Consiliul
Uniunii Europene

Bruxelles, 12 ianuarie 2017
(OR. en)

5034/17

Dosar interinstituțional:
2017/0002 (COD)

DATAPROTECT 2
JAI 2
DAPIX 2
FREMP 1
DIGIT 2
CODEC 4

PROPUNERE

Sursă:	Secretar general al Comisiei Europene, sub semnătura dlui Jordi AYET PUIGARNAU, director
Data primirii:	12 ianuarie 2017
Destinatar:	Dl Jeppe TRANHOLM-MIKKELSEN, Secretarul General al Consiliului Uniunii Europene
Nr. doc. Csie:	COM(2017) 8 final
Subiect:	Propunere de REGULAMENT AL PARLAMENTULUI EUROPEAN ŞI AL CONSILIULUI 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

În anexă, se pune la dispoziția delegațiilor documentul COM(2017) 8 final.

Anexă: COM(2017) 8 final

COMISIA
EUROPEANĂ

Bruxelles, 10.1.2017
COM(2017) 8 final

2017/0002 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ŞI AL CONSILIULUI

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

EXPUNERE DE MOTIVE

1. CONTEXTUL

• Temeiurile și obiectivele propunerii

Articolul 16 alineatul (1) din Tratatul privind funcționarea Uniunii Europene (TFUE), introdus prin Tratatul de la Lisabona, stabilește principiul conform căruia orice persoană are dreptul la protecția datelor cu caracter personal care o privesc. Mai mult, la articolul 16 alineatul (2) din TFUE, Tratatul de la Lisabona a introdus un temei juridic specific pentru adoptarea de norme privind protecția datelor cu caracter personal. Articolul 8 din Carta drepturilor fundamentale a Uniunii Europene consacră protecția datelor cu caracter personal ca drept fundamental.

Dreptul la protecția datelor cu caracter personal se aplică, de asemenea, prelucrării de date cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii. Regulamentul (CE) nr. 45/2001[1], principalul act din legislația UE privind protecția datelor cu caracter personal în instituțiile Uniunii, a fost adoptat în 2001, urmărindu-se două obiective: protejarea dreptului fundamental la protecția datelor și garantarea liberei circulații a datelor cu caracter personal în întreaga Uniune. Acesta a fost completată prin Decizia 1247/2002/CE[2].

La 27 aprilie 2016, Parlamentul European și Consiliul au adoptat Regulamentul general privind protecția datelor [Regulamentul (UE) 2016/679], care va deveni aplicabil de la data de 25 mai 2018. Prezentul regulament solicită ca Regulamentul (CE) nr. 45/2001 să fie adaptat la principiile și normele stabilite în Regulamentul (UE) 2016/679, pentru a asigura un cadru solid și coerent în materie de protecție a datelor în Uniune și a permite ca cele două instrumente să poată fi aplicate în același timp[3].

Alinierea, în măsura în care acest lucru este posibil, a normelor de protecție a datelor aplicabile instituțiilor, organelor, oficiilor și agențiilor Uniunii la normele de protecție a datelor adoptate de statele membre este consecventă cu abordarea coerentă a protecției datelor cu caracter personal aplicată în întreaga Uniune. Ori de câte ori o dispoziție a propunerii se bazează pe aceeași noțiune ca și o dispoziție a Regulamentului (UE) 2016/679, aceste două dispoziții ar trebui să fie interpretate în mod omogen, în special pentru că structura propunerii ar trebui înțeleasă ca fiind similară structurii Regulamentului (UE) 2016/679[4].

De asemenea, revizuirea Regulamentului (CE) nr. 45/2001 ia în considerare rezultatele anchetelor și ale consultărilor cu părțile interesate, precum și studiul de evaluare privind aplicarea acestui regulament în ultimii 15 de ani.

---

[1] 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.

[2] 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.

[3] A se vedea Regulamentul (UE) nr. 20016/679, articolul 98 și considerentul 17.

[4] A se vedea Hotărârea CJUE din 9 martie 2010, Comisia/Germania, cauza C-518/07, ECLI:EU:C:2010:125, punctele 26 și 28.

Această inițiativă nu se înscrie în cadrul Programului privind o reglementare adecvată și funcțională (REFIT).

- **Coerența cu dispozițiile existente în domeniul de politică**

Propunerea urmărește să alinieze dispozițiile Regulamentului (CE) nr. 45/2001 la principiile și normele stabilite de Regulamentul (UE) nr. 2016/679 pentru a asigura un cadru solid și coerent în materie de protecție a datelor în Uniune. Propunerea încorporează, de asemenea, normele relevante stabilite în Regulamentul (CE) XXXX/XX [Regulamentul privind confidențialitatea și comunicațiile electronice] în ceea ce privește protecția echipamentelor terminale ale utilizatorilor finali.

- **Coerența cu alte politici ale Uniunii**

Nu se aplică.

2. TEMEIUL JURIDIC, SUBSIDIARITATEA ȘI PROPORȚIONALITATEA

- **Temei juridic**

Protecția persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal constituie un drept fundamental, consacrat la articolul 8 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene.

Prezenta propunere se bazează pe articolul 16 din TFUE, care este temeiul juridic pentru adoptarea normelor în materie de protecție a datelor. Articolul susmenționat permite adoptarea de norme privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii în exercitarea activităților care fac parte din domeniul de aplicare a dreptului Uniunii. De asemenea, articolul în cauză permite adoptarea de norme referitoare la libera circulație a datelor cu caracter personal, inclusiv a datelor cu caracter personal prelucrate de aceste instituții, organe, oficii și agenții.

- **Subsidiaritatea (în cazul competențelor neexclusive)**

Obiectul prezentului regulament se încadrează în domeniul de competență exclusivă a Uniunii, întrucât numai Uniunea poate adopta norme care reglementează prelucrarea datelor cu caracter personal de către instituțiile sale.

- **Proporționalitate**

În conformitate cu principiul proporționalității, este necesar și adecvat, în vederea îndeplinirii obiectivelor fundamentale - de a garanta un nivel echivalent de protecție a persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și de a asigura libera circulație a datelor cu caracter personal în întreaga Uniune, să se stabilească norme privind prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii. Prezentul regulament nu depășește ceea ce este necesar pentru realizarea obiectivelor urmărite, în conformitate cu articolul 5 alineatul (4) din Tratatul privind Uniunea Europeană.

- **Alegerea instrumentului**

Se consideră că regulamentul este instrumentul juridic adecvat pentru definirea cadrului privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și libera circulație a unor astfel de date. Acesta oferă persoanelor fizice drepturi opozabile din punct de vedere juridic și precizează obligațiile în materie de prelucrare a datelor care le revin operatorilor din instituțiile, organele, oficiile și agențiile Uniunii. Regulamentul prevede, de asemenea, o autoritate independentă de supraveghere, Autoritatea Europeană pentru Protecția Datelor, care să fie responsabilă cu monitorizarea prelucrării datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii.

3. REZULTATELE EVALUĂRILOR *EX POST*, ALE CONSULTĂRILOR CU PĂRȚILE INTERESATE ȘI ALE EVALUĂRILOR IMPACTULUI

Comisia a purtat consultări cu părțile interesate în 2010 și 2011 și a efectuat o evaluare a impactului în cadrul acțiunilor pregătitoare premergătoare pachetului de reforme privind protecția datelor, care oferă informații cu privire la propunerile de modificări la Regulamentul (CE) nr. 45/2001. În acest context, Comisia a realizat, de asemenea, un sondaj în rândul coordonatorilor săi pentru protecția datelor (CPD)[5].

În ceea ce privește aplicarea practică a Regulamentului (CE) nr. 45/2001 de către instituțiile, organele, oficiile și agențiile Uniunii, s-au colectat informații din partea Autorității Europene pentru Protecția Datelor (AEPD), a altor instituții, organe, oficii și agenții ale Uniunii, a altor DG-uri ale Comisiei, precum și din partea unui contractant extern. De asemenea, a fost trimis un chestionar rețelei responsabililor cu protecția datelor (RPD)[6].

Responsabilii cu protecția datelor dintr-o serie de instituții, organe, oficii și agenții ale Uniunii au organizat ateliere privind reformarea Regulamentului nr. 45/2001 în datele de 9 iulie 2015, 22 octombrie 2015, 19 ianuarie 2016 și 15 martie 2016.

Comisia a decis, în 2013, să realizeze un studiu de evaluare privind aplicarea până în prezent a Regulamentului (CE) nr. 45/2001, încredințând această sarcină unui contractant extern. Rezultatele finale ale studiului de evaluare (raportul final, cinci studii de caz și analiza articol cu articol) au fost transmise Comisiei la 8 iunie 2015[7].

Evaluarea a demonstrat că sistemul de guvernanță structurat în jurul RPD și al AEPD este eficace. Din evaluare reiese că partajarea competențelor între responsabilii cu protecția datelor și AEPD este clară și bine echilibrată și că ambele părți dispun de o gamă adecvată de competențe. Cu toate acestea, lipsa de autoritate cauzată de sprijinul insuficient acordat responsabililor cu protecția datelor de către superiorii lor ierarhici ar putea crea dificultăți.

