REGULAMENTUL (UE) 2018/1725 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

din 23 octombrie 2018

privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE

(Text cu relevanță pentru SEE)

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 16 alineatul (2),

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Comitetului Economic și Social European ([1]),

hotărând în conformitate cu procedura legislativă ordinară ([2]),

întrucât:

(1) Protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal este un drept fundamental. Articolul 8 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene („Carta") și articolul 16 alineatul (1) din Tratatul privind funcționarea Uniunii Europene (TFUE) prevăd dreptul oricărei persoane la protecția datelor cu caracter personal care o privesc. De asemenea, acest drept este garantat și în temeiul articolului 8 din Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale.

(2) Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului ([3]) conferă persoanelor fizice drepturi garantate din punct de vedere juridic, definește obligațiile în materie de prelucrare a datelor care le revin operatorilor în instituțiile și organele comunitare și prevede instituirea unei autorități independente de supraveghere, Autoritatea Europeană pentru Protecția Datelor, care să răspundă de monitorizarea prelucrării datelor cu caracter personal de către instituțiile și organele Uniunii. Cu toate acestea, regulamentul menționat nu se aplică prelucrării datelor cu caracter personal în cursul unei activități desfășurate de către instituții și organe ale Uniunii care nu intră în domeniul de aplicare al dreptului Uniunii.

(3) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului ([4]) și Directiva (UE) 2016/680 a Parlamentului European și a Consiliului ([5]) au fost adoptate la 27 aprilie 2016. În timp ce regulamentul stabilește norme generale menite să protejeze persoanele fizice în ceea ce privește prelucrarea datelor cu caracter personal și să asigure libera circulație a datelor cu caracter personal în Uniune, directiva stabilește norme specifice menite să protejeze persoanele fizice în ceea ce privește prelucrarea datelor cu caracter personal și să asigure libera circulație a acestor date în Uniune în domeniile cooperării judiciare în materie penală și al cooperării polițienești.

(4) Regulamentul (UE) 2016/679 prevede adaptarea Regulamentului (CE) nr. 45/2001 pentru a asigura un cadru solid și coerent în materia protecției datelor în Uniune și a permite aplicarea în paralel a acestuia din urmă cu Regulamentul (UE) 2016/679.

(5) Este în interesul unei abordări coerente a protecției datelor cu caracter personal în întreaga Uniune, precum și al liberei circulații a datelor cu caracter personal în Uniune, ca normele de protecție a datelor ale instituțiilor, organelor, oficiilor și agențiilor Uniunii să fie aliniate cât mai mult posibil la normele de protecție a datelor adoptate pentru sectorul public din statele membre. Ori de câte ori dispozițiile din prezentul regulament urmează aceleași principii ca

([1]) JO C 288, 31.8.2017, p. 107.

([2]) Poziția Parlamentului European din 13 septembrie 2018 (nepublicată încă în Jurnalul Oficial) și Decizia Consiliului din 11 octombrie 2018.

([3]) Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date (JO L 8, 12.1.2001, p. 1).

([4]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1.).

([5]) Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului (JO L 119, 4.5.2016, p. 89).

dispozițiile Regulamentului (UE) 2016/679, aceste două seturi de dispoziții ar trebui, în temeiul jurisprudenței Curții de Justiție a Uniunii Europene („Curtea de Justiție"), să fie interpretate în mod omogen, în special pentru că structura prezentului regulament ar trebui înțeleasă ca fiind similară structurii Regulamentului (UE) 2016/679.

(6) Persoanele ale căror date cu caracter personal sunt prelucrate de către instituțiile sau organele Uniunii indiferent de context, de exemplu pentru că persoanele menționate mai sus sunt angajate de către aceste instituții sau organe, ar trebui să fie protejate. Prezentul regulament nu ar trebui să se aplice prelucrării datelor cu caracter personal ale persoanelor decedate. Prezentul regulament nu se aplică prelucrării datelor cu caracter personal care privesc persoane juridice și, în special, întreprinderi cu personalitate juridică, inclusiv numele și tipul de persoană juridică și datele de contact ale persoanei juridice.

(7) Pentru a preveni apariția unui risc major de eludare, protecția persoanelor fizice ar trebui să fie neutră din punct de vedere tehnologic și să nu depindă de tehnologiile utilizate.

(8) Prezentul regulament ar trebui să se aplice prelucrării datelor cu caracter personal de către toate instituțiile, organele, oficiile și agențiile Uniunii. Regulamentul ar trebui să se aplice prelucrării datelor cu caracter personal, efectuate total sau parțial prin mijloace automatizate, precum și prelucrării, prin alte mijloace decât cele automatizate, a datelor cu caracter personal care fac parte dintr-un sistem de evidență sau care sunt destinate să facă parte dintr-un sistem de evidență. Dosarele sau seturile de dosare, precum și copertele acestora, care nu sunt structurate în conformitate cu criterii specifice nu ar trebui să intre în domeniul de aplicare al prezentului regulament.

(9) În Declarația nr. 21 cu privire la protecția datelor cu caracter personal în domeniul cooperării judiciare în materie penală și al cooperării polițienești, anexată actului final al Conferinței interguvernamentale care a adoptat Tratatul de la Lisabona, conferința a recunoscut că s-ar putea dovedi necesare norme specifice privind protecția datelor cu caracter personal și libera circulație a datelor cu caracter personal în domeniul cooperării judiciare în materie penală și al cooperării polițienești în temeiul articolului 16 din TFUE, având în vedere natura specifică a acestor domenii. Un capitol distinct din prezentul regulament cuprinzând norme generale ar trebui, prin urmare, să se aplice prelucrării datelor operaționale cu caracter personal, precum datele cu caracter personal prelucrate în vederea anchetelor penale de către organele, oficiile sau agențiile Uniunii atunci când desfășoară activități în domeniile cooperării judiciare în materie penală și al cooperării polițienești.

(10) Directiva (UE) 2016/680 stabilește norme armonizate pentru protecția și libera circulație a datelor cu caracter personal prelucrate în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau în scopul executării pedepselor, inclusiv în scopul protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora. În vederea asigurării aceluiași nivel de protecție pentru persoanele fizice prin drepturi opozabile în întreaga Uniune și a preîntâmpinării discrepanțelor care împiedică schimbul de date cu caracter personal între organele, oficiile sau agențiile Uniunii atunci când desfășoară activități care intră în domeniul de aplicare al părții a treia titlul V capitolul 4 sau capitolul 5 din TFUE și autoritățile competente, normele pentru protecția și libera circulație a datelor operaționale cu caracter personal prelucrate de către aceste organe, oficii sau agenții ale Uniunii ar trebui să fie coerente cu Directiva (UE) 2016/680.

(11) Normele generale ale capitolului din prezentul regulament referitor la prelucrarea datelor operaționale cu caracter personal ar trebui să se aplice fără a aduce atingere normelor specifice aplicabile prelucrării de date operaționale cu caracter personal efectuate de organele, oficiile și agențiile Uniunii atunci când desfășoară activități care intră sub incidența părții a treia titlul V capitolul 4 sau capitolul 5 din TFUE. Aceste norme specifice ar trebui să fie considerate *lex specialis* în raport cu dispozițiile de la capitolul din prezentul regulament referitor la prelucrarea datelor operaționale cu caracter personal (*lex specialis derogat legi generali*). Pentru a reduce fragmentarea juridică, normele specifice de protecție a datelor aplicabile prelucrării de date operaționale cu caracter personal de către organele, oficiile sau agențiile Uniunii atunci când desfășoară activități care intră sub incidența părții a treia titlul V capitolul 4 sau capitolul 5 din TFUE ar trebui să fie în concordanță cu principiile care stau la baza capitolului din prezentul regulament referitor la prelucrarea datelor operaționale cu caracter personal, precum și cu dispozițiile din prezentul regulament privind controlul independent, căile de atac, răspunderea și sancțiunile.

(12) Capitolul din prezentul regulament referitor la prelucrarea datelor operaționale cu caracter personal ar trebui să se aplice organelor, oficiilor și agențiilor Uniunii atunci când desfășoară activități care intră sub incidența părții a treia titlul V capitolul 4 sau capitolul 5 din TFUE, indiferent dacă desfășoară aceste activități ca sarcini principale sau auxiliare în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor. Cu toate acestea, capitolul în cauză nu ar trebui să se aplice Europol sau Parchetului European până când actele juridice de instituire a Europol și a Parchetului European nu sunt modificate, cu scopul de a face capitolul din prezentul regulament referitor la prelucrarea datelor operaționale cu caracter personal, în forma adaptată, aplicabil acestora.

(13) Comisia ar trebui să revizuiască prezentul regulament, în special capitolul din prezentul regulament referitor la prelucrarea datelor operaționale cu caracter personal. Comisia ar trebui, de asemenea, să revizuiască alte acte juridice, adoptate pe baza tratatelor, care reglementează prelucrarea datelor operaționale cu caracter personal de

către organele, oficiile sau agențiile Uniunii atunci când desfășoară activități care intră sub incidența părții a treia titlul V capitolul 4 sau capitolul 5 din TFUE. După această revizuire, în vederea asigurării unei protecții uniforme și consecvente a persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, Comisia ar trebui să poată face orice propuneri legislative corespunzătoare, inclusiv orice adaptări necesare ale capitolului din prezentul regulament referitor la prelucrarea datelor operaționale cu caracter personal, în vederea aplicării acestuia Europol și Parchetului European. Adaptările ar trebui să ia în considerare dispoziții referitoare la supravegherea independentă, căile de atac, răspunderea și sancțiunile.

(14) Prelucrarea datelor administrative cu caracter personal, cum ar fi datele privind personalul, de către organele, oficiile sau agențiile Uniunii care desfășoară activități care intră sub incidența părții a treia titlul V capitolul 4 sau capitolul 5 din TFUE ar trebui reglementată de prezentul regulament.

(15) Prezentul regulament ar trebui să se aplice prelucrării datelor cu caracter personal de către instituțiile, organele, oficiile sau agențiile Uniunii care desfășoară activități care intră în domeniul de aplicare al titlului V capitolul 2 din Tratatul privind Uniunea Europeană (TUE). Prezentul regulament nu ar trebui să se aplice prelucrării datelor cu caracter personal de către misiunile menționate la articolul 42 alineatul (1) și la articolele 43 și 44 din TUE, care pun în aplicare politica de securitate și apărare comună. Dacă este cazul, pentru a reglementa în mod mai specific prelucrarea de date cu caracter personal în domeniul politicii de securitate și apărare comune, ar trebui prezentate propuneri corespunzătoare.

(16) Principiile protecției datelor ar trebui să se aplice oricărei informații referitoare la o persoană fizică identificată sau identificabilă. Datele cu caracter personal care au fost supuse pseudonimizării, care ar putea fi atribuite unei persoane fizice prin utilizarea de informații suplimentare, ar trebui considerate informații referitoare la o persoană fizică identificabilă. Pentru a se determina dacă o persoană fizică este identificabilă, ar trebui să se ia în considerare toate mijloacele, cum ar fi individualizarea, pe care este probabil, în mod rezonabil, să le utilizeze fie operatorul, fie o altă persoană, în scopul identificării, în mod direct sau indirect, a persoanei fizice respective. Pentru a se determina dacă este probabil, în mod rezonabil, să fie utilizate mijloace pentru identificarea persoanei fizice, ar trebui luați în considerare toți factorii obiectivi, precum costurile și intervalul de timp necesare pentru identificare, ținându-se seama atât de tehnologia disponibilă la momentul prelucrării, cât și de dezvoltarea tehnologică. Principiile protecției datelor ar trebui, prin urmare, să nu se aplice informațiilor anonime, adică informațiilor care nu sunt legate de o persoană fizică identificată sau identificabilă sau datelor cu caracter personal care sunt anonimizate astfel încât persoana vizată nu este sau nu mai este identificabilă. Prin urmare, prezentul regulament nu se aplică prelucrării unor astfel de informații anonime, inclusiv în cazul în care acestea sunt utilizate în scopuri statistice sau de cercetare.

(17) Aplicarea pseudonimizării datelor cu caracter personal poate reduce riscurile pentru persoanele vizate și poate ajuta operatorii și persoanele împuternicite de către operatori să își îndeplinească obligațiile de protecție a datelor. Introducerea explicită a conceptului de „pseudonimizare” în prezentul regulament nu este destinată să împiedice alte eventuale măsuri de protecție a datelor.

(18) Persoanele fizice pot fi asociate cu identificatorii online furnizați de dispozitivele, aplicațiile, instrumentele și protocoalele lor, cum ar fi adresele IP, identificatorii cookie sau alți identificatori, precum etichetele de identificare prin frecvențe radio. Aceștia pot lăsa urme care, în special atunci când sunt combinate cu identificatori unici și cu alte informații primite de servere, pot fi utilizate pentru crearea de profiluri ale persoanelor fizice și pentru identificarea lor.

(19) Consimțământul ar trebui acordat printr-o acțiune neechivocă care să constituie o manifestare liber exprimată, specifică, în cunoștință de cauză și clară a acordului persoanei vizate pentru prelucrarea datelor sale cu caracter personal, cum ar fi o declarație făcută în scris, inclusiv în format electronic, sau verbal. Aceasta ar putea include bifarea unei căsuțe atunci când persoana vizitează un website, alegerea parametrilor tehnici pentru serviciile societății informaționale sau orice altă declarație sau acțiune care indică în mod clar în acest context acceptarea de către persoana vizată a prelucrării propuse a datelor sale cu caracter personal. Prin urmare, absența unui răspuns, căsuțele bifate în prealabil sau absența unei acțiuni nu ar trebui să constituie un consimțământ. Consimțământul ar trebui să vizeze toate activitățile de prelucrare efectuate în același scop sau în aceleași scopuri. Dacă prelucrarea datelor se face în mai multe scopuri, consimțământul ar trebui dat pentru toate scopurile prelucrării. În cazul în care consimțământul persoanei vizate trebuie acordat în urma unei cereri transmise pe cale electronică, cererea respectivă trebuie să fie clară și concisă și să nu perturbe în mod inutil utilizarea serviciului pentru care se acordă consimțământul. În același timp, persoana vizată ar trebui să aibă dreptul de a-și retrage în orice moment consimțământul, fără ca acest fapt să afecteze legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia. Pentru a garanta faptul că a fost acordat în mod liber, consimțământul nu ar trebui să constituie un temei juridic valabil pentru prelucrarea datelor cu caracter personal în cazul particular în care există un dezechilibru evident între persoana vizată și operator, iar acest lucru face improbabilă acordarea consimțământului

în mod liber în toate circumstanțele aferente respectivei situații particulare. Adesea nu este posibil, în momentul colectării datelor cu caracter personal, să se identifice pe deplin scopul prelucrării datelor în scopuri de cercetare științifică. Din acest motiv, persoanelor vizate ar trebui să li se permită să își exprime consimțământul pentru anumite domenii ale cercetării științifice atunci când sunt respectate standardele etice recunoscute pentru cercetarea științifică. Persoanele vizate ar trebui să aibă posibilitatea de a-și exprima consimțământul doar pentru anumite domenii de cercetare sau părți ale proiectelor de cercetare în măsura permisă de scopul preconizat.

(20) Orice prelucrare de date cu caracter personal ar trebui să fie legală și echitabilă. Ar trebui să fie transparent pentru persoanele fizice faptul că sunt colectate, utilizate, consultate sau prelucrate în alt mod datele cu caracter personal care le privesc și în ce măsură datele cu caracter personal sunt sau vor fi prelucrate. Principiul transparenței prevede că orice informații și comunicări referitoare la prelucrarea respectivelor date cu caracter personal sunt ușor accesibile și ușor de înțeles și că se utilizează un limbaj simplu și clar. Acest principiu se referă în special la informarea persoanelor vizate privind identitatea operatorului și scopurile prelucrării, precum și la oferirea de informații suplimentare, pentru a asigura o prelucrare echitabilă și transparentă în ceea ce privește persoanele fizice vizate și dreptul acestora de a li se confirma și comunica datele cu caracter personal care le privesc care sunt prelucrate. Persoanele fizice ar trebui informate cu privire la riscurile, normele, garanțiile și drepturile în materie de prelucrare a datelor cu caracter personal și cu privire la modul în care să își exercite drepturile în legătură cu prelucrarea. În special, scopurile specifice în care datele cu caracter personal sunt prelucrate ar trebui să fie explicite și legitime și să fie determinate la momentul colectării datelor respective. Datele cu caracter personal ar trebui să fie adecvate, relevante și limitate la ceea ce este necesar pentru scopurile în care sunt prelucrate. Aceasta necesită, în special, asigurarea faptului că perioada pentru care datele cu caracter personal sunt stocate este limitată strict la minimum. Datele cu caracter personal ar trebui prelucrate doar dacă scopul prelucrării nu poate fi îndeplinit în mod rezonabil prin alte mijloace. În vederea asigurării faptului că datele cu caracter personal nu sunt păstrate mai mult timp decât este necesar, ar trebui să se stabilească de către operator termene pentru ștergere sau pentru o revizuire periodică. Ar trebui să fie luate toate măsurile rezonabile pentru a se asigura că datele cu caracter personal care sunt inexacte sunt rectificate sau șterse. Datele cu caracter personal ar trebui prelucrate într-un mod care să asigure în mod adecvat securitatea și confidențialitatea acestora, inclusiv în scopul prevenirii accesului neautorizat la acestea sau utilizarea neautorizată a datelor cu caracter personal și a echipamentului utilizat pentru prelucrare și pentru a preveni dezvăluirea neautorizată în cursul transmiterii.

(21) În conformitate cu principiul responsabilității, în cazul în care instituții sau organe ale Uniunii transmit date cu caracter personal în cadrul aceleiași instituții sau aceluiași organ, iar destinatarul nu face parte din operator, sau în cazul în care transmit date cu caracter personal către alte instituții sau organe ale Uniunii, respectivele instituții și organe ar trebui să verifice dacă aceste date cu caracter personal sunt necesare pentru îndeplinirea legitimă a sarcinilor care sunt de competența destinatarului. În special, după ce destinatarul i-a adresat o cerere de transmitere a unor date cu caracter personal, operatorul ar trebui să verifice existența unui motiv relevant pentru prelucrarea legală a datelor cu caracter personal, precum și competența destinatarului. Operatorul ar trebui, de asemenea, să efectueze o evaluare provizorie a necesității transmiterii datelor. Dacă apar îndoieli în privința necesității acestui transfer, operatorul ar trebui să solicite destinatarului mai multe informații. Destinatarul ar trebui să se asigure că necesitatea transmiterii datelor poate fi verificată ulterior.

(22) Pentru ca prelucrarea datelor cu caracter personal să fie legală, la baza acesteia ar trebui să stea necesitatea îndeplinirii de către instituțiile și organele Uniunii a unei sarcini de interes public sau care rezultă din exercitarea autorității publice cu care sunt învestite, necesitatea respectării unei obligații legale care îi revine operatorului sau un alt motiv legitim în temeiul prezentului regulament, inclusiv consimțământul persoanei vizate, necesitatea prelucrării în vederea executării unui contract la care persoana vizată este parte sau necesitatea parcurgerii etapelor premergătoare încheierii unui contract, la solicitarea persoanei vizate. Prelucrarea datelor cu caracter personal în scopul îndeplinirii unor misiuni de interes public de către instituțiile și organele Uniunii include prelucrarea datelor cu caracter personal necesare administrării și funcționării acestor instituții și organe. Prelucrarea datelor cu caracter personal ar trebui, de asemenea, să fie considerată legală în cazul în care este necesară în scopul asigurării protecției unui interes care este esențial pentru viața persoanei vizate sau pentru viața unei alte persoane fizice. Prelucrarea datelor cu caracter personal care are drept temei interesele vitale ale unei alte persoane fizice ar trebui, în principiu, să fie efectuată numai în cazul în care prelucrarea nu se poate baza în mod evident pe un alt temei juridic. Unele tipuri de prelucrare pot servi atât unor motive importante de interes public, cât și intereselor vitale ale persoanei vizate, de exemplu în cazul în care prelucrarea este necesară în scopuri umanitare, inclusiv în vederea monitorizării unei epidemii și a răspândirii acesteia sau în situații de urgențe umanitare, în special în situații de dezastre naturale sau provocate de om.

(23) Dreptul Uniunii menționat în prezentul regulament ar trebui să fie clar și precis, iar aplicarea sa ar trebui să fie previzibilă pentru persoanele vizate de acesta, în conformitate cu cerințele prevăzute în Cartă și în Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale.

(24) Normele interne menționate în prezentul regulament ar trebui să fie acte clare și precise, general aplicabile, menite să producă efecte juridice față de persoanele vizate. Acestea ar trebui adoptate la cel mai înalt nivel de conducere al instituțiilor și organelor Uniunii, în limita competențelor acestora și în chestiuni legate de funcționarea lor. Acestea ar trebui publicate în *Jurnalul Oficial al Uniunii Europene*. Aplicarea normelor respective ar trebui să fie previzibilă pentru persoanele vizate, în conformitate cu cerințele prevăzute în Cartă și în Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale. Normele interne ar putea lua forma unor decizii, în special atunci când sunt adoptate de instituțiile Uniunii.

(25) Prelucrarea datelor cu caracter personal în alte scopuri decât scopurile pentru care datele cu caracter personal au fost inițial colectate ar trebui să fie permisă doar atunci când prelucrarea este compatibilă cu scopurile pentru care datele cu caracter personal au fost inițial colectate. În acest caz nu este necesar un temei juridic separat de cel pe baza căruia a fost permisă colectarea datelor cu caracter personal. În cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul, dreptul Uniunii poate stabili și specifica sarcinile și scopurile pentru care prelucrarea ulterioară ar trebui considerată a fi compatibilă și legală. Prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice ar trebui considerată ca reprezentând operațiuni de prelucrare legale compatibile. Temeiul juridic prevăzut în dreptul Uniunii pentru prelucrarea datelor cu caracter personal poate constitui, de asemenea, un temei juridic pentru prelucrarea ulterioară. Pentru a stabili dacă scopul prelucrării ulterioare este compatibil cu scopul pentru care au fost colectate inițial datele cu caracter personal, operatorul, după ce a îndeplinit toate cerințele privind legalitatea prelucrării inițiale, ar trebui să țină seama, printre altele, de orice legătură existentă între respectivele scopuri și scopurile prelucrării ulterioare preconizate, de contextul în care au fost colectate datele cu caracter personal, în special de așteptările rezonabile ale persoanelor vizate, bazate pe relația lor cu operatorul, în ceea ce privește utilizarea ulterioară a datelor; de natura datelor cu caracter personal, de consecințele pe care prelucrarea ulterioară preconizată le va avea asupra persoanelor vizate, precum și de existența unor garanții corespunzătoare atât în cadrul operațiunilor de prelucrare inițiale, cât și în cadrul operațiunilor de prelucrare ulterioare preconizate.

(26) În cazul în care prelucrarea se bazează pe consimțământul persoanei vizate, operatorul ar trebui să fie în măsură să demonstreze faptul că persoana vizată și-a dat consimțământul pentru operațiunea de prelucrare. În special, în contextul unei declarații scrise cu privire la un alt aspect, garanțiile ar trebui să asigure că persoana vizată este conștientă de faptul că și-a dat consimțământul și în ce măsură a făcut acest lucru. În conformitate cu Directiva 93/13/CEE a Consiliului ([1]), ar trebui furnizată o declarație de consimțământ formulată în prealabil de către operator, într-o formă inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu, iar această declarație nu ar trebui să conțină clauze abuzive. Pentru ca acordarea consimțământului să fie în cunoștință de cauză, persoana vizată ar trebui să fie la curent cel puțin cu identitatea operatorului și cu scopurile prelucrării pentru care sunt destinate datele cu caracter personal. Consimțământul nu ar trebui considerat ca fiind acordat în mod liber dacă persoana vizată nu dispune cu adevărat de libertatea de alegere sau nu este în măsură să refuze sau să își retragă consimțământul fără a fi prejudiciată.

(27) Copiii au nevoie de o protecție specifică a datelor lor cu caracter personal, întrucât pot fi mai puțin conștienți de riscurile, consecințele, garanțiile în cauză și drepturile lor în ceea ce privește prelucrarea datelor cu caracter personal. O astfel de protecție specifică ar trebui să se aplice în special creării de profiluri de personalitate și colectării de date cu caracter personal privind copiii cu ocazia oferirii serviciilor direct copiilor pe website-urile instituțiilor și organelor Uniunii, cum ar fi serviciile de comunicare interpersonală sau vânzarea online de bilete, iar prelucrarea datelor cu caracter personal se bazează pe consimțământ.

(28) Atunci când destinatari stabiliți în Uniune, alții decât instituțiile și organele Uniunii, ar dori ca instituții și organe ale Uniunii să le transmită date cu caracter personal, destinatarii respectivi ar trebui să demonstreze că este necesar ca datele să fie transmise acestor destinatari pentru îndeplinirea sarcinii lor executate în interes public sau în cadrul exercitării unei autorități oficiale cu care sunt învestiți. În mod alternativ, destinatarii respectivi ar trebui să demonstreze că transmiterea este necesară pentru un scop specific în interesul public iar operatorul ar trebui să stabilească dacă există vreun motiv să se presupună că interesele legitime ale persoanei vizate ar putea fi afectate. În astfel de cazuri, în mod demonstrabil, operatorul ar trebui să cântărească diferitele interese pentru a evalua

([1]) Directiva 93/13/CEE a Consiliului din 5 aprilie 1993 privind clauzele abuzive în contractele încheiate cu consumatorii (JO L 95, 21.4.1993, p. 29).

proporționalitatea transmiterii solicitate de date cu caracter personal. Scopul specific în interesul public ar putea să se refere la transparența instituțiilor și organelor Uniunii. În plus, instituțiile și organele Uniunii ar trebui să demonstreze această necesitate atunci când inițiază ele însele o transmitere, în conformitate cu principiul transparenței și al bunei administrări. Cerințele stabilite în prezentul regulament privind transmiterile către destinatari stabiliți în Uniune, alții decât instituții și organe ale Uniunii, ar trebui să fie înțelese ca fiind complementare condițiilor pentru prelucrarea legală.

(29) Datele cu caracter personal care sunt, prin natura lor, deosebit de sensibile în ceea ce privește drepturile și libertățile fundamentale necesită o protecție specifică, deoarece contextul prelucrării acestora ar putea genera riscuri considerabile la adresa drepturilor și libertăților fundamentale. Aceste date cu caracter personal nu ar trebui prelucrate dacă nu sunt îndeplinite condițiile specifice prevăzute de prezentul regulament. Aceste date cu caracter personal ar trebui să includă datele cu caracter personal care dezvăluie originea rasială sau etnică, utilizarea termenului „origine rasială" în prezentul regulament neimplicând o acceptare de către Uniune a teoriilor care urmăresc să stabilească existența unor rase umane separate. Prelucrarea fotografiilor nu ar trebui să fie considerată în mod sistematic ca fiind o prelucrare de categorii speciale de date cu caracter personal, întrucât fotografiile intră sub incidența definiției datelor biometrice doar în cazurile în care sunt prelucrate prin mijloace tehnice specifice care permit identificarea unică sau autentificarea unei persoane fizice. Pe lângă cerințele specifice privind prelucrarea datelor sensibile, ar trebui să se aplice principiile generale și alte norme prevăzute de prezentul regulament, în special în ceea ce privește condițiile pentru prelucrarea legală. Ar trebui prevăzute în mod explicit derogări de la interdicția generală de prelucrare a acestor categorii speciale de date cu caracter personal, printre altele atunci când persoana vizată își dă consimțământul explicit sau în ceea ce privește nevoi specifice, în special atunci când prelucrarea este efectuată în cadrul unor activități legitime de către anumite asociații sau fundații al căror scop este de a permite exercitarea libertăților fundamentale.

(30) Categoriile speciale de date cu caracter personal, care necesită un nivel mai ridicat de protecție, ar trebui prelucrate în scopuri legate de sănătate doar atunci când este necesar pentru realizarea acestor scopuri, în beneficiul persoanelor fizice și al societății în general, în special în contextul gestionării serviciilor și sistemelor de sănătate sau de asistență socială. Prin urmare, prezentul regulament ar trebui să prevadă condiții armonizate pentru prelucrarea categoriilor speciale de date cu caracter personal privind sănătatea, în ceea ce privește nevoile specifice, în special atunci când prelucrarea acestor date este efectuată în anumite scopuri legate de sănătate de către persoane care fac obiectul unei obligații legale de a păstra secretul profesional. Dreptul Uniunii ar trebui să prevadă măsuri specifice și adecvate pentru a proteja drepturile fundamentale și datele cu caracter personal ale persoanelor fizice.

(31) Prelucrarea categoriilor speciale de date cu caracter personal poate fi necesară din motive de interes public în domeniile sănătății publice, fără consimțământul persoanei vizate. O astfel de prelucrare ar trebui condiționată de măsuri adecvate și specifice destinate să protejeze drepturile și libertățile persoanelor fizice. În acest context, conceptul de „sănătate publică" ar trebui interpretat astfel cum este definit în Regulamentul (CE) nr. 1338/2008 al Parlamentului European și al Consiliului ([1]), și anume toate elementele referitoare la sănătate și anume starea de sănătate, inclusiv morbiditatea sau handicapul, factorii determinanți care au efect asupra stării de sănătate, necesitățile în domeniul asistenței medicale, resursele alocate asistenței medicale, furnizarea asistenței medicale și asigurarea accesului universal la aceasta, precum și cheltuielile și sursele de finanțare în domeniul sănătății și cauzele mortalității. Această prelucrare a datelor privind sănătatea din motive de interes public nu ar trebui să ducă la prelucrarea acestor date în alte scopuri.

(32) Dacă datele cu caracter personal prelucrate de un operator nu îi permit acestuia să identifice o persoană fizică, operatorul de date nu ar trebui să aibă obligația de a obține informații suplimentare în vederea identificării persoanei vizate, cu unicul scop de a respecta oricare dintre dispozițiile prezentului regulament. Cu toate acestea, operatorul nu ar trebui să refuze să preia informațiile suplimentare furnizate de persoana vizată cu scopul de a sprijini exercitarea drepturilor acesteia. Identificarea ar trebui să includă identificarea digitală a unei persoane vizate, de exemplu prin mecanisme de autentificare precum aceleași acreditări utilizate de către persoana vizată pentru a accesa serviciile online oferite de operatorul de date.

