (EF) nr. 1049/2001 ([1]), Kommissionens afgørelse 2002/47/ EF, EFSF, Euratom ([2]), Europa-Parlamentets og Rådets forordning (EU, Euratom) nr. 883/2013 ([3]) og afgørelse 1999/352/EF, EKSF, Euratom.

Artikel 18

Ophævelse og overgangsbestemmelser

Afgørelse C(2006) 3602 af 16. august 2006 ophæves.

Gennemførelsesbestemmelserne og de IT-sikkerhedsstandarder, som blev vedtaget i henhold til artikel 10 i afgørelse C (2006) 3602, er fortsat gældende, i det omfang de ikke strider mod denne afgørelse, indtil de erstattes af de gennemførelsesbestemmelser og standarder, som skal vedtages i henhold til artikel 13 i denne afgørelse. Enhver henvisning til artikel 10 i afgørelse C(2006) 3602 skal læses som en henvisning til artikel 13 i denne afgørelse.

Artikel 19

Ikrafttræden

Denne afgørelse træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Udfærdiget i Bruxelles, den 10. januar 2017.

På Kommissionens vegne
Jean-Claude JUNCKER
Formand

([1]) Europa-Parlamentets og Rådets forordning (EF) nr. 1049/2001 af 30. maj 2001 om aktindsigt i Europa-Parlamentets, Rådets og Kommissionens dokumenter (EFT L 145 af 31.5.2001, s. 43).

([2]) Kommissionens afgørelse 2002/47/EF, EKSF, Euratom af 23. januar 2002 om ændring af dens forretningsorden (EFT L 21 af 24.1.2002, s. 23).

([3]) Europa-Parlamentets og Rådets forordning (EU, Euratom) nr. 883/2013 af 11. september 2013 om undersøgelser, der foretages af Det Europæiske Kontor for Bekæmpelse af Svig (OLAF) og om ophævelse af Europa-Parlamentets og Rådets forordning (EF) nr. 1073/1999 og Rådets forordning (Euratom) nr. 1074/1999 (EUT L 248 af 18.9.2013, s. 1).