---

5 A se consulta adresa: http://ec.europa.eu/justice/data-protection/reform/index_en.htm

6 A se vedea raportul general al Autorității Europene pentru Protecția Datelor privind „Evaluarea respectării Regulamentului (CE) nr. 45/2001 în instituțiile UE («Ancheta 2013»)” și „Avizul 3/2015: «Marea oportunitate pentru Europa: recomandări ale AEPD referitoare la opțiunile UE în materie de reformă a protecției datelor»”.

7 JUST/2013/FRAC/FW/0157/A4 în contextul contractului-cadru multiplu JUST/2011/EVAL/01 (RS 2013/05) - Studiu de evaluare privind Regulamentul (CE) nr. 45/2001, de Ernst and Young, disponibil la adresa: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=51087

Studiul de evaluare a arătat că aplicarea Regulamentului (CE) nr. 45/2001 ar putea fi mai bine asigurată dacă AEPD ar recurge la sancțiuni. O utilizare sporită a competențelor sale de autoritate de supraveghere ar putea conduce la o mai bună aplicare a normelor privind protecția datelor. O altă concluzie a fost că operatorii de date ar trebui să adopte o abordare privind gestionarea riscurilor și să realizeze evaluări ale riscului înainte de a efectua operațiuni de prelucrare pentru a pune în aplicare mai bine cerințele privind păstrarea și securitatea datelor.

Studiul a arătat, de asemenea, că normele în vigoare prevăzute la capitolul IV, privind sectorul telecomunicațiilor, din Regulamentul (CE) nr. 45/2001 sunt depășite și că este necesar ca acest capitol să fie aliniat la Directiva asupra confidențialității și comunicațiilor electronice. Potrivit studiului de evaluare, este necesar, de asemenea, să se clarifice unele definiții-cheie din Regulamentul (CE) nr. 45/2001. Printre acestea se numără identificarea operatorilor de date din instituțiile, organele, oficiile și agențiile Uniunii, definiția destinatarilor și extinderea obligației de păstrare a confidențialității la persoanele externe împuternicite de către operator.

Studiul de evaluare a evidențiat, de asemenea, necesitatea de a simplifica regimul notificărilor și verificărilor prealabile, în vederea creșterii eficienței și a reducerii sarcinii administrative.

Evaluatorul a efectuat un sondaj online în cadrul a 64 de instituții, agenții, oficii și organe ale Uniunii. La întrebările sondajului au răspuns 422 de funcționari operatori de date, 73 de RPD, 118 de CPD și 109 de respondenți care lucrează în domeniul IT. Evaluatorul a purtat, de asemenea, o serie de interviuri cu părți interesate. La 26 martie 2015, evaluatorul și Comisia au organizat un atelier final, la care au participat o serie de operatori de date, de RPD, de CPD, de respondenți care lucrează în domeniul IT, alături de reprezentanți ai AEPD.

- **Obținerea și utilizarea expertizei**

A se vedea trimiterea la studiul de evaluare de la punctul anterior.

- **Evaluarea impactului**

Impactul prezentei propuneri va fi resimțit în principal de instituțiile, organele, oficiile și agențiile Uniunii. Acest lucru a fost confirmat de informațiile colectate de la AEPD, de la alte instituții, organe, oficii și agenții ale Uniunii, de la unele DG-uri din cadrul Comisiei și de la contractantul extern. În plus, impactul noilor obligații care decurg din Regulamentul (UE) 2016/679, la care trebuie aliniat prezentul regulament, a fost evaluat în contextul lucrărilor pregătitoare pentru acesta din urmă. Astfel, este inutil să se efectueze în mod expres o evaluare a impactului pentru prezentul regulament.

- **Adecvarea și simplificarea reglementărilor**

Nu se aplică.

- **Drepturi fundamentale**

Dreptul la protecția datelor cu caracter personal este prevăzut la articolul 8 din Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „Carta”), la articolul 16 din TFUE și la articolul 8 din Convenția europeană a drepturilor omului. Așa cum subliniază

Curtea de Justiție a Uniunii Europene[8], dreptul la protecția datelor cu caracter personal nu este un drept absolut, ci trebuie să fie luat în considerare în raport cu funcția sa în societate[9]. De asemenea, protecția datelor este strâns legată de respectarea vieții private și a celei de familie, protejate prin articolul 7 din cartă.

Prezenta propunere stabilește norme privind protecția persoanelor fizice în legătură cu prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și libera circulație a acestor date.

Alte drepturi fundamentale consacrate în Cartă cărora li s-ar putea, eventual, aduce atingere sunt următoarele: libertatea de exprimare (articolul 11); dreptul la proprietate și, în special, protecția proprietății intelectuale [articolul 17 alineatul (2)]; interzicerea oricărei discriminări bazate pe motive de rasă, origine etnică, caracteristici genetice, religie sau convingeri, opinii politice sau de orice altă natură, un handicap sau orientare sexuală (articolul 21); drepturile copilului (articolul 24); dreptul la un nivel ridicat de protecție a sănătății umane (articolul 35); dreptul de acces la documente (articolul 42), precum și dreptul la o cale de atac eficientă și la un proces echitabil (articolul 47*).*

4. IMPLICAȚIILE BUGETARE

A se vedea fișa financiară din anexă.

5. ALTE ELEMENTE

- **Planuri de punere în aplicare și măsuri de monitorizare, evaluare și raportare**

Nu se aplică.

- **Documente explicative (în cazul directivelor)**

Nu se aplică.

CAPITOLUL I - DISPOZIȚII GENERALE

Articolul 1 definește obiectul regulamentului, și, precum articolul 1 din Regulamentul (CE) nr. 45/2001, stabilește cele două obiective urmărite de regulament: protejarea dreptului fundamental la protecția datelor și garantarea liberei circulații a datelor cu caracter personal în întreaga Uniune. Acesta prevede, de asemenea, principalele sarcini ale Autorității Europene pentru Protecția Datelor.

Articolul 2 stabilește domeniul de aplicare al regulamentului: acesta se aplică prelucrării de date cu caracter personal efectuate, prin mijloace automatizate sau în alt mod, de toate instituțiile și organele Uniunii, în măsura în care această prelucrare se înscrie în desfășurarea

[8] CJUE, 9 noiembrie 2010, Volker und Markus Schecke și Eifert, cauzele conexate C-92/09 și C-93/09, ECLI:EU:C:2009:284, punctul 48.

[9] În conformitate cu articolul 52 alineatul (1) din Cartă, pot fi impuse limitări privind exercitarea dreptului la protecția datelor, atât timp cât acestea sunt prevăzute prin lege, respectă substanța acestor drepturi și libertăți și, sub rezerva principiului proporționalității, sunt necesare și numai dacă răspund efectiv obiectivelor de interes general recunoscute de Uniune sau necesității protejării drepturilor și libertăților celorlalți.

activităților care intră integral sau parțial sub incidența dreptului Uniunii. Domeniul de aplicare material al prezentului regulament este neutru din punct de vedere tehnologic. Protecția datelor cu caracter personal ar trebui să se aplice prelucrării datelor cu caracter personal prin mijloace automatizate, precum și prelucrării manuale, în cazul în care datele cu caracter personal sunt cuprinse sau destinate să fie cuprinse într-un sistem de evidență.

Articolul 3 cuprinde definițiile termenilor utilizați în regulament. În afară de definițiile termenilor „instituții și organe ale Uniunii", „operator", „utilizator" și „repertoriu", care sunt specifici prezentului regulament, termenii utilizați în prezentul regulament sunt definiți în Regulamentul (UE) 2016/679, în Regulamentul (UE) 0000/00 [noul regulament privind viața privată și comunicațiile electronice], în Directiva 00/0000/UE [Directiva de instituire a Codului european al comunicațiilor electronice] și în Directiva 2008/63/CE a Comisiei.

CAPITOLUL II – PRINCIPII

Articolul 4 enunță principiile legate de prelucrarea datelor cu caracter personal, care corespund celor prevăzute la articolul 5 din Regulamentul (UE) 2016/679. Comparativ cu Regulamentul (CE) nr. 45/2001, acesta adaugă noul principiu al transparenței și pe cel al integrității și confidențialității.

Articolul 5 se bazează pe articolul 6 din Regulamentul (UE) 2016/679 și stabilește criteriile privind legalitatea prelucrării, cu singura excepție a criteriului interesului legitim al operatorului, care nu se aplică sectorului public și, prin urmare, nu ar trebui să se aplice instituțiilor și organelor Uniunii. Articolul 5 menține criteriile deja stabilite în la articolul 5 din Regulamentul (CE) nr. 45/2001.

Articolul 6 oferă clarificări cu privire la condițiile pentru prelucrarea în alt scop compatibil în conformitate cu articolul 6 alineatul (4) din Regulamentul (UE) 2016/679. Comparativ cu articolul 6 din Regulamentul (CE) nr. 45/2001, această nouă dispoziție asigură o mai mare flexibilitate și un grad sporit de securitate juridică în ceea ce privește prelucrarea ulterioară în scopuri compatibile.

Articolul 7 clarifică, în conformitate cu articolul 7 din Regulamentul (UE) 2016/679, condițiile în care consimțământul constituie un temei juridic valabil pentru legalitatea prelucrării.

Articolul 8 stabilește, în conformitate cu articolul 8 din Regulamentul (UE) 2016/679, condiții suplimentare pentru legalitatea prelucrării datelor cu caracter personal ale copiilor în ceea ce privește serviciile societății informaționale care le sunt oferite în mod direct. Acesta stabilește că vârsta minimă pentru ca un consimțământ dat de un copil să fie valabil este de 13 ani.