(33) Prelucrarea datelor cu caracter personal în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice ar trebui să facă, în conformitate cu prezentul regulament, obiectul unor garanții adecvate pentru drepturile și libertățile persoanei vizate. Respectivele garanții ar trebui să asigure faptul că au fost instituite măsuri tehnice și organizatorice necesare pentru a se asigura, în special, principiul reducerii la minimum a datelor. Prelucrarea ulterioară a datelor cu caracter personal în scopuri de arhivare în interes public, în scopuri de

([1]) Regulamentul (CE) nr. 1338/2008 al Parlamentului European și al Consiliului din 16 decembrie 2008 privind statisticile comunitare referitoare la sănătatea publică, precum și la sănătatea și siguranța la locul de muncă (JO L 354, 31.12.2008, p. 70).

cercetare științifică sau istorică ori în scopuri statistice se efectuează atunci când operatorul a evaluat fezabilitatea pentru îndeplinirea acestor obiective prin prelucrarea unor date cu caracter personal care nu permit sau nu mai permit identificarea persoanelor vizate, cu condiția să existe garanții adecvate (cum ar fi pseudonimizarea datelor cu caracter personal). Instituțiile și organele Uniunii ar trebui să prevadă în dreptul Uniunii, eventual în normele interne adoptate de instituțiile și organele Uniunii în chestiuni legate de funcționarea lor, garanții adecvate pentru prelucrarea datelor cu caracter personal în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice.

(34) Ar trebui să fie prevăzute modalități de facilitare a exercitării de către persoana vizată a drepturilor care îi sunt conferite prin prezentul regulament, inclusiv mecanismele prin care aceasta poate solicita și, dacă este cazul, obține, în mod gratuit, în special, acces la datele cu caracter personal, precum și rectificarea sau ștergerea acestora, și exercitarea dreptului la opoziție. Operatorul ar trebui să ofere, de asemenea, modalități de introducere a cererilor pe cale electronică, mai ales în cazul în care datele cu caracter personal sunt prelucrate prin mijloace electronice. Operatorul ar trebui să aibă obligația de a răspunde cererilor persoanelor vizate fără întârzieri nejustificate și cel târziu în termen de o lună și, în cazul în care nu intenționează să dea curs respectivelor cereri, să motiveze acest refuz.

(35) Conform principiilor prelucrării echitabile și transparente, persoana vizată este informată cu privire la existența unei operațiuni de prelucrare și la scopurile acesteia. Operatorul ar trebui să furnizeze persoanei vizate orice informații suplimentare necesare pentru a asigura o prelucrare echitabilă și transparentă, ținând seama de circumstanțele specifice și de contextul în care sunt prelucrate datele cu caracter personal. În plus, persoana vizată ar trebui informată cu privire la crearea de profiluri, precum și la consecințele acesteia. Atunci când datele cu caracter personal sunt colectate de la persoana vizată, aceasta ar trebui informată, de asemenea, dacă are obligația de a furniza datele cu caracter personal și cu privire la consecințe în cazul unui refuz. Aceste informații pot fi furnizate în combinație cu pictograme standardizate pentru a oferi într-un mod ușor vizibil, inteligibil și clar lizibil o imagine de ansamblu semnificativă asupra prelucrării avute în vedere. În cazul în care pictogramele sunt prezentate în format electronic, acestea ar trebui să poată fi citite automat.

(36) Informațiile în legătură cu prelucrarea datelor cu caracter personal referitoare la persoana vizată ar trebui furnizate acesteia la momentul colectării de la persoana vizată sau, în cazul în care datele cu caracter personal sunt obținute din altă sursă, într-o perioadă rezonabilă, în funcție de circumstanțele cazului. În cazul în care datele cu caracter personal pot fi divulgate în mod legitim unui alt destinatar, persoana vizată ar trebui informată atunci când datele cu caracter personal sunt divulgate pentru prima dată destinatarului. În cazul în care operatorul intenționează să prelucreze datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost colectate, operatorul ar trebui să furnizeze persoanei vizate, înainte de această prelucrare ulterioară, informații privind scopul secundar respectiv și alte informații necesare. În cazul în care originea datelor cu caracter personal nu a putut fi comunicată persoanei vizate din cauză că au fost utilizate surse diverse, informațiile generale ar trebui furnizate.

(37) O persoană vizată ar trebui să aibă drept de acces la datele cu caracter personal colectate care o privesc și ar trebui să își exercite acest drept cu ușurință și la intervale de timp rezonabile, pentru a fi informată cu privire la prelucrare și pentru a verifica legalitatea acesteia. Acest lucru include dreptul persoanelor vizate de a avea acces la date privind sănătatea lor, de exemplu datele din registrele lor medicale conținând informații precum diagnostice, rezultate ale examinărilor, evaluări ale medicilor curanți și orice tratament sau intervenție efectuată. Orice persoană vizată ar trebui, prin urmare, să aibă dreptul de a cunoaște și de a i se comunica în special scopurile în care sunt prelucrate datele cu caracter personal, dacă este posibil perioada pentru care se prelucrează datele cu caracter personal, destinatarii datelor cu caracter personal, logica de prelucrare automată a datelor cu caracter personal și, cel puțin în cazul în care se bazează pe crearea de profiluri, consecințele unei astfel de prelucrări. Acest drept nu ar trebui să aducă atingere drepturilor sau libertăților altora, inclusiv secretului comercial sau proprietății intelectuale și, în special, drepturilor de autor care asigură protecția programelor software. Cu toate acestea, considerațiile de mai sus nu ar trebui să aibă drept rezultat refuzul de a furniza toate informațiile persoanei vizate. Atunci când operatorul prelucrează un volum mare de informații privind persoana vizată, operatorul ar trebui să poată solicita ca, înainte de a îi fi furnizate informațiile, persoana vizată să precizeze informațiile sau activitățile de prelucrare la care se referă cererea sa.

(38) O persoană vizată ar trebui să aibă dreptul la rectificarea datelor cu caracter personal care o privesc și „dreptul de a fi uitată”, în cazul în care păstrarea acestor date încalcă prezentul regulament sau dreptul Uniunii sub incidența căruia intră operatorul. Persoanele vizate ar trebui să aibă dreptul ca datele lor cu caracter personal să fie șterse și să nu mai fie prelucrate, în cazul în care datele cu caracter personal nu mai sunt necesare pentru scopurile în care sunt colectate sau sunt prelucrate, în cazul în care persoanele vizate și-au retras consimțământul pentru prelucrare sau în cazul în care acestea se opun prelucrării datelor cu caracter personal care le privesc sau în cazul în care prelucrarea datelor cu caracter personal ale acestora nu este conformă cu prezentul regulament. Acest drept este relevant în special în cazul

în care persoana vizată și-a dat consimțământul când era copil și nu cunoștea pe deplin riscurile pe care le implică prelucrarea, iar ulterior dorește să elimine astfel de date cu caracter personal, în special de pe internet. Persoana vizată ar trebui să aibă posibilitatea de a-și exercita acest drept în pofida faptului că nu mai este copil. Cu toate acestea, păstrarea în continuare a datelor cu caracter personal ar trebui să fie legală în cazul în care este necesară pentru exercitarea dreptului la libertatea de exprimare și de informare, pentru respectarea unei obligații legale, pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul, din motive de interes public în domeniul sănătății publice, în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice sau pentru constatarea, exercitarea sau apărarea unui drept în instanță.

(39) Pentru a se consolida „dreptul de a fi uitat" în mediul online, dreptul de ștergere ar trebui să fie extins astfel încât un operator care a făcut publice date cu caracter personal ar trebui să aibă obligația de a informa operatorii care prelucrează respectivele date cu caracter personal să șteargă orice linkuri către datele respective sau copii sau reproduceri ale acestora. În acest scop, operatorul în cauză ar trebui să ia măsuri rezonabile, ținând seama de tehnologia disponibilă și de mijloacele aflate la dispoziția lui, inclusiv măsuri tehnice, pentru a informa operatorii care prelucrează datele cu caracter personal cu privire la cererea persoanei vizate.

(40) Metodele de restricționare a prelucrării de date cu caracter personal ar putea include, printre altele, mutarea temporară a datelor cu caracter personal selectate într-un alt sistem de prelucrare, sau anularea accesului utilizatorilor la datele selectate sau înlăturarea temporară a datelor publicate de pe un site. În ceea ce privește sistemele automatizate de evidență a datelor, restricționarea prelucrării ar trebui, în principiu, asigurată prin mijloace tehnice în așa fel încât datele cu caracter personal să nu facă obiectul unor operațiuni de prelucrare ulterioară și să nu mai poată fi schimbate. Faptul că prelucrarea datelor cu caracter personal este restricționată ar trebui indicat în mod clar în sistem.

(41) Pentru a spori și mai mult controlul asupra propriilor date, persoana vizată ar trebui, în cazul în care datele cu caracter personal sunt prelucrate prin mijloace automate, să poată primi datele cu caracter personal care o privesc și pe care le-a furnizat unui operator, într-un format structurat, utilizat în mod curent, prelucrabil automat și interoperabil și să le poată transmite unui alt operator. Operatorii de date ar trebui să fie încurajați să dezvolte formate interoperabile care să permită portabilitatea datelor. Acest drept ar trebui să se aplice în cazul în care persoana vizată a furnizat datele cu caracter personal pe baza propriului consimțământ sau în cazul în care prelucrarea datelor este necesară pentru executarea unui contract. Prin urmare, acesta nu ar trebui să se aplice în cazul în care prelucrarea de date cu caracter personal este necesară în vederea respectării unei obligații legale căreia îi este supus operatorul sau în cazul îndeplinirii unei sarcini care servește unui interes public sau care rezultă din exercitarea unei autorități publice cu care este învestit operatorul. Dreptul persoanei vizate de a transmite sau de a primi date cu caracter personal care o privesc nu ar trebui să creeze pentru operatori obligația de a adopta sau de a menține sisteme de prelucrare care să fie compatibile din punct de vedere tehnic. În cazul în care, într-un anumit set de date cu caracter personal, sunt implicate mai multe persoane vizate, dreptul de a primi datele cu caracter personal nu ar trebui să aducă atingere drepturilor și libertăților altor persoane vizate, în conformitate cu prezentul regulament. De asemenea, acest drept nu ar trebui să aducă atingere dreptului persoanei vizate de a obține ștergerea datelor cu caracter personal și limitărilor dreptului respectiv, astfel cum se prevede în prezentul regulament, și nu ar trebui, în special, să implice ștergerea acelor date cu caracter personal referitoare la persoana vizată care au fost furnizate de către aceasta în vederea executării unui contract, în măsura în care și atât timp cât datele respective sunt necesare pentru executarea contractului. Persoana vizată ar trebui să aibă dreptul ca datele cu caracter personal să fie transmise direct de la un operator la altul, dacă acest lucru este fezabil din punct de vedere tehnic.

(42) În cazurile în care datele cu caracter personal ar putea fi prelucrate în mod legal, deoarece prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul, o persoană vizată ar trebui să aibă totuși dreptul de a se opune prelucrării oricăror date cu caracter personal care se referă la situația sa particulară. Ar trebui să revină operatorului sarcina de a demonstra că interesele sale legitime și imperioase prevalează asupra intereselor sau a drepturilor și libertăților fundamentale ale persoanei vizate.

(43) Persoana vizată ar trebui să aibă dreptul de a nu face obiectul unei decizii ce poate include o măsură prin care se evaluează aspecte personale legate de persoana vizată, care se bazează exclusiv pe prelucrarea automată și care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă, cum ar fi practicile de recrutare pe cale electronică fără intervenție umană. O astfel de prelucrare include „crearea de profiluri", care constă în orice formă de prelucrare automată a datelor cu caracter personal prin evaluarea aspectelor personale referitoare la o persoană fizică, în special în vederea analizării sau preconizării anumitor aspecte privind

randamentul la locul de muncă al persoanei vizate, situația economică, starea de sănătate, preferințele sau interesele personale, fiabilitatea sau comportamentul, locația sau deplasările, atunci când aceasta produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă.

Cu toate acestea, luarea de decizii pe baza acestei prelucrări, inclusiv crearea de profiluri, ar trebui permisă în cazul în care este autorizată în mod expres de dreptul Uniunii. În orice caz, o astfel de prelucrare ar trebui să facă obiectul unor garanții corespunzătoare, care ar trebui să includă o informare specifică a persoanei vizate și dreptul acesteia de a obține o intervenție umană, de a-și exprima punctul de vedere, de a primi o explicație privind decizia luată în urma unei astfel de evaluări, precum și dreptul de a contesta decizia. O astfel de măsură nu ar trebui să se refere la copii. Pentru a asigura o prelucrare echitabilă și transparentă în ceea ce privește persoana vizată, având în vedere circumstanțele specifice și contextul în care sunt prelucrate datele cu caracter personal, operatorul ar trebui să utilizeze proceduri matematice sau statistice adecvate pentru crearea de profiluri, să implementeze măsuri tehnice și organizatorice adecvate pentru a asigura în special faptul că factorii care duc la inexactități ale datelor cu caracter personal sunt corectați și că riscul de erori este redus la minimum, precum și să securizeze datele cu caracter personal într-un mod care să țină seama de pericolele potențiale la adresa intereselor și drepturilor persoanei vizate și să prevină, printre altele, efectele discriminatorii împotriva persoanelor pe motiv de rasă sau origine etnică, opinii politice, religie sau convingeri, apartenență sindicală, caracteristici genetice, stare de sănătate sau orientare sexuală sau prelucrări care să ducă la măsuri care să aibă astfel de efecte. Procesul decizional automatizat și crearea de profiluri pe baza unor categorii speciale de date cu caracter personal ar trebui permise numai în condiții specifice.

(44) Actele juridice adoptate în temeiul tratatelor sau normele interne adoptate de instituțiile și organele Uniunii în chestiuni referitoare la funcționarea lor pot impune restricții în privința unor principii specifice, în privința dreptului de informare, a dreptului de acces la date cu caracter personal și de rectificare sau ștergere a acestora, în privința dreptului la portabilitatea datelor, a dreptului la confidențialitatea datelor transmise în cadrul comunicațiilor electronice, precum și în privința comunicării unei încălcări a securității datelor cu caracter personal persoanei vizate și a anumitor obligații conexe ale operatorilor, în măsura în care acest lucru este necesar și proporțional într-o societate democratică pentru a se garanta siguranța publică și pentru prevenirea, investigarea și urmărirea penală a infracțiunilor sau executarea pedepselor. Aceasta include protejarea împotriva amenințărilor la adresa securității publice și prevenirea acestora, inclusiv protecția vieții oamenilor, în special ca răspuns la dezastre naturale sau provocate de om, protejarea securității interne a instituțiilor și organelor Uniunii, alte obiective importante de interes public general ale Uniunii sau ale unui stat membru, în special obiectivele politicii externe și de securitate comune a Uniunii sau un interes economic sau financiar important al Uniunii sau al unui stat membru, și păstrarea de registre publice din motive de interes public general sau protecția persoanei vizate ori a drepturilor și libertăților altora, inclusiv protecția socială, sănătatea publică și scopurile umanitare.

(45) Ar trebui să se stabilească responsabilitatea și răspunderea operatorului pentru orice prelucrare a datelor cu caracter personal efectuată de către acesta sau în numele său. În special, operatorul ar trebui să fie obligat să implementeze măsuri adecvate și eficace și să fie în măsură să demonstreze conformitatea activităților de prelucrare cu prezentul regulament, inclusiv eficacitatea măsurilor. Aceste măsuri ar trebui să țină seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscul pentru drepturile și libertățile persoanelor fizice.

(46) Riscul pentru drepturile și libertățile persoanelor fizice, prezentând grade diferite de probabilitate de materializare și de gravitate, poate fi rezultatul unei prelucrări a datelor cu caracter personal care ar putea genera prejudicii de natură fizică, materială sau morală, în special în cazurile în care: prelucrarea poate conduce la discriminare, furt sau fraudă a identității, pierdere financiară, compromiterea reputației, pierderea confidențialității datelor cu caracter personal protejate prin secret profesional, inversarea neautorizată a pseudonimizării sau la orice alt dezavantaj semnificativ de natură economică sau socială; persoanele vizate ar putea fi private de drepturile și libertățile lor sau împiedicate să-și exercite controlul asupra datelor lor cu caracter personal; datele cu caracter personal prelucrate sunt date care dezvăluie originea rasială sau etnică, opiniile politice, religia sau convingerile filozofice, apartenența sindicală, sunt prelucrate date genetice, date privind sănătatea sau date privind viața sexuală sau privind condamnările penale și infracțiunile sau măsurile de securitate conexe; sunt evaluate aspecte de natură personală, în special analizarea sau previzionarea unor aspecte privind randamentul la locul de muncă, situația economică, starea de sănătate, preferințele sau interesele personale, fiabilitatea sau comportamentul, locația sau deplasările, în scopul de a se crea sau de a se utiliza profiluri personale; sunt prelucrate date cu caracter personal ale unor persoane vulnerabile, în special ale unor copii; sau prelucrarea implică un volum mare de date cu caracter personal și afectează un număr larg de persoane vizate.

(47) Probabilitatea de a se materializa și gravitatea riscului pentru drepturile și libertățile persoanei vizate ar trebui să fie determinate în funcție de natura, domeniul de aplicare, contextul și scopurile prelucrării datelor cu caracter personal. Riscul ar trebui apreciat pe baza unei evaluări obiective prin care se stabilește dacă operațiunile de prelucrare a datelor prezintă un risc sau un risc ridicat.

(48) Protecția drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal necesită adoptarea de măsuri tehnice și organizatorice corespunzătoare, pentru a se asigura îndeplinirea cerințelor prezentului regulament. Pentru a putea demonstra conformitatea cu prezentul regulament, operatorul ar trebui să adopte politici interne și să pună în aplicare măsuri care să respecte îndeosebi principiul luării în considerare a protecției datelor începând cu momentul conceperii și pe cel al protecției implicite a datelor. Astfel de măsuri ar putea consta, printre altele, în reducerea la minimum a prelucrării datelor cu caracter personal, pseudonimizarea acestor date cât mai curând posibil, asigurarea transparenței în ceea ce privește funcțiile și prelucrarea datelor cu caracter personal, abilitarea persoanei vizate să monitorizeze prelucrarea datelor, abilitarea operatorului să creeze elemente de siguranță și să le îmbunătățească. Principiul protecției datelor începând cu momentul conceperii și cel al protecției implicite a datelor ar trebui să fie luate în considerare și în contextul licitațiilor publice.

(49) Regulamentul (UE) 2016/679 prevede ca operatorii să demonstreze conformitatea prin aderarea la mecanisme de certificare aprobate. În mod similar, instituțiile și organele Uniunii ar trebui să poată demonstra conformitatea cu prezentul regulament prin obținerea unei certificări în conformitate cu articolul 42 din Regulamentul (UE) 2016/679.

(50) Protecția drepturilor și libertăților persoanelor vizate, precum și responsabilitatea și răspunderea operatorilor și a persoanelor împuternicite de operatori necesită o atribuire clară a responsabilităților în temeiul prezentului regulament, inclusiv în cazul în care un operator stabilește scopurile și mijloacele prelucrării împreună cu alți operatori sau în cazul în care o operațiune de prelucrare este efectuată în numele unui operator.

(51) Pentru a asigura respectarea cerințelor impuse de prezentul regulament în ceea ce privește prelucrarea care trebuie efectuată în numele operatorului de către persoana împuternicită de operator, atunci când încredințează activități de prelucrare unei persoane împuternicite de operator, operatorul ar trebui să utilizeze numai persoane împuternicite de operator care oferă garanții suficiente, în special în ceea ce privește cunoștințele de specialitate, fiabilitatea și resursele, pentru a implementa măsuri tehnice și organizatorice care îndeplinesc cerințele impuse de prezentul regulament, inclusiv pentru securitatea prelucrării. Aderarea persoanelor împuternicite de operator, altele decât instituțiile și organele Uniunii, la un cod de conduită aprobat sau la un mecanism de certificare aprobat poate fi utilizată drept element care să demonstreze respectarea obligațiilor de către operator. Efectuarea prelucrării de către o persoană împuternicită de un operator, alta decât o instituție sau un organ al Uniunii, ar trebui să fie reglementată printr-un contract sau, în cazul instituțiilor și organelor Uniunii care acționează ca persoane împuternicite de operator, printr-un contract sau un alt tip de act juridic, în temeiul dreptului Uniunii, care creează obligații pentru persoana împuternicită de operator în raport cu operatorul și care stabilește obiectul și durata prelucrării, natura și scopurile prelucrării, tipul de date cu caracter personal și categoriile de persoane vizate, și ar trebui să țină seama de sarcinile și responsabilitățile specifice ale persoanei împuternicite de operator în contextul prelucrării care urmează a fi efectuată, precum și de riscul pentru drepturile și libertățile persoanei vizate. Operatorul și persoana împuternicită de operator ar trebui să poată opta pentru recurgerea la un contract individual sau la clauze contractuale standard care sunt adoptate fie direct de Comisie, fie de Autoritatea Europeană pentru Protecția Datelor și, ulterior, de Comisie. După finalizarea prelucrării în numele operatorului, persoana împuternicită de operator ar trebui să returneze sau să șteargă, în funcție de opțiunea operatorului, datele cu caracter personal, cu excepția cazului în care există o cerință de stocare a acestor date cu caracter personal în temeiul dreptului Uniunii sau al dreptului intern care instituie obligații pentru persoana împuternicită de operator.

(52) În vederea demonstrării conformității cu prezentul regulament, operatorii ar trebui să păstreze evidențe ale activităților de prelucrare aflate în responsabilitatea lor, iar persoanele împuternicite de către operator ar trebui să păstreze evidențe ale categoriilor de activități de prelucrare aflate în responsabilitatea lor. Instituțiile și organele Uniunii ar trebui să aibă obligația de a coopera cu Autoritatea Europeană pentru Protecția Datelor și de a își pune evidențele la dispoziția acesteia, la cerere, pentru a putea fi utilizate în scopul monitorizării operațiunilor de prelucrare respective. Cu excepția cazului în care nu este oportun, ținând seama de mărimea unei instituții sau a unui organ al Uniunii, instituțiile și organele Uniunii ar trebui să aibă posibilitatea de a institui un registru central al evidențelor activităților de prelucrare. Din motive de transparență, ele ar trebui, de asemenea, să poată face public acest registru.

(53) În vederea menținerii securității și a prevenirii prelucrărilor care încalcă prezentul regulament, operatorul sau persoana împuternicită de operator ar trebui să evalueze riscurile inerente prelucrării și să implementeze măsuri pentru atenuarea acestor riscuri, cum ar fi criptarea. Măsurile respective ar trebui să asigure un nivel corespunzător de securitate, inclusiv confidențialitatea, luând în considerare stadiul actual al dezvoltării și costurile implementării în

raport cu riscurile și cu natura datelor cu caracter personal a căror protecție trebuie asigurată. La evaluarea riscului pentru securitatea datelor, ar trebui să se acorde atenție riscurilor pe care le prezintă prelucrarea datelor cu caracter personal, cum ar fi distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod, în mod accidental sau ilegal, care pot duce în special la prejudicii fizice, materiale sau morale.

(54) Instituțiile și organele Uniunii ar trebui să asigure confidențialitatea comunicațiilor electronice, astfel cum prevede articolul 7 din Cartă. În special, instituțiile și organele Uniunii ar trebui să asigure securitatea propriilor rețele de comunicații electronice. Acestea ar trebui să protejeze informațiile legate de echipamentele terminale ale utilizatorilor care le oferă acces la site-urile lor internet publice și la aplicațiile lor mobile, în conformitate cu Directiva 2002/58/CE a Parlamentului European și a Consiliului ([1]). Acestea ar trebui, de asemenea, să protejeze confidențialitatea datelor personale stocate în repertoriile cu utilizatori.

(55) Dacă nu este soluționată la timp și într-un mod adecvat, o încălcare a securității datelor cu caracter personal ar putea conduce la prejudicii fizice, materiale sau morale aduse persoanelor fizice Prin urmare, de îndată ce a luat cunoștință de producerea unei încălcări a securității datelor cu caracter personal, operatorul ar trebui să notifice această încălcare Autorității Europene pentru Protecția Datelor, fără întârziere nejustificată și, dacă este posibil, în cel mult 72 de ore după ce a luat la cunoștință de existența acesteia, cu excepția cazului în care operatorul este în măsură să demonstreze, în conformitate cu principiul responsabilității, că încălcarea securității datelor cu caracter personal nu este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice. Atunci când această notificare nu se poate realiza în termen de 72 de ore, ea ar trebui să fie însoțită de o explicație privind întârzierea, iar informațiile pot fi furnizate în mai multe etape, fără altă întârziere nejustificată. În cazul în care această întârziere este justificată, ar trebui comunicate în cel mai scurt termen posibil informații mai puțin sensibile sau mai puțin specifice cu privire la această încălcare, în loc să se soluționeze complet incidentul aflat la originea încălcării înainte de a se proceda la notificare.

(56) Operatorul ar trebui să comunice persoanei vizate o încălcare a securității datelor cu caracter personal, fără întârzieri nejustificate, atunci când încălcarea este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanei fizice, pentru a-i permite să ia măsurile de precauție necesare. Comunicarea ar trebui să descrie natura încălcării securității datelor cu caracter personal și să cuprindă recomandări pentru persoana fizică în cauză în scopul atenuării eventualelor efecte negative. Comunicările către persoanele vizate ar trebui efectuate în cel mai scurt timp posibil în mod rezonabil și în strânsă cooperare cu Autoritatea Europeană pentru Protecția Datelor, respectându-se orientările furnizate de aceasta sau de alte autorități competente, cum ar fi autoritățile de aplicare a legii.

(57) Regulamentul (CE) nr. 45/2001 prevede o obligație generală a unui operator de a notifica prelucrarea datelor cu caracter personal responsabilului cu protecția datelor. Cu excepția cazului în care nu este oportun, ținând seama de mărimea instituției sau a organului Uniunii, responsabilul cu protecția datelor trebuie să țină un registru al operațiunilor de prelucrare ce i-au fost notificate. Pe lângă această obligație generală, ar trebui instituite proceduri și mecanisme eficace de monitorizare a operațiunilor de prelucrare susceptibile să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice prin însăși natura lor, prin domeniul lor de aplicare, prin contextul și prin scopurile lor. Astfel de proceduri ar trebui instituite, de asemenea, în special, în situațiile în care operațiunile de prelucrare presupun utilizarea unor noi tehnologii sau care reprezintă un nou tip de operațiuni în legătură cu care nicio evaluare a impactului asupra protecției datelor nu a fost efectuată anterior de către operator ori când acestea devin necesare dată fiind perioada de timp care s-a scurs de la prelucrarea inițială. În astfel de cazuri, operatorul ar trebui să efectueze, înainte de prelucrare, o evaluare a impactului asupra protecției datelor, în scopul evaluării gradului specific de probabilitate a materializării riscului ridicat și gravitatea acestuia, având în vedere natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și sursele riscului. Respectiva evaluare a impactului ar trebui să includă, în special, măsurile, garanțiile și mecanismele avute în vedere pentru atenuarea riscului respectiv, pentru asigurarea protecției datelor cu caracter personal și pentru demonstrarea conformității cu prezentul regulament.

(58) În cazul în care o evaluare a impactului asupra protecției datelor arată că prelucrarea ar genera, în absența garanțiilor, măsurilor de securitate și mecanismelor de atenuare a riscului, un risc ridicat pentru drepturile și libertățile persoanelor fizice, iar operatorul consideră că riscul nu poate fi atenuat prin mijloace rezonabile sub aspectul tehnologiilor disponibile și al costurilor implementării, Autoritatea Europeană pentru Protecția Datelor ar trebui să fie consultată înainte de începerea activităților de prelucrare. Un astfel de risc ridicat este susceptibil să fie generat de anumite tipuri de prelucrare, precum și de amploarea și frecvența prelucrării, care ar putea duce și la producerea unor prejudicii sau pot atinge drepturile și libertățile persoanelor fizice. Autoritatea Europeană pentru Protecția Datelor ar trebui să răspundă cererii de consultare într-un anumit termen. Cu toate acestea, lipsa unei reacții din

([1]) Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) (JO L 201, 31.7.2002, p. 37).

partea Autorității Europene pentru Protecția Datelor în termenul respectiv ar trebui să nu aducă atingere niciunei intervenții a Autorității Europene pentru Protecția Datelor în conformitate cu sarcinile și competențele sale prevăzute în prezentul regulament, inclusiv competența de a interzice operațiuni de prelucrare. Ca parte a acestui proces de consultare, rezultatul unei evaluări a impactului asupra protecției datelor efectuate cu privire la prelucrarea în cauză ar trebui să poată fi transmis Autorității Europene pentru Protecția Datelor, în special măsurile avute în vedere pentru a atenua riscul pentru drepturile și libertățile persoanelor fizice.

(59) Autoritatea Europeană pentru Protecția Datelor ar trebui să fie informată cu privire la măsurile administrative și consultată cu privire la normele interne adoptate de instituțiile și organele Uniunii în chestiuni legate de funcționarea lor când acestea prevăd prelucrarea de date cu caracter personal, stabilesc condiții cu privire la restricționarea drepturilor persoanelor vizate sau oferă garanții corespunzătoare în ceea ce privește drepturile persoanelor vizate, pentru a asigura că prelucrarea în cauză este conformă cu prezentul regulament și, în special, în ceea ce privește atenuarea riscurilor la care este expusă persoana vizată.