Articolul 9 stabilește, în conformitate cu articolul 8 din Regulamentul (CE) nr. 45/2001, norme care prevăd un nivel de protecție specific pentru transmiterea de date cu caracter personal către destinatari, alții decât instituțiile și organele Uniunii, stabiliți în Uniune și care intră sub incidența Regulamentului (UE) 2016/679 sau al Directivei (UE) 2016/680. Se clarifică faptul că, în cazul în care transmiterea are loc la inițiativa operatorului, acesta ar trebui să demonstreze necesitatea și proporționalitatea transmiterii.

Articolul 10, care se bazează pe articolul 9 din Regulamentul (UE) 2016/679 și dezvoltă în continuare articolul 10 din Regulamentul (CE) nr. 45/2001, prevede interdicția generală privind prelucrarea categoriilor speciale de date cu caracter personal și excepțiile de la această regulă generală.

Articolul 11 stabilește, în conformitate cu articolul 10 din Regulamentul (UE) 2016/679 și în concordanță cu articolul 10 alineatul (5) din Regulamentul (CE) nr. 45/2001, condițiile pentru prelucrarea datelor cu caracter personal referitoare la condamnări penale și infracțiuni.

Articolul 12 clarifică obligațiile în materie de informare ale operatorului față de persoana vizată, în conformitate cu articolul 11 din Regulamentul (UE) 2016/679, prevăzând că, 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 doar în scopul 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.

Articolul 13 prevede, pe baza articolului 89 alineatul (1) din Regulamentul (UE) 2016/679, normele referitoare la garanțiile privind prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice.

CAPITOLUL III - DREPTURILE PERSOANEI VIZATE

Secțiunea 1 – Transparență și modalități

Articolul 14 introduce, pe baza articolului 12 din Regulamentul (UE) 2016/679, obligația care le revine operatorilor de a oferi informații transparente, ușor accesibile și ușor de înțeles și de a prevedea proceduri și mecanisme care să permită persoanei vizate să își exercite drepturile, inclusiv, după caz, mijloace pentru depunerea unor cereri pe cale electronică, stabilirea unui termen pentru oferirea unui răspuns la o cerere a persoanei vizate și motivarea refuzurilor. Întrucât nu este de așteptat ca instituțiile și organele Uniunii să solicite, indiferent de împrejurări, plata unor taxe legate de costurile administrative ocazionate de furnizarea informațiilor, această posibilitate nu a fost preluată din Regulamentul (UE) 2016/679.

Secțiunea 2 – Informare și acces la date

Bazându-se pe articolul 13 din Regulamentul (UE) 2016/679 și dezvoltând în continuare articolul 11 din Regulamentul (CE) nr. 45/2001, articolul 15 precizează obligațiile în materie de informare ale operatorului față de persoana vizată în cazul în care datele cu caracter personal sunt colectate de la aceasta din urmă, și anume comunicarea de informații persoanei vizate, inclusiv cu privire la perioada de stocare a datelor și la dreptul de a înainta o plângere, precum și cu privire la transferurile internaționale.

Bazându-se pe articolul 14 din Regulamentul (UE) 2016/679 și dezvoltând în continuare articolul 12 din Regulamentul (CE) nr. 45/2001, articolul 16 precizează în mai mare detaliu obligațiile în materie de informare care îi revin operatorului față de persoana vizată în cazul în care datele cu caracter personal nu au fost obținute de la persoana vizată, și anume furnizarea de informații cu privire la sursa de proveniență a datelor. De asemenea, acest articol menține posibilele derogări cuprinse în Regulamentul (UE) 2016/679, cum ar fi faptul că nu va exista o astfel de obligație în cazul în care persoana vizată deține deja informațiile, în cazul în care furnizarea acestor informații se dovedește imposibilă sau ar presupune un efort disproporționat din partea operatorului, în cazul în care datele trebuie să rămână confidențiale în temeiul unei obligații statutare de secret profesional reglementate de dreptul Uniunii sau în cazul în care înregistrarea sau divulgarea datelor este prevăzută în mod expres prin lege. Această situație se poate aplica de exemplu în cazul procedurilor desfășurate de serviciile competente în materie de securitate socială sau de sănătate.

Articolul 17 prevede, în conformitate cu articolul 15 din Regulamentul (UE) nr. 2016/679 și dezvoltând în continuare articolul 13 din Regulamentul (CE) nr. 45/2001, dreptul persoanei vizate de a avea acces la propriile date cu caracter personal, adăugând elemente noi, cum ar fi obligația de a informa persoana vizată cu privire la perioada de stocare a datelor, la drepturile sale de rectificare și de ștergere a datelor și cu privire la dreptul de a depune o plângere.

Secțiunea 3 – Rectificare și ștergere

Articolul 18 prevede dreptul persoanei vizate la rectificarea datelor și se bazează pe articolul 16 din Regulamentul (UE) 2016/679, dezvoltând în continuare articolul 14 din Regulamentul (CE) nr. 45/2001.

În conformitate cu articolul 17 din Regulamentul (UE) 2016/679 și dezvoltând în continuare articolul 16 din Regulamentul (CE) nr. 45/2001, articolul 19 stabilește „dreptul de a fi uitat” și dreptul la ștergerea datelor al persoanei vizate. Articolul stabilește condițiile privind „dreptul de a fi uitat”, inclusiv obligația operatorului care a făcut publice datele cu caracter personal de a informa părțile terțe cu privire la cererea persoanei vizate privind ștergea oricăror linkuri către datele sale cu caracter personal sau a oricărei copii ori reproduceri a acestora.

Articolul 20 introduce dreptul la restricționarea prelucrării datelor în anumite cazuri, evitând termenul echivoc de „blocare” utilizat în Regulamentul (CE) nr. 45/2001 și asigurând coerența cu noua terminologie de la articolul 18 din Regulamentul (UE) 2016/679.

În conformitate cu articolul 19 din Regulamentul (UE) 2016/679 și dezvoltând în continuare articolul 17 din Regulamentul (CE) nr. 45/2001, articolul 21 prevede obligația operatorului de a comunica destinatarilor cărora le-au fost divulgate datele cu caracter personal orice rectificare sau ștergere a datelor cu caracter personal sau orice restricționare a prelucrării, cu excepția cazului în care acest lucru se dovedește imposibil sau presupune eforturi disproporționate. De asemenea, operatorul trebuie să informeze persoana vizată cu privire la destinatarii respectivi, dacă persoana vizată solicită acest lucru.

Articolul 22 introduce, în conformitate cu articolul 20 din Regulamentul (UE) 2016/679, dreptul persoanei vizate la portabilitatea datelor, adică dreptul de a primi datele cu caracter personal care o privesc și pe care le-a furnizat operatorului sau dreptul ca datele respective să fie transmise direct unui alt operator, atunci când acest lucru este fezabil din punct de vedere tehnic. Ca o condiție preliminară și pentru a îmbunătăți în continuare accesul persoanelor fizice la datele lor cu caracter personal, articolul prevede dreptul de a obține datele respective de la operator într-un format structurat, utilizat în mod curent și care poate fi citit automat. Acest drept se aplică doar în cazul în care prelucrarea se bazează pe consimțământul persoanei vizate sau pe un contract încheiat de aceasta.

Secțiunea 4 – Dreptul la opoziție și procesul decizional individual automatizat

Articolul 23 prevede că persoana vizată are dreptul de a se opune și se bazează pe articolul 21 din Regulamentul (UE) 2016/679, dezvoltând în continuare articolul 18 din Regulamentul (CE) nr. 45/2001.

Articolul 24 se referă la dreptul persoanei vizate de a nu face obiectul unei măsuri care se bazează exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, în conformitate cu articolul 22 din Regulamentul (UE) 2016/679 și dezvoltând în continuare articolul 19 din Regulamentul (CE) nr. 45/2001.

Secțiunea 5 – Restricții

Articolul 25 permite impunerea de restricții cu privire la drepturile persoanei vizate prevăzute la articolele 14-22 și la articolele 34 și 38, precum și cu privire la principiile stabilite la articolul 4 (în măsura în care dispozițiile acestuia corespund drepturilor și obligațiilor prevăzute la articolele 14-22). Aceste restricții ar trebui să fie prevăzute în actele juridice adoptate în temeiul tratatelor sau în normele interne ale instituțiilor și organelor Uniunii. În cazul în care posibilitatea de a impune o astfel de restricție nu este prevăzută de actele juridice adoptate în temeiul tratatelor sau de normele lor interne ale instituțiilor și organelor Uniunii, acestea din urmă pot impune o restricție ad-hoc dacă aceasta respectă esența drepturilor și libertăților fundamentale, în ceea ce privește o anumită operațiune de prelucrare, și dacă reprezintă o măsură necesară și proporțională într-o societate democratică pentru a asigura protecția unuia sau a mai multora dintre obiectivele care permit impunerea de restricții asupra drepturilor persoanei vizate. Această abordare este conformă cu articolul 23 din Regulamentul (UE) 2016/679. Cu toate acestea, spre deosebire de articolul 23 din Regulamentul (UE) 2016/679 și în conformitate cu articolul 20 din Regulamentul (CE) nr. 45/2001, această dispoziție nu prevede posibilitatea de a restricționa dreptul la opoziție și dreptul de a nu face obiectul unor decizii bazate exclusiv pe prelucrarea automată. Cerințele aplicabile restricțiilor sunt conforme cu Carta drepturilor fundamentale a Uniunii Europene și cu Convenția europeană a drepturilor omului, astfel cum sunt interpretate acestea de Curtea de Justiție a Uniunii Europene și, respectiv, de Curtea Europeană a Drepturilor Omului.

CAPITOLUL IV - OPERATORUL ȘI PERSOANA ÎMPUTERNICITĂ DE CĂTRE OPERATOR

Secțiunea 1 – Obligații generale

Articolul 26 se bazează pe articolul 24 din Regulamentul (UE) 2016/679 și introduce „principiul responsabilității”, descriind obligația, care ține de responsabilitatea operatorului, de a respecta dispozițiile prezentului regulament și de a demonstra conformitatea, inclusiv prin adoptarea de măsuri tehnice și organizatorice corespunzătoare și, dacă este cazul, de politici și mecanisme interne care să asigure această conformitate. Articolul 24 alineatul (3) din Regulamentul (UE) 2016/679 nu a fost păstrat în această dispoziție întrucât instituțiile și organele Uniunii nu ar trebui să fie obligate să respecte coduri de conduită sau mecanisme de certificare.

Articolul 27 stabilește, în conformitate cu articolul 25 din Regulamentul (UE) 2016/679, obligațiile operatorului care decurg din principiile protecției datelor începând cu momentul conceperii și al protecției datelor în mod implicit.

Articolul 28 privind operatorii asociați se bazează pe articolul 26 din Regulamentul (UE) 2016/679, având drept scop clarificarea responsabilităților operatorilor asociați, indiferent dacă aceștia sunt sau nu instituții sau organe ale Uniunii, în ceea ce privește relațiile lor interne și cu persoana vizată. Această dispoziție reglementează situația în care același regim juridic (prezentul regulament) se aplică tuturor operatorilor asociați și situația în care unii dintre aceștia intră sub incidența prezentului regulament, iar ceilalți sub cea a unui alt instrument juridic [Regulamentul (UE) 2016/679, Directiva (UE) 2016/680, Directiva (UE) 2016/681 și alte regimuri specifice de protecție a datelor care privesc instituțiile sau organele Uniunii].

Articolul 29 se bazează pe articolul 28 din Regulamentul (UE) 2016/679 și dezvoltă în continuare articolul 23 din Regulamentul (CE) nr. 45/2001 pentru a clarifica funcția și obligațiile persoanelor împuternicite de către operator, stabilind inclusiv faptul că o persoană împuternicită de operator care încălcă prezentul regulament, prin stabilirea scopurilor prelucrării datelor cu caracter personal și a mijloacelor de prelucrare, este considerată a fi operator în ceea ce privește prelucrarea respectivă.

Articolul 30, care se referă la desfășurarea activității de prelucrare sub autoritatea operatorului și a persoanei împuternicite de către operator, se bazează pe articolul 29 din Regulamentul (UE) 2016/679, interzicând persoanei împuternicite de operator sau oricărei persoane care acționează sub autoritatea operatorului ori a persoanei împuternicite de operator și care are acces la date cu caracter personal să prelucreze datele respective, cu excepția cazului în care operatorul a transmis instrucțiuni în acest sens sau a cazului în care dreptul Uniunii ori dreptul intern îl obligă să facă acest lucru.

Articolul 31 se bazează pe articolul 30 din Regulamentul (UE) 2016/679 și introduce obligația operatorilor și a persoanelor împuternicite de operator de a păstra o documentație a operațiunilor de prelucrare desfășurate sub responsabilitatea lor, în locul unei notificări prealabile a AEPD, astfel cum se prevede la articolul 25 din Regulamentul (CE) nr. 45/2001, și al înscrierii în registrul RPD. Spre deosebire de Regulamentul (UE) 2016/679, această dispoziție nu face trimitere la reprezentanți, întrucât instituțiile nu vor dispune de reprezentanți, ci vor avea întotdeauna responsabili cu protecția datelor. Nn au fost menținute trimiterile la transferuri bazate pe derogări pentru situații specifice, astfel cum apar în Regulamentul (UE) 2016/679, întrucât prezentul regulament nu are în vedere aceste tipuri de transferuri. Obligația de a ține o evidență a activităților de prelucrare poate fi centralizată la nivelul unei instituții sau al unui organ al Uniunii. În acest caz, instituțiile și organele Uniunii au posibilitatea de a ține evidența activităților de prelucrare sub forma unui registru accesibil publicului.

Bazându-se pe articolul 31 din Regulamentul (UE) 2016/679, articolul 32 clarifică obligațiile instituțiilor și organelor Uniunii în ceea ce privește cooperarea cu AEPD.

Secțiunea 2 – Securitatea datelor cu caracter personal și confidențialitatea comunicațiilor electronice

Articolul 33 prevede, în conformitate cu articolul 32 din Regulamentul (UE) 2016/679 și dezvoltând în continuare articolul 22 din Regulamentul (CE) nr. 45/2001, faptul că operatorul are obligația de a pune în aplicare măsurile adecvate pentru securizarea prelucrării datelor, extinzând această obligație la persoanele împuternicite de operator, indiferent de tipul de contract încheiat cu operatorul.

Articolul 34 se bazează pe articolul 36 din Regulamentul (CE) nr. 45/2001 și asigură confidențialitatea comunicațiilor electronice în cadrul instituțiilor și organelor Uniunii.

Articolul 35 se bazează pe actuala practică a instituțiilor și organelor Uniunii și protejează informațiile legate de echipamentele terminale ale utilizatorilor finali accesează site-urile web publice și aplicațiile mobile oferite de acestea, în conformitate cu Regulamentul (UE) XX/XXXX [noul regulament privind viața privată și comunicațiile electronice), în special articolul 8.

Articolul 36 se bazează pe articolul 38 din Regulamentul (CE) nr. 45/2001 și protejează datele cu caracter personal care apar în repertoriile publice și private ale instituțiilor și organelor Uniunii.

Articolele 37 și 38 introduc obligația de a notifica încălcările securității datelor cu caracter personal, în conformitate cu articolele 33 și 34 din Regulamentul (UE) 2016/679.

Secțiunea 3 – Evaluarea impactului asupra protecției datelor și consultarea prealabilă

Articolul 39 se bazează pe articolul 35 din Regulamentul (UE) 2016/679 și instituie obligația operatorilor și a persoanelor împuternicite de operatori de a realiza o evaluare a impactului asupra protecției datelor înainte de a efectua operațiuni de prelucrare ce pot avea drept rezultat un risc ridicat la adresa drepturilor și libertăților persoanelor fizice. Această obligație se va aplica în special în cazul evaluării sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, pe prelucrarea pe scară largă a unor categorii speciale de date sau pe monitorizarea sistematică pe scară largă a unei zone accesibile publicului.

Articolul 40 se bazează pe articolul 36 din Regulamentul (UE) 2016/679 și se referă la cazurile în care autorizarea de către AEPD și consultarea acesteia sunt obligatorii înainte de prelucrarea datelor. Cu toate acestea, primul alineat de la articolul 40 reia considerentul 94 din Regulamentul (UE) 2016/679 și vizează clarificarea domeniului de aplicare al obligației de consultare.

Secțiunea 4 – Informații și consultare legislativă

Articolul 41 prevede că instituțiile și organele Uniunii au obligația de a informa Autoritatea Europeană pentru Protecția Datelor atunci când stabilește măsuri administrative sau norme interne legate de prelucrarea datelor cu caracter personal.

Articolul 42 instituie obligația Comisiei de a consulta AEPD în urma adoptării unor propuneri de acte legislative și de recomandări sau propuneri adresate Consiliului în temeiul articolului 218 din TFUE și atunci când elaborează acte delegate sau acte de punere în aplicare care au un impact asupra protecției drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal. În cazul în actele respective prezintă o deosebită importanță pentru protecția drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, Comisia poate consulta, de asemenea, Comitetul european pentru protecția datelor. În astfel de cazuri, ambele entități ar trebui să își coordoneze activitatea în vederea emiterii unui aviz comun. Se instituie un termen de 8 săptămâni pentru emiterea de avize în cazurile menționate anterior, prevăzându-se posibilitatea de a acorda derogări pentru situații de urgență sau dacă acestea se justifică din alte motive, de exemplu atunci când Comisia pregătește acte delegate și de punere în aplicare.

Secțiunea 5 – Obligația de a răspunde la acuzații

Articolul 43 stabilește că operatorii și persoanele împuternicite de aceștia au obligația de a răspunde la acuzații după ce AEPD a decis să îi sesizeze.

Secțiunea 6 – Responsabilul cu protecția datelor

Articolul 44 se bazează pe articolul 37 alineatul (1) din Regulamentul (UE) 2016/679 și pe articolul 24 din Regulamentul (CE) nr. 45/2001 pentru a stabili că instituțiile și organele Uniunii sunt obligate să desemneze un RPD.

Articolul 45 se bazează pe articolul 38 din Regulamentul (UE) 2016/679 și pe articolul 24 din Regulamentul (CE) nr. 45/2001 pentru a stabili funcția RPD.

Articolul 46 se bazează pe articolul 39 din Regulamentul (UE) 2016/679 și pe articolul 24 din Regulamentul (CE) nr. 45/2001, precum și pe punctele 2 și 3 din anexa la acesta din urmă, pentru a stabili principalele sarcini ale RPD.