(60) Regulamentul (UE) 2016/679 a instituit Comitetul european pentru protecția datelor, cu statutul de organ independent cu personalitate juridică al Uniunii. Comitetul ar trebui să contribuie la aplicarea consecventă a Regulamentului (UE) 2016/679 și a Directivei (UE) 2016/680 în întreaga Uniune, inclusiv prin oferirea de consiliere Comisiei. În același timp, Autoritatea Europeană pentru Protecția Datelor ar trebui să continue să își exercite funcțiile de supraveghere și de consiliere a tuturor instituțiilor și organelor Uniunii, din proprie inițiativă sau la cerere. Pentru a asigura coerența normelor în materie de protecție a datelor în întreaga Uniune, în momentul în care aceasta elaborează propuneri sau recomandări, Comisia ar trebui să depună eforturi pentru a consulta Autoritatea Europeană pentru Protecția Datelor. Comisia ar trebui să aibă obligația de a organiza o consultare în urma adoptării de acte legislative sau în cursul acțiunilor de pregătire a actelor delegate și a actelor de punere în aplicare, astfel cum sunt definite la articolele 289, 290 și 291 din TFUE, precum și în urma adoptării de recomandări și de propuneri referitoare la acorduri cu țări terțe și organizații internaționale, astfel cum se prevede la articolul 218 din TFUE, care au repercusiuni asupra dreptului la protecția datelor cu caracter personal. În astfel de cazuri, Comisia ar trebui să fie obligată să consulte Autoritatea Europeană pentru Protecția Datelor, cu excepția cazului în care Regulamentul (UE) 2016/679 prevede consultarea obligatorie a Comitetului european pentru protecția datelor, de exemplu cu privire la deciziile privind caracterul adecvat al nivelului de protecție sau actele delegate privind pictogramele standardizate și cerințele referitoare la mecanismele de certificare. Atunci când actul în cauză este deosebit de important pentru protecția drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, Comisia ar trebui să aibă în plus posibilitatea de a consulta Comitetul european pentru protecția datelor. În cazurile respective, Autoritatea Europeană pentru Protecția Datelor, în calitate de membră a Comitetului european pentru protecția datelor, își coordonează activitatea cu comitetul în vederea emiterii unui aviz comun. Autoritatea Europeană pentru Protecția Datelor și, după caz, Comitetul european pentru protecția datelor ar trebui să ofere consiliere în scris în termen de opt săptămâni. Acest termen ar trebui să fie redus în cazuri urgente sau în alte cazuri în care este necesar, de exemplu atunci când Comisia pregătește acte delegate și acte de punere în aplicare.

(61) În conformitate cu articolul 75 din Regulamentul (UE) 2016/679, Autoritatea Europeană pentru Protecția Datelor ar trebui să asigure secretariatul Comitetului european pentru protecția datelor.

(62) În toate instituțiile și organele Uniunii, un responsabil cu protecția datelor ar trebui să asigure aplicarea dispozițiilor prezentului regulament și să ofere consiliere operatorilor și persoanelor împuternicite de operatori în ceea ce privește îndeplinirea obligațiilor ce le revin. Acest responsabil ar trebui să fie o persoană care deține cunoștințe de specialitate în materie de legislație și practici privind protecția datelor la un nivel stabilit mai ales în funcție de operațiunile de prelucrare a datelor efectuate de operator sau de persoana împuternicită de operator, și de nivelul de protecție impus pentru datele cu caracter personal respective. Acești responsabili cu protecția datelor ar trebui să fie în măsură să își îndeplinească îndatoririle și sarcinile în mod independent.

(63) În cazul în care se transferă date cu caracter personal de la instituții și organe ale Uniunii către operatori, persoane împuternicite de operatori sau alți destinatari din țări terțe sau către organizații internaționale, nivelul de protecție a persoanelor fizice asigurat în Uniune prin prezentul regulament ar trebui să fie garantat. Aceleași garanții ar trebui să se aplice inclusiv în cazurile de transferuri ulterioare de date cu caracter personal dinspre țara terță sau organizația internațională către operatori, persoane împuternicite de operatori din aceeași sau dintr-o altă țară terță sau organizație internațională. În orice caz, transferurile către țări terțe și organizații internaționale pot fi realizate numai în conformitate deplină cu prezentul regulament și cu respectarea drepturilor și libertăților fundamentale consacrate de Cartă. Un transfer ar putea avea loc numai dacă, sub rezerva respectării celorlalte dispoziții ale prezentului regulament, operatorul sau persoana împuternicită de operator îndeplinește condițiile prevăzute de dispozițiile prezentului regulament referitoare la transferul de date cu caracter personal către țări terțe sau către organizații internaționale.

(64) Comisia poate să decidă, în temeiul articolului 45 din Regulamentul (UE) 2016/679 sau al articolului 36 din Directiva (UE) 2016/680, că o țară terță, un teritoriu sau un anumit sector dintr-o țară terță sau o organizație internațională asigură un nivel adecvat de protecție a datelor. În aceste cazuri, transferurile de date cu caracter personal efectuate de o instituție sau un organ al Uniunii către țara terță sau organizația internațională respectivă pot avea loc fără a fi necesar să se obțină autorizări suplimentare.

(65) În absența unei decizii privind caracterul adecvat al nivelului de protecție, operatorul sau persoana împuternicită de operator ar trebui să adopte măsuri pentru a compensa lipsa protecției datelor într-o țară terță prin intermediul unor garanții adecvate pentru persoana vizată. Astfel de garanții adecvate pot consta în utilizarea clauzelor standard de protecție a datelor adoptate de Comisie, a clauzelor standard de protecție a datelor adoptate de Autoritatea Europeană pentru Protecția Datelor sau a clauzelor contractuale autorizate de Autoritatea Europeană pentru Protecția Datelor. În cazul în care persoana împuternicită de operator nu este o instituție sau un organ al Uniunii, respectivele garanții corespunzătoare pot consta, de asemenea, în reguli corporative obligatorii, coduri de conduită și mecanisme de certificare utilizate pentru transferurile internaționale efectuate în temeiul Regulamentului (UE) 2016/679. Respectivele garanții ar trebui să asigure respectarea cerințelor în materie de protecție a datelor și drepturi ale persoanelor vizate corespunzătoare prelucrării în interiorul Uniunii, inclusiv disponibilitatea unor drepturi opozabile ale persoanelor vizate și a unor căi de atac eficiente, printre care dreptul de acces la reparații efective pe cale administrativă sau judiciară și dreptul de a solicita despăgubiri, în Uniune sau într-o țară terță. Acestea ar trebui să fie legate în special de respectarea principiilor generale privind prelucrarea datelor cu caracter personal: principiul protecției datelor începând cu momentul conceperii și principiul protecției implicite a datelor. Transferurile pot fi efectuate și de către instituțiile și organele Uniunii către autorități sau organisme publice din țări terțe sau către organizații internaționale cu atribuții și funcții corespunzătoare, inclusiv pe baza dispozițiilor care prevăd drepturi opozabile și efective pentru persoanele vizate, care trebuie introduse în acordurile administrative, cum ar fi un memorandum de înțelegere. Autorizația din partea Autorității Europene pentru Protecția Datelor ar trebui obținută atunci când garanțiile sunt oferite în cadrul unor acorduri administrative fără caracter juridic obligatoriu.

(66) Posibilitatea ca operatorul sau persoana împuternicită de operator să utilizeze clauze standard în materie de protecție a datelor, adoptate de Comisie sau de Autoritatea Europeană pentru Protecția Datelor, nu ar trebui să împiedice operatorii sau persoanele împuternicite de operatori să includă clauzele standard în materie de protecție a datelor într-un contract mai amplu, precum un contract între persoana împuternicită de operator și o altă persoană împuternicită de operator, și nici să adauge alte clauze sau garanții suplimentare, atât timp cât acestea nu contravin, direct sau indirect, clauzelor contractuale standard adoptate de Comisie sau de Autoritatea Europeană pentru Protecția Datelor sau nu prejudiciază drepturile sau libertățile fundamentale ale persoanelor vizate. Operatorii și persoanele împuternicite de operatori ar trebui să fie încurajați să ofere garanții suplimentare prin intermediul unor angajamente contractuale care să completeze clauzele standard în materie de protecție a datelor.

(67) Unele țări terțe au adoptat legi, reglementări și alte acte juridice care au drept obiectiv să reglementeze în mod direct activitățile de prelucrare a datelor ale instituțiilor și organelor Uniunii. Acestea pot include hotărâri ale instanțelor judecătorești sau decizii ale autorităților administrative din țări terțe care solicită unui operator sau unei persoane împuternicite de operator să transfere sau să divulge date cu caracter personal și care nu se bazează pe un acord internațional în vigoare între țara terță solicitantă și Uniune. Aplicarea extrateritorială a acestor legi, reglementări și alte acte juridice poate încălca dreptul internațional și poate împiedica asigurarea protecției persoanelor fizice asigurată în Uniune prin prezentul regulament. Transferurile ar trebui să fie permise numai în cazul îndeplinirii condițiilor prevăzute de prezentul regulament pentru un transfer către țări terțe. Acesta ar putea fi cazul, printre altele, atunci când divulgarea este necesară dintr-un motiv important de interes public recunoscut în dreptul Uniunii.

(68) În situații specifice, ar trebui să se prevadă posibilitatea de a se efectua transferuri în anumite circumstanțe în care persoana vizată și-a dat consimțământul explicit, în care transferul este ocazional și necesar în legătură cu un contract sau cu o acțiune în justiție, indiferent dacă este în contextul unei proceduri judiciare sau în contextul unei proceduri administrative sau extrajudiciare, inclusiv în cadrul procedurilor înaintate organismelor de reglementare. De asemenea, ar trebui să se prevadă posibilitatea de a se efectua transferuri în cazul în care motive importante de interes public stabilite de dreptul Uniunii impun acest lucru sau în cazul în care transferul se efectuează dintr-un registru instituit prin lege și destinat să fie consultat de către public sau de către persoane care au un interes legitim. În acest ultim caz, un astfel de transfer nu ar trebui să implice totalitatea datelor cu caracter personal sau ansamblul categoriilor de date conținute în registru, cu excepția cazului în care este autorizat de dreptul Uniunii, iar atunci când registrul este destinat să fie consultat de persoane care au un interes legitim, transferul ar trebui să fie efectuat doar la cererea persoanelor respective sau dacă acestea sunt destinatarii, luând pe deplin în considerare interesele și drepturile fundamentale ale persoanei vizate.

(69) Aceste derogări ar trebui să se aplice, în special, transferurilor de date solicitate și necesare din considerente importante de interes public, de exemplu în cazul schimbului internațional de date între instituțiile și organele Uniunii și autorități din domeniul concurenței, administrații fiscale sau vamale, autorități de supraveghere financiară și servicii competente în materie de securitate socială sau de sănătate publică, precum în cazul depistării punctelor de contact pentru bolile contagioase sau pentru reducerea și/sau eliminarea dopajului în sport. Un transfer de date cu caracter personal ar trebui, de asemenea, să fie considerat legal în cazul în care este necesar în scopul protejării unui

interes care este esențial pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane, inclusiv pentru integritatea fizică sau pentru viața acesteia, în cazul în care persona vizată nu are capacitatea să își dea consimțământul. În absența unei decizii privind caracterul adecvat al nivelului de protecție, dreptul Uniunii poate, din considerente importante de interes public, stabili în mod expres limite asupra transferului unor categorii specifice de date către o țară terță sau o organizație internațională. Orice transfer către o organizație umanitară internațională al datelor cu caracter personal ale unei persoane vizate care se află în incapacitate fizică sau juridică de a își da consimțământul, în vederea îndeplinirii unei sarcini care decurge din Convențiile de la Geneva sau în vederea conformării cu dreptul internațional umanitar aplicabil în conflictele armate, ar putea fi considerat necesar pentru un motiv important de interes public sau pentru că este în interesul vital al persoanei vizate.

(70) În orice caz, atunci când Comisia nu a luat o decizie cu privire la nivelul adecvat de protecție a datelor dintr-o țară terță, operatorul sau persoana împuternicită de operator ar trebui să utilizeze soluții care să ofere persoanelor vizate drepturi opozabile și efective în ceea ce privește prelucrarea datelor lor în Uniune odată ce aceste date au fost transferate, astfel încât persoanele vizate să beneficieze în continuare de drepturi fundamentale și de garanții.

(71) Fluxul transfrontalier de date cu caracter personal în afara Uniunii poate expune unui risc sporit capacitatea persoanelor fizice de a-și exercita drepturile în materie de protecție a datelor, în special pentru a-și asigura protecția împotriva utilizării sau a divulgării ilegale a acestor informații. În același timp, autoritățile naționale de supraveghere și Autoritatea Europeană pentru Protecția Datelor, se pot afla în imposibilitatea de a trata plângeri sau de a efectua investigații referitoare la activitățile desfășurate în afara competenței lor judiciare. Eforturile acestora de a conlucra în context transfrontalier pot fi, de asemenea, îngreunate de insuficiența competențelor de prevenire sau remediere, de caracterul eterogen al regimurilor juridice și de existența unor obstacole de ordin practic, cum ar fi constrângerile în materie de resurse. Prin urmare, ar trebui să se promoveze o cooperare mai strânsă între Autoritatea Europeană pentru Protecția Datelor și autoritățile naționale de supraveghere, pentru a le ajuta să facă schimb de informații cu omologii lor internaționali.

(72) Instituirea, prin Regulamentul (CE) nr. 45/2001, a Autorității Europene pentru Protecția Datelor, care este împuternicită să își îndeplinească sarcinile și să își exercite competențele în deplină independență, este un element esențial al protecției persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal. Prezentul regulament ar trebui să consolideze și să clarifice și mai mult rolul și independența acestei autorități. Autoritatea Europeană pentru Protecția Datelor ar trebui să fie o persoană care oferă toate garanțiile de independență și care posedă experiența și competențele necesare îndeplinirii atribuțiilor de Autoritate Europeană pentru Protecția Datelor, de exemplu deoarece a fost membru al uneia dintre autoritățile de supraveghere instituite în temeiul articolului 51 din Regulamentul (UE) 2016/679.

(73) Pentru a se asigura coerența monitorizării și aplicării normelor privind protecția datelor în întreaga Uniune, Autoritatea Europeană pentru Protecția Datelor ar trebui să aibă aceleași sarcini și competențe efective ca autoritățile naționale de supraveghere, inclusiv competențe de investigare, competențe corective și de a aplica sancțiuni, competențe de autorizare și de consiliere, în special în cazul plângerilor depuse de persoane fizice, precum și competența de a sesiza Curtea de Justiție cu privire la cazurile de încălcare a prezentului regulament și competența de a acționa în justiție în conformitate cu dreptul primar. Aceste competențe ar trebui să includă și competența de a impune o limitare temporară sau definitivă, inclusiv o interdicție, asupra prelucrării. Pentru a se evita costurile inutile și inconvenientele excesive pentru persoanele în cauză care ar putea fi prejudiciate, fiecare măsură a Autorității Europene pentru Protecția Datelor ar trebui să fie adecvată, necesară și proporțională în vederea asigurării conformității cu dispozițiile prezentului regulament, să ia în considerare circumstanțele fiecărui caz în parte și să respecte dreptul oricărei persoane de a fi audiată înainte de luarea oricărei măsuri individuale în cauză. Fiecare măsură obligatorie din punct de vedere juridic luată de Autoritatea Europeană pentru Protecția Datelor ar trebui să fie prezentată în scris, să fie clară și lipsită de ambiguitate, să indice data emiterii măsurii, să poarte semnătura Autorității Europene pentru Protecția Datelor, să indice motivele pentru care s-a luat măsura și să facă trimitere la dreptul la o cale de atac eficientă.

(74) Competența de supraveghere a Autorității Europene pentru Protecția Datelor nu ar trebui să vizeze prelucrarea datelor cu caracter personal de către Curtea de Justiție atunci când își exercită atribuțiile judiciare, în scopul garantării independenței Curții în îndeplinirea sarcinilor sale judiciare, inclusiv în luarea deciziilor. Pentru astfel de operațiuni de prelucrare, Curtea ar trebui să instituie o supraveghere independentă, în conformitate cu articolul 8 alineatul (3) din Cartă, de exemplu prin intermediul unui mecanism intern.

(75) Deciziile Autorității Europene pentru Protecția Datelor privind excepțiile, garanțiile, autorizațiile și condițiile privind operațiunile de prelucrare a datelor, astfel cum sunt acestea definite în prezentul regulament, ar trebui să fie publicate în raportul de activitate. Independent de publicarea unui raport anual de activitate, Autoritatea Europeană pentru Protecția Datelor poate publica rapoarte pe teme specifice.

(76) Autoritatea Europeană pentru Protecția Datelor ar trebui să respecte Regulamentul (CE) nr. 1049/2001 al Parlamentului European și al Consiliului ([1]).

(77) Autoritățile naționale de supraveghere monitorizează aplicarea Regulamentului (UE) 2016/679 și contribuie la aplicarea coerentă a acestuia în întreaga Uniune, în scopul asigurării protecției persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal și al facilitării liberei circulații a datelor cu caracter personal în cadrul pieței interne. Pentru a asigura un grad sporit de coerență în aplicarea normelor privind protecția datelor în vigoare din statele membre și a normelor privind protecția datelor aplicabile instituțiilor și organelor Uniunii, Autoritatea Europeană pentru Protecția Datelor ar trebui să coopereze în mod eficace cu autoritățile naționale de supraveghere.

(78) În anumite cazuri, dreptul Uniunii prevede un model de supraveghere coordonată, repartizată între Autoritatea Europeană pentru Protecția Datelor și autoritățile naționale de supraveghere. Autoritatea Europeană pentru Protecția Datelor este, de asemenea, autoritatea de supraveghere a Europol și, în acest scop a fost întocmit un anumit model de cooperare cu autoritățile naționale de supraveghere, prin intermediul unui consiliu de cooperare cu rol consultativ. În vederea îmbunătățirii supravegherii și aplicării efective a normelor de fond în materie de protecție a datelor, la nivelul Uniunii ar trebui să se instituie un model unic și coerent de supraveghere coordonată. Prin urmare, Comisia ar trebui să prezinte propuneri legislative, atunci când este cazul, în vederea modificării actelor juridice ale Uniunii care prevăd un model de supraveghere coordonată, pentru a le alinia la modelul de supraveghere coordonată menționat în prezentul regulament. Comitetul european pentru protecția datelor ar trebui să exercite rolul de forum unic pentru asigurarea supravegherii efective coordonate în toate domeniile.

(79) Orice persoană vizată ar trebui să aibă dreptul de a depune o plângere la Autoritatea Europeană pentru Protecția Datelor și dreptul de a introduce o cale de atac eficientă la Curtea de Justiție în conformitate cu tratatele, în cazul în care persoana vizată consideră că drepturile de care se bucură în temeiul prezentului regulament îi sunt încălcate sau în cazul în care Autoritatea Europeană pentru Protecția Datelor nu reacționează la o plângere, respinge sau refuză parțial ori total o plângere sau nu acționează atunci când o astfel de acțiune este necesară pentru asigurarea protecției drepturilor persoanei vizate. Investigația în urma unei plângeri ar trebui să fie efectuată, sub control judiciar, în măsura în care este necesar, în funcție de caz. Autoritatea Europeană pentru Protecția Datelor ar trebui să informeze persoana vizată cu privire la stadiul în care se află plângerea și cu privire la soluționarea acesteia într-un termen rezonabil. În eventualitatea în care cazul necesită coordonarea ulterioară cu o autoritate națională de supraveghere, ar trebui să se furnizeze informații intermediare persoanei vizate. În vederea facilitării depunerii plângerilor, Autoritatea Europeană pentru Protecția Datelor ar trebui să ia măsuri precum punerea la dispoziție a unui formular de depunere a plângerii, care să poată fi completat inclusiv în format electronic, fără a exclude alte mijloace de comunicare.

(80) Orice persoană care a suferit un prejudiciu material sau moral ca urmare a unei încălcări a prezentului regulament ar trebui să aibă dreptul de a obține despăgubiri de la operator sau de la persoana împuternicită de operator pentru prejudiciul suferit, în condițiile prevăzute în tratate.

(81) În vederea întăririi rolului de supraveghere exercitat de Autoritatea Europeană pentru Protecția Datelor și a punerii efective în aplicare a prezentului regulament, Autoritatea Europeană pentru Protecția Datelor ar trebui să aibă competența de a aplica amenzi administrative, ca sancțiune de ultimă instanță. Aceste amenzi ar trebui să urmărească sancționarea mai degrabă a instituției sau a organului Uniunii în cauză, decât a persoanelor fizice, în caz de nerespectare a prezentului regulament, astfel încât să descurajeze viitoare încălcări ale prezentului regulament și să promoveze o cultură a protecției datelor cu caracter personal în instituțiile și organele Uniunii. Prezentul regulament ar trebui să indice încălcările care fac obiectul unor amenzi administrative și limitele maxime și criteriile pentru stabilirea amenzilor aferente. Autoritatea Europeană pentru Protecția Datelor ar trebui să determine cuantumul amenzii în fiecare caz în parte, ținând seama de toate circumstanțele relevante ale situației specifice, luându-se în considerare în mod corespunzător natura, gravitatea și durata încălcării, consecințele acesteia și măsurile luate pentru a se asigura respectarea obligațiilor prevăzute de prezentul regulament și pentru a se preveni sau atenua consecințele încălcării. Atunci când aplică o amendă administrativă unei instituții sau unui organ al Uniunii, Autoritatea Europeană pentru Protecția Datelor ar trebui să ia în considerare proporționalitatea cuantumului amenzii. Procedura administrativă de aplicare a amenzilor instituțiilor și organelor Uniunii ar trebui să respecte principiile generale ale dreptului Uniunii, astfel cum sunt interpretate de Curtea de Justiție.

(82) În cazul în care persoana vizată consideră că drepturile de care beneficiază în temeiul prezentului regulament îi sunt încălcate, aceasta ar trebui să aibă dreptul de a mandata un organism, o organizație sau o asociație fără scop lucrativ care este înființat(ă) în conformitate cu dreptul Uniunii sau cu dreptul intern al unui stat membru, ale cărui (cărei) obiective statutare sunt în interesul public și care își desfășoară activitatea în domeniul asigurării protecției datelor cu

([1]) Regulamentul (CE) nr. 1049/2001 al Parlamentului European și al Consiliului din 30 mai 2001 privind accesul public la documentele Parlamentului European, ale Consiliului și ale Comisiei (JO L 145, 31.5.2001, p. 43).

caracter personal, să depună o plângere în numele său la Autoritatea Europeană pentru Protecția Datelor. Un astfel de organism, organizație sau asociație ar trebui, de asemenea, să fie în măsură să exercite dreptul la o cale de atac în numele persoanelor vizate sau să exercite dreptul de a primi despăgubiri în numele persoanelor vizate.

(83) Împotriva funcționarilor sau altor agenți ai Uniunii care nu respectă obligațiile ce le revin în temeiul dispozițiilor prezentului regulament ar trebui să se poată lua măsuri disciplinare sau alt tip de măsuri, în conformitate cu normele și procedurile prevăzute în Statutul funcționarilor Uniunii Europene și în Regimul aplicabil celorlalți agenți ai Uniunii Europene, stabilite prin Regulamentul (CEE, Euratom, CECA) nr. 259/68 al Consiliului ([1]) („Statutul funcționarilor").

(84) În vederea asigurării unor condiții uniforme de punere în aplicare a prezentului regulament, Comisia ar trebui învestită cu competențe de executare. Competențele respective ar trebui să fie exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului ([2]). Procedura de examinare ar trebui utilizată pentru adoptarea de clauze contractuale standard între operatori și persoanele împuternicite de operatori, precum și între persoanele împuternicite de operatori, pentru adoptarea unei liste a operațiunilor de prelucrare în cazul cărora este necesară o consultare prealabilă a Autorității Europene pentru Protecția Datelor de către operatorii care efectuează activități de prelucrare a datelor cu caracter personal necesare pentru îndeplinirea unei sarcini de interes public, precum și pentru adoptarea unor clauze contractuale standard care oferă garanții adecvate pentru transferurile internaționale.

(85) Informațiile confidențiale pe care autoritățile statistice de la nivelul Uniunii și de la nivel național le colectează în vederea elaborării de statistici europene și naționale oficiale ar trebui să fie protejate. Statisticile europene ar trebui concepute, elaborate și difuzate în conformitate cu principiile statistice prevăzute la articolul 338 alineatul (2) din TFUE. Regulamentul (CE) nr. 223/2009 al Parlamentului European și al Consiliului ([3]) prevede specificații suplimentare privind confidențialitatea datelor statistice pentru statisticile europene.

(86) Regulamentul (CE) nr. 45/2001 și Decizia nr. 1247/2002/CE a Parlamentului European, a Consiliului și a Comisiei ([4]) ar trebui abrogate. Trimiterile la regulamentul și la decizia abrogate ar trebui interpretate ca trimiteri la prezentul regulament.

(87) În scopul garantării independenței depline a membrilor autorității independente de supraveghere, prezentul regulament nu ar trebui să aducă atingere mandatelor actualei Autorități Europene pentru Protecția Datelor și a actualului său adjunct. Actualul adjunct al acestei autorități ar trebui să rămână în funcție până la sfârșitul mandatului său, cu excepția cazului în care este îndeplinită una dintre condițiile prevăzute de prezentul regulament pentru încetarea anticipată a mandatului Autorității Europene pentru Protecția Datelor. Dispozițiile relevante ale prezentului regulament ar trebui să se aplice adjunctului Autorității Europene pentru Protecția Datelor până la sfârșitul mandatului său.

(88) În conformitate cu principiul proporționalității, este necesar și oportun, în vederea realizării obiectivului fundamental al asigurării unui nivel echivalent de protecție a persoanelor fizice cu privire la prelucrarea datelor cu caracter personal și al liberei circulații a datelor cu caracter personal în întreaga Uniune, să se stabilească norme privind prelucrarea datelor cu caracter personal în instituțiile și organele Uniunii. Prezentul regulament nu depășește ceea ce este necesar pentru realizarea obiectivelor urmărite, în conformitate cu articolul 5 alineatul (4) din TUE.

(89) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001 și a emis un aviz la 15 martie 2017 ([5]),

---

([1]) JO L 56, 4.3.1968, p. 1.

([2]) Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului din 16 februarie 2011 de stabilire a normelor și principiilor generale privind mecanismele de control de către statele membre al exercitării competențelor de executare de către Comisie (JO L 55, 28.2.2011, p. 13).

([3]) Regulamentul (CE) nr. 223/2009 al Parlamentului European și al Consiliului din 11 martie 2009 privind statisticile europene și de abrogare a Regulamentului (CE, Euratom) nr. 1101/2008 al Parlamentului European și al Consiliului privind transmiterea de date statistice confidențiale Biroului Statistic al Comunităților Europene, a Regulamentului (CE) nr. 322/97 al Consiliului privind statisticile comunitare și a Deciziei 89/382/CEE, Euratom a Consiliului de constituire a Comitetului pentru programele statistice ale Comunităților Europene (JO L 87, 31.3.2009, p. 164).

([4]) Decizia nr. 1247/2002/CE a Parlamentului European, a Consiliului și a Comisiei din 1 iulie 2002 privind statutul și condițiile generale de exercitare a atribuțiilor Autorității Europene pentru Protecția Datelor (JO L 183, 12.7.2002, p. 1).

([5]) JO C 164, 24.5.2017, p. 2.

ADOPTĂ PREZENTUL REGULAMENT:

CAPITOLUL I

DISPOZIȚII GENERALE

Articolul 1

Obiect și obiective

(1) Prezentul regulament stabilește normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile și organele Uniunii precum și normele referitoare la libera circulație a datelor cu caracter personal între acestea sau către alți destinatari stabiliți în Uniune.

(2) Prezentul regulament asigură protecția drepturilor și libertăților fundamentale ale persoanelor fizice și, în special, a dreptului acestora la protecția datelor cu caracter personal.

(3) Autoritatea Europeană pentru Protecția Datelor monitorizează aplicarea dispozițiilor prezentului regulament în ceea ce privește toate operațiunile de prelucrare efectuate de către o instituție sau un organ al Uniunii.

Articolul 2

Domeniul de aplicare

(1) Prezentul regulament se aplică prelucrării datelor cu caracter personal efectuate de toate instituțiile și organele Uniunii.

(2) Doar articolul 3 și capitolul IX din prezentul regulament se aplică prelucrării datelor operaționale cu caracter personal efectuate de organele, oficiile și agențiile Uniunii atunci când acestea desfășoară activități care intră sub incidența părții a treia titlul V capitolul 4 sau capitolul 5 din TFUE.

(3) Prezentul regulament nu se aplică prelucrării datelor operaționale cu caracter personal efectuate de Europol și de Parchetul European, până la adaptarea Regulamentului (UE) 2016/794 al Parlamentului European și al Consiliului ([1]) și a Regulamentului (UE) 2017/1939 al Consiliului ([2]) în conformitate cu articolul 98 din prezentul regulament.

(4) Prezentul regulament nu se aplică prelucrării datelor cu caracter personal de către misiunile menționate la articolul 42 alineatul (1) și la articolele 43 și 44 din TUE.

(5) Prezentul regulament se aplică prelucrării datelor cu caracter personal, efectuate total sau parțial prin mijloace automatizate, precum și prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidență sau care sunt destinate să facă parte dintr-un sistem de evidență.

Articolul 3

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

1. „date cu caracter personal” înseamnă orice informație privind o persoană fizică identificată sau identificabilă („persoana vizată”); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale a persoanei fizice respective;

2. „date operaționale cu caracter personal” înseamnă toate datele cu caracter personal prelucrate de organe, oficii sau agenții ale Uniunii care desfășoară activități care intră sub incidența părții a treia titlul V capitolul 4 sau capitolul 5 din TFUE în vederea îndeplinirii obiectivelor și sarcinilor prevăzute în actele juridice de înființare a respectivelor organe, oficii sau agenții;

([1]) Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului din 11 mai 2016 privind Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) și de înlocuire și de abrogare a Deciziilor 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI și 2009/968/JAI ale Consiliului (JO L 135, 24.5.2016, p. 53).

([2]) Regulamentul (UE) 2017/1939 al Consiliului din 12 octombrie 2017 de punere în aplicare a unei forme de cooperare consolidată în ceea ce privește instituirea Parchetului European (EPPO) (JO L 283, 31.10.2017, p. 1).