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

Articolul 47 aprofundează articolul 9 din Regulamentul (CE) nr. 45/2001 și prevede principiul general potrivit căruia, în conformitate cu articolul 44 din Regulamentul (UE) 2016/679, respectarea celorlalte dispoziții ale prezentului regulament și a condițiilor prevăzute în capitolul V este obligatorie pentru orice transferuri de date cu caracter personal către țări terțe sau organizații internaționale, inclusiv pentru 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.

Articolul 48 prevede că un transfer de date cu caracter personal către o țară terță sau o organizație internațională poate avea loc în cazul în care Comisia a decis, în temeiul articolului 45 alineatul (3) din Regulamentul (UE) 2016/679, că este asigurat un nivel adecvat de protecție în țara terță, într-un teritoriu ori unul sau mai multe sectoare specificate din acea țară terță sau organizație internațională, iar datele cu caracter personal sunt transferate exclusiv pentru a permite îndeplinirea sarcinilor care sunt de competența operatorului, care urmează să fie efectuate. Alineatele (2) și (3) de la acest articol au fost preluate de la articolul 9 din Regulamentul (CE) nr. 45/2001, constituind elemente utile pentru monitorizarea nivelului de protecție din țările terțe și din organizațiile internaționale.

Articolul 49 se bazează pe articolul 46 din Regulamentul (UE) 2016/679 și prevede ca transferurile către țări terțe, cu privire la care Comisia nu a adoptat o decizie privind caracterul adecvat al nivelului de protecție, trebuie să prezinte garanții corespunzătoare, în special clauze standard de protecție a datelor și clauze contractuale. Persoanele împuternicite de operatori, care nu sunt instituții și organe ale Uniunii, ar putea recurge la reguli corporative obligatorii, la coduri de conduită și la mecanisme de certificare, în conformitate cu Regulamentul (UE) 2016/679. Alineatul (4) de la acest articol, care prevede că instituțiile și organele Uniunii au obligația de a informa AEPD cu privire la categoriile de cazuri în care au aplicat acest articol, corespunde articolului 9 alineatul (8) din Regulamentul (CE) nr. 45/2001 și este păstrat datorită caracterului său specific. Alineatul (5) se bazează pe clauza privind drepturile obținute anterior aplicată autorizațiilor existente prevăzute la articolul 46 alineatul (5) din Regulamentul (UE) 2016/679.

Articolul 50 clarifică, în conformitate cu articolul 48 din Regulamentul (UE) 2016/679, faptul că hotărârile pronunțate de instanțe sau tribunale sau deciziile autorităților administrative din țări terțe care impun transferul sau divulgarea de date cu caracter personal pot fi recunoscute sau executate 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 acestui capitol.

Articolul 51 se bazează pe articolul 49 din Regulamentul (UE) 2016/679 și definește și clarifică derogările aplicabile în cazul realizării unui transfer de date. Această dispoziție se aplică, în special, transferurilor de date solicitate și necesare din motive importante de interes public, de exemplu în cazul transferurilor internaționale de date între autoritățile de concurență, administrațiile fiscale sau vamale sau între servicii competente în materie de securitate socială sau de gestionare a pescuitului. Alineatul (5), referitor la obligația de a informa AEPD cu privire la categoriile de cazuri în care au fost invocate derogări pentru realizarea unui transfer, corespunde textului actual al articolului 9 alineatul (8) din Regulamentul (CE) nr. 45/2001.

Articolul 52 se bazează pe articolul 50 din Regulamentul (UE) 2016/679 și prevede în mod explicit mecanisme de cooperare internațională pentru protecția datelor cu caracter personal între AEPD, în cooperare cu Comisia și cu Comitetul european pentru protecția datelor, și autoritățile de supraveghere din țările terțe.

CAPITOLUL VI – AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR

Articolul 53 se bazează pe articolul 41 din Regulamentul (CE) nr. 45/2001 și se referă la instituirea AEPD.

Articolul 54 se bazează pe articolul 42 din Regulamentul (CE) nr. 45/2001 și pe articolul 3 din Decizia 1247/2002/CE și stabilește normele privind numirea AEPD de către Parlamentul European și Consiliu. Articolul precizează, de asemenea, durata mandatului acesteia: cinci ani.

Articolul 55 se bazează pe articolul 43 din Regulamentul (CE) nr. 45/2001 și pe articolul 1 din Decizia 1247/2002/CE și stabilește statutul și condițiile generale de exercitare a atribuțiilor de către AEPD, precum și resursele umane și financiare ale acesteia.

Articolul 56 se bazează pe articolul 52 din Regulamentul (UE) 2016/679 și pe articolul 44 din Regulamentul (CE) nr. 45/2001 și clarifică condițiile de garantare a independenței AEPD, ținând seama de jurisprudența Curții de Justiție a Uniunii Europene.

Articolul 57 stabilește, pe baza articolului 45 din Regulamentul (CE) nr. 45/2001, obligațiile în materie de secret profesional care îi revin AEPD pe durata mandatului și după încetarea acestuia în ceea ce privește informațiile confidențiale de care a luat cunoștință în cursul executării atribuțiilor oficiale.

Articolul 58 se bazează pe articolul 57 din Regulamentul (UE) 2016/679 și pe articolul 46 din Regulamentul (CE) nr. 45/2001 și stabilește sarcinile AEPD, care constau, printre altele, în audierea și examinarea plângerilor și în sensibilizarea publicului cu privire la riscurile, normele, garanțiile și drepturile din acest domeniu.

Articolul 59 se bazează pe articolul 58 din Regulamentul (UE) 2016/679 și pe articolul 47 din Regulamentul (CE) nr. 45/2001 și stabilește competențele AEPD.

Articolul 60 se bazează pe articolul 59 din Regulamentul (UE) 2016/679 și pe articolul 48 din Regulamentul (CE) nr. 45/2001 și stabilește obligația AEPD de a întocmi un raport anual de activitate.

CAPITOLUL VII – COOPERARE ȘI COERENȚĂ

Articolul 61 se bazează pe articolul 61 din Regulamentul (UE) 2016/679 și pe articolul 46 litera (f) din Regulamentul (CE) nr. 45/2001 și instituie reguli explicite privind cooperarea AEPD cu autoritățile naționale de supraveghere.

Articolul 62 prevede obligațiile care revin AEPD în cazul în care alte acte ale Uniunii fac trimitere la acest articol în contextul supravegherii coordonate cu autoritățile naționale de supraveghere. Acesta urmărește punerea în aplicare a unui model unic de supraveghere coordonată. Modelul ar putea fi utilizat nu numai pentru supravegherea coordonată a sistemelor informatice de mari dimensiuni, cum ar fi Eurodac, Sistemul de informații Schengen II, Sistemul de informații privind vizele, Sistemul de informații al vămilor și Sistemul de informare al pieței interne, ci și pentru supravegherea unor agenții ale Uniunii în cazul în care a fost stabilit un anumit model de cooperare între AEPD și autoritățile naționale, precum Europol. Comitetul european pentru protecția datelor ar trebui să exercite rolul de forum unic care asigură supravegherea efectivă coordonată la toate nivelurile.

CAPITOLUL VIII - CĂI DE ATAC, RĂSPUNDERE ȘI SANCȚIUNI

Articolul 63 se bazează pe articolul 77 din Regulamentul (UE) 2016/679 și pe articolul 32 din Regulamentul (CE) nr. 45/2001 și prevede dreptul oricărei persoane vizate de a depune o plângere la AEPD. Acest articol stabilește, de asemenea, obligația AEPD de a da curs plângerii și de a informa persoana vizată cu privire la stadiul în care se află acest proces și cu privire la soluția oferită într-un termen de trei luni, după acest termen considerându-se că plângerea a fost respinsă.

Articolul 64 păstrează dispozițiile articolului 32 alineatul (1) din Regulamentul (CE) nr. 45/2001, stabilind competența Curții de Justiție a Uniunii Europene de a judeca toate litigiile privind dispozițiile prezentului regulament, inclusiv cererile de despăgubire.

Articolul 65 stabilește dreptul la despăgubiri, atât pentru prejudiciul material, cât și pentru cel moral, sub rezerva îndeplinirii condițiilor prevăzute în tratate, inclusiv în ceea ce privește răspunderea.

Articolul 66 se bazează pe articolul 83 din Regulamentul (UE) 2016/679 și prevede că AEPD dispune de competența de a aplica amenzi administrative instituțiilor și organelor Uniunii, cu titlu de sancțiune în ultimă instanță și numai în cazul în care instituțiile sau organele Uniunii nu au respectat un ordin al AEPD menționat la articolul 59 alineatul (2) literele (a)-(h) și (j). Articolul precizează, de asemenea, criteriile pe baza cărora este decis cuantumul amenzii administrative în fiecare caz în parte, în timp ce plafoanele maxime anuale se bazează pe cuantumurile amenzilor aplicabile în unele state membre.

Articolul 67 autorizează, în conformitate cu articolul 80 alineatul (1) din Regulamentul (UE) 2016/679, anumite organisme, organizații sau asociații să depună o plângere în numele persoanei vizate.

Articolul 68 prevede, în conformitate cu articolul 33 din Regulamentul (CE) nr. 45/2001, norme specifice care vizează protejarea membrilor personalului Uniunii care depun o plângere la AEPD cu privire la o presupusă încălcare a dispozițiilor prezentului regulament, fără a acționa pe căi oficiale.

Articolul 69 se bazează pe articolul 49 din Regulamentul (CE) nr. 45/2001 și prevede sancțiuni aplicabile în caz de nerespectare a obligațiilor prevăzute de prezentul regulament de către funcționarii publici sau alți agenți ai Uniunii Europene.

CAPITOLUL IX – ACTE DE PUNERE ÎN APLICARE

Articolul 70 cuprinde dispoziții privind procedura comitetului necesară pentru a acorda Comisiei competențe de executare, în cazurile în care, în conformitate cu articolul 291 din TFUE, sunt necesare condiții uniforme de punere în aplicare a actelor obligatorii din punct de vedere juridic ale Uniunii. În acest caz, se aplică procedura de examinare.

CAPITOLUL X - DISPOZIȚII FINALE

Articolul 71 abrogă Regulamentul (CE) nr. 45/2001 și Decizia 1247/2002/CE și prevede că trimiterile la cele două instrumente abrogate se interpretează ca trimiteri la prezentul regulament.

Articolul 72 clarifică faptul că prezentul regulament nu aduce atingere actualului mandat al Autorității Europene pentru Protecția Datelor și al adjunctului acesteia și că articolul 54 alineatele (4), (5) și (7) și articolele 56 și 57 din regulament se aplică actualului adjunct al AEPD până la încheierea mandatului său, și anume până la 5 decembrie 2019.

Articolul 73 stabilește că data de intrare în vigoare a prezentului regulament este 25 mai 2018, pentru a asigura coerența cu data de la care se aplică Regulamentul (UE) 2016/679.

2017/0002 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ŞI AL CONSILIULUI

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

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[10],

[10] JO C , , p. .

hotărând în conformitate cu procedura legislativă ordinară,

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.

(2) Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului[11] oferă persoanelor fizice drepturi opozabile din punct de vedere juridic, precizează obligațiile în materie de prelucrare a datelor care le revin operatorilor din 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 mai sus 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[12] și Directiva (UE) 2016/680 a Parlamentului European și a Consiliului[13] 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 subliniază că trebuie să se aducă adaptările necesare Regulamentului (CE) nr. 45/2001 pentru a asigura un cadru solid și coerent în materie de protecție a datelor în Uniune și a permite aplicarea în același timp 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 și organelor 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 o dispoziție a prezentului regulament se

---

11 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).

12 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) (Text cu relevanță pentru SEE), JO L 119, 4.5.2016, p. 1-88.

13 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. 89-131.

bazează pe aceeași noțiune ca și o dispoziție a Regulamentului (UE) 2016/679, aceste două dispoziții ar trebui să fie interpretate în mod omogen, în special pentru că structura propunerii 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. Protecția persoanelor fizice ar trebui să se aplice prelucrării datelor cu caracter personal prin mijloace automatizate, precum și prelucrării manuale, în cazul în care datele cu caracter personal sunt cuprinse sau destinate să fie cuprinse într-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.

(8) În Declarația nr. 21 cu privire la protecția datelor cu caracter personal în domeniul cooperării judiciare în materie penală și al cooperării polițienești, anexată la actul 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. Prin urmare, prezentul regulament ar trebui să se aplice agențiilor Uniunii care desfășoară activități în domeniile cooperării judiciare în materie penală și al cooperării polițienești numai în măsura în care dreptul Uniunii aplicabil acestor agenții nu prevede norme specifice privind prelucrarea datelor cu caracter personal.

(9) Directiva (UE) 2016/680 prevede norme armonizate pentru protecția și libera circulație a datelor cu caracter personal prelucrate în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora. În vederea promovării aceluiași nivel de protecție pentru persoanele fizice prin drepturi opozabile din punct de vedere juridic în întreaga Uniune și a preîntâmpinării discrepanțelor care împiedică schimbul de date cu caracter personal între agențiile Uniunii care desfășoară activități în domeniile cooperării judiciare în materie penală și al cooperării polițienești și autoritățile competente ale statelor membre, normele pentru protecția și libera circulație a datelor cu caracter personal operaționale prelucrate de aceste agenții ale Uniunii ar trebui să se bazeze pe principiile care stau la baza prezentului regulament și să fie coerente cu Directiva (UE) 2016/680.

(10) În cazul în care actul de înființare a unei agenții a Uniunii care desfășoară activități ce intră în domeniul de aplicare a capitolelor 4 și 5 de la titlul V din tratat stabilește un regim de protecție a datelor de sine stătător pentru prelucrarea datelor operaționale cu

caracter personal, aceste regimuri ar trebui să nu fie afectate de prezentul regulament. Cu toate acestea, în conformitate cu articolul 62 din Directiva (UE) 2016/680, Comisia ar trebui, până la 6 mai 2019, să revizuiască actele Uniunii care reglementează prelucrarea (datelor cu caracter personal) de către autoritățile competente în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora și, după caz, să prezinte propunerile necesare de modificare a actelor respective pentru a asigura o abordare uniformă a protecției datelor cu caracter personal în domeniile cooperării judiciare în materie penală și al cooperării polițienești.

(11) 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.

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

(13) 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.

(14) 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.

(15) 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 a utilizării neautorizate a datelor cu caracter personal și a echipamentului utilizat pentru prelucrare.

(16) În conformitate cu principiul responsabilității, în cazul în care date cu caracter personal sunt transmise între instituții sau organe ale Uniunii ori în cadrul acestora, 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 cazul în care destinatarul nu face parte din operator. În particular, 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 de prelucrare legală a datelor cu caracter personal, precum și competența destinatarului și 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.

(17) 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 acestea, necesitatea respectării obligației legale care îi revine operatorului sau un alt motiv legitim menționat în prezentul regulament, inclusiv consimțământul persoanei vizate sau 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.

(18) Dreptul Uniunii, inclusiv normele interne menționate 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 jurisprudența Curții de Justiție a Uniunii Europene și a Curții Europene a Drepturilor Omului.

(19) 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.

(20) 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 de sfera de acoperire a acestuia. În conformitate cu Directiva 93/13/CEE a Consiliului[14], 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 căreia îi 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.

(21) 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. Această 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 utilizării serviciilor oferite direct copiilor pe website-urile instituțiilor și organelor Uniunii, cum ar fi serviciile de comunicare interpersonală sau vânzarea online de bilete, precum și atunci când prelucrarea datelor cu caracter personal se bazează pe consimțământ.

(22) Atunci când destinatari stabiliți în Uniune și care intră sub incidența Regulamentului (UE) 2016/679 sau a Directivei (UE) 2016/680 doresc să li se transmită date cu caracter personal de către instituții și organe ale Uniunii, destinatarii respectivi ar trebui să demonstreze că transmiterea de date este necesară pentru realizarea obiectivului lor, este proporțională și nu depășește ceea ce este necesar pentru îndeplinirea obiectivului respectiv. Instituțiile și organele Uniunii ar trebui să demonstreze această necesitate atunci când inițiază ele însele transmiterea, în conformitate cu principiul transparenței.

(23) 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 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

[14] 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).

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.

(24) 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[15], 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 de către părți terțe.

(25) 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.

(26) 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 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 norme interne, 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.

---

15 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).

(27) 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.

(28) 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.

(29) 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.

(30) 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.

(31) 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.

(32) 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.

(33) 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 web. 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.

(34) 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.

(35) 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.

(36) 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 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 un copil. 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 care 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 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.

(37) Actele juridice adoptate în temeiul tratatelor sau normele interne ale instituțiilor și organelor Uniunii pot impune restricții în privința unor principii specifice, în privința dreptului de informare, a dreptului de acces la datele cu caracter personal și de rectificare sau ștergere a acestora, în privința dreptului la portabilitatea datelor, a dreptului la confidențialitatea 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, prevenirea, investigarea și urmărirea penală a infracțiunilor sau executarea pedepselor, inclusiv 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, pentru a se asigura securitatea internă a instituțiilor și organelor Uniunii, alte obiective importante de interes public general ale Uniunii sau ale unui stat membru, în special un interes economic sau financiar important al Uniunii sau al unui stat membru, pentru menținerea de registre publice din motive de interes public general sau protecția persoanei vizate ori a drepturilor și libertăților unor terți, inclusiv protecția socială, sănătatea publică și scopurile umanitare.

În cazul în care o restricție nu este prevăzută de acte juridice adoptate în temeiul tratatelor sau de normele lor interne, instituțiile și organele Uniunii pot impune, într-un caz specific, o restricție ad-hoc asupra unor principii specifice și asupra drepturilor persoanei vizate, dacă această restricție respectă esența drepturilor și libertăților fundamentale și, în ceea ce privește o anumită operație de prelucrare, este necesară și proporțională într-o societate democratică, pentru a asigura unul sau mai multe din obiectivele menționate la primul paragraf. Restricția ar trebui să fie notificată responsabilului cu protecția datelor. Toate restricțiile ar trebui să fie conforme cu cerințele prevăzute de cartă și de Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale.

(38) 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. 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. 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.

(39) 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.

(40) Protecția drepturilor și libertăților persoanelor vizate, precum și responsabilitatea și răspunderea operatorilor și a persoanelor împuternicite de operator 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.

(41) 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 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 ar trebui să fie reglementată printr-un contract sau un alt tip de act juridic, în temeiul dreptului Uniunii sau al dreptului intern, 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.

(42) 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. 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.

(43) 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.