3. „prelucrare” înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;

4. „restricționarea prelucrării” înseamnă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;

5. „creare de profiluri” înseamnă orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia;

6. „pseudonimizare” înseamnă prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;

7. „sistem de evidență a datelor” înseamnă orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcționale sau geografice;

8. „operator” înseamnă instituția sau organul Uniunii ori direcția generală sau orice altă entitate organizațională care stabilește, singură sau împreună cu altele, scopurile și mijloacele de prelucrare a datelor cu caracter personal; în cazul în care scopurile și mijloacele prelucrării sunt stabilite printr-un act specific al Uniunii, dreptul Uniunii poate stabili operatorul sau criteriile specifice necesare desemnării acestuia;

9. „operatori, alții decât instituții și organe ale Uniunii” înseamnă operatori în sensul articolului 4 punctul 7 din Regulamentul (UE) 2016/679 și operatori în sensul articolului 3 punctul 8 din Directiva (UE) 2016/680;

10. „instituții și organe ale Uniunii” înseamnă instituțiile, organele, oficiile și agențiile înființate prin TUE, TFUE sau Tratatul Euratom sau în temeiul acestora;

11. „autoritate competentă” înseamnă orice autoritate publică a unui stat membru competentă în materie de prevenire, depistare, investigare sau urmărire penală a infracțiunilor sau de executare a pedepselor, inclusiv în materie de protejare împotriva amenințărilor la adresa securității publice și de prevenire a acestora;

12. „persoană împuternicită de operator” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează date cu caracter personal în numele operatorului;

13. „destinatar” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Cu toate acestea, autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autoritățile publice în cauză respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării;

14. „parte terță” înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;

15. „consimțământ” al persoanei vizate înseamnă orice manifestare de voință liberă, specifică, în cunoștință de cauză și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune pozitivă fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;

16. „încălcarea securității datelor cu caracter personal” înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate în alt mod, sau la accesul neautorizat la acestea;

17. „date genetice” înseamnă datele cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care oferă informații unice privind fiziologia sau sănătatea persoanei respective și care rezultă, în special, dintr-o analiză a unei mostre de material biologic recoltate de la persoana în cauză;

18. „date biometrice” înseamnă date cu caracter personal rezultate din aplicarea unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice, care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice;

19. „date privind sănătatea” înseamnă date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia;

20. „serviciile societății informaționale” înseamnă un serviciu astfel cum este definit la articolul 1 alineatul (1) litera (b) din Directiva (UE) 2015/1535 a Parlamentului European și a Consiliului ([1]);

21. „organizație internațională” înseamnă o organizație și organismele sale subordonate reglementate de dreptul internațional public sau orice alt organism care este instituit printr-un acord încheiat între două sau mai multe țări sau în temeiul unui astfel de acord;

22. „autoritate națională de supraveghere” înseamnă o autoritate publică independentă înființată de un stat membru în temeiul articolului 51 din Regulamentul (UE) 2016/679 sau în temeiul articolului 41 din Directiva (UE) 2016/680;

23. „utilizator” înseamnă orice persoană fizică care folosește o rețea sau un echipament terminal care funcționează sub controlul unei instituții sau al unui organ al Uniunii;

24. „anuar” înseamnă un repertoriu al utilizatorilor accesibil publicului sau un repertoriu intern al utilizatorilor disponibil într-o instituție sau într-un organ al Uniunii sau partajat între instituții și organe ale Uniunii, indiferent dacă este tipărit sau în format electronic;

25. „rețea de comunicații electronice” înseamnă un sistem de transmisie, indiferent dacă este bazat pe o infrastructură permanentă sau pe o capacitate de administrare centralizată, și, după caz, echipamente de comutare sau de rutare și alte resurse, inclusiv elemente de rețea care nu sunt active, care permit transmiterea semnalelor prin cablu, unde radio, prin mijloace optice sau prin alte mijloace electromagnetice, inclusiv rețele de comunicații prin satelit, rețele terestre fixe (cu comutare de circuite și cu comutare de pachete, inclusiv internet) și mobile, rețele electrice, în măsura în care sunt utilizate pentru transmiterea de semnale, rețele utilizate pentru difuzarea programelor de radio și de televiziune și rețele de televiziune prin cablu, indiferent de tipul de informație transmisă;

26. „echipament terminal” înseamnă echipament terminal astfel cum este definit la articolul 1 punctul 1 din Directiva 2008/63/CE a Comisiei ([2]).

CAPITOLUL II

PRINCIPII GENERALE

Articolul 4

Principii legate de prelucrarea datelor cu caracter personal

(1) Datele cu caracter personal sunt:

(a) prelucrate în mod legal, echitabil și transparent față de persoana vizată („legalitate, echitate și transparență”);

(b) colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice nu este considerată, în conformitate cu articolul 13, incompatibilă cu scopurile inițiale („limitări în funcție de scop”);

(c) adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate („reducerea la minimum a datelor”);

(d) exacte și, dacă este necesar, actualizate; trebuie să se ia toate măsurile rezonabile pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere („exactitate”);

([1]) Directiva (UE) 2015/1535 a Parlamentului European și a Consiliului din 9 septembrie 2015 referitoare la procedura de furnizare de informații în domeniul reglementărilor tehnice și al normelor privind serviciile societății informaționale (JO L 241, 17.9.2015, p. 1).

([2]) Directiva 2008/63/CE a Comisiei din 20 iunie 2008 privind concurența pe piețele echipamentelor terminale pentru telecomunicații (JO L 162, 21.6.2008, p. 20).

(e) păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele cu caracter personal; datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu articolul 13, sub rezerva punerii în aplicare a măsurilor de ordin tehnic și organizatoric adecvate prevăzute în prezentul regulament în vederea garantării drepturilor și libertăților persoanei vizate („limitări legate de stocare”);

(f) prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare („integritate și confidențialitate”).

(2) Operatorul este responsabil de respectarea alineatului (1) și poate demonstra această respectare („responsabilitate”).

Articolul 5

Legalitatea prelucrării

(1) Prelucrarea este legală numai dacă și în măsura în care se aplică cel puțin una dintre următoarele condiții:

(a) prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestită instituția sau organul Uniunii;

(b) prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;

(c) prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;

(d) persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;

(e) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice.

(2) Temeiurile pentru prelucrarea menționată la alineatul (1) literele (a) și (b) sunt prevăzute în dreptul Uniunii.

Articolul 6

Prelucrarea într-un alt scop compatibil

În cazul în care prelucrarea în alt scop decât cel pentru care datele cu caracter personal au fost colectate nu se bazează pe consimțământul persoanei vizate sau pe dreptul Uniunii care constituie o măsură necesară și proporțională într-o societate democratică pentru a proteja obiectivele menționate la articolul 25 alineatul (1), operatorul, pentru a stabili dacă prelucrarea în alt scop este compatibilă cu scopul pentru care datele cu caracter personal au fost colectate inițial, ia în considerare, printre altele:

(a) orice legătură dintre scopurile în care datele cu caracter personal au fost colectate și scopurile prelucrării ulterioare preconizate;

(b) contextul în care datele cu caracter personal au fost colectate, în special în ceea ce privește relația dintre persoanele vizate și operator;

(c) natura datelor cu caracter personal, în special în cazul prelucrării unor categorii speciale de date cu caracter personal, în conformitate cu articolul 10, sau în cazul în care sunt prelucrate date cu caracter personal referitoare la condamnări penale și infracțiuni, în conformitate cu articolul 11;

(d) posibilele consecințe asupra persoanelor vizate ale prelucrării ulterioare preconizate;

(e) existența unor garanții adecvate, care pot include criptarea sau pseudonimizarea.

Articolul 7

Condiții privind consimțământul

(1) În cazul în care prelucrarea se bazează pe consimțământ, operatorul trebuie să fie în măsură să demonstreze că persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal.

(2) În cazul în care consimțământul persoanei vizate este dat în contextul unei declarații scrise care se referă și la alte aspecte, cererea privind consimțământul trebuie să fie prezentată într-o formă care o diferențiază în mod clar de celelalte aspecte, într-o formă inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu. Nicio parte a respectivei declarații care constituie o încălcare a prezentului regulament nu este obligatorie.

(3) Persoana vizată are dreptul să își retragă în orice moment consimțământul. Retragerea consimțământului nu afectează legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia. Înainte de acordarea consimțământului, persoana vizată este informată cu privire la acest lucru. Retragerea consimțământului se face la fel de simplu ca acordarea acestuia.

(4) Atunci când se evaluează dacă consimțământul este dat în mod liber, se ține seama cât mai mult de faptul că, printre altele, executarea unui contract, inclusiv prestarea unui serviciu, este condiționată de consimțământul cu privire la prelucrarea datelor cu caracter personal care nu este necesară pentru executarea acestui contract.

Articolul 8

Condiții aplicabile în ceea ce privește consimțământul copilului în legătură cu serviciile societății informaționale

(1) În cazul în care se aplică articolul 5 alineatul (1) litera (d), în ceea ce privește oferirea de servicii ale societății informaționale în mod direct unui copil, prelucrarea datelor cu caracter personal ale unui copil este legală dacă copilul are cel puțin vârsta de 13 ani. Dacă copilul are sub vârsta de 13 ani, respectiva prelucrare este legală numai dacă și în măsura în care consimțământul respectiv este acordat sau autorizat de titularul răspunderii părintești asupra copilului.

(2) Operatorul depune toate eforturile rezonabile pentru a verifica în astfel de cazuri că titularul răspunderii părintești asupra copilului a acordat sau a autorizat consimțământul, ținând seama de tehnologiile disponibile.

(3) Alineatul (1) nu afectează dreptul general al contractelor aplicabil în statele membre, cum ar fi normele privind valabilitatea, încheierea sau efectele unui contract în legătură cu un copil.

Articolul 9

Transmiterile de date cu caracter personal către destinatari stabiliți în Uniune, alții decât instituțiile și organele Uniunii

(1) Fără a aduce atingere articolelor 4-6 și 10, datele cu caracter personal se transmit destinatarilor stabiliți în Uniune, alții decât instituții și organe ale Uniunii, numai dacă:

(a) destinatarul demonstrează că datele sunt necesare pentru îndeplinirea unei sarcini de interes public sau în exercitarea autorității publice cu care este învestit destinatarul; sau

(b) destinatarul stabilește că transmiterea datelor este necesară într-un scop specific de interes public, iar operatorul, în cazul în care are motive să presupună că interesele legitime ale persoanei vizate ar putea fi prejudiciate, stabilește că transmiterea datelor cu caracter personal pentru acel scop specific este proporțională, după ce a evaluat, într-un mod demonstrabil, diversele interese concurente.

(2) În cazul în care operatorul inițiază transmiterea în temeiul prezentului articol, acesta trebuie să demonstreze că transmiterea datelor cu caracter personal este necesară și proporțională cu scopul transmiterii, prin aplicarea criteriilor stabilite la alineatul (1) litera (a) sau (b).

(3) Instituțiile și organele Uniunii asigură echilibrul între dreptul la protecția datelor cu caracter personal și dreptul de acces la documente în conformitate cu dreptul Uniunii.

Articolul 10

Prelucrarea de categorii speciale de date cu caracter personal

(1) Se interzice prelucrarea datelor cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea datelor genetice, a datelor biometrice pentru identificarea unică a unei persoane fizice, a datelor privind sănătatea sau a datelor privind viața sexuală sau orientarea sexuală a unei persoane fizice.

(2) Alineatul (1) nu se aplică în următoarele situații:

(a) persoana vizată și-a dat consimțământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri precizate, cu excepția cazului în care dreptul Uniunii prevede ca interdicția menționată la alineatul (1) să nu poată fi ridicată prin consimțământul persoanei vizate;

(b) prelucrarea este necesară în scopul îndeplinirii obligațiilor și al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forței de muncă și al securității sociale și protecției sociale, în măsura în care această prelucrare este autorizată de dreptul Uniunii care prevede garanții adecvate pentru drepturile fundamentale și interesele persoanei vizate;

(c) prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale altei persoane, atunci când persoana vizată se află în incapacitate fizică sau juridică de a-și da consimțământul;

(d) prelucrarea este efectuată, în cadrul activităților sale legitime și cu garanții adecvate, de către un organism cu scop nelucrativ care constituie o entitate integrată într-o instituție sau un organ al Uniunii, care urmărește un obiectiv politic, filozofic, religios sau sindical, cu condiția ca prelucrarea să se refere numai la membrii sau la foștii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente în legătură cu scopurile sale și ca datele să nu fie comunicate terților fără consimțământul persoanelor vizate;

(e) prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod manifest de către persoana vizată;

(f) prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept sau ori de câte ori Curtea de Justiție acționează în exercițiul funcției sale judiciare;

(g) prelucrarea este necesară din motive de interes public major, în temeiul unei dispoziții din dreptul Uniunii care este proporțională cu obiectivul urmărit, respectă esența dreptului la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate;

(h) prelucrarea este necesară în scopuri legate de medicina preventivă sau a muncii, de evaluarea capacității de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistență medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor și serviciilor de sănătate sau de asistență socială, în temeiul dreptului Uniunii sau în temeiul unui contract încheiat cu un cadru medical și sub rezerva respectării condițiilor și garanțiilor prevăzute la alineatul (3);

(i) prelucrarea este necesară din motive de interes public în domeniul sănătății publice, cum ar fi protecția împotriva amenințărilor transfrontaliere grave la adresa sănătății sau asigurarea de standarde ridicate de calitate și siguranță a asistenței medicale și a medicamentelor sau a dispozitivelor medicale, în temeiul dreptului Uniunii care prevăd măsuri adecvate și specifice pentru protejarea drepturilor și libertăților persoanei vizate, în special a secretului profesional; sau

(j) prelucrarea este necesară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în baza dispozițiilor dreptului Uniunii care sunt proporționale cu obiectivul urmărit, respectă esența dreptului la protecția datelor și prevăd măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate.

(3) Datele cu caracter personal menționate la alineatul (1) se pot prelucra pentru scopurile menționate la alineatul (2) litera (h) în cazul în care datele respective sunt prelucrate de către un profesionist supus obligației de păstrare a secretului profesional sau sub responsabilitatea acestuia, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul normelor stabilite de organisme naționale competente, sau de către o altă persoană care este, de asemenea, supusă unei obligații de confidențialitate în temeiul dreptului Uniunii sau al dreptului intern ori al unor normelor stabilite de organisme naționale competente.

Articolul 11

Prelucrarea datelor cu caracter personal referitoare la condamnări penale și infracțiuni

Prelucrarea de date cu caracter personal referitoare la condamnări penale și infracțiuni sau la măsuri de securitate conexe în temeiul articolului 5 alineatul (1) se efectuează numai sub controlul autorității de stat sau atunci când prelucrarea este autorizată de dreptul Uniunii care prevede garanții adecvate pentru drepturile și libertățile persoanelor vizate.

Articolul 12

Prelucrarea care nu necesită identificare

(1) În cazul în care scopurile pentru care un operator prelucrează date cu caracter personal nu necesită sau nu mai necesită identificarea unei persoane vizate de către operator, operatorul nu are obligația de a păstra, obține sau prelucra informații suplimentare pentru a identifica persoana vizată în scopul unic al respectării prezentului regulament.

(2) Dacă, în cazurile menționate la alineatul (1) din prezentul articol, operatorul poate demonstra că nu este în măsură să identifice persoana vizată, operatorul informează persoana vizată în mod corespunzător, în cazul în care este posibil. În astfel de cazuri, articolele 17-22 nu se aplică, cu excepția cazului în care persoana vizată, în scopul exercitării drepturilor sale în temeiul respectivelor articole, oferă informații suplimentare care permit identificarea sa.

Articolul 13

Garanții privind prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice

Prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice are loc cu condiția existenței unor garanții corespunzătoare, în conformitate cu prezentul regulament, pentru drepturile și libertățile persoanelor vizate. Respectivele garanții asigură faptul că au fost instituite măsuri tehnice și organizatorice necesare pentru a se asigura, în special, respectarea principiului reducerii la minimum a datelor. Respectivele măsuri pot include pseudonimizarea, cu condiția ca respectivele scopuri să fie îndeplinite în acest mod. Atunci când respectivele scopuri pot fi îndeplinite printr-o prelucrare ulterioară care nu permite sau nu mai permite identificarea persoanelor vizate, scopurile respective sunt îndeplinite în acest mod.

CAPITOLUL III

DREPTURILE PERSOANEI VIZATE

SECȚIUNEA 1

Transparență și modalități

Articolul 14

Transparența informațiilor, a comunicărilor și a modalităților de exercitare a drepturilor persoanei vizate

(1) Operatorul ia măsuri adecvate pentru a furniza persoanei vizate orice informații menționate la articolele 15 și 16 și pentru a efectua orice comunicări în temeiul articolelor 17-24 și 35 referitoare la prelucrare, într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu, în special pentru orice informații adresate în mod specific unui copil. Informațiile se furnizează în scris sau prin alte mijloace, inclusiv, atunci când este oportun, în format electronic. La solicitarea persoanei vizate, informațiile pot fi furnizate verbal, cu condiția ca identitatea persoanei vizate să fie dovedită prin alte mijloace.

(2) Operatorul facilitează exercitarea drepturilor persoanei vizate prevăzute la articolele 17-24. În cazurile menționate la articolul 12 alineatul (2), operatorul nu refuză să dea curs cererii persoanei vizate de a-și exercita drepturile prevăzute la articolele 17-24, cu excepția cazului în care operatorul demonstrează că nu este în măsură să identifice persoana vizată.

(3) Operatorul furnizează persoanei vizate informații privind acțiunile întreprinse în urma unei cereri în temeiul articolelor 17-24, fără întârzieri nejustificate și, în orice caz, în cel mult o lună de la primirea cererii. Această perioadă poate fi prelungită cu două luni atunci când este necesar, ținându-se seama de complexitatea și numărul cererilor. Operatorul informează persoana vizată cu privire la orice astfel de prelungire, în termen de o lună de la primirea cererii, prezentând și motivele întârzierii. În cazul în care persoana vizată introduce o cerere în format electronic, informațiile sunt furnizate în format electronic acolo unde este posibil, cu excepția cazului în care persoana vizată solicită un alt format.

(4) Dacă nu ia măsuri cu privire la cererea persoanei vizate, operatorul informează persoana vizată, fără întârziere și în termen de cel mult o lună de la primirea cererii, cu privire la motivele pentru care nu ia măsuri și la posibilitatea de a depune o plângere la Autoritatea Europeană pentru protecția Datelor și de a introduce o cale de atac judiciară.

(5) Informațiile furnizate în temeiul articolelor 15 și 16, orice comunicare și orice măsuri luate în temeiul articolelor 17-24 și 35 sunt gratuite. În cazul în care cererile din partea unei persoane vizate sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, operatorul poate refuza să dea curs cererii. Operatorului îi revine sarcina de a demonstra caracterul vădit nefondat sau excesiv al cererii.

(6) Fără a aduce atingere articolului 12, în cazul în care are îndoieli întemeiate cu privire la identitatea persoanei fizice care înaintează cererea menționată la articolele 17-23, operatorul poate solicita furnizarea de informații suplimentare necesare pentru a confirma identitatea persoanei vizate.

(7) Informațiile care urmează să fie furnizate persoanelor vizate în temeiul articolelor 15 și 16 pot fi furnizate în combinație cu pictograme standardizate pentru a oferi într-un mod ușor vizibil, inteligibil și clar lizibil o imagine de ansamblu semnificativă asupra prelucrării avute în vedere. În cazul în care pictogramele sunt prezentate în format electronic, acestea trebuie să poată fi citite automat.

(8) În cazul în care Comisia adoptă acte delegate în temeiul articolului 12 alineatul (8) din Regulamentul (UE) 2016/679 în vederea stabilirii informațiilor care trebuie să fie prezentate de pictograme și a procedurilor pentru furnizarea de pictograme standardizate, instituțiile și organele Uniunii, acolo unde este cazul, pun la dispoziție informațiile furnizate în temeiul articolelor 15 și 16 din prezentul regulament în combinație cu aceste pictograme standardizate.

SECȚIUNEA 2

informare și acces la date cu caracter personal

Articolul 15

Informații care se furnizează în cazul în care date cu caracter personal sunt colectate de la persoana vizată

(1) În cazul în care date cu caracter personal referitoare la o persoană vizată se colectează de la aceasta, operatorul, în momentul obținerii acestor date cu caracter personal, furnizează persoanei vizate toate informațiile următoare:

(a) identitatea și datele de contact ale operatorului;

(b) datele de contact ale responsabilului cu protecția datelor;

(c) scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării;

(d) destinatarii sau categoriile de destinatari ai datelor cu caracter personal, după caz;

(e) dacă este cazul, intenția operatorului de a transfera date cu caracter personal către o țară terță sau o organizație internațională și existența sau absența unei decizii a Comisiei privind caracterul adecvat al nivelului de protecție sau, în cazul transferurilor menționate la articolul 48, o trimitere la garanțiile adecvate sau corespunzătoare și mijloacele de a obține o copie a acestora, în cazul în care au fost puse la dispoziție.

(2) În plus față de informațiile menționate la alineatul (1), în momentul în care datele cu caracter personal sunt obținute, operatorul furnizează persoanei vizate următoarele informații suplimentare necesare pentru a asigura o prelucrare echitabilă și transparentă:

(a) perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;

(b) existența dreptului de a solicita operatorului, în ceea ce privește datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ștergerea acestora sau restricționarea prelucrării sau, după caz, a dreptului de a se opune prelucrării, precum și a dreptului la portabilitatea datelor;

(c) atunci când prelucrarea se bazează pe articolul 5 alineatul (1) litera (d) sau pe articolul 10 alineatul (2) litera (a), existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia;

(d) dreptul de a depune o plângere la Autoritatea Europeană pentru Protecția Datelor;

(e) dacă furnizarea de date cu caracter personal reprezintă o obligație legală sau contractuală sau o obligație necesară pentru încheierea unui contract, precum și dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal și care sunt eventualele consecințe ale nerespectării acestei obligații;

(f) existența unui proces decizional automatizat incluzând crearea de profiluri, menționat la articolul 24 alineatele (1) și (4), precum și, cel puțin în cazurile respective, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

(3) În cazul în care operatorul intenționează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost colectate, operatorul furnizează persoanei vizate, înainte de această prelucrare ulterioară, informații privind scopul secundar respectiv și orice informații suplimentare relevante, în conformitate cu alineatul (2).

(4) Alineatele (1), (2) și (3) nu se aplică dacă și în măsura în care persoana vizată deține deja informațiile respective.

Articolul 16

Informații care se furnizează în cazul în care datele cu caracter personal nu au fost obținute de la persoana vizată

(1) În cazul în care datele cu caracter personal nu au fost obținute de la persoana vizată, operatorul furnizează persoanei vizate următoarele informații:

(a) identitatea și datele de contact ale operatorului;

(b) datele de contact ale responsabilului cu protecția datelor;

(c) scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării;

(d) categoriile de date cu caracter personal vizate;

(e) destinatarii sau categoriile de destinatari ai datelor cu caracter personal, după caz;

(f) dacă este cazul, intenția operatorului de a transfera date cu caracter personal către un destinatar dintr-o țară terță sau o organizație internațională și existența sau absența unei decizii a Comisiei privind caracterul adecvat al nivelului de protecție sau, în cazul transferurilor menționate la articolul 48, o trimitere la garanțiile adecvate sau corespunzătoare și mijloacele de a obține o copie a acestora sau locul în care acestea au fost puse la dispoziție.

(2) Pe lângă informațiile menționate la alineatul (1), operatorul furnizează persoanei vizate următoarele informații suplimentare necesare pentru a asigura o prelucrare echitabilă și transparentă în ceea ce privește persoana vizată:

(a) perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;

(b) existența dreptului de a solicita operatorului, în ceea ce privește datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ștergerea acestora sau restricționarea prelucrării sau, după caz, a dreptului de a se opune prelucrării, precum și a dreptului la portabilitatea datelor;

(c) atunci când prelucrarea se bazează pe articolul 5 alineatul (1) litera (d) sau pe articolul 10 alineatul (2) litera (a), existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia;

(d) dreptul de a depune o plângere la Autoritatea Europeană pentru Protecția Datelor;

(e) sursa din care provin datele cu caracter personal și, dacă este cazul, dacă acestea provin din surse disponibile public;

(f) existența unui proces decizional automatizat incluzând crearea de profiluri, menționat la articolul 24 alineatele (1) și (4), precum și, cel puțin în cazurile respective, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

(3) Operatorul furnizează informațiile menționate la alineatele (1) și (2):

(a) într-un termen rezonabil după obținerea datelor cu caracter personal, dar nu mai mare de o lună, ținându-se seama de circumstanțele specifice în care sunt prelucrate datele cu caracter personal;

(b) dacă datele cu caracter personal urmează să fie utilizate pentru comunicarea cu persoana vizată, cel târziu în momentul primei comunicări către persoana vizată respectivă; sau

(c) dacă se intenționează divulgarea datelor cu caracter personal către un alt destinatar, cel mai târziu la data la care acestea sunt divulgate pentru prima oară.

(4) În cazul în care operatorul intenționează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost obținute, operatorul furnizează persoanei vizate, înainte de această prelucrare ulterioară, informații privind scopul secundar respectiv și orice informații suplimentare relevante, în conformitate cu alineatul (2).

(5) Alineatele (1)-(4) nu se aplică dacă și în măsura în care:

(a) persoana vizată deține deja informațiile;

(b) furnizarea acestor informații se dovedește a fi imposibilă sau ar implica eforturi disproporționate, în special în cazul prelucrării în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice sau în măsura în care obligația menționată la alineatul (1) din prezentul articol este susceptibilă să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective;

(c) obținerea sau divulgarea datelor este prevăzută în mod expres de dreptul Uniunii, care prevede măsuri adecvate pentru a proteja interesele legitime ale persoanei vizate; sau

(d) în cazul în care datele cu caracter personal trebuie să rămână confidențiale în temeiul unei obligații de secret profesional reglementate de dreptul Uniunii, inclusiv al unei obligații legale de a păstra secretul.

(6) În cazurile menționate la alineatul (5) litera (b), operatorul ia măsuri adecvate pentru a proteja drepturile, libertățile și interesele legitime ale persoanei vizate, inclusiv punerea informațiilor la dispoziția publicului.

Articolul 17

Dreptul de acces al persoanei vizate

(1) Persoana vizată are dreptul de a obține din partea operatorului o confirmare că se prelucrează sau nu date cu caracter personal care o privesc și, în caz afirmativ, acces la datele respective și la următoarele informații:

(a) scopurile prelucrării;

(b) categoriile de date cu caracter personal vizate;

(c) destinatarii sau categoriile de destinatari cărora datele cu caracter personal le-au fost sau urmează să le fie divulgate, în special destinatari din țări terțe sau organizații internaționale;

(d) acolo unde este posibil, perioada pentru care se preconizează că vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;

(e) existența dreptului de a solicita operatorului rectificarea sau ștergerea datelor cu caracter personal ori restricționarea prelucrării datelor cu caracter personal referitoare la persoana vizată sau a dreptului de a se opune prelucrării;

(f) dreptul de a depune o plângere la Autoritatea Europeană pentru Protecția Datelor;

(g) în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, orice informații disponibile privind sursa acestora;

(h) existența unui proces decizional automatizat incluzând crearea de profiluri, menționat la articolul 24 alineatele (1) și (4), precum și, cel puțin în cazurile respective, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

(2) În cazul în care datele cu caracter personal sunt transferate către o țară terță sau o organizație internațională, persoana vizată are dreptul să fie informată cu privire la garanțiile adecvate în temeiul articolului 48 referitoare la transfer.

(3) Operatorul furnizează o copie a datelor cu caracter personal care fac obiectul prelucrării. În cazul în care persoana vizată introduce cererea în format electronic și cu excepția cazului în care persoana vizată solicită un alt format, informațiile sunt furnizate într-un format electronic utilizat în mod curent.

(4) Dreptul de a obține o copie menționată la alineatul (3) nu aduce atingere drepturilor și libertăților altora.

SECȚIUNEA 3

Rectificare și ștergere

Articolul 18

Dreptul la rectificare

Persoana vizată are dreptul de a obține de la operator, fără întârzieri nejustificate, rectificarea datelor cu caracter personal inexacte care o privesc. Ținându-se seama de scopurile în care au fost prelucrate datele, persoana vizată are dreptul de a obține completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declarații suplimentare.

Articolul 19

Dreptul la ștergerea datelor („dreptul de a fi uitat”)

(1) Persoana vizată are dreptul de a obține din partea operatorului ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, iar operatorul are obligația de a șterge datele cu caracter personal fără întârzieri nejustificate în cazul în care se aplică unul dintre următoarele motive:

(a) datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;

(b) persoana vizată își retrage consimțământul pe baza căruia are loc prelucrarea, în conformitate cu articolul 5 alineatul (1) litera (d) sau cu articolul 10 alineatul (2) litera (a), și nu există niciun alt temei juridic pentru prelucrare;

(c) persoana vizată se opune prelucrării în temeiul articolului 23 alineatul (1) și nu există motive legitime care să prevaleze în ceea ce privește prelucrarea;

(d) datele cu caracter personal au fost prelucrate ilegal;

(e) datele cu caracter personal trebuie șterse pentru respectarea unei obligații legale care revine operatorului;

(f) datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale societății informaționale menționate la articolul 8 alineatul (1).

(2) În cazul în care operatorul a făcut publice datele cu caracter personal și este obligat, în temeiul alineatului (1), să le șteargă, operatorul, ținând seama de tehnologia disponibilă și de costul implementării, ia măsuri rezonabile, inclusiv măsuri tehnice, pentru a informa operatorii sau operatorii, alții decât instituții și organe ale Uniunii care prelucrează datele cu caracter personal că persoana vizată a solicitat ștergerea de către acești operatori, a oricăror linkuri către datele respective sau a oricăror copii sau reproduceri ale acestor date cu caracter personal.

(3) Alineatele (1) și (2) nu se aplică în măsura în care prelucrarea este necesară:

(a) pentru exercitarea dreptului la liberă exprimare și la informare;

(b) pentru respectarea unei obligații legale care revine operatorului sau pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorități oficiale cu care este învestit operatorul;

(c) din motive de interes public în domeniul sănătății publice, în conformitate cu articolul 10 alineatul (2) literele (h) și (i) și cu articolul 10 alineatul (3);

(d) în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în măsura în care dreptul menționat la alineatul (1) ar putea să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective; sau

(e) pentru constatarea, exercitarea sau apărarea unui drept în instanță.

Articolul 20

Dreptul la restricționarea prelucrării

(1) Persoana vizată are dreptul de a obține din partea operatorului restricționarea prelucrării în următoarele cazuri:

(a) persoana vizată contestă exactitatea datelor cu caracter personal, pentru o perioadă care îi permite operatorului să verifice exactitatea datelor cu caracter personal, inclusiv dacă acestea sunt complete;

(b) prelucrarea este ilegală, iar persoana vizată se opune ștergerii datelor cu caracter personal și solicită, în schimb, restricționarea utilizării lor;

(c) operatorul nu mai are nevoie de datele cu caracter personal în scopul prelucrării, dar persoana vizată i le solicită pentru constatarea, exercitarea sau apărarea unui drept în instanță;

(d) persoana vizată s-a opus prelucrării în conformitate cu articolul 23 alineatul (1), pentru intervalul de timp în care se verifică dacă drepturile legitime ale operatorului prevalează asupra celor ale persoanei vizate.

(2) În cazul în care prelucrarea a fost restricționată în temeiul alineatului (1), astfel de date cu caracter personal pot, cu excepția stocării, să fie prelucrate numai cu consimțământul persoanei vizate sau pentru constatarea, exercitarea sau apărarea unui drept în instanță sau pentru protecția drepturilor unei alte persoane fizice sau juridice sau din motive de interes public important al Uniunii sau al unui stat membru.

(3) O persoană vizată care a obținut restricționarea prelucrării în temeiul alineatului (1) este informată de către operator înainte de ridicarea restricției de prelucrare.

(4) În cazul sistemelor automatizate de evidență a datelor, restricționarea prelucrării se asigură, în principiu, prin mijloace tehnice. Faptul că prelucrarea datelor cu caracter personal este restricționată se indică în sistem în așa fel încât să devină evident că acele date cu caracter personal nu pot fi utilizate.

Articolul 21

Obligația de notificare privind rectificarea sau ștergerea datelor cu caracter personal sau restricționarea prelucrării

Operatorul comunică fiecărui destinatar căruia i-au fost divulgate datele cu caracter personal orice rectificare sau ștergere a datelor cu caracter personal sau restricționare a prelucrării efectuate în conformitate cu articolul 18, articolul 19 alineatul (1) și articolul 20, cu excepția cazului în care acest lucru se dovedește imposibil sau presupune eforturi disproporționate. Operatorul informează persoana vizată cu privire la destinatarii respectivi dacă persoana vizată solicită acest lucru.

Articolul 22

Dreptul la portabilitatea datelor

(1) Persoana vizată are dreptul de a primi datele cu caracter personal care o privesc și pe care le-a furnizat operatorului într-un format structurat, utilizat în mod curent și care poate fi citit automat și are dreptul de a transmite aceste date altui operator, fără obstacole din partea operatorului căruia i-au fost furnizate datele cu caracter personal, în cazul în care:

(a) prelucrarea se bazează pe consimțământ în temeiul articolului 5 alineatul (1) litera (d) sau al articolului 10 alineatul (2) litera (a) sau pe un contract în temeiul articolului 5 alineatul (1) litera (c); și

(b) prelucrarea este efectuată prin mijloace automate.

(2) În exercitarea dreptului său la portabilitatea datelor în temeiul alineatului (1), persoana vizată are dreptul ca datele cu caracter personal să fie transmise direct de la un operator la altul sau către operatori, alții decât instituții și organe ale Uniunii, acolo unde acest lucru este fezabil din punct de vedere tehnic.

(3) Exercitarea dreptului menționat la alineatul (1) din prezentul articol nu aduce atingere articolului 19. Respectivul drept nu se aplică prelucrării necesare pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorități oficiale cu care este învestit operatorul.

(4) Dreptul menționat la alineatul (1) nu aduce atingere drepturilor și libertăților altora.

SECȚIUNEA 4

Dreptul la opoziție și procesul decizional individual automatizat

Articolul 23

Dreptul la opoziție

(1) În orice moment, persoana vizată are dreptul să se opună, din motive legate de situația particulară în care se află, prelucrării în temeiul articolului 5 alineatul (1) litera (a), a datelor cu caracter personal care o privesc, inclusiv creării de profiluri pe baza respectivei dispoziții. Operatorul nu mai prelucrează datele cu caracter personal, cu excepția cazului în care operatorul demonstrează că are motive legitime și imperioase care justifică prelucrarea și care prevalează asupra intereselor, drepturilor și libertăților persoanei vizate sau că scopul este constatarea, exercitarea sau apărarea unui drept în instanță.

(2) Cel târziu în momentul primei comunicări cu persoana vizată, dreptul menționat la alineatul (1) este adus în mod explicit în atenția persoanei vizate și este prezentat în mod clar și separat de orice alte informații.

(3) Fără a aduce atingere articolelor 36 și 37, în contextul utilizării serviciilor societății informaționale, persoana vizată își poate exercita dreptul de a se opune prin mijloace automatizate care folosesc specificații tehnice.

(4) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare științifică sau istorică sau în scopuri statistice, persoana vizată, din motive legate de situația sa particulară, are dreptul de a se opune prelucrării datelor cu caracter personal care o privesc, cu excepția cazului în care prelucrarea este necesară pentru îndeplinirea unei sarcini din motive de interes public.

Articolul 24

Procesul decizional individual automatizat, inclusiv crearea de profiluri

(1) Persoana vizată are dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă.

(2) Alineatul (1) nu se aplică în cazul în care decizia:

(a) este necesară pentru încheierea sau executarea unui contract între persoana vizată și operator;

(b) este autorizată prin dreptul Uniunii care prevede, de asemenea, măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate; sau

(c) are la bază consimțământul explicit al persoanei vizate.

(3) În cazurile menționate la alineatul (2) literele (a) și (c), operatorul pune în aplicare măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate, cel puțin dreptul acesteia de a obține intervenție umană din partea operatorului, de a-și exprima punctul de vedere și de a contesta decizia.

(4) Deciziile menționate la alineatul (2) de la prezentul articol nu au la bază categoriile speciale de date cu caracter personal menționate la articolul 10 alineatul (1), cu excepția cazului în care se aplică articolul 10 alineatul (2) litera (a) sau (g) și în care au fost instituite măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate.

SECȚIUNEA 5

Restricții

Articolul 25

Restricții

(1) Actele legislative adoptate în baza tratatelor sau, în chestiuni legate de funcționarea instituțiilor și organelor Uniunii, normele interne prevăzute de acestea din urmă pot restricționa aplicarea articolelor 14-22, 35 și 36, precum și a articolului 4 în măsura în care dispozițiile acestuia corespund drepturilor și obligațiilor prevăzute la articolele 14-22, atunci când o astfel de restricție respectă esența drepturilor și libertăților fundamentale și constituie o măsură necesară și proporțională într-o societate democratică, pentru a garanta:

(a) securitatea națională, securitatea publică sau apărarea statelor membre;

(b) prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor sau executarea sancțiunilor penale, inclusiv protejarea împotriva amenințărilor la adresa securității publice și prevenirea acestora;

(c) alte obiective importante de interes public general ale Uniunii sau ale unui stat membru, în special obiectivele politicii externe și de securitate comune ale Uniunii sau un interes economic sau financiar important al Uniunii sau al unui stat membru, inclusiv în domeniile monetar, bugetar și fiscal și în domeniul sănătății publice și al securității sociale;

(d) securitatea internă a instituțiilor și organelor Uniunii, inclusiv a rețelelor lor de comunicații electronice;

(e) protejarea independenței judiciare și a procedurilor judiciare;

(f) prevenirea, depistarea, investigarea și urmărirea penală a încălcării eticii în cazul profesiilor reglementate;

(g) o funcție de monitorizare, inspecție sau reglementare legată, chiar și ocazional, de exercitarea autorității oficiale în cazurile menționate la literele (a)-(c);

(h) protecția persoanei vizate sau a drepturilor și libertăților altora;

(i) executarea hotărârilor pronunțate în acțiuni în pretenții formulate în temeiul dreptului civil.

(2) În special, orice act juridic sau normă internă menționată la alineatul (1) conține dispoziții specifice privind, dacă este cazul:

(a) scopurile prelucrării sau ale categoriilor de prelucrare;

(b) categoriile de date cu caracter personal;

(c) domeniul de aplicare al restricțiilor introduse;

(d) garanțiile pentru a preveni abuzurile sau accesul sau transferul ilegal;

(e) specificațiile operatorului sau ale categoriilor de operatori;

(f) perioadele de stocare și garanțiile aplicabile având în vedere caracterul, domeniul de aplicare și scopurile prelucrării sau ale categoriilor de prelucrare; și

(g) riscurile pentru drepturile și libertățile persoanelor vizate.

(3) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare științifică sau istorică ori în scopuri statistice, dreptul Uniunii, care poate include norme interne adoptate de instituțiile și organele Uniunii în chestiuni referitoare la funcționarea lor, poate să prevadă derogări de la drepturile menționate la articolele 17, 18, 20 și 23, sub rezerva condițiilor și a garanțiilor prevăzute la articolul 13, în măsura în care drepturile respective sunt de natură să facă imposibilă sau să afecteze în mod grav realizarea scopurilor specifice, iar derogările respective sunt necesare pentru îndeplinirea acestor scopuri.

(4) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de arhivare de interes public, dreptul Uniunii, care poate include norme interne adoptate de instituțiile și organele Uniunii în chestiuni referitoare la funcționarea lor, poate să prevadă derogări de la drepturile menționate la articolele 17, 18, 20, 21, 22 și 23, sub rezerva condițiilor și a garanțiilor prevăzute la articolul 13, în măsura în care drepturile respective sunt de natură să facă imposibilă sau să afecteze în mod grav realizarea scopurilor specifice, iar derogările respective sunt necesare pentru îndeplinirea acestor scopuri.

(5) Normele interne menționate la alineatele (1), (3) și (4) sunt acte clare și precise cu domeniu de aplicare general, menite să producă efecte juridice față de persoanele vizate, adoptate la cel mai înalt nivel de conducere din instituțiile și organele Uniunii și se publică în *Jurnalul Oficial al Uniunii Europene*.

(6) În cazul în care se impune o restricție în temeiul alineatului (1), persoana vizată este informată, în conformitate cu dreptul Uniunii, cu privire la motivele principale care stau la baza aplicării restricției și cu privire la dreptul său de a depune o plângere la Autoritatea Europeană pentru Protecția Datelor.

(7) În cazul în care o restricție impusă în temeiul alineatului (1) este invocată pentru a se refuza accesul persoanei vizate, Autoritatea Europeană pentru Protecția Datelor, atunci când examinează plângerea, doar o va informa dacă datele au fost prelucrate în mod corect și, dacă nu, dacă au fost efectuate corecțiile necesare.

(8) Furnizarea informațiilor menționate la alineatele (6) și (7) de la prezentul articol și la articolul 45 alineatul (2) poate fi amânată, omisă sau refuzată în cazul în care aceasta ar anula efectul restricției impuse în temeiul alineatului (1) de la prezentul articol.

CAPITOLUL IV

OPERATORUL ȘI PERSOANA ÎMPUTERNICITĂ DE CĂTRE OPERATOR

SECȚIUNEA 1

Obligații generale

Articolul 26

Responsabilitatea operatorului

(1) Ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul regulament. Respectivele măsuri se revizuiesc și se actualizează dacă este necesar.

(2) Atunci când sunt proporționale în raport cu operațiunile de prelucrare, măsurile menționate la alineatul (1) includ punerea în aplicare de către operator a unor politici adecvate de protecție a datelor.

(3) Aderarea la mecanismele de certificare aprobate, menționate la articolul 42 din Regulamentul (UE) 2016/679, poate fi utilizată ca element care să demonstreze respectarea obligațiilor de către operator.

Articolul 27

Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit

(1) Având în vedere stadiul actual al tehnologiei, costurile implementării și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice pe care le prezintă prelucrarea, operatorul, atât în momentul stabilirii mijloacelor de prelucrare, cât și în cel al prelucrării în sine, pune în aplicare măsuri tehnice și organizatorice adecvate, cum ar fi pseudonimizarea, care sunt destinate să pună în aplicare în mod eficient principiile de protecție a datelor, precum reducerea la minimum a datelor, și să integreze garanțiile necesare în cadrul prelucrării, pentru a îndeplini cerințele prezentului regulament și a proteja drepturile persoanelor vizate.

(2) Operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura că, în mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării. Respectiva obligație se aplică volumului de date colectate, gradului de prelucrare a acestora, perioadei lor de stocare și accesibilității lor. În special, astfel de măsuri asigură că, în mod implicit, datele cu caracter personal nu pot fi accesate, fără intervenția persoanei, de un număr nelimitat de persoane.

(3) Un mecanism de certificare aprobat în conformitate cu articolul 42 din Regulamentul (UE) 2016/679 poate fi utilizat drept element care să demonstreze îndeplinirea cerințelor prevăzute la alineatele (1) și (2) din prezentul articol.

Articolul 28

Operatorii asociați

(1) În cazul în care doi sau mai mulți operatori sau unul sau mai mulți operatori împreună cu unul sau mai mulți operatori, alții decât instituții și organe ale Uniunii, stabilesc în comun scopurile și mijloacele prelucrării, aceștia sunt operatori asociați. Aceștia stabilesc într-un mod transparent responsabilitățile fiecăruia în ceea ce privește îndeplinirea obligațiilor care le revin în materie de protecție a datelor, în special în ceea ce privește exercitarea drepturilor persoanelor vizate și îndatoririle fiecărui operator de a furniza informațiile prevăzute la articolele 15 și 16, prin intermediul unui acord între ei, cu excepția cazului și în măsura în care responsabilitățile operatorilor asociați sunt stabilite în dreptul Uniunii sau în dreptul intern al statului membru care se aplică acestora. Acordul poate să desemneze un punct de contact pentru persoanele vizate.

(2) Acordul menționat la alineatul (1) reflectă în mod adecvat rolurile și raporturile respective ale operatorilor asociați față de persoanele vizate. Esența acestui acord este făcută cunoscută persoanei vizate.

(3) Indiferent de clauzele acordului menționat la alineatul (1), persoana vizată își poate exercita drepturile de care beneficiază în temeiul prezentului regulament în legătură cu sau împotriva fiecăruia dintre operatori.

Articolul 29

Persoana împuternicită de operator

(1) În cazul în care prelucrarea urmează să fie realizată în numele unui operator, operatorul recurge doar la persoane împuternicite care oferă garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să respecte cerințele prevăzute în prezentul regulament și să asigure protecția drepturilor persoanei vizate.

(2) Persoana împuternicită de operator nu recrutează o altă persoană împuternicită de operator fără a primi în prealabil o autorizație scrisă, specifică sau generală, din partea operatorului. În cazul unei autorizații generale scrise, persoana împuternicită de operator informează operatorul cu privire la orice modificări preconizate privind adăugarea sau înlocuirea altor persoane împuternicite de operator, oferind astfel operatorului posibilitatea de a formula obiecții față de aceste modificări.

(3) Prelucrarea de către o persoană împuternicită de un operator este reglementată printr-un contract sau un alt act juridic în temeiul dreptului Uniunii sau al dreptului intern care are caracter obligatoriu pentru persoana împuternicită de operator în raport cu operatorul și care stabilește obiectul și durata prelucrării, natura și scopul prelucrării, tipul de date cu caracter personal și categoriile de persoane vizate și obligațiile și drepturile operatorului. Respectivul contract sau act juridic prevede în special că persoana împuternicită de operator:

(a) prelucrează datele cu caracter personal numai pe baza unor instrucțiuni susținute de documente din partea operatorului, inclusiv în ceea ce privește transferurile de date cu caracter personal către o țară terță sau o organizație internațională, cu excepția cazului în care această obligație îi revine în temeiul dreptului Uniunii sau al dreptului statului membru care i se aplică; în acest caz, persoana împuternicită de operator notifică această obligație juridică operatorului înainte de prelucrare, cu excepția cazului în care legislația respectivă interzice această informare din motive importante legate de interesul public;

(b) se asigură că persoanele autorizate să prelucreze datele cu caracter personal s-au angajat să respecte confidențialitatea sau au o obligație legală adecvată de confidențialitate;

(c) adoptă toate măsurile necesare în conformitate cu articolul 33;

(d) respectă condițiile menționate la alineatele (2) și (4) privind recrutarea unei alte persoane împuternicite de operator;

(e) ținând seama de natura prelucrării, oferă asistență operatorului prin măsuri tehnice și organizatorice adecvate, în măsura în care acest lucru este posibil, pentru îndeplinirea obligației operatorului de a răspunde cererilor privind exercitarea de către persoana vizată a drepturilor prevăzute în capitolul III;

(f) ajută operatorul să asigure respectarea obligațiilor prevăzute la articolele 33-41, ținând seama de caracterul prelucrării și de informațiile aflate la dispoziția persoanei împuternicite de operator;

(g) la alegerea operatorului, șterge sau returnează operatorului toate datele cu caracter personal după încetarea furnizării serviciilor legate de prelucrare și elimină copiile existente, cu excepția cazului în care dreptul Uniunii sau dreptul intern impune stocarea datelor cu caracter personal;

(h) pune la dispoziția operatorului toate informațiile necesare pentru a demonstra respectarea obligațiilor prevăzute la prezentul articol, permite desfășurarea auditurilor, inclusiv a inspecțiilor, efectuate de operator sau alt auditor mandatat și contribuie la acestea.

În ceea ce privește primul paragraf litera (h), persoana împuternicită de operator informează imediat operatorul în cazul în care, în opinia sa, o instrucțiune încalcă prezentul regulament sau alte dispoziții din dreptul intern sau din dreptul Uniunii referitoare la protecția datelor.

(4) În cazul în care o persoană împuternicită de un operator recrutează o altă persoană împuternicită pentru efectuarea de activități de prelucrare specifice în numele operatorului, aceleași obligații privind protecția datelor prevăzute în contractul sau în alt act juridic încheiat între operator și persoana împuternicită de operator, astfel cum se prevede la alineatul (3), revin celei de a doua persoane împuternicite, prin intermediul unui contract sau al unui alt act juridic, în temeiul dreptului Uniunii sau al dreptului intern, în special furnizarea de garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să îndeplinească cerințele prezentului regulament. În cazul în care această a doua persoană împuternicită nu își respectă obligațiile privind protecția datelor, persoana împuternicită inițială rămâne pe deplin răspunzătoare față de operator în ceea ce privește îndeplinirea obligațiilor acestei a doua persoane împuternicite.

(5) În cazul în care o persoană împuternicită de un operator nu este o instituție sau un organ al Uniunii, aderarea la un cod de conduită aprobat, menționat la articolul 40 alineatul (5) din Regulamentul (UE) 2016/679, sau la un mecanism de certificare aprobat, menționat la articolul 42 din Regulamentul (UE) 2016/679, poate fi utilizată ca element prin care să se demonstreze existența unor garanții suficiente, astfel cum sunt menționate la alineatele (1) și (4) din prezentul articol.

(6) Fără a aduce atingere unui contract individual încheiat între operator și persoana împuternicită de operator, contractul sau celălalt act juridic menționat la alineatele (3) și (4) din prezentul articol se poate baza, integral sau parțial, pe clauzele contractuale standard menționate la alineatele (7) și (8) din prezentul articol, inclusiv atunci când fac parte dintr-o certificare acordată persoanei împuternicite de operator, care nu este o instituție sau un organ al UE, în temeiul articolului 42 din Regulamentul (UE) 2016/679.

(7) Comisia poate să prevadă clauze contractuale standard pentru aspectele menționate la alineatele (3) și (4) din prezentul articol și în conformitate cu procedura de examinare menționată la articolul 96 alineatul (2).

(8) Autoritatea Europeană pentru Protecția Datelor poate să adopte clauze contractuale standard pentru aspectele menționate la alineatele (3) și (4).

(9) Contractul sau celălalt act juridic menționat la alineatele (3) și (4) se formulează în scris, inclusiv în format electronic.

(10) Fără a aduce atingere articolelor 65 și 66, în cazul în care o persoană împuternicită de operator încalcă prezentul regulament prin stabilirea scopurilor prelucrării și a mijloacelor de prelucrare, persoana împuternicită de operator este considerată a fi un operator în ceea ce privește prelucrarea respectivă.

Articolul 30

Desfășurarea activității de prelucrare sub autoritatea operatorului sau a persoanei împuternicite de către operator

Persoana împuternicită de operator și orice persoană care acționează sub autoritatea operatorului sau a persoanei împuternicite de operator, care are acces la date cu caracter personal, nu le prelucrează decât la cererea operatorului, cu excepția cazului în care dreptul Uniunii sau dreptul unui stat membru îl obligă să facă acest lucru.

Articolul 31

Evidențele activităților de prelucrare

(1) Fiecare operator păstrează o evidență a activităților de prelucrare desfășurate sub responsabilitatea sa. Respectiva evidență cuprinde toate informațiile următoare:

(a) numele și datele de contact ale operatorului, ale responsabilului cu protecția datelor și, dacă este cazul, ale persoanei împuternicite de către operator și ale operatorului asociat;

(b) scopurile prelucrării;

(c) o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal;

(d) categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din statele membre, țări terțe sau organizații internaționale;

(e) dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și documentația care dovedește existența unor garanții adecvate;

(f) acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date;

(g) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 33.

(2) Fiecare persoană împuternicită de operator păstrează o evidență a tuturor categoriilor de activități de prelucrare desfășurate în numele operatorului, care cuprinde:

(a) numele și datele de contact ale persoanei sau persoanelor împuternicite de către operator, ale fiecărui operator în numele căruia acționează această persoană și ale responsabilului cu protecția datelor;

(b) categoriile de activități de prelucrare desfășurate în numele fiecărui operator;

(c) dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și documentația care dovedește existența unor garanții adecvate;

(d) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 33.

(3) Evidențele menționate la alineatele (1) și (2) se formulează în scris, inclusiv în format electronic.

(4) Instituțiile și organele Uniunii pun evidențele la dispoziția Autorității Europene pentru Protecția Datelor, la cerere.

(5) Cu excepția cazului în care nu este adecvat, ținând cont de dimensiunea instituției sau a organului Uniunii, instituțiile și organele Uniunii își păstrează evidențele activităților de prelucrare într-un registru central. Acestea pun registrul la dispoziția publicului.

Articolul 32

Cooperarea cu Autoritatea Europeană pentru Protecția Datelor

Instituțiile și organele Uniunii cooperează, la cerere, cu Autoritatea Europeană pentru Protecția Datelor în îndeplinirea sarcinilor sale.

SECȚIUNEA 2

Securitatea datelor cu caracter personal

Articolul 33

Securitatea prelucrării

(1) Având în vedere stadiul actual al dezvoltării, costurile implementării și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscurile cu diferite grade de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul și persoana împuternicită de acesta implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând, printre altele, după caz:

(a) pseudonimizarea și criptarea datelor cu caracter personal;

(b) capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare;

(c) capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;

(d) un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

(2) La evaluarea nivelului adecvat de securitate, se ține seama în special de riscurile prezentate de prelucrare, generate, în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.

(3) Operatorul și persoana împuternicită de acesta iau măsuri pentru a se asigura că orice persoană fizică ce acționează sub autoritatea operatorului sau a persoanei împuternicite de operator și care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepția cazului în care această obligație îi revine în temeiul dreptului Uniunii.

(4) Aderarea la un mecanism de certificare aprobat, astfel cum se prevede la articolul 42 din Regulamentul (UE) 2016/679, poate fi utilizată drept element care să demonstreze îndeplinirea cerințelor prevăzute la alineatul (1) din prezentul articol.

Articolul 34

Notificarea Autorității Europene pentru Protecția Datelor în cazul încălcării securității datelor cu caracter personal

(1) În cazul în care are loc o încălcare a securității datelor cu caracter personal, operatorul notifică acest lucru Autorității Europene pentru Protecția Datelor, fără întârzieri nejustificate și, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta, cu excepția cazului în care este puțin probabil să genereze un risc pentru drepturile și libertățile persoanelor fizice. În cazul în care notificarea către Autoritatea Europeană pentru Protecția Datelor nu are loc în termen de 72 de ore, aceasta este însoțită de o explicație privind motivele întârzierii.

(2) Persoana împuternicită de operator înștiințează operatorul fără întârzieri nejustificate după ce ia cunoștință de o încălcare a securității datelor cu caracter personal.

(3) Notificarea menționată la alineatul (1), cel puțin:

(a) descrie caracterul încălcării securității datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile și numărul aproximativ al persoanelor vizate în cauză, precum și categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;

(b) comunică numele și datele de contact ale responsabilului cu protecția datelor;

(c) descrie consecințele probabile ale încălcării securității datelor cu caracter personal;

(d) descrie măsurile luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

(4) Atunci când și în măsura în care nu este posibil să se furnizeze informațiile în același timp, acestea pot fi furnizate în mai multe etape, fără întârzieri nejustificate.

(5) Operatorul informează responsabilul cu protecția datelor cu privire la încălcarea securității datelor cu caracter personal.

(6) Operatorul păstrează documente referitoare la toate cazurile de încălcare a securității datelor cu caracter personal, care cuprind o descriere a situației de fapt în care a avut loc încălcarea securității datelor cu caracter personal, a efectelor acesteia și a măsurilor de remediere întreprinse. Această documentație permite Autorității Europene pentru Protecția Datelor să verifice respectarea prezentului articol.

Articolul 35

Informarea persoanei vizate cu privire la încălcarea securității datelor cu caracter personal

(1) În cazul în care încălcarea securității datelor cu caracter personal este de natură să ducă la apariția unui risc ridicat la adresa drepturilor și libertăților persoanelor fizice, operatorul informează persoana vizată fără întârzieri nejustificate cu privire la această încălcare.

(2) În informarea transmisă persoanei vizate prevăzută la alineatul (1) din prezentul articol se include o descriere într-un limbaj clar și simplu a caracterului încălcării securității datelor cu caracter personal, precum și cel puțin informațiile și măsurile menționate la articolul 34 alineatul (3) literele (b), (c) și (d).

(3) Informarea persoanei vizate menționată la alineatul (1) nu este necesară în cazul în care oricare dintre următoarele condiții este îndeplinită:

(a) operatorul a implementat măsuri de protecție tehnice și organizatorice adecvate, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securității datelor cu caracter personal, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea;

(b) operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat pentru drepturile și libertățile persoanelor vizate menționat la alineatul (1) nu mai poate să se materializeze;

(c) ar necesita un efort disproporționat. În această situație, se efectuează în loc o informare publică sau se ia o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficace.

(4) În cazul în care operatorul nu a comunicat deja persoanei vizate încălcarea securității datelor cu caracter personal, Autoritatea Europeană pentru Protecția Datelor, după ce a luat în considerare probabilitatea ca încălcarea securității datelor cu caracter personal să ducă la apariția unui risc ridicat, poate să îi solicite acestuia să facă acest lucru sau poate decide că oricare dintre condițiile menționate la alineatul (3) sunt îndeplinite.

SECȚIUNEA 3

Confidențialitatea comunicațiilor electronice

Articolul 36

Confidențialitatea comunicațiilor electronice

Instituțiile și organele Uniunii asigură confidențialitatea comunicațiilor electronice, în special prin securizarea propriilor rețele de comunicații electronice.

Articolul 37

Protecția informațiilor transmise către, stocate în, aferente, prelucrate de și colectate de la echipamentele terminale ale utilizatorilor

Instituțiile și organele Uniunii protejează informațiile transmise către, stocate în, aferente, prelucrate și colectate de la echipamentele terminale ale utilizatorilor, accesând site-urile internet disponibile public și aplicațiile pentru dispozitive mobile ale acestora în conformitate cu articolul 5 alineatul (3) din Directiva 2002/58/CE.

Articolul 38

Anuare de utilizatori

(1) Datele cu caracter personal cuprinse în anuarele de utilizatori și accesul la aceste anuare se limitează la ceea ce este strict necesar pentru scopurile specifice ale anuarului respectiv.

(2) Instituțiile și organele Uniunii iau toate măsurile necesare pentru a împiedica folosirea datelor cu caracter personal conținute în aceste anuare în scopuri de marketing direct, indiferent dacă datele sunt accesibile sau nu publicului.

SECȚIUNEA 4

Evaluarea impactului asupra protecției datelor și consultarea prealabilă

Articolul 39

Evaluarea impactului asupra protecției datelor

(1) Având în vedere natura, domeniul de aplicare, contextul și scopurile prelucrării, în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este de natură să ducă la apariția unui risc ridicat la adresa drepturilor și libertăților persoanelor fizice, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operațiunilor de prelucrare prevăzute asupra protecției datelor cu caracter personal. O evaluare unică poate aborda un set de operațiuni de prelucrare similare care prezintă riscuri ridicate similare.

(2) La realizarea unei evaluări a impactului asupra protecției datelor, operatorul solicită consiliere din partea responsabilului cu protecția datelor.

(3) Evaluarea impactului asupra protecției datelor menționată la alineatul (1) se impune mai ales în cazul:

(a) unei evaluări sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, și care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;

(b) prelucrării pe scară largă a unor categorii speciale de date, menționată la articolul 10, sau a unor date cu caracter personal privind condamnări penale și infracțiuni, menționată la articolul 11; sau

(c) unei monitorizări sistematice pe scară largă a unei zone accesibile publicului.

(4) Autoritatea Europeană pentru Protecția Datelor întocmește și publică o listă a tipurilor de operațiuni de prelucrare care fac obiectul cerinței de efectuare a unei evaluări a impactului asupra protecției datelor în conformitate cu alineatul (1).

(5) Autoritatea Europeană pentru Protecția Datelor poate, de asemenea, să întocmească și să pună la dispoziția publicului o listă a tipurilor de operațiuni de prelucrare pentru care nu este necesară o evaluare a impactului asupra protecției datelor.

(6) Înainte de adoptarea listelor menționate la alineatele (4) și (5) de la prezentul articol, Autoritatea Europeană pentru Protecția Datelor solicită Comitetului european pentru protecția datelor instituit în temeiul articolului 68 din Regulamentul (UE) 2016/679 să examineze aceste liste în conformitate cu articolul 70 alineatul (1) litera (e) din regulamentul menționat în cazul în care acestea vizează operațiuni de prelucrare efectuate de un operator care acționează împreună cu unul sau mai mulți operatori alții decât instituțiile și organele Uniunii.

(7) Evaluarea conține cel puțin:

(a) o descriere sistematică a operațiunilor de prelucrare preconizate și a scopurilor prelucrării;

(b) o evaluare a necesității și proporționalității operațiunilor de prelucrare în legătură cu aceste scopuri;

(c) o evaluare a riscurilor pentru drepturile și libertățile persoanelor vizate menționate la alineatul (1); și

(d) măsurile preconizate în vederea abordării riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze conformitatea cu dispozițiile prezentului regulament, luând în considerare drepturile și interesele legitime ale persoanelor vizate și ale altor persoane interesate.