(44) Instituțiile și organele Uniunii ar trebui să asigure confidențialitatea comunicațiilor electronice, astfel cum prevede articolul 7 din Cartă. În particular, instituțiile și organele Uniunii ar trebui să asigure securitatea propriilor rețele de comunicații electronice, să protejeze informațiile legate de echipamentele terminale ale utilizatorilor finali care le oferă acces la site-urile lor web publice și la aplicațiile lor mobile, în conformitate cu Regulamentul (UE) XX/XXXX [noul regulament privind viața privată și comunicațiile electronice] și să protejeze confidențialitatea datelor personale cuprinse în repertoriile cu utilizatori.

(45) 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.

(46) 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.

(47) Regulamentul (CE) nr. 45/2001 prevede că operatorul are o obligație generală de a notifica prelucrarea de date cu caracter personal responsabilului cu protecția datelor, care, la rândul lui, ar urma să țină un registru al operațiunilor de prelucrare ce i-au fost notificate. Cu toate că obligația respectivă generează sarcini administrative și financiare, aceasta nu a contribuit întotdeauna la îmbunătățirea protecției datelor cu caracter personal. Prin urmare, astfel de obligații de notificare generală nediferențiată ar trebui să fie abrogate și înlocuite cu proceduri și mecanisme eficace care să pună accentul, în schimb, pe acele tipuri de operațiuni 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 tipuri de operațiuni de prelucrare ar putea fi cele care presupun, în special, utilizarea unor noi tehnologii sau care reprezintă un nou tip de operațiuni, pentru care nicio evaluare a impactului asupra protecției datelor nu a fost efectuată anterior de către operator ori care 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.

(48) 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 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.

(49) Autoritatea Europeană pentru Protecția Datelor ar trebui să fie informată cu privire la măsurile administrative și normele interne ale instituțiilor și organelor Uniunii care prevăd prelucrarea de date cu caracter personal, stabilesc condiții cu privire la restricțiile impuse drepturilor persoanelor vizate sau oferă garanții corespunzătoare în ceea ce privește drepturile persoanelor vizate, pentru a asigura conformitatea cu prezentul regulament a prelucrării avute în vedere și, în special, pentru a atenua riscurile la care este expusă persoana vizată.

(50) Regulamentul (UE) nr. 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 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, 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) nr. 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 caz de urgență sau în alte cazuri în care este necesar, de exemplu atunci când Comisia pregătește acte delegate și acte de punere în aplicare.

(51) În cadrul fiecărei instituții sau al fiecărui organ al Uniunii, un responsabil cu protecția datelor ar trebui să asigure aplicarea dispozițiilor prezentului regulament și să ofere consiliere operatorilor și persoanelor împuternicite de aceștia 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 și de nivelul de protecție impus pentru datele cu caracter personal prelucrate de operator sau de persoana împuternicită de operator. Acești responsabili cu protecția datelor ar trebui să fie în măsură să își îndeplinească îndatoririle și sarcinile în mod independent.

(52) 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 nu ar trebui să fie diminuat, 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. 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.

(53) Comisia poate să decidă, în temeiul articolului 45 din Regulamentul (UE) 2016/679, 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.

(54) 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.

(55) 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 aceștia 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.

(56) 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.

(57) 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.

(58) 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.

(59) 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.

(60) 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 de supraveghere din Uniune, inclusiv 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 alte autorități de supraveghere a protecției datelor, pentru a le ajuta să facă schimb de informații cu omologii lor internaționali.

(61) Instituirea, prin Regulamentul (CE) nr. 45/2001, a Autorității Europene pentru Protecția Datelor, 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.

(62) 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 de supraveghere din statele membre, 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 a Uniunii Europene cu privire la cazurile de încălcare a prezentului regulament și 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. 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.

(63) 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.

(64) 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.

(65) În anumite cazuri, dreptul Uniunii prevede un model de supraveghere coordonată, repartizată între Autoritatea Europeană pentru Protecția Datelor și autoritățile naționale de supraveghere. În plus, Autoritatea Europeană pentru Protecția Datelor este autoritatea de supraveghere a Europol, existând 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, dacă este cazul, propuneri legislative 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 care asigură supravegherea efectivă coordonată la toate nivelurile.

(66) 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 a Uniunii Europene 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.

(67) 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 tratat.

(68) 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 organului 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, limitele maxime și criteriile pentru stabilirea amenzilor administrative aferente. Autoritatea Europeană pentru Protecția Datelor ar trebui să determine cuantumul amenzilor 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, precum și 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 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 a Uniunii Europene.

(69) 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 caracter personal, să depună o plângere în numele său la Autoritatea Europeană pentru Protecția Datelor. Aceste organisme, organizații sau asociații 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.

(70) 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 de alt tip, în conformitate cu normele și procedurile prevăzute în Statutul funcționarilor Uniunii Europene și în Regimul aplicabil celorlalți agenți ai Uniunii Europene.

(71) În vederea asigurării unor condiții uniforme de punere în aplicare a prezentului regulament, Comisia ar trebui învestită cu competențe de executare în situațiile stabilite de prezentul regulament. Competențele respective ar trebui să fie exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului[16]. 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 listei operațiunilor de prelucrare în cazul cărora operatorii care efectuează activități de prelucrare necesare pentru îndeplinirea unei sarcini de interes public trebuie să consulte în prealabil Autoritatea Europeană pentru Protecția Datelor, precum și pentru adoptarea unor clauze contractuale standard care oferă garanții adecvate pentru transferurile internaționale.

(72) 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

[16] 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).

Consiliului prevede[17] specificații suplimentare privind confidențialitatea datelor statistice pentru statisticile europene.

(73) Regulamentul (CE) nr. 45/2001 și Decizia 1247/2002/CE ar trebui abrogate. Trimiterile la regulamentul și la decizia abrogate ar trebui interpretate ca trimiteri la prezentul regulament.

(74) 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.

(75) În conformitate cu principiul proporționalității, este necesar și adecvat, în vederea îndeplinirii obiectivului fundamental al asigurării unui nivel echivalent de protecție a persoanelor fizice 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 Tratatul privind Uniunea Europeană.

(76) 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 XX/XX/XXXX,

ADOPTĂ PREZENTUL REGULAMENT:

CAPITOLUL I

DISPOZIȚII GENERALE

Articolul 1
Obiect și obiective

(1) Prezentul regulament stabilește norme privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și norme privind libera circulație a datelor cu caracter personal

[17] 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).

între acestea sau către destinatari stabiliți în Uniune și care intră sub incidența Regulamentului (UE) 2016/679[18] sau a dispozițiilor de drept intern adoptate în temeiul Directivei (UE) 2016/680[19].

(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 (denumită în continuare „AEPD") 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 de date cu caracter personal efectuate de toate instituțiile și organele Uniunii în măsura în care această prelucrare face parte din desfășurarea activităților care intră integral sau parțial sub incidența dreptului Uniunii.

(2) Prezentul regulament se aplică prelucrării de date 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

(1) În sensul prezentului regulament, se aplică următoarele definiții:

(a) definițiile din Regulamentul (UE) nr. 2016/679, cu excepția definiției termenului „operator" de la articolul 4 punctul 7 din regulament susmențional;

(b) definiția termenului „comunicații electronice" de la articolul 4 alineatul (2) litera (a) din Regulamentul (UE) XX/XXXX [Regulamentul privind viața privată și comunicațiile electronice];

(c) definițiile termenilor „rețea de comunicații electronice" și „utilizator final" de la articolul 2 alineatele (1) și, respectiv, (14) din Directiva 00/0000/UE [Directiva de instituire a Codului european al comunicațiilor electronice];

---

[18] 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) (Text cu relevanță pentru SEE), JO L 119, 4.5.2016, p. 1-88.

[19] 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. 89-131.

(d) definiția termenului „echipament terminal” de la articolul 1 alineatul (1) din Directiva 2008/63/CE a Comisiei[20].

(2) În plus, în sensul prezentului regulament, se aplică următoarele definiții:

(a) „instituții și organe ale Uniunii” înseamnă instituțiile, organele, oficiile și agențiile înființate prin Tratatul privind Uniunea Europeană, Tratatul privind funcționarea Uniunii Europene sau Tratatul Euratom sau în temeiul acestora;

(b) „operator” înseamnă instituția, organul, oficiul sau agenția 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;

(c) „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;

(d) „repertoriu” 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.

CAPITOLUL II

PRINCIPII

Articolul 4
Principii legate de prelucrarea datelor cu caracter personal

(1) Datele cu caracter personal trebuie:

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

(b) să fie colectate în scopuri determinate, explicite și legitime și să nu fie prelucrate mai departe 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”);

[20] 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).

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

(d) să fie exacte și, dacă este necesar, actualizate. Se iau toate măsurile rezonabile pentru a se asigura că datele inexacte sau incomplete, având în vedere scopurile pentru care au fost colectate sau pentru care sunt prelucrate ulterior, sunt șterse sau rectificate fără întârziere („exactitatea”);

(e) să fie păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor pentru 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 („limitările legate de stocare”);

(f) să fie 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 („responsabilitatea”).