(8) La evaluarea impactului operațiunilor de prelucrare efectuate de persoanele împuternicite de operatori relevante, altele decât instituțiile și organele Uniunii, se are în vedere în mod corespunzător respectarea de către persoanele împuternicite respective a codurilor de conduită aprobate menționate la articolul 40 din Regulamentul (UE) 2016/679, în special în vederea unei evaluări a impactului asupra protecției datelor.

(9) Operatorul solicită, acolo unde este cazul, avizul persoanelor vizate sau al reprezentanților acestora privind prelucrarea prevăzută, fără a aduce atingere protecției intereselor publice ori securității operațiunilor de prelucrare.

(10) Atunci când prelucrarea efectuată în temeiul articolului 5 alineatul (1) litera (a) sau (b) are drept temei juridic un act legislativ adoptat în baza tratatelor, care reglementează operațiunea de prelucrare specifică sau setul de operațiuni în cauză, și atunci când s-a efectuat deja o evaluare a impactului asupra protecției datelor ca parte a unei evaluări generale a impactului prealabile adoptării respectivului act legislativ, alineatele (1)-(6) din prezentul articol nu se aplică, cu excepția cazului în care acel act legislativ prevede acest lucru.

(11) Acolo unde este necesar, operatorul efectuează o analiză pentru a evalua dacă prelucrarea are loc în conformitate cu evaluarea impactului asupra protecției datelor, cel puțin atunci când are loc o modificare a riscului reprezentat de operațiunile de prelucrare.

Articolul 40

Consultarea prealabilă

(1) Operatorul consultă Autoritatea Europeană pentru Protecția Datelor înainte de prelucrare în cazul în care o evaluare a impactului asupra protecției datelor efectuată în temeiul articolului 39 arată că prelucrarea ar duce, în absența garanțiilor, măsurilor de securitate și mecanismelor de atenuare a riscului, la apariția unui risc ridicat la adresa drepturilor și libertăților persoanelor fizice, iar operatorul consideră că riscul nu poate fi atenuat prin mijloace rezonabile având în vedere tehnologiile disponibile și costurile implementării. Operatorul solicită consiliere din partea responsabilului cu protecția datelor cu privire la necesitatea consultării prealabile.

(2) Atunci când Autoritatea Europeană pentru Protecția Datelor consideră că prelucrarea prevăzută, astfel cum este menționată la alineatul (1), ar încălca prezentul regulament, în special atunci când riscul nu a fost identificat sau atenuat într-o măsură suficientă de către operator, Autoritatea Europeană pentru Protecția Datelor oferă consiliere în scris operatorului și, după caz, persoanei împuternicite de operator, în termen de cel mult opt săptămâni de la primirea cererii de consultare, și își poate exercita oricare dintre competențele menționate la articolul 58. Această perioadă poate fi prelungită cu șase săptămâni, ținându-se seama de complexitatea prelucrării prevăzute. Autoritatea Europeană pentru Protecția Datelor informează operatorul și, după caz, persoana împuternicită de operator în termen de o lună de la primirea cererii de consultare cu privire la orice astfel de prelungire, prezentând motivele întârzierii. Aceste perioade pot fi suspendate până când Autoritatea Europeană pentru Protecția Datelor a obținut informațiile pe care le-a solicitat în scopul consultării.

(3) Cu ocazia consultării Autorității Europene pentru Protecția Datelor în temeiul alineatului (1), operatorul furnizează Autorității Europene pentru Protecția Datelor:

(a) dacă este cazul, responsabilitățile respective ale operatorului, ale operatorilor asociați și ale persoanelor împuternicite de operator implicate în activitățile de prelucrare;

(b) scopurile și mijloacele prelucrării preconizate;

(c) măsurile și garanțiile prevăzute pentru protecția drepturilor și libertăților persoanelor vizate, în conformitate cu prezentul regulament;

(d) datele de contact ale responsabilului cu protecția datelor;

(e) evaluarea impactului asupra protecției datelor prevăzută la articolul 39; și

(f) orice alte informații solicitate de Autoritatea Europeană pentru Protecția Datelor.

(4) Comisia poate, prin intermediul unui act de punere în aplicare, să stabilească o listă de cazuri în care operatorii se consultă cu Autoritatea Europeană pentru Protecția Datelor și obțin o autorizație prealabilă de la aceasta în ceea ce privește prelucrarea datelor cu caracter personal pentru îndeplinirea unei sarcini executate de operator în interes public, inclusiv prelucrarea unor astfel de date în legătură cu protecția socială și sănătatea publică.

SECȚIUNEA 5

Informare și consultare legislativă

Articolul 41

Informare și consultare

(1) Instituțiile și organele Uniunii informează Autoritatea Europeană pentru Protecția Datelor în cazul elaborării de măsuri administrative și de norme interne referitoare la prelucrarea datelor cu caracter personal de către o instituție sau un organ al Uniunii, singur sau împreună cu altele.

(2) Instituțiile și organele Uniunii consultă Autoritatea Europeană pentru Protecția Datelor atunci când elaborează normele interne menționate la articolul 25.

Articolul 42

Consultare legislativă

(1) În urma adoptării unor propuneri de acte legislative, a unor recomandări sau a unor propuneri adresate Consiliului în temeiul articolului 218 din TFUE sau atunci când elaborează acte delegate sau acte de punere în aplicare, Comisia consultă Autoritatea Europeană pentru Protecția Datelor atunci când există un impact asupra protecției drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.

(2) În cazul în care un act menționat la alineatul (1) este deosebit de important pentru protecția drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, Comisia poate, de asemenea, să consulte Comitetul european pentru protecția datelor. În astfel de cazuri, Autoritatea Europeană pentru Protecția Datelor și Comitetul european pentru protecția datelor își coordonează activitatea în vederea emiterii unui aviz comun.

(3) Consilierea menționată la alineatele (1) și (2) se furnizează în scris, în termen de maximum opt săptămâni de la primirea cererii de consultare menționate la alineatele (1) și (2). În cazuri urgente sau oportune, Comisia poate să reducă termenul stabilit.

(4) Prezentul articol nu se aplică în cazul în care Comisia este obligată, în conformitate cu Regulamentul (UE) 2016/679, să consulte Comitetul european pentru protecția datelor.

SECȚIUNEA 6

Responsabilul cu protecția datelor

Articolul 43

Desemnarea responsabilului cu protecția datelor

(1) Fiecare instituție sau organ al Uniunii desemnează un responsabil cu protecția datelor.

(2) Instituțiile și organele Uniunii pot desemna un responsabil unic cu protecția datelor pentru mai multe dintre ele, ținând seama de structura organizatorică și de dimensiunea acestora.

(3) Responsabilul cu protecția datelor este desemnat pe baza calităților profesionale și, în special, a cunoștințelor de specialitate în dreptul și practicile din domeniul protecției datelor, precum și pe baza capacității de a îndeplini sarcinile prevăzute la articolul 45.

(4) Responsabilul cu protecția datelor este un membru al personalului instituției sau organului Uniunii. Având în vedere dimensiunea lor și dacă opțiunea în temeiul alineatului (2) nu este exercitată, instituțiile și organele Uniunii pot desemna un responsabil cu protecția datelor care își îndeplinește atribuțiile în baza unui contract de servicii.

(5) Instituțiile și organele Uniunii publică datele de contact ale responsabilului cu protecția datelor și le comunică Autorității Europene pentru Protecția Datelor.

Articolul 44

Funcția responsabilului cu protecția datelor

(1) Instituțiile și organele Uniunii se asigură că responsabilul cu protecția datelor este implicat în mod corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal.

(2) Instituțiile și organele Uniunii sprijină responsabilul cu protecția datelor în îndeplinirea sarcinilor menționate la articolul 45, asigurându-i resursele necesare pentru executarea acestor sarcini, precum și accesul la date cu caracter personal și la operațiunile de prelucrare a acestora, și oferindu-i posibilitatea de a-și actualiza cunoștințele de specialitate.

(3) Instituțiile și organele Uniunii se asigură că responsabilul cu protecția datelor nu primește niciun fel de instrucțiuni în ceea ce privește îndeplinirea acestor sarcini. Acesta nu este demis sau sancționat de către operator sau de persoana împuternicită de operator pentru îndeplinirea sarcinilor sale. Responsabilul cu protecția datelor răspunde direct în fața celui mai înalt nivel al conducerii operatorului sau persoanei împuternicite de operator.

(4) Persoanele vizate pot contacta responsabilul cu protecția datelor cu privire la toate chestiunile legate de prelucrarea datelor lor și la exercitarea drepturilor lor în temeiul prezentului regulament.

(5) Responsabilul cu protecția datelor și personalul acestuia au obligația de a respecta secretul sau confidențialitatea în ceea ce privește îndeplinirea sarcinilor lor, în conformitate cu dreptul Uniunii.

(6) Responsabilul cu protecția datelor poate îndeplini și alte sarcini și atribuții. Operatorul sau persoana împuternicită de operator se asigură că niciuna dintre aceste sarcini și atribuții nu generează un conflict de interese.

(7) Responsabilul cu protecția datelor poate fi consultat de către operator sau de către persoana împuternicită de acesta, de către Comitetul pentru personal și de către orice persoană fizică, în orice problemă privind interpretarea sau aplicarea prezentului regulament, fără să se recurgă la căile oficiale. Nimeni nu poate suferi un prejudiciu ca urmare a unui fapt adus la cunoștința responsabilului competent cu protecția datelor, despre care se susține că ar reprezenta o încălcare a dispozițiilor prezentului regulament.

(8) Responsabilul cu protecția datelor este desemnat pentru un mandat de trei până la cinci ani și este eligibil pentru o nouă numire. Acesta nu poate fi eliberat din funcția de responsabil cu protecția datelor de către instituția sau organul Uniunii care l-a desemnat, dacă nu mai îndeplinește condițiile necesare pentru exercitarea atribuțiilor sale, decât cu acordul Autorității Europene pentru Protecția Datelor.

(9) După desemnarea responsabilului cu protecția datelor, numele acestuia se comunică Autorității Europene pentru Protecția Datelor de către instituția sau organul Uniunii care l-a desemnat.

Articolul 45

Sarcinile responsabilului cu protecția datelor

(1) Responsabilul cu protecția datelor are următoarele sarcini:

(a) informarea și consilierea operatorului sau a persoanei împuternicite de operator, precum și a angajaților care se ocupă de prelucrare cu privire la obligațiile care le revin în temeiul prezentului regulament și al altor dispoziții de drept al Uniunii referitoare la protecția datelor;

(b) asigurarea în mod independent a aplicării interne a prezentului regulament și monitorizarea respectării prezentului regulament, a altor dispoziții de drept al Uniunii în vigoare referitoare la protecția datelor și a politicilor operatorului sau ale persoanei împuternicite de operator în ceea ce privește protecția datelor cu caracter personal, inclusiv alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;

(c) asigurarea informării tuturor persoanelor vizate cu privire la drepturile și obligațiile ce le revin în temeiul prezentului regulament;

(d) furnizarea de consiliere, la cerere, în ceea ce privește necesitatea unei notificări sau a unei comunicări a unei încălcări a datelor cu caracter personal, în temeiul articolelor 34 și 35;

(e) furnizarea de consiliere, la cerere, în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea realizării acestei evaluări în temeiul articolului 39 și consultarea Autorității Europene pentru Protecția Datelor în cazul în care există îndoieli cu privire la necesitatea efectuării unei evaluări a impactului asupra protecției datelor;

(f) furnizarea de consiliere, la cerere, în ceea ce privește necesitatea unei consultări prealabile a Autorității Europene pentru Protecția Datelor în temeiul articolului 40; consultarea acesteia în cazul în care există îndoieli cu privire la necesitatea unei consultări prealabile;

(g) onorarea cererilor Autorității Europene pentru Protecția Datelor; în cadrul sferei sale de competență, cooperarea și consultarea cu Autoritatea Europeană pentru Protecția Datelor, la cererea acesteia din urmă sau din proprie inițiativă;

(h) garantarea faptului că operațiunile de prelucrare nu afectează negativ drepturile și libertățile persoanelor vizate.

(2) Responsabilul cu protecția datelor poate face recomandări operatorului și persoanei împuternicite de acesta în vederea îmbunătățirii concrete a protecției datelor și le poate acorda consultanță cu privire la aspecte referitoare la aplicarea dispozițiilor privind protecția datelor. Mai mult, din proprie inițiativă sau la cererea operatorului ori a persoanei împuternicite de acesta, a Comitetului pentru personal în cauză sau a oricărei alte persoane fizice, poate să cerceteze problemele și faptele legate direct de sarcinile sale, care i-au fost aduse la cunoștință, prezentând un raport persoanei care a solicitat cercetarea sau operatorului ori persoanei împuternicite de acesta.

(3) Fiecare instituție sau organ al Uniunii adoptă norme complementare de punere în aplicare cu privire la responsabilul cu protecția datelor. Normele de aplicare se referă în special la sarcinile, atribuțiile și competențele responsabilului cu protecția datelor.

CAPITOLUL V

TRANSFERURILE DE DATE CU CARACTER PERSONAL CĂTRE ȚĂRI TERȚE SAU ORGANIZAȚII INTERNAȚIONALE

Articolul 46

Principiul general al transferurilor

Orice date cu caracter personal care fac obiectul prelucrării sau care urmează a fi prelucrate după ce sunt transferate într-o țară terță sau către o organizație internațională pot fi transferate doar dacă, sub rezerva celorlalte dispoziții ale prezentului regulament, condițiile prevăzute în prezentul capitol sunt respectate de operator și de persoana împuternicită de operator, inclusiv în ceea ce privește transferurile ulterioare de date cu caracter personal din țara terță sau de la organizația internațională către o altă țară terță sau către o altă organizație internațională. Toate dispozițiile din prezentul capitol se aplică pentru a se asigura că nivelul de protecție a persoanelor fizice garantat prin prezentul regulament nu este subminat.

Articolul 47

Transferuri în temeiul unei decizii privind caracterul adecvat al nivelului de protecție

(1) Transferul de date cu caracter personal către o țară terță sau o organizație internațională se poate realiza atunci când Comisia a decis, în temeiul articolului 45 alineatul (3) din Regulamentul (UE) 2016/679 sau al articolului 36 alineatul (3) din Directiva (UE) 2016/680, că țara terță, un teritoriu ori unul sau mai multe sectoare specificate din acea țară terță sau organizația internațională în cauză asigură un nivel de protecție adecvat, și atunci când datele cu caracter personal sunt transferate exclusiv pentru a permite îndeplinirea sarcinilor care sunt de competența operatorului.

(2) Instituțiile și organele Uniunii informează Comisia și Autoritatea Europeană pentru Protecția Datelor despre situațiile în care consideră că o țară terță, un teritoriu sau unul sau mai multe sectoare specificate dintr-o țară terță sau o organizație internațională în cauză nu asigură un nivel adecvat de protecție în sensul alineatului (1).

(3) Instituțiile și organele Uniunii iau măsurile necesare pentru a se conforma deciziilor luate de către Comisie, care hotărăște, în temeiul articolului 45 alineatul (3) sau (5) din Regulamentul (UE) 2016/679 sau în temeiul articolului 36 alineatul (3) sau (5) din Directiva (UE) 2016/680, dacă o țară terță, un teritoriu sau unul sau mai multe sectoare specificate dintr-o țară terță sau o organizație internațională asigură sau nu mai asigură un nivel adecvat de protecție.

Articolul 48

Transferuri în baza unor garanții adecvate

(1) În absența unei decizii în temeiul articolului 45 alineatul (3) din Regulamentul (UE) 2016/679 sau al articolului 36 alineatul (3) din Directiva (UE) 2016/680, un operator sau persoana împuternicită de operator poate transfera date cu caracter personal către o țară terță sau o organizație internațională numai dacă operatorul sau persoana împuternicită de operator a oferit garanții adecvate și cu condiția să existe drepturi opozabile și căi de atac eficiente pentru persoanele vizate.

(2) Garanțiile adecvate menționate la alineatul (1) pot fi furnizate fără să fie nevoie de vreo autorizație specifică din partea Autorității Europene pentru Protecția Datelor, sub formele următoare:

(a) printr-un instrument obligatoriu din punct de vedere juridic și executoriu între autoritățile sau organismele publice;

(b) prin clauze standard de protecție a datelor adoptate de Comisie în conformitate cu procedura de examinare menționată la articolul 96 alineatul (2);

(c) prin clauze standard de protecție a datelor adoptate de Autoritatea Europeană pentru Protecția Datelor și aprobate de Comisie în conformitate cu procedura de examinare menționată la articolul 96 alineatul (2);

(d) în cazul în care persoana împuternicită de operator nu este o instituție sau un organ al Uniunii, prin reguli corporative obligatorii, coduri de conduită sau mecanisme de certificare, în conformitate cu articolul 46 alineatul (2) literele (b), (e) și (f) din Regulamentul (UE) 2016/679.

(3) Sub rezerva autorizării din partea Autorității Europene pentru Protecția Datelor, garanțiile adecvate menționate la alineatul (1) pot fi furnizate, de asemenea, în special, prin:

(a) clauze contractuale între operator sau persoana împuternicită de operator și operatorul, persoana împuternicită de operator sau destinatarul datelor cu caracter personal din țara terță sau organizația internațională; sau

(b) dispoziții care urmează să fie incluse în acordurile administrative dintre autoritățile sau organismele publice, care includ drepturi opozabile și efective pentru persoanele vizate.

(4) Autorizațiile acordate de Autoritatea Europeană pentru Protecția Datelor în temeiul articolului 9 alineatul (7) din Regulamentul (CE) nr. 45/2001 sunt valabile până la data la care sunt modificate, înlocuite sau abrogate, dacă este necesar, de Autoritatea Europeană pentru Protecția Datelor.

(5) Instituțiile și organele Uniunii informează Autoritatea Europeană Pentru Protecția Datelor despre categoriile de cazuri în care a fost aplicat prezentul articol.

Articolul 49

Transferurile sau divulgările de informații neautorizate de dreptul Uniunii

Orice hotărâre a unei instanțe sau a unui tribunal și orice decizie a unei autorități administrative a unei țări terțe care impun unui operator sau persoanei împuternicite de operator să transfere sau să divulge date cu caracter personal poate fi recunoscută sau executată în orice fel numai dacă se bazează pe un acord internațional, cum ar fi un tratat de asistență judiciară reciprocă în vigoare între țara terță solicitantă și Uniune, fără a se aduce atingere altor motive de transfer în temeiul prezentului capitol.

Articolul 50

Derogări pentru situații specifice

(1) În absența unei decizii privind caracterul adecvat al nivelului de protecție în conformitate cu articolul 45 alineatul (3) din Regulamentul (UE) 2016/679 sau în conformitate cu articolul 36 alineatul (3) din Directiva (UE) 2016/680 sau a unor garanții adecvate în conformitate cu articolul 48 din prezentul regulament, un transfer sau o serie de transferuri de date cu caracter personal către o țară terță sau o organizație internațională are loc numai în condițiile în care:

(a) persoana vizată și-a exprimat în mod explicit acordul cu privire la transferul propus, după ce a fost informată asupra posibilelor riscuri pe care astfel de transferuri le pot implica pentru persoana vizată ca urmare a lipsei unei decizii privind caracterul adecvat al nivelului de protecție și a unor garanții adecvate;

(b) transferul este necesar pentru executarea unui contract între persoana vizată și operator sau pentru aplicarea unor măsuri precontractuale adoptate la cererea persoanei vizate;

(c) transferul este necesar pentru încheierea unui contract sau pentru executarea unui contract încheiat în interesul persoanei vizate între operator și o altă persoană fizică sau juridică;

(d) transferul este necesar din considerente importante de interes public;

(e) transferul este necesar pentru stabilirea, exercitarea sau apărarea unui drept în instanță;

(f) transferul este necesar pentru protejarea intereselor vitale ale persoanei vizate sau ale altor persoane, atunci când persoana vizată nu are capacitatea fizică sau juridică de a-și exprima acordul; sau

(g) transferul este efectuat dintr-un registru care, în conformitate cu dreptul Uniunii, are rolul de a oferi informații publicului și care este deschis spre consultare fie publicului în general, fie oricărei persoane care justifică un interes legitim, dar numai în măsura în care condițiile stabilite în dreptul Uniunii pentru consultare sunt îndeplinite pentru fiecare caz în parte.

(2) Literele (a), (b) și (c) de la alineatul (1) nu se aplică activităților desfășurate de instituții și organe ale Uniunii în exercitarea competențelor lor publice.

(3) Interesul public menționat la alineatul (1) litera (d) este recunoscut în dreptul Uniunii.

(4) Un transfer în temeiul alineatului (1) litera (g) nu implică totalitatea datelor cu caracter personal și nici totalitatea categoriilor de date cu caracter personal cuprinse în registru, cu excepția cazului în care este autorizat de dreptul Uniunii. Atunci când registrul urmează a fi consultat de către persoane care au un interes legitim, transferul se efectuează numai la cererea persoanelor respective sau în cazul în care acestea vor fi destinatarii.

(5) În absența unei decizii privind caracterul adecvat al nivelului de protecție, dreptul Uniunii poate, din considerente importante de interes public, să stabilească în mod expres limite asupra transferului unor categorii specifice de date cu caracter personal către o țară terță sau o organizație internațională.

(6) Instituțiile și organele Uniunii informează Autoritatea Europeană Pentru Protecția Datelor despre categoriile de cazuri în care a fost aplicat prezentul articol.

Articolul 51

Cooperarea internațională în domeniul protecției datelor cu caracter personal

În ceea ce privește țările terțe și organizațiile internaționale, Autoritatea Europeană pentru Protecția Datelor, în cooperare cu Comisia și cu Comitetul european pentru protecția datelor, ia măsurile corespunzătoare pentru:

(a) elaborarea de mecanisme de cooperare internațională pentru a facilita asigurarea aplicării efective a legislației privind protecția datelor cu caracter personal;

(b) acordarea de asistență internațională reciprocă în asigurarea aplicării legislației din domeniul protecției datelor cu caracter personal, inclusiv prin notificare, transferul plângerilor, asistență în investigații și schimb de informații, sub rezerva unor garanții adecvate pentru protecția datelor cu caracter personal și a altor drepturi și libertăți fundamentale;

(c) implicarea părților interesate relevante în discuțiile și activitățile care au ca scop intensificarea cooperării internaționale în domeniul aplicării legislației privind protecția datelor cu caracter personal;

(d) promovarea schimbului reciproc și a documentației cu privire la legislația și practicile în materie de protecție a datelor cu caracter personal, inclusiv în ceea ce privește conflictele jurisdicționale cu țările terțe.

CAPITOLUL VI

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR

Articolul 52

Autoritatea Europeană pentru Protecția Datelor

(1) Se instituie prin prezenta Autoritatea Europeană pentru Protecția Datelor.

(2) În ceea ce privește prelucrarea datelor cu caracter personal, Autoritatea Europeană pentru Protecția Datelor răspunde de asigurarea respectării de către instituțiile și organele Uniunii a drepturilor și libertăților fundamentale ale persoanelor fizice și, în special, a dreptului acestora la protecția datelor.

(3) Autoritatea Europeană pentru Protecția Datelor răspunde de monitorizarea și asigurarea aplicării dispozițiilor prezentului regulament și a oricărui alt act al Uniunii referitor la protecția drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal efectuată de către o instituție sau un organ al Uniunii, precum și de consilierea instituțiilor și organelor Uniunii și a persoanelor vizate cu privire la toate aspectele legate de prelucrarea de date cu caracter personal. În aceste scopuri, Autoritatea Europeană pentru Protecția Datelor îndeplinește sarcinile prevăzute la articolul 57 și exercită competențele care i-au fost conferite prin articolul 58.

(4) Regulamentul (CE) nr. 1049/2001 se aplică documentelor deținute de Autoritatea Europeană pentru Protecția Datelor. Autoritatea Europeană pentru Protecția Datelor adoptă norme detaliate pentru aplicarea Regulamentului (CE) nr. 1049/2001 cu privire la documentele respective.

Articolul 53

Numirea Autorității Europene pentru Protecția Datelor

(1) Parlamentul European și Consiliul numesc de comun acord Autoritatea Europeană pentru Protecția Datelor pentru un mandat de cinci ani, pe baza unei liste întocmite de Comisie în urma unui anunț public de depunere a candidaturilor. Anunțul de depunere a candidaturilor le permite tuturor părților interesate din întreaga Uniune să-și prezinte candidatura. Lista candidaților întocmită de Comisie este publică și conține cel puțin trei candidați. Pe baza listei întocmite de Comisie, comisia competentă a Parlamentului European poate decide organizarea unei audieri care să îi permită să își exprime preferința pentru un candidat.

(2) Lista candidaților menționată la alineatul (1) este alcătuită din personalități care oferă toate garanțiile de independență și care posedă cunoștințe de specialitate în domeniul protecției datelor, precum și experiența și competențele necesare îndeplinirii atribuțiilor de Autoritate Europeană pentru Protecția Datelor.

(3) Mandatul Autorității Europene pentru Protecția Datelor poate fi reînnoit o singură dată.

(4) Atribuțiile Autorității Europene Pentru Protecția Datelor încetează în următoarele situații:

(a) dacă Autoritatea Europeană pentru Protecția Datelor este înlocuită;

(b) dacă Autoritatea Europeană pentru Protecția Datelor demisionează;

(c) în cazul în care Autoritatea Europeană pentru Protecția Datelor este eliberată din funcție sau i se cere să se pensioneze din oficiu.

(5) Autoritatea Europeană pentru Protecția Datelor poate fi demisă sau decăzută din dreptul la pensie sau la alte avantaje echivalente de către Curtea de Justiție, la cererea Parlamentului European, a Consiliului sau a Comisiei, dacă nu mai îndeplinește condițiile necesare pentru exercitarea atribuțiilor sale sau dacă a săvârșit o greșeală gravă.

(6) În cazul înlocuirii obișnuite sau a demisiei voluntare, Autoritatea Europeană pentru Protecția Datelor rămâne totuși în funcție până la numirea unui înlocuitor.

(7) Articolele 11-14 și 17 din Protocolul privind privilegiile și imunitățile Uniunii Europene se aplică și Autorității Europene pentru Protecția Datelor.

Articolul 54

Statutul și condițiile generale de exercitare a atribuțiilor de către Autoritatea Europeană pentru Protecția Datelor, resurse umane și financiare

(1) Autoritatea Europeană pentru Protecția Datelor este asimilată unui judecător al Curții de Justiție în ceea ce privește stabilirea remunerației, a indemnizațiilor, a pensiei pentru limită de vârstă și a oricăror altor prestații care țin loc de remunerație.

(2) Autoritatea bugetară se asigură că Autoritatea Europeană pentru Protecția Datelor dispune de resursele umane și financiare necesare îndeplinirii îndatoririlor sale.

(3) Bugetul Autorității Europene pentru Protecția Datelor figurează la o rubrică bugetară separată a secțiunii referitoare la cheltuielile administrative din bugetul general al Uniunii.

(4) Autoritatea Europeană pentru Protecția Datelor este asistată de un secretariat. Funcționarii și ceilalți membri ai personalului din cadrul secretariatului sunt numiți de Autoritatea Europeană pentru Protecția Datelor, iar superiorul lor ierarhic este Autoritatea Europeană pentru Protecția Datelor. Aceștia se află exclusiv sub conducerea sa. Numărul lor este stabilit în fiecare an în cadrul procedurii bugetare. Articolul 75 alineatul (2) din Regulamentul (UE) 2016/679 se aplică personalului Autorității Europene pentru Protecția Datelor implicat în îndeplinirea sarcinilor conferite Comitetului european pentru protecția datelor de dreptul Uniunii.

(5) Funcționarii și ceilalți membri de personal ai secretariatului Autorității Europene pentru Protecția Datelor intră sub incidența normelor și reglementărilor aplicabile funcționarilor și altor agenți ai Uniunii.

(6) Sediul Autorității Europene pentru Protecția Datelor este la Bruxelles.

Articolul 55

Independența

(1) Autoritatea Europeană pentru Protecția Datelor beneficiază de independență deplină în îndeplinirea sarcinilor sale și în exercitarea competențelor sale în conformitate cu prezentul regulament.

(2) Autoritatea Europeană pentru Protecția Datelor, în cadrul îndeplinirii sarcinilor și al exercitării competențelor sale în conformitate cu prezentul regulament, rămâne independentă de orice influență externă directă sau indirectă și nici nu solicită, nici nu acceptă instrucțiuni de la o parte externă.

(3) Autoritatea Europeană pentru Protecția Datelor se abține de la orice act incompatibil cu caracterul atribuțiilor sale și, pe durata mandatului, nu poate exercita nici o altă activitate, remunerată sau nu.

(4) După încetarea mandatului său, Autoritatea Europeană pentru Protecția Datelor este obligată să manifeste integritate și discreție în ceea ce privește acceptarea anumitor funcții sau beneficii.

Articolul 56

Secretul profesional

Autoritatea Europeană pentru Protecția Datelor, precum și personalul acesteia, atât pe durata mandatului, cât și după încetarea acestuia, au obligația să respecte secretul profesional cu privire la informațiile confidențiale la care au avut acces în îndeplinirea îndatoririlor lor.

Articolul 57

Sarcini

(1) Fără a aduce atingere altor sarcini stabilite în temeiul prezentului regulament, Autoritatea Europeană pentru Protecția Datelor:

(a) monitorizează și asigură aplicarea prezentului regulament de către instituțiile și organele Uniunii, cu excepția prelucrării de date cu caracter personal de către Curtea de Justiție în exercitarea atribuțiilor sale judiciare;

(b) promovează acțiuni de sensibilizare și de înțelegere în rândul publicului a riscurilor, normelor, garanțiilor și drepturilor în materie de prelucrare. Se acordă atenție specială activităților care se adresează în mod specific copiilor;

(c) promovează acțiuni de sensibilizare a operatorilor și a persoanelor împuternicite de aceștia cu privire la obligațiile care le revin în temeiul prezentului regulament;

(d) la cerere, furnizează informații oricărei persoane vizate în legătură cu exercitarea drepturilor sale prevăzute în prezentul regulament și, dacă este cazul, cooperează cu autoritățile naționale de supraveghere în acest scop;

(e) tratează plângerile depuse de o persoană vizată, un organism, o organizație sau o asociație în conformitate cu articolul 67 și investighează într-o măsură adecvată obiectul plângerii și informează reclamantul cu privire la evoluția și rezultatul investigației, într-un termen rezonabil, în special dacă este necesară efectuarea unei investigații mai amănunțite sau coordonarea cu o altă autoritate de supraveghere;

(f) desfășoară investigații privind aplicarea prezentului regulament, inclusiv pe baza unor informații primite de la o altă autoritate de supraveghere sau de la o altă autoritate publică;

(g) oferă consiliere, din proprie inițiativă sau la cerere, tuturor instituțiilor și organelor Uniunii cu privire la măsurile legislative și administrative referitoare la protecția drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal;

(h) monitorizează noutățile care prezintă interes, dacă acestea au incidență asupra protecției datelor cu caracter personal, în special evoluția tehnologiei informațiilor și a comunicațiilor;

(i) adoptă clauzele contractuale standard menționate la articolul 29 alineatul (8) și la articolul 48 alineatul (2) litera (c);

(j) întocmește și menține la zi o listă în legătură cu cerința privind evaluarea impactului asupra protecției datelor, în conformitate cu articolul 39 alineatul (4);

(k) participă la activitățile Comitetului european pentru protecția datelor;

(l) asigură secretariatul Comitetului european pentru protecția datelor, în conformitate cu articolul 75 din Regulamentul (UE) 2016/679;

(m) oferă consiliere cu privire la operațiunile de prelucrare menționate la articolul 40 alineatul (2);

(n) autorizează clauzele și dispozițiile contractuale menționate la articolul 48 alineatul (3);

(o) menține la zi evidențe interne privind încălcările prezentului regulament și măsurile luate în conformitate cu articolul 58 alineatul (2);

(p) îndeplinește orice alte sarcini legate de protecția datelor cu caracter personal; și

(q) își elaborează regulamentul de procedură.

(2) Autoritatea Europeană pentru Protecția Datelor facilitează depunerea plângerilor menționate la alineatul (1) litera (e) printr-un formular de depunere a plângerii care poate fi completat și în format electronic, fără a exclude alte mijloace de comunicare.

(3) Îndeplinirea sarcinilor de către Autoritatea Europeană pentru Protecția Datelor este gratuită pentru persoana vizată.

(4) În cazul în care cererile sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, Autoritatea Europeană pentru Protecția Datelor poate refuza să le dea curs. Sarcina de a demonstra caracterul vădit nefondat sau excesiv al cererii revine Autorității Europene pentru Protecția Datelor.

Articolul 58

Competențe

(1) Autoritatea Europeană pentru Protecția Datelor deține următoarele competențe de investigare:

(a) de a da dispoziții operatorului și persoanei împuternicite de operator să furnizeze orice informații pe care le solicită în vederea îndeplinirii sarcinilor sale;

(b) de a efectua investigații sub formă de audituri privind protecția datelor;

(c) de a notifica operatorul sau persoana împuternicită de operator cu privire la o presupusă încălcare a prezentului regulament;

(d) de a obține, din partea operatorului și a persoanei împuternicite de operator, accesul la toate datele cu caracter personal și la toate informațiile necesare pentru îndeplinirea sarcinilor sale;

(e) de a obține accesul la oricare dintre incintele operatorului și ale persoanei împuternicite de operator, inclusiv la orice echipamente și mijloace de prelucrare a datelor, în conformitate cu dreptul Uniunii.

(2) Autoritatea Europeană pentru Protecția Datelor deține următoarele competențe corective:

(a) de a emite avertizări în atenția unui operator sau a unei persoane împuternicite de operator cu privire la probabilitatea ca operațiunile de prelucrare prevăzute să încalce dispozițiile prezentului regulament;

(b) de a emite mustrări adresate unui operator sau unei persoane împuternicite de operator în cazul în care operațiunile de prelucrare au încălcat dispozițiile prezentului regulament;

(c) de a sesiza operatorul sau persoana împuternicită de operator în cauză și, dacă este necesar, Parlamentul European, Consiliul și Comisia;

(d) de a da dispoziții operatorului sau persoanei împuternicite de operator să respecte cererile persoanei vizate de a-și exercita drepturile în temeiul prezentului regulament;

(e) de a da dispoziții operatorului sau persoanei împuternicite de operator să asigure conformitatea operațiunilor de prelucrare cu dispozițiile prezentului regulament, specificând, după caz, modalitatea și termenul-limită pentru aceasta;

(f) de a obliga operatorul să informeze persoana vizată cu privire la o încălcare a protecției datelor cu caracter personal;

(g) de a impune o limitare temporară sau definitivă, inclusiv o interdicție asupra prelucrării;

(h) de a dispune rectificarea sau ștergerea datelor cu caracter personal sau restricționarea prelucrării, în temeiul articolelor 18, 19 și 20, precum și notificarea acestor acțiuni destinatarilor cărora le-au fost divulgate datele cu caracter personal, în conformitate cu articolul 19 alineatul (2) și cu articolul 21;

(i) de a aplica amenzi administrative în temeiul articolului 66 în cazul în care o instituție sau un organ al Uniunii nu respectă una dintre măsurile menționate la literele (d)-(h) și (j) de la prezentul alineat, în funcție de circumstanțele fiecărui caz în parte;

(j) de a dispune suspendarea fluxurilor de date către un destinatar dintr-un stat membru, dintr-o țară terță sau către o organizație internațională.

(3) Autoritatea Europeană pentru Protecția Datelor deține următoarele competențe de autorizare și de consiliere:

(a) de a oferi consiliere persoanelor vizate în ceea ce privește exercitarea drepturilor acestora;

(b) de a oferi consiliere operatorului în conformitate cu procedura de consultare prealabilă menționată la articolul 40, în conformitate cu articolul 41 alineatul (2);

(c) de a emite avize, din proprie inițiativă sau la cerere, adresate instituțiilor și organelor Uniunii, precum și publicului, cu privire la orice aspect legat de protecția datelor cu caracter personal;

(d) de a adopta clauzele standard în materie de protecție a datelor menționate la articolul 29 alineatul (8) și la articolul 48 alineatul (2) litera (c);

(e) de a autoriza clauzele contractuale menționate la articolul 48 alineatul (3) litera (a);

(f) de a autoriza acordurile administrative menționate la articolul 48 alineatul (3) litera (b).

(g) de a autoriza operațiuni de prelucrare în conformitate cu acte de punere în aplicare adoptate în temeiul articolului 40 alineatul (4).

(4) Autoritatea Europeană pentru Protecția Datelor are competența de a sesiza Curtea de Justiție în condițiile prevăzute de tratate și de a interveni în acțiunile introduse la Curtea de Justiție.

(5) Exercitarea competențelor conferite Autorității Europene pentru Protecția Datelor în temeiul prezentului articol face obiectul unor garanții adecvate, inclusiv căi de atac judiciare eficiente și procese echitabile, prevăzute în dreptul Uniunii.

Articolul 59

Obligația operatorilor și a persoanelor împuternicite de operator de a răspunde la acuzații

În cazul în care Autoritatea Europeană pentru Protecția Datelor își exercită competențele prevăzute la articolul 58 alineatul (2) literele (a), (b) și (c), operatorul sau persoana împuternicită de operator în cauză informează Autoritatea Europeană pentru Protecția Datelor cu privire la opinia sa într-un termen rezonabil care urmează să fie precizat de către Autoritatea Europeană pentru Protecția Datelor ținând cont de circumstanțele fiecărui caz în parte. Răspunsul conține, de asemenea, o descriere a măsurilor întreprinse, dacă acestea există, ca răspuns la observațiile Autorității Europene pentru Protecția Datelor.

Articolul 60

Raport de activitate

(1) Autoritatea Europeană pentru Protecția Datelor prezintă Parlamentului European, Consiliului și Comisiei un raport anual privind activitățile sale, pe care îl publică în același timp.

(2) Autoritatea Europeană pentru Protecția Datelor trimite raportul menționat la alineatul (1) celorlalte instituții și organe ale Uniunii, care pot prezenta observații în vederea unei posibile examinări a raportului de către Parlamentul European.

CAPITOLUL VII

COOPERARE ȘI COERENȚĂ

Articolul 61

Cooperarea dintre Autoritatea Europeană pentru Protecția Datelor și autoritățile naționale de supraveghere

Autoritatea Europeană pentru Protecția Datelor cooperează cu autoritățile naționale de supraveghere și cu autoritatea comună de control instituită în temeiul articolului 25 din Decizia 2009/917/JAI a Consiliului ([1]) în măsura în care este necesar pentru îndeplinirea atribuțiilor care revin fiecăreia, în special transmițându-și reciproc informații relevante, solicitându-și reciproc să își exercite competențele și răspunzând la cererile fiecăreia.

Articolul 62

Supravegherea coordonată de către Autoritatea Europeană pentru Protecția Datelor și de către autoritățile naționale de supraveghere

(1) În cazul în care un act al Uniunii face trimitere la prezentul articol, Autoritatea Europeană pentru Protecția Datelor și autoritățile naționale de supraveghere cooperează în mod activ în cadrul responsabilităților lor respective, fiecare acționând în cadrul competențelor sale, pentru a asigura o supraveghere eficace a sistemelor informatice la scară largă și a organelor, oficiilor și agențiilor Uniunii.

(2) Acționând fiecare în cadrul propriilor competențe și responsabilități acestea fac, dacă este necesar, schimb de informații relevante, își acordă reciproc asistență în efectuarea de audituri și inspecții, examinează dificultățile de interpretare sau de aplicare a prezentului regulament și a altor acte aplicabile ale Uniunii, studiază problemele legate de exercitarea supravegherii independente sau de exercitarea drepturilor persoanelor vizate, redactează propuneri armonizate privind soluții la eventualele probleme și promovează sensibilizarea cu privire la drepturile privind protecția datelor.

(3) În scopurile enunțate la alineatul (2), Autoritatea Europeană pentru Protecția Datelor și autoritățile naționale de supraveghere se întâlnesc cel puțin de două ori pe an în cadrul Comitetului european pentru protecția datelor. În acest scop, Comitetul european pentru protecția datelor poate elabora alte metode de lucru, dacă este necesar.

(4) Comitetul european pentru protecția datelor transmite Parlamentului European, Consiliului și Comisiei, o dată la doi ani, un raport comun al activităților în ceea ce privește supravegherea coordonată.

([1]) Decizia 2009/917/JAI a Consiliului din 30 noiembrie 2009 privind utilizarea tehnologiei informației în domeniul vamal (JO L 323, 10.12.2009, p. 20).

CAPITOLUL VIII

CĂI DE ATAC, RĂSPUNDERE ȘI SANCȚIUNI

Articolul 63

Dreptul de a depune o plângere la Autoritatea Europeană pentru Protecția Datelor

(1) Fără a aduce atingere oricărei căi de atac judiciare, administrative sau nejudiciare, orice persoană vizată are dreptul de a depune o plângere la Autoritatea Europeană pentru Protecția Datelor în cazul în care consideră că prelucrarea datelor sale cu caracter personal încalcă prevederile prezentului regulament.

(2) Autoritatea Europeană pentru Protecția Datelor informează reclamantul cu privire la evoluția și soluționarea plângerii, inclusiv cu privire la posibilitatea de a exercita o cale de atac judiciară în temeiul articolului 64.

(3) În cazul în care Autoritatea Europeană pentru Protecția Datelor nu se ocupă de o plângere sau nu informează persoana vizată în termen de trei luni cu privire la evoluția sau la soluționarea plângerii, se consideră că Autoritatea Europeană pentru Protecția Datelor a adoptat o decizie negativă.

Articolul 64

Dreptul la o cale de atac judiciară eficientă

(1) Curtea de Justiție are competența de a soluționa orice litigiu privind dispozițiile prezentului regulament, inclusiv de a se pronunța asupra cererilor de despăgubiri.

(2) Acțiunile împotriva deciziilor Autorității Europene pentru Protecția Datelor, inclusiv împotriva deciziilor în temeiul articolului 63 alineatul (3), sunt introduse în fața Curții de Justiție.

(3) Curtea de Justiție are competența de fond în materie de control al amenzilor administrative menționate la articolul 66. Aceasta poate anula, reduce sau majora amenzile respective în limitele articolului 66.

Articolul 65

Dreptul la despăgubiri

Orice persoană care a suferit un prejudiciu material sau moral ca urmare a unei încălcări a prezentului regulament are dreptul să obțină despăgubiri de la instituția sau organul Uniunii pentru prejudiciul suferit, în condițiile prevăzute de tratate.

Articolul 66

Amenzi administrative

(1) Autoritatea Europeană pentru Protecția Datelor poate aplica amenzi administrative instituțiilor și organelor Uniunii, în funcție de circumstanțele fiecărui caz în parte, în cazul în care o instituție sau un organ al Uniunii nu se supune unui ordin al Autorității Europene pentru Protecția Datelor în temeiul articolului 58 alineatul (2) literele (d)-(h) și (j). Atunci când se ia decizia privind oportunitatea aplicării unei amenzi administrative și decizia cu privire la valoarea amenzii administrative în fiecare caz în parte, se acordă atenția cuvenită următoarelor aspecte:

(a) natura, gravitatea și durata încălcării, ținându-se seama de natura, domeniul de aplicare sau scopul prelucrării în cauză, precum și de numărul persoanelor vizate afectate și de nivelul prejudiciilor suferite de acestea;

(b) orice acțiune întreprinsă de instituția sau organul Uniunii pentru a reduce prejudiciul suferit de persoanele vizate;

(c) gradul de responsabilitate al instituției sau al organului Uniunii, ținându-se seama de măsurile tehnice și organizatorice puse în aplicare de acestea în temeiul articolelor 27 și 33;

(d) eventuale încălcări anterioare similare comise de instituția sau de organul Uniunii;

(e) gradul de cooperare cu Autoritatea Europeană pentru Protecția Datelor pentru a remedia încălcarea și a atenua posibilele efecte negative ale acesteia;

(f) categoriile de date cu caracter personal afectate de încălcare;

(g) modul în care încălcarea a fost adusă la cunoștința Autorității Europene pentru Protecția Datelor, în special dacă și în ce măsură instituția sau organul Uniunii a notificat încălcarea;

(h) respectarea oricăreia dintre măsurile menționate la articolul 58 luate anterior împotriva instituției sau a organului Uniunii cu privire la aceeași chestiune. Procedurile care conduc la aplicarea acestor amenzi se desfășoară într-un interval de timp rezonabil în funcție de circumstanțele cazului și luând în considerare acțiunile și procedurile relevante menționate la articolul 69.

(2) Încălcările obligațiilor prevăzute la articolele 8, 12, 27-35, 39, 40, 43, 44 și 45, săvârșite de către instituția sau organul Uniunii fac, în conformitate cu alineatul (1) de la prezentul articol, obiectul unor amenzi administrative de până la 25 000 EUR pentru fiecare încălcare, în limita unui cuantum total de 250 000 EUR pe an.

(3) Încălcările următoarelor prevederi de către instituția sau organul Uniunii fac, în conformitate cu alineatul (1), obiectul unor amenzi administrative de până la 50 000 EUR pentru fiecare încălcare, în limita unui cuantum total de 500 000 EUR pe an:

(a) principiile de bază pentru prelucrare, inclusiv condițiile privind consimțământul, în conformitate cu articolele 4, 5, 7 și 10;

(b) drepturile persoanelor vizate în conformitate cu articolele 14-24;

(c) transferurile de date cu caracter personal către un destinatar dintr-o țară terță sau o organizație internațională, în conformitate cu articolele 46-50.

(4) În cazul în care o instituție sau un organ al Uniunii, pentru aceeași operațiune de prelucrare sau pentru operațiuni de prelucrare conexe sau continue, încalcă mai multe dispoziții din prezentul regulament sau aceeași dispoziție din regulament de mai multe ori, cuantumul total al amenzii administrative nu depășește suma prevăzută pentru cea mai gravă încălcare.

(5) Înaintea adoptării unor decizii în temeiul prezentului articol, Autoritatea Europeană pentru Protecția Datelor oferă instituției sau organului Uniunii care face obiectul procedurilor desfășurate de Autoritatea Europeană pentru Protecția Datelor posibilitatea de a se exprima în cadrul unei audieri în legătură cu aspectele cu privire la care Autoritatea Europeană pentru Protecția Datelor a ridicat obiecții. Autoritatea Europeană pentru Protecția Datelor își fundamentează deciziile doar pe obiecțiile asupra cărora părțile în cauză au putut formula observații. Reclamanții sunt implicați îndeaproape în proceduri.

(6) Drepturile la apărare ale părților în cauză sunt pe deplin garantate în cadrul procedurilor. Părțile au drept de acces la dosarul Autorității Europene pentru Protecția Datelor, sub rezerva interesului legitim al persoanelor fizice sau al întreprinderilor în ceea ce privește protecția datelor cu caracter personal sau a secretelor comerciale ale acestora.

(7) Fondurile colectate prin aplicarea amenzilor prevăzute la prezentul articol constituie venituri la bugetul general al Uniunii.

Articolul 67

Reprezentarea persoanelor vizate

Persoana vizată are dreptul de a mandata un organism, o organizație sau o asociație fără scop lucrativ, care au fost constituite în mod corespunzător în conformitate cu dreptul Uniunii sau cu dreptul unui stat membru, ale căror obiective statutare sunt de interes public, care sunt active în domeniul protecției drepturilor și libertăților persoanelor vizate în ceea ce privește protecția datelor lor cu caracter personal, să depună plângerea în numele său la Autoritatea Europeană pentru Protecția Datelor, să exercite în numele său drepturile menționate la articolele 63 și 64, precum și să exercite, în numele său, dreptul de a primi despăgubiri menționat la articolul 65.

Articolul 68

Plângerile înaintate de personalul Uniunii

Orice persoană angajată de o instituție sau un organ al Uniunii poate depune o plângere la Autoritatea Europeană pentru Protecția Datelor privind o presupusă încălcare a dispozițiilor prezentului regulament, inclusiv fără a acționa pe căi oficiale. Nimeni nu trebuie să sufere prejudicii din cauza unei plângeri depuse la Autoritatea Europeană pentru Protecția Datelor care susține existența unei astfel de încălcări.

Articolul 69

Sancțiuni

În cazul în care un funcționar sau un alt agent al Uniunii Europene nu respectă obligațiile prevăzute de prezentul regulament, fie intenționat sau din neglijență, funcționarul sau agentul Uniunii Europene este pasibil de sancțiuni disciplinare sau alte măsuri, conform normelor și procedurilor prevăzute de Statutul funcționarilor.

CAPITOLUL IX

PRELUCRAREA DATELOR OPERAȚIONALE CU CARACTER PERSONAL DE CĂTRE ORGANELE, OFICIILE ȘI AGENȚIILE UNIUNII ATUNCI CÂND ACESTEA DESFĂȘOARĂ ACTIVITĂȚI CARE INTRĂ SUB INCIDENȚA PĂRȚII A TREIA TITLUL V CAPITOLUL 4 SAU CAPITOLUL 5 DIN TFUE

Articolul 70

Domeniul de aplicare al prezentului capitol

Prezentul capitol se aplică exclusiv prelucrării datelor operaționale cu caracter personal de către organele, oficiile și agențiile Uniunii atunci când acestea desfășoară activități care intră sub incidența părții a treia titlul V capitolul 4 sau capitolul 5 din TFUE, fără a aduce atingere normelor specifice de protecție a datelor aplicabile acestor organe, oficii sau agenții ale Uniunii.

Articolul 71

Principii legate de prelucrarea datelor operaționale cu caracter personal

(1) Datele operaționale cu caracter personal:

(a) sunt prelucrate în mod legal și echitabil („legalitate și echitate”);

(b) sunt colectate într-un scop determinat, explicit și legitim și nu sunt prelucrate într-un mod incompatibil cu acest scop („limitarea scopului”);

(c) sunt adecvate, pertinente și neexcesive în raport cu scopul în care sunt prelucrate („reducerea la minimum a datelor”);

(d) sunt exacte și, dacă este necesar, actualizate; se iau toate măsurile rezonabile pentru a se garanta că datele operaționale cu caracter personal care sunt inexacte, având în vedere scopul pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere („exactitatea”);

(e) sunt păstrate într-o formă care permite identificarea persoanelor vizate fără a se depăși timpul necesar realizării scopului în care sunt prelucrate datele operaționale cu caracter personal („limitarea timpului de păstrare”);

(f) sunt prelucrate într-un mod care asigură un grad adecvat de securitate a datelor operaționale cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, fiind luate măsuri tehnice sau organizatorice corespunzătoare („integritate și confidențialitate”).

(2) Se permite prelucrarea de către același operator sau de către un alt operator, în oricare dintre scopurile stabilite în actul juridic de instituire a organului, a oficiului sau a agenției Uniunii pe lângă scopul pentru care au fost colectate datele operaționale cu caracter personal, în măsura în care:

(a) operatorul este autorizat să prelucreze astfel de date operaționale cu caracter personal în scopul respectiv în conformitate cu dreptul Uniunii; și

(b) prelucrarea este necesară și proporțională în raport cu scopul secundar respectiv, în conformitate cu dreptul Uniunii.

(3) Prelucrarea de către același operator sau de către un alt operator poate include arhivarea în interes public sau în scopuri științifice, statistice sau istorice, pentru scopurile stabilite în actul juridic de instituire a respectivului organ, oficiu sau agenție a Uniunii, cu condiția unor garanții adecvate privind respectarea drepturilor și a libertăților persoanelor vizate.

(4) Operatorul este responsabil de respectarea alineatelor (1), (2) și (3) și este în măsură să demonstreze că aceste dispoziții au fost respectate.

Articolul 72

Legalitatea prelucrării datelor operaționale cu caracter personal

(1) Prelucrarea datelor operaționale cu caracter personal este legală numai dacă și în măsura în care prelucrarea în cauză este necesară pentru executarea unei sarcini realizate de către organele, oficiile și agențiile Uniunii atunci când desfășoară activități care intră sub incidența părții a treia titlul V capitolul 4 sau capitolul 5 din TFUE și se întemeiază pe dreptul Uniunii.

(2) În actele juridice specifice ale Uniunii prin care se reglementează prelucrarea în temeiul prezentului capitol se precizează cel puțin obiectivele prelucrării, datele operaționale cu caracter personal ce urmează să fie prelucrate, scopul prelucrării și perioada de păstrare a datelor operaționale cu caracter personal sau periodicitatea cu care este examinată necesitatea ca datele operaționale respective cu caracter personal să fie păstrate în continuare.

Articolul 73

Deosebirea dintre diferitele categorii de persoane vizate

După caz și în măsura posibilului, operatorul face o distincție clară între datele operaționale cu caracter personal ale diferitelor categorii de persoane vizate, precum categoriile enumerate în actele juridice de instituire a organelor, oficiilor și agențiilor Uniunii.

Articolul 74

Deosebirea diferitelor tipuri de date operaționale cu caracter personal și verificarea calității datelor operaționale cu caracter personal

(1) Operatorul face deosebirea, în măsura posibilului, între datele operaționale cu caracter personal ce se bazează pe fapte și datele operaționale cu caracter personal ce se bazează pe o apreciere personală.

(2) Operatorul ia toate măsurile rezonabile pentru a se asigura că datele operaționale cu caracter personal care sunt inexacte, incomplete sau perimate nu sunt transmise sau puse la dispoziție. În acest scop, operatorul verifică, în măsura în care este posibil și relevant, calitatea datelor cu caracter personal înainte ca acestea să fie transmise sau puse la dispoziție, de exemplu consultând autoritatea competentă de la care provin datele. În măsura în care acest lucru este posibil, de fiecare dată când transmite date operaționale cu caracter personal, operatorul adaugă informațiile necesare care să-i permită destinatarului să evalueze gradul de exactitate, caracterul integral, gradul de fiabilitate al datelor operaționale cu caracter personal, precum și măsura în care acestea sunt actuale.

(3) În cazul în care se constată că au fost transmise date operaționale cu caracter personal incorecte sau au fost transmise date operaționale cu caracter personal în mod ilegal, acest lucru se comunică de îndată destinatarului. În acest caz, datele operaționale cu caracter personal respective sunt rectificate ori șterse sau prelucrarea lor este limitată în conformitate cu articolul 82.

Articolul 75

Condiții specifice de prelucrare

(1) Atunci când dreptul Uniunii aplicabilă operatorului care transmite datele prevede condiții specifice de prelucrare, operatorul informează destinatarul datelor operaționale cu caracter personal cu privire la aceste condiții și la obligația de a le respecta.

(2) Operatorul respectă condițiile specifice de prelucrare prevăzute de autoritatea națională competentă care transmite datele în conformitate cu articolul 9 alineatele (3) și (4) din Directiva (UE) 2016/680.

Articolul 76

Prelucrarea categoriilor speciale de date operaționale cu caracter personal

(1) Prelucrarea datelor cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice și afilierea sindicală, precum și prelucrarea datelor genetice, a datelor biometrice pentru identificarea unică a unei persoane fizice, a datelor operaționale cu caracter personal privind starea sănătății sau viața sexuală ori orientarea sexuală a unei persoane fizice este autorizată numai atunci când este strict necesară în scopuri operaționale și se încadrează în mandatul respectivului organ, oficiu sau agenție a Uniunii și sub rezerva unor garanții adecvate pentru drepturile și libertățile persoanei vizate. Este interzisă discriminarea persoanelor fizice pe baza acestor date cu caracter personal.

(2) Responsabilul cu protecția datelor este informat imediat cu privire la cazurile în care se aplică prezentul articol.

Articolul 77

Procesul decizional individual automatizat, inclusiv crearea de profiluri

(1) O decizie bazată numai pe prelucrarea automatizată, inclusiv întocmirea unui profil, care produce un efect juridic advers privind persoana vizată sau care o afectează în mod semnificativ, este interzisă, cu excepția cazului în care acest lucru este autorizat de dreptul Uniunii care îl vizează pe operator și care oferă garanții adecvate privind drepturile și libertățile persoanei vizate, cel puțin privind dreptul la o intervenție umană din partea operatorului.

(2) Deciziile menționate la alineatul (1) din prezentul articol nu se întemeiază pe categoriile speciale de date cu caracter personal menționate la articolul 76, cu excepția cazului în care au fost instituite măsuri corespunzătoare pentru protejarea drepturilor, a libertăților și a intereselor legitime ale persoanei vizate.

(3) În conformitate cu dreptul Uniunii, este interzisă crearea de profiluri care are drept rezultat discriminarea persoanelor fizice pe baza categoriilor speciale de date cu caracter personal menționate la articolul 76.

Articolul 78

Comunicarea și modalitățile de exercitare a drepturilor persoanei vizate

(1) Operatorul ia măsuri rezonabile pentru a transmite persoanei vizate toate informațiile menționate la articolul 79 și îi transmite acesteia toate comunicările în legătură cu articolele 80-84 și cu articolul 92 referitoare la prelucrare, într-o formă concisă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu. Informațiile se transmit prin orice mijloace adecvate, inclusiv prin mijloace electronice. Ca regulă generală, operatorul transmite informațiile în același format în care a fost primită cererea.

(2) Operatorul facilitează exercitarea drepturilor persoanei vizate în temeiul articolelor 79-84.

(3) Operatorul informează în scris persoana vizată cu privire la modul în care a dat curs cererii acesteia, fără întârzieri nejustificate și, în orice caz, în termen de trei luni de la primirea cererii din partea persoanei vizate.

(4) Operatorul transmite gratuit informațiile vizate la articolul 79 și realizează gratuit comunicările și măsurile prevăzute la articolele 80-84 și la articolul 92. În cazul în care cererile din partea unei persoane vizate sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, operatorul poate refuza să dea curs cererii. În aceste cazuri, operatorului îi revine sarcina de a demonstra caracterul vădit nefondat sau excesiv al cererii.

(5) În cazul în care are îndoieli întemeiate cu privire la identitatea persoanei fizice care înaintează cererea menționată la articolul 80 sau 82, operatorul poate solicita să-i prezinte informații suplimentare, necesare pentru a confirma identitatea persoanei vizate.

Articolul 79

Informații care se pun la dispoziția persoanei vizate sau se comunică acesteia

(1) Operatorul pune la dispoziția persoanei vizate cel puțin următoarele informații:

(a) identitatea și datele de contact ale organului, oficiului sau agenției Uniunii;

(b) datele de contact ale responsabilului cu protecția datelor;

(c) scopul în care sunt prelucrate datele operaționale cu caracter personal;

(d) dreptul de a depune o plângere la Autoritatea Europeană pentru Protecția Datelor și datele de contact ale acesteia;

(e) existența dreptului de a solicita operatorului acces la datele operaționale cu caracter personal referitoare la persoana vizată și rectificarea sau ștergerea datelor respective sau restricționarea prelucrării lor.

(2) În plus față de informațiile menționate la alineatul (1), operatorul îi comunică persoanei vizate, în anumite cazuri prevăzute de legislația Uniunii, următoarele informații suplimentare, pentru a-i permite acesteia să-și exercite drepturile:

(a) temeiul juridic al prelucrării;

(b) perioada în care vor fi păstrate datele operaționale cu caracter personal sau, în cazul în care nu este posibil, criteriile utilizate pentru a stabili această perioadă;

(c) dacă este cazul, categoriile de destinatari ai datelor operaționale cu caracter personal, inclusiv în țări terțe sau organizații internaționale;

(d) în cazul în care este necesar, informații suplimentare, în special atunci când datele operaționale cu caracter personal sunt colectate fără știrea persoanei vizate.

(3) Operatorul poate amâna, restricționa sau omite furnizarea de informații persoanei vizate în conformitate cu alineatul (2) în măsura în care și atât timp cât o astfel de măsură constituie o măsură necesară și proporțională într-o societate democratică, ținând seama în mod corespunzător de drepturile fundamentale și de interesele legitime ale persoanei fizice în cauză, pentru:

(a) a evita obstrucționarea cercetărilor, anchetelor sau procedurilor oficiale sau juridice;

(b) a nu prejudicia prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor sau executarea pedepselor;

(c) a proteja securitatea publică a statelor membre;

(d) a proteja securitatea națională a statelor membre;

(e) a proteja drepturile și libertățile altora, de exemplu ale victimelor și martorilor.

Articolul 80

Dreptul de acces al persoanei vizate

Persoana vizată are dreptul de a obține din partea operatorului o confirmare dacă se prelucrează sau nu date cu caracter personal care o privesc și, în caz afirmativ, are dreptul de a obține acces la datele operaționale cu caracter personal și la următoarele informații:

(a) scopurile și temeiul juridic al prelucrării;

(b) categoriile datelor operaționale cu caracter personal vizate;

(c) destinatarii sau categoriile de destinatari cărora le-au fost divulgate datele operaționale cu caracter personal, în special destinatarii din țări terțe sau organizații internaționale;

(d) acolo unde este posibil, perioada pentru care se preconizează că vor fi stocate datele operaționale cu caracter personal sau, dacă nu este posibil, criteriile utilizate pentru a determina această perioadă;

(e) existența dreptului de a solicita de la operator rectificarea sau ștergerea datelor operaționale cu caracter personal sau restricționarea prelucrării datelor operaționale cu caracter personal referitoare la persoana vizată;

(f) dreptul de a depune o plângere la Autoritatea Europeană pentru Protecția Datelor și datele de contact ale acesteia;

(g) comunicarea datelor operaționale cu caracter personal care sunt în curs de prelucrare și a oricăror informații disponibile cu privire la originea acestora.

Articolul 81

Limitarea dreptului de acces

(1) Operatorul poate limita, integral sau parțial, dreptul de acces al persoanei vizate în măsura în care și atât timp cât o astfel de limitare, parțială sau totală, constituie o măsură necesară și proporțională într-o societate democratică, ținând seama în mod corespunzător de drepturile fundamentale și de interesele legitime ale persoanei fizice în cauză, pentru:

(a) a evita obstrucționarea cercetărilor, anchetelor sau procedurilor oficiale sau juridice;

(b) a nu prejudicia prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor sau executarea pedepselor;

(c) a proteja securitatea publică a statelor membre;

(d) a proteja securitatea națională a statelor membre;

(e) a proteja drepturile și libertățile altora, de exemplu ale victimelor și martorilor.

(2) În cazurile prevăzute la alineatul (1), operatorul informează în scris persoana vizată, fără întârzieri nejustificate, cu privire la orice refuz sau restricționare a accesului și la motivele refuzului sau ale restricționării. Aceste informații pot fi omise atunci când furnizarea lor ar contraveni unuia dintre scopurile de la alineatul (1). Operatorul informează persoana vizată cu privire la posibilitatea de a depune o plângere la Autoritatea Europeană pentru Protecția Datelor sau de a introduce o cale de atac în fața Curții de Justiție. Operatorul justifică motivele de fapt sau de drept pe care se întemeiază decizia. Aceste informații sunt puse la dispoziția Autorității Europene pentru Protecția Datelor, la cerere.

Articolul 82

Dreptul la rectificarea sau ștergerea datelor operaționale cu caracter personal și restricționarea prelucrării acestora

(1) Orice persoană vizată are dreptul de a obține de la operator, fără întârzieri nejustificate, rectificarea datelor operaționale cu caracter personal inexacte care o privesc. Ținându-se seama de scopul prelucrării datelor, persoana vizată are dreptul de a obține completarea datelor operaționale cu caracter personal care sunt incomplete, inclusiv prin transmiterea unei declarații suplimentare.

(2) Operatorul șterge datele operaționale cu caracter personal fără întârzieri nejustificate, iar persoana vizată are dreptul de a obține din partea operatorului ștergerea datelor operaționale cu caracter personal care o privesc fără întârzieri nejustificate în cazul în care prelucrarea încalcă dispozițiile articolului 71, articolului 72 alineatul (1) sau ale articolului 76 sau în cazul în care datele operaționale cu caracter personal trebuie șterse pentru îndeplinirea unei obligații legale ce îi revine operatorului.

(3) În loc de ștergere, operatorul restricționează prelucrarea în cazul în care:

(a) exactitatea datelor cu caracter personal este contestată de persoana vizată, iar exactitatea sau inexactitatea datelor respective nu poate fi stabilită; sau

(b) datele cu caracter personal trebuie să fie păstrate ca mijloace de probă.

În cazul în care prelucrarea este restricționată în conformitate cu litera (a) de la primul paragraf, operatorul informează persoana vizată înainte de ridicarea restricțiilor de prelucrare.

Datele restricționate se prelucrează doar în scopul pentru care nu au fost șterse.

(4) Operatorul informează în scris persoana vizată cu privire la orice refuz de rectificare sau de ștergere a datelor operaționale cu caracter personal sau la restricționarea prelucrării și motivele refuzului. Operatorul poate restricționa, integral sau parțial, furnizarea unor astfel de informații în măsura în care o astfel de restricționare constituie o măsură necesară și proporțională într-o societate democratică, ținând seama în mod corespunzător de drepturile fundamentale și de interesele legitime ale persoanei fizice vizate pentru:

(a) a evita obstrucționarea cercetărilor, anchetelor sau procedurilor oficiale sau juridice;

(b) a nu prejudicia prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor sau executarea pedepselor;

(c) a proteja securitatea publică a statelor membre;

(d) a proteja securitatea națională a statelor membre;

(e) a proteja drepturile și libertățile altora, de exemplu ale victimelor și martorilor.

Operatorul informează persoana vizată cu privire la posibilitatea de a depune o plângere la Autoritatea Europeană pentru Protecția Datelor sau de a introduce o cale de atac în fața Curții de Justiție.

(5) Operatorul comunică rectificarea datelor operaționale cu caracter personal inexacte autorității competente de la care provin datele operaționale cu caracter personal inexacte.

(6) În cazul în care datele operaționale cu caracter personal au fost rectificate sau șterse sau a fost restricționată prelucrarea lor în temeiul alineatului (1), (2) sau (3), operatorul aduce la cunoștința destinatarilor aceste fapte și îi informează că trebuie să rectifice sau să șteargă datele operaționale cu caracter personal sau să restricționeze prelucrarea datelor operaționale cu caracter personal aflate în responsabilitatea lor.

Articolul 83

Dreptul de acces în cadrul anchetelor penale și al procedurilor penale

În cazul în care datele operaționale cu caracter personal provin de la o autoritate competentă, organele, oficiile și agențiile Uniunii verifică la autoritatea competentă în cauză, înainte de a lua o decizie cu privire la dreptul de acces al persoanei vizate, dacă aceste date cu caracter personal sunt incluse într-o hotărâre judiciară, într-un registru sau într-o cauză judiciară prelucrată în cadrul unor anchete penale și al unor proceduri penale din statul membru al autorității competente în cauză. Dacă răspunsul este afirmativ, se ia o decizie cu privire la dreptul de acces în consultare și în strânsă cooperare cu autoritatea competentă în cauză.

Articolul 84

Exercitarea drepturilor de către persoana vizată și verificarea de către Autoritatea Europeană pentru Protecția Datelor

(1) În cazurile menționate la articolul 79 alineatul (3), articolul 81 și articolul 82 alineatul (4), drepturile persoanei vizate pot fi exercitate și prin intermediul Autorității Europene pentru Protecția Datelor.

(2) Operatorul informează persoana vizată cu privire la posibilitatea de a-și exercita drepturile prin intermediul Autorității Europene pentru Protecția Datelor în temeiul alineatului (1).

(3) Atunci când dreptul menționat la alineatul (1) este exercitat, Autoritatea Europeană pentru Protecția Datelor informează persoana vizată cel puțin cu privire la faptul că a realizat toate verificările necesare sau o analiză. Autoritatea Europeană pentru Protecția Datelor informează, de asemenea, persoana vizată în legătură cu dreptul acesteia de a introduce o cale de atac în fața Curții de Justiție.

Articolul 85

Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit

(1) Având în vedere stadiul actual al tehnologiei, costurile de punere în aplicare și natura, amploarea, contextul și scopurile prelucrării, precum și riscurile cu grade diferite de probabilitate și de gravitate la adresa drepturilor și libertăților persoanelor fizice pe care le prezintă prelucrarea, operatorul, atât la momentul stabilirii mijloacelor de prelucrare, cât și la momentul prelucrării propriu-zise, pune în aplicare măsuri tehnice și organizatorice adecvate, cum ar fi pseudonimizarea, care sunt destinate să pună în aplicare în mod eficace principiile de protecție a datelor, precum reducerea la minimum a datelor, și să integreze garanțiile necesare în cadrul prelucrării, pentru a îndeplini cerințele prezentului regulament și ale actului juridic de instituire care îl vizează pe operator, precum și pentru a proteja drepturile persoanelor vizate.

(2) Operatorul pune în aplicare măsuri tehnice și organizatorice corespunzătoare pentru a asigura că, în mod implicit, sunt prelucrate numai date operaționale cu caracter personal care sunt adecvate și pertinente și nu sunt excesive în raport cu scopul în care sunt prelucrate. Această obligație se aplică volumului de date operaționale cu caracter personal colectate, gradului de prelucrare a acestora, perioadei lor de păstrare și accesibilității lor. În special, astfel de măsuri garantează că, în mod implicit, datele operaționale cu caracter personal nu pot fi accesate de un număr nelimitat de persoane fizice fără intervenția persoanei vizate.

Articolul 86

Operatorii asociați

(1) În cazul în care doi sau mai mulți operatori sau unul sau mai mulți operatori împreună cu unul sau mai mulți operatori, alții decât instituții și organe ale Uniunii, stabilesc în comun scopurile și mijloacele prelucrării, aceștia sunt operatori asociați. Aceștia stabilesc într-un mod transparent responsabilitățile fiecăruia în ceea ce privește îndeplinirea obligațiilor care le revin în materie de protecție a datelor, în special în ceea ce privește exercitarea drepturilor persoanelor vizate și îndatoririle fiecărui operator de a transmite informațiile prevăzute la articolul 79, prin intermediul unui acord între ei, cu excepția cazului și în măsura în care responsabilitățile operatorilor asociați sunt stabilite în dreptul Uniunii sau în dreptul intern al statelor membre care se aplică operatorilor asociați. Acordul poate să desemneze un punct de contact pentru persoanele vizate.

(2) Acordul menționat la alineatul (1) reflectă în mod corespunzător rolurile respective ale operatorilor asociați și raporturile lor cu persoana vizată. Esența acestui acord este făcută cunoscută persoanei vizate.

(3) Indiferent de clauzele acordului menționat la alineatul (1), persoana vizată își poate exercita drepturile în temeiul prezentului regulament cu privire la fiecare dintre operatori și în raport cu fiecare dintre operatori.

Articolul 87

Persoana împuternicită de operator

(1) În cazul în care prelucrarea urmează să fie realizată în numele unui operator, operatorul recurge doar la persoane împuternicite care oferă garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să respecte cerințele prevăzute în prezentul regulament și în actul juridic de instituire a operatorului și să asigure protecția drepturilor persoanei vizate.

(2) Persoana împuternicită de operator nu recrutează o altă persoană împuternicită fără a primi în prealabil o autorizație scrisă, specifică sau generală, din partea operatorului. În cazul unei autorizații generale scrise, persoana împuternicită de operator informează operatorul cu privire la orice modificare preconizată privind adăugarea sau înlocuirea altor persoane împuternicite, oferind astfel operatorului posibilitatea de a formula obiecții față de aceste modificări.

(3) Prelucrarea de către o persoană împuternicită de un operator este reglementată printr-un contract sau un alt act juridic în temeiul dreptului Uniunii sau al dreptului intern, care are caracter obligatoriu pentru persoana împuternicită de operator în raport cu operatorul și care stabilește obiectul și durata prelucrării, natura și scopul prelucrării, tipul de date operaționale cu caracter personal și categoriile de persoane vizate și obligațiile și drepturile operatorului. Respectivul contract sau act juridic prevede în special că persoana împuternicită de operator:

(a) acționează numai pe baza instrucțiunilor operatorului;

(b) se asigură că persoanele autorizate să prelucreze datele operaționale cu caracter personal s-au angajat să respecte confidențialitatea sau fac obiectul unei obligații statutare corespunzătoare de confidențialitate;

(c) asistă operatorul prin orice mijloace adecvate pentru a asigura respectarea dispozițiilor privind drepturile persoanei vizate;

(d) la alegerea operatorului, șterge sau returnează operatorului toate datele operaționale cu caracter personal după încetarea serviciilor legate de prelucrare și elimină copiile existente, cu excepția cazului în care dreptul Uniunii sau dreptul intern impune păstrarea datelor operaționale cu caracter personal;

(e) pune la dispoziția operatorului toate informațiile necesare pentru a demonstra respectarea obligațiilor prevăzute la prezentul articol;

(f) respectă condițiile menționate la alineatul (2) și la prezentul alineat pentru recrutarea unei alte persoane împuternicite.

(4) Contractul sau un alt act juridic menționat la alineatul (3) se întocmește în scris, inclusiv în format electronic.

(5) În cazul în care o persoană împuternicită de către operator încalcă prezentul regulament sau actul juridic de instituire a operatorului prin stabilirea scopurilor și mijloacelor prelucrării, persoana împuternicită este considerată ca fiind operator în ceea ce privește prelucrarea respectivă.

Articolul 88

Înregistrarea

(1) Operatorul înregistrează oricare dintre următoarele operațiuni de prelucrare în sistemele de prelucrare automată: colectarea, modificarea, accesul, consultarea, divulgarea (inclusiv transferurile), combinarea și ștergerea de date operaționale cu caracter personal. Înregistrările consultărilor și ale dezvăluirilor fac posibilă determinarea motivelor, a datei și a orei efectuării acestor operațiuni, identificarea persoanei care a consultat sau a dezvăluit date operaționale cu caracter personal și, în măsura în care este posibil, identitatea destinatarilor acestor date operaționale cu caracter personal.

(2) Înregistrările sunt utilizate numai pentru verificarea legalității prelucrării, monitorizare proprie, asigurarea integrității și a securității datelor operaționale cu caracter personal și în cadrul unor proceduri penale. Aceste înregistrări sunt șterse după trei ani, cu excepția cazului în care sunt necesare pentru un control în curs.

(3) Operatorul pune înregistrările la dispoziția responsabilului cu protecția datelor din cadrul său și la dispoziția Autorității Europene pentru Protecția Datelor, la cerere.

Articolul 89

Evaluarea impactului asupra protecției datelor

(1) În cazul în care un tip de prelucrare, în special care implică utilizarea de noi tehnologii, și ținând seama de natura, amploarea, contextul și scopurile prelucrării, este susceptibil să genereze un risc ridicat la adresa drepturilor și libertăților persoanelor fizice, operatorul efectuează, înainte de prelucrare, o evaluare a impactului operațiunilor de prelucrare preconizate asupra protecției datelor operaționale cu caracter personal.

(2) Evaluarea menționată la alineatul (1) cuprinde cel puțin o descriere generală a operațiunilor de prelucrare preconizate, o evaluare a riscurilor la adresa drepturilor și libertăților persoanelor vizate, măsurile preconizate în vederea eliminării riscurilor, garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor operaționale cu caracter personal și să demonstreze respectarea normelor de protecție a datelor, luând în considerare drepturile și interesele legitime ale persoanelor vizate și ale celorlalte persoane interesate.

Articolul 90

Consultarea prealabilă a Autorității Europene pentru Protecția Datelor

(1) Operatorul consultă Autoritatea Europeană pentru Protecția Datelor înainte de prelucrarea care va face parte dintr-un nou sistem de evidență care urmează a fi creat, în cazul în care:

(a) o evaluare a impactului asupra protecției datelor, în temeiul articolului 89, indică faptul că prelucrarea ar genera un risc ridicat în absența unor măsuri din partea operatorului pentru atenuarea riscului; sau

(b) tipul de prelucrare, în special în cazul în care se utilizează noi tehnologii, mecanisme sau proceduri, implică un risc ridicat la adresa drepturilor și libertăților persoanelor vizate.

(2) Autoritatea Europeană pentru Protecția Datelor poate stabili o listă a operațiunilor de prelucrare care fac obiectul consultării prealabile în conformitate cu alineatul (1).

(3) Operatorul transmite Autorității Europene pentru Protecția Datelor evaluarea impactului asupra protecției datelor menționată la articolul 89 și, la cererea acesteia, orice altă informație care îi permite Autorității Europene pentru Protecția Datelor să evalueze conformitatea prelucrării și, în special, riscurile la adresa protecției datelor operaționale cu caracter personal ale persoanei vizate și garanțiile aferente.

(4) Atunci când Autoritatea Europeană pentru Protecția Datelor consideră că prelucrarea preconizată, menționată la alineatul (1), ar încălca dispozițiile prezentului regulament sau ale actului juridic de instituire a organului, oficiului sau agenției Uniunii, în special în cazul în care riscul nu a fost identificat sau atenuat într-o măsură suficientă de către operator, Autoritatea Europeană pentru Protecția Datelor îi transmite operatorului recomandări scrise în termen de cel mult șase săptămâni de la primirea cererii de consultare. Termenul menționat poate fi prelungit cu o lună, ținându-se seama de complexitatea prelucrării preconizate. Autoritatea Europeană pentru Protecția Datelor informează operatorul cu privire la o astfel de prelungire în termen de o lună de la primirea cererii de consultare, prezentând motivele întârzierii.

Articolul 91

Securitatea prelucrării datelor operaționale cu caracter personal

(1) Având în vedere stadiul actual al tehnologiei și costurile implementării și ținând seama de natura, amploarea, contextul și scopurile prelucrării, precum și de riscurile cu grade diferite de probabilitate și de gravitate la adresa drepturilor și libertăților persoanelor fizice, operatorul și persoana împuternicită de operator pun în aplicare măsuri tehnice și organizatorice corespunzătoare în vederea asigurării unui nivel de securitate corespunzător acestui risc, în special în ceea ce privește prelucrarea categoriilor speciale de date operaționale cu caracter personal.

(2) În ceea ce privește prelucrarea automată, operatorul și persoana împuternicită de operator pun în aplicare, în urma unei evaluări a riscurilor, măsuri menite:

(a) să împiedice accesul persoanelor neautorizate la echipamentele de prelucrare a datelor utilizate pentru prelucrare („controlul accesului la echipamente”);

(b) să împiedice citirea, copierea, modificarea sau îndepărtarea neautorizată a suporturilor de date („controlul suporturilor de date”);

(c) să împiedice introducerea neautorizată de date operaționale cu caracter personal și inspectarea, modificarea sau ștergerea neautorizată a datelor operaționale cu caracter personal stocate („controlul stocării”);

(d) să împiedice utilizarea sistemelor de prelucrare automată de către persoane neautorizate cu ajutorul echipamentelor de comunicare a datelor („controlul utilizatorului”);

(e) să asigure faptul că persoanele autorizate să utilizeze un sistem de prelucrare automată au acces numai la datele operaționale cu caracter personal vizate de autorizația lor de acces („controlul accesului la date”);

(f) să asigure că este posibilă verificarea și identificarea organismelor cărora le-au fost transmise sau puse la dispoziție sau s-ar putea să le fie transmise sau puse la dispoziție date operaționale cu caracter personal utilizându-se comunicarea datelor („controlul comunicării”);

(g) să asigure posibilitatea verificării și determinării ulterioare a datelor operaționale cu caracter personal care au fost introduse în sisteme de prelucrare automată a datelor, precum și a datei în care au fost introduse datele operaționale cu caracter personal și a persoanei care le-a introdus („controlul introducerii datelor”);

(h) să împiedice consultarea, copierea, modificarea sau ștergerea neautorizată a datelor operaționale cu caracter personal pe parcursul transferurilor de date operaționale cu caracter personal sau pe parcursul transportului suporturilor de date („controlul transportului”);

(i) să asigure posibilitatea recuperării sistemelor instalate în cazul unei întreruperi („recuperarea”);

(j) să asigure funcționarea sistemului, raportarea defecțiunilor de funcționare („fiabilitate”) și imposibilitatea coruperii datelor operaționale cu caracter personal stocate, din cauza funcționării defectuoase a sistemului („integritate”).

Articolul 92

Notificarea Autorității Europene pentru Protecția Datelor a unei încălcări a securității datelor cu caracter personal

(1) În cazul în care are loc o încălcare a securității datelor cu caracter personal, operatorul notifică acest lucru Autorității Europene pentru Protecția Datelor, fără întârzieri nejustificate și, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta, cu excepția cazului în care este puțin probabil să genereze un risc pentru drepturile și libertățile persoanelor fizice. În cazul în care notificarea Autorității Europene pentru Protecția Datelor nu are loc în termen de 72 de ore, aceasta este însoțită de o explicație privind motivele întârzierii.

(2) Notificarea menționată la alineatul (1) trebuie cel puțin:

(a) să descrie caracterul încălcării securității datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile și numărul aproximativ de persoane vizate, precum și categoriile și numărul aproximativ de înregistrări de date operaționale cu caracter personal vizate;

(b) să comunice numele și datele de contact ale responsabilului cu protecția datelor;

(c) să descrie consecințele probabile ale încălcării securității datelor cu caracter personal;

(d) să descrie măsurile luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

(3) Atunci când și în măsura în care nu este posibil să se pună la dispoziție informațiile menționate la alineatul (2) în același timp, acestea pot fi transmise în mai multe etape, fără întârzieri nejustificate.

(4) Operatorul păstrează documente referitoare la toate cazurile de încălcare a securității datelor cu caracter personal menționate la alineatul (1), care cuprind o descriere a situației în care a avut loc încălcarea securității datelor cu caracter personal, a efectelor acesteia și a măsurilor de remediere întreprinse. Această documentație îi permite Autorității Europene pentru Protecția Datelor să verifice respectarea prezentului articol.

(5) În cazul în care încălcarea securității datelor operaționale cu caracter personal vizează date cu caracter personal care au fost transmise de către autoritățile competente sau autorităților competente, operatorul comunică fără întârzieri nejustificate informațiile menționate la alineatul (2) autorităților competente în cauză.

Articolul 93

Informarea persoanei vizate cu privire la încălcarea securității datelor cu caracter personal

(1) În cazul în care încălcarea securității datelor cu caracter personal este de natură să ducă la apariția unui risc ridicat la adresa drepturilor și libertăților persoanelor fizice, operatorul informează persoana vizată fără întârzieri nejustificate cu privire la această încălcare.

(2) Informarea persoanei vizate menționată la alineatul (1) din prezentul articol include o descriere, într-un limbaj simplu și clar, a caracterului încălcării securității datelor cu caracter personal, precum și cel puțin informațiile și recomandările prevăzute la articolul 92 alineatul (2) literele (b), (c) și (d).

(3) Informarea persoanei vizate menționată la alineatul (1) nu este necesară în cazul în care este îndeplinită oricare dintre următoarele condiții:

(a) operatorul a pus în aplicare măsuri tehnologice și organizatorice adecvate de protecție, iar aceste măsuri au fost aplicate datelor operaționale cu caracter personal afectate de încălcarea securității datelor cu caracter personal, în special măsuri prin care se asigură că datele operaționale cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea;

(b) operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat la adresa drepturilor și libertăților persoanelor vizate menționat la alineatul (1) nu mai este susceptibil să se materializeze;

(c) aceasta ar necesita un efort disproporționat. În acest caz, informarea se înlocuiește printr-o informare publică sau o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficace.

(4) În cazul în care operatorul nu a comunicat deja persoanei vizate încălcarea securității datelor cu caracter personal, Autoritatea Europeană pentru Protecția Datelor poate să îi solicite operatorului, după ce analizează probabilitatea ca încălcarea securității datelor cu caracter personal să ducă la apariția unui risc ridicat, să facă acest lucru sau poate decide că este îndeplinită oricare dintre condițiile menționate la alineatul (3).

(5) Informarea persoanei vizate menționată la alineatul (1) din prezentul articol poate fi amânată, restricționată sau omisă, sub rezerva condițiilor și a motivelor menționate la articolul 79 alineatul (3).

Articolul 94

Transferul de date operaționale cu caracter personal către țări terțe și organizații internaționale

(1) Sub rezerva restricțiilor și a condițiilor prevăzute în actele juridice de instituire a organului, oficiului sau agenției Uniunii, operatorul poate să transfere datele operaționale cu caracter personal unei autorități dintr-o țară terță sau unei organizații internaționale în măsura în care acest transfer este necesar pentru executarea de către operator a sarcinilor sale și numai dacă sunt îndeplinite condițiile prevăzute la prezentul articol, și anume:

(a) Comisia a adoptat o decizie privind caracterul adecvat al nivelului de protecție în conformitate cu articolul 36 alineatul (3) din Directiva (UE) 2016/680, conform căreia țara terță sau un teritoriu sau un sector de prelucrare din țara terță respectivă ori organizația internațională în cauză asigură un nivel adecvat de protecție;

(b) în cazul în care Comisia nu a adoptat o decizie privind caracterul adecvat al nivelului de protecție în temeiul literei (a), a fost încheiat un acord internațional între Uniune și țara terță sau organizația internațională respectivă în temeiul articolului 218 din TFUE, în care se prevăd garanții adecvate în ceea ce privește protecția vieții private și a drepturilor și libertăților fundamentale ale persoanelor fizice;

(c) în cazul în care Comisia nu a adoptat o decizie privind caracterul adecvat al nivelului de protecție în temeiul literei (a) sau nu a fost încheiat un acord internațional în temeiul literei (b), a fost încheiat un acord de cooperare care permite schimburile de date operaționale cu caracter personal înainte de data aplicării actului juridic de instituire a organului, oficiului sau agenției Uniunii în cauză, între respectivul organ, oficiu sau agenție a Uniunii și țara terță în cauză.

(2) Actele juridice de instituire a organelor, oficiilor și agențiilor Uniunii pot menține sau introduce dispoziții mai specifice privind condițiile pentru transferurile internaționale de date operaționale cu caracter personal, în special privind transferurile care fac obiectul unor garanții corespunzătoare și derogări pentru situații specifice.

(3) Operatorul publică și menține la zi pe site-ul său de internet o listă care conține deciziile privind caracterul adecvat menționate la alineatul (1) litera (a), acordurile, mecanismele administrative și alte instrumente legate de transferul de date operaționale cu caracter personal în conformitate cu alineatul (1).

(4) Operatorul ține o evidență detaliată a tuturor transferurilor efectuate în temeiul prezentului articol.

Articolul 95

Caracterul secret al anchetelor judiciare și al procedurilor penale

Actele juridice de instituire a organelor, oficiilor sau agențiilor Uniunii referitoare la activitățile care intră sub incidența părții a treia titlul V capitolul 4 sau capitolul 5 din TFUE pot să oblige Autoritatea Europeană pentru Protecția Datelor să țină seama în cel mai strict mod, atunci când își exercită competențele de supraveghere, de caracterul secret al anchetelor judiciare și al procedurilor penale, în conformitate cu dreptul Uniunii sau cu dreptul intern.

CAPITOLUL X

ACTE DE PUNERE ÎN APLICARE

Articolul 96

Procedura comitetului

(1) Comisia este asistată de comitetul instituit prin articolul 93 din Regulamentul (UE) 2016/679. Respectivul comitet reprezintă un comitet în înțelesul Regulamentului (UE) nr. 182/2011.

(2) Atunci când se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.

CAPITOLUL XI

REVIZUIREA

Articolul 97

Clauză de revizuire

Până la 30 aprilie 2022 și, ulterior, o dată la cinci ani, Comisia prezintă Parlamentului European și Consiliului un raport privind aplicarea prezentului regulament, însoțit, dacă este necesar, de propuneri legislative corespunzătoare.

Articolul 98

Revizuirea actelor juridice ale Uniunii

(1) Până la 30 aprilie 2022, Comisia analizează actele juridice adoptate în temeiul tratatelor, care reglementează prelucrarea datelor operaționale cu caracter personal de organele, oficiile și agențiile Uniunii atunci când desfășoară activități care intră în domeniul de aplicare al părții a treia titlul V capitolul 4 sau capitolul 5 din TFUE, pentru:

(a) a le evalua coerența cu Directiva (UE) 2016/680 și cu capitolul IX din prezentul regulament;

(b) a depista eventuale discrepanțe care pot să împiedice schimbul de date operaționale cu caracter personal între organele, oficiile și agențiile Uniunii atunci când desfășoară activități în domeniile respective și autoritățile competente; și

(c) a depista orice discrepanțe care pot să genereze o fragmentare juridică în Uniune a legislației privind protecția datelor.

(2) Pe baza rezultatelor acestei analize, în vederea asigurării unei protecții uniforme și consecvente a persoanelor fizice în ceea ce privește prelucrarea, Comisia poate să prezinte propuneri legislative corespunzătoare, în special în vederea aplicării capitolului IX din prezentul regulament Europol și Parchetului European și care să includă, dacă este necesar, propuneri de adaptare a capitolului IX din prezentul regulament.

CAPITOLUL XII

DISPOZIȚII FINALE

Articolul 99

Abrogarea Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE

Regulamentul (CE) nr. 45/2001 și Decizia nr. 1247/2002/CE se abrogă cu efect de la 11 decembrie 2018. Trimiterile la regulamentul și decizia abrogate se interpretează ca trimiteri la prezentul regulament.

Articolul 100

Măsuri tranzitorii

(1) Decizia 2014/886/UE a Parlamentului European și a Consiliului ([1]) și actualul mandat al Autorității Europene pentru Protecția Datelor și al adjunctului acesteia nu sunt afectate de prezentul regulament.

([1]) Decizia 2014/886/UE a Parlamentului European și a Consiliului din 4 decembrie 2014 de numire a Autorității Europene pentru Protecția Datelor și a adjunctului acesteia (JO L 351, 9.12.2014, p. 9).

(2) Adjunctul autorității este asimilat grefierului Curții de Justiție în ceea ce privește stabilirea remunerației, a indemnizațiilor, a pensiei pentru limită de vârstă și a oricăror alte prestații care țin loc de remunerație.

(3) Articolul 53 alineatele (4), (5) și (7), precum și articolele 55 și 56 din prezentul regulament se aplică adjunctului actual al autorității până la sfârșitul mandatului său.

(4) Adjunctul autorității asistă Autoritatea Europeană pentru Protecția Datelor în îndeplinirea atribuțiilor acesteia din urmă și o înlocuiește atunci când este absentă sau nu își poate îndeplini atribuțiile respective, până la sfârșitul mandatului adjunctului autorității.

Articolul 101

Intrarea în vigoare și aplicarea

(1) Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

(2) Cu toate acestea, prezentul regulament se aplică prelucrării datelor cu caracter personal de către Eurojust de la 12 decembrie 2019.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Strasbourg, 23 octombrie 2018.

Pentru Parlamentul European	*Pentru Consiliu*
Președintele	*Președintele*
A. TAJANI	K. EDTSTADLER