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 în baza sau în 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, la cererea persoanei vizate, demersuri prealabile încheierii 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) Sarcinile menționate la alineatul (1) litera (a) 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 o dispoziție din 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 temeiul articolului 10, sau în cazul în care sunt prelucrate date cu caracter personal referitoare la condamnări penale și infracțiuni, în temeiul articolului 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 se prezintă într-o formă care o diferențiază în mod clar de celelalte aspecte, 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 copiilor 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 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, alții decât instituțiile și organele Uniunii, stabiliți în Uniune și care intră sub incidența Regulamentului (UE) 2016/679 sau a Directivei (UE) 2016/680

(1) Fără a aduce atingere articolelor 4, 5, 6 și 10, datele cu caracter personal sunt transmise numai destinatarilor stabiliți în Uniune și care intră sub incidența Regulamentului (UE) 2016/679 sau a legislației naționale adoptate în temeiul Directivei (UE) 2016/680, dacă destinatarul demonstrează că:

(a) datele sunt necesare pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice sau că

(b) transmiterea datelor este necesară, este proporțională cu scopul ei și nu există niciun motiv să se presupună că drepturile, libertățile și interesele legitime ale persoanei vizate ar putea fi afectate.

(2) În cazul în care transmiterea în temeiul prezentului articol are loc la inițiativa operatorului, operatorul demonstrează că transmiterea de date cu caracter personal este necesară și proporțională cu scopul ei, prin aplicarea criteriilor stabilite la alineatul 1 literele (a) sau (b).

Articolul 10

Prelucrarea de categorii speciale de date cu caracter personal

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

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

(c) prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale altei persoane, atunci când persoana vizată se află în incapacitatea 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 periodice legate de 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 ori de câte ori Curtea de Justiție a Uniunii Europene 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 dispozițiilor 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 unor dispozițiilor ale 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 în temeiul legislației Uniunii sau sub responsabilitatea unui astfel de profesionist.

Articolul 11
Prelucrarea de date 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) poate fi efectuată numai dacă este autorizată de dispoziții ale dreptului Uniunii, care pot include norme interne și care oferă garanții specifice 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 măsurile 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 38 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 care sunt 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 38 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.

În aceste cazuri, 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 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 datele cu caracter personal referitoare la o persoană vizată sunt colectate 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 sau, în cazul transferurilor menționate la articolul 49, 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 din cadrul unei organizații internaționale și existența sau absența unei decizii a Comisiei privind caracterul adecvat sau, în cazul transferurilor menționate la articolul 49, o trimitere la garanțiile pertinente 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 ar putea 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; sau

(d) în cazul în care datele cu caracter personal trebuie să rămână confidențiale în temeiul unei obligații statutare de secret profesional reglementate de dreptul Uniunii.

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 49 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 care prelucrează datele cu caracter personal că persoana vizată a solicitat ștergerea de către aceștia 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 cazul în care se aplică unul din 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 acestora este ilegală, iar persoana vizată se opune ștergerii datelor, solicitând, 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 datele cu caracter personal sunt restricționate 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 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 de a se opune, 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 34 și 35, 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 de date 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) 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, 34 și 38, 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, investigarea, depistarea 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 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, investigarea, depistarea 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) Atunci când o restricție nu este prevăzută de un act legislativ adoptat în temeiul tratatelor sau de o normă internă în conformitate cu alineatul (1), instituțiile și organele Uniunii pot restricționa aplicarea articolelor 14-22, 34 și 38, 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 în ceea ce privește o anumită operațiune de prelucrare și constituie o măsură necesară și proporțională într-o

societate democratică pentru a garanta unul sau mai multe dintre obiectivele menționate la alineatul (1). Restricția se notifică responsabilului cu protecția datelor competent.

(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, 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, 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 suficient de clare și de precise și se publică în mod corespunzător.

(6) În cazul în care este impusă o restricție în temeiul alineatului (1) sau (2), 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) sau (2) 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) și la articolul 46 alineatul (2) poate fi amânată, omisă sau refuzată în cazul în care aceasta ar anula efectul restricției impuse în temeiul alineatului (1) sau (2).

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.

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.

Articolul 28
Operatorii asociați

(1) În cazul în care o instituție sau un organ al Uniunii, împreună cu unul sau mai mulți operatori, care pot fi sau nu instituții sau organe ale Uniunii, stabilesc în comun scopurile prelucrării și mijloacele de realizare a ei, 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 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) Persoana vizată își poate exercita drepturile de care beneficiază în temeiul prezentului regulament în legătură cu sau împotriva unuia sau mai multora dintre operatorii asociați, ținând seama de rolurile lor astfel cum au fost stabilite în conformitate cu termenii acordului menționat la alineatul (1).

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 33-40, 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, aplicarea unui cod de conduită aprobat, menționat la articolul 40 alineatul (5) din Regulamentul (UE) 2016/679, sau a unui 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 70 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 încălcă 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 și 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) Instituțiile și organele Uniunii pot decide să își păstreze evidențele activităților de prelucrare într-un registru central. În acest caz, ele pot, de asemenea, să decidă să pună 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 ȘI CONFIDENȚIALITATEA COMUNICAȚIILOR ELECTRONICE

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 riscul 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.

Articolul 34
Confidențialitatea comunicațiilor electronice

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

Articolul 35
Protecția informațiilor legate de echipamentele terminale ale utilizatorilor finali

Instituțiile și organele Uniunii protejează informațiile legate de echipamentele terminale prin intermediul cărora utilizatorii finali accesează site-urile lor web publice și aplicațiile lor mobile publice, în conformitate cu Regulamentul (UE) XX/XXXX [noul regulament privind viața privată și comunicațiile electronice), în special articolul 8.

Articolul 36
Repertorii de utilizatori

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

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

Articolul 37
Notificarea către Autoritatea Europeană 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 încălcarea securității datelor cu caracter personal nu este de natură să ducă la apariția unui risc la adresa drepturilor și libertăților 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 38

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 37 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

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) 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 la adresa drepturilor și libertăților persoanelor vizate, menționată 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.

(7) 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.

(8) 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.

(9) 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) nu se aplică, cu excepția cazului în care dreptul Uniunii prevede acest lucru.

(10) 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 59. 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 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 4

INFORMARE ȘI CONSULTARE LEGISLATIVĂ

Articolul 41
Informare

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 care implică o instituție sau un organ al Uniunii singur sau împreună cu altele.

Articolul 42
Consultare legislativă

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

(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 menționată 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 5

OBLIGAȚIA DE A RĂSPUNDE LA ACUZAȚII

Articolul 43
Obligația de a răspunde la acuzații

În cazul în care Autoritatea Europeană pentru Protecția Datelor își exercită competențele prevăzute la articolul 59 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.

SECȚIUNEA 6

RESPONSABILUL CU PROTECȚIA DATELOR

Articolul 44
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 46.

(4) Responsabilul cu protecția datelor poate fi un membru al personalului instituției sau organului Uniunii sau poate să își îndeplinească sarcinile 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 45
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 46, 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, fără să se recurgă la căile oficiale, în orice problemă privind interpretarea sau aplicarea prezentului regulament. 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 decât cu acordul Autorității Europene pentru Protecția Datelor, dacă nu mai îndeplinește condițiile necesare pentru exercitarea atribuțiilor sale.

(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 46
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 privind încălcarea securității datelor cu caracter personal, în temeiul articolelor 37 și 38;

(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 și consultarea acesteia în cazul în care există îndoieli cu privire la necesitatea unei consultări prealabile;

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

(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 47
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 48
Transferuri în temeiul unei decizii privind caracterul adecvat al nivelului de protecție

(1) Un transfer de date cu caracter personal către o țară terță sau o organizație internațională poate avea loc în cazul în care Comisia a decis, în temeiul articolului 45 alineatul (3) din Regulamentul (UE) 2016/679, că este asigurat un nivel adecvat de protecție în țara terță, într-un teritoriu ori unul sau mai multe sectoare specificate din acea țară terță sau în cadrul organizației internaționale, iar 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 țara terță sau organizația 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 alineatele (3) și (5) din Regulamentul (UE) 2016/679, dacă o țară terță sau o organizație internațională asigură sau nu mai asigură un nivel adecvat de protecție.

Articolul 49
Transferuri în baza unor garanții adecvate

(1) În absența unei decizii în temeiul articolului 45 alineatul (3) din Regulamentul (UE) 2016/679, 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 70 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 70 alineatul (2);

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

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

(5) 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.

Articolul 50
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 51
Derogări pentru situații specifice

(1) În absența unei decizii în temeiul articolului 45 alineatul (3) din Regulamentul (UE) 2016/679 sau a unor garanții adecvate în conformitate cu articolul 49, 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; sau

(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) 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.

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

(4) 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.

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

Articolul 52
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 53
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 58 și exercită competențele care i-au fost conferite prin articolul 59.

Articolul 54
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 se publică. 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 întocmită de Comisie, de pe care este aleasă Autoritatea Europeană pentru Protecția Datelor, este alcătuită din personalități care oferă toate garanțiile de

independență și care posedă experiența și competențele necesare îndeplinirii atribuțiilor de Autoritate Europeană pentru Protecția Datelor, de exemplu deoarece sunt sau au fost membri ai autorităților de supraveghere instituite în temeiul articolului 41 din Regulamentul (UE) 2016/679.

(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 a Uniunii Europene, 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 55
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 a Uniunii Europene 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 IX din bugetul general al Uniunii Europene.

(4) Autoritatea Europeană pentru Protecția Datelor este asistată de un secretariat. Funcționarii și ceilalți membri de personal ai 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.

(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 Europene.

(6) Autoritatea Europeană pentru Protecția Datelor își are sediul la Bruxelles.

Articolul 56
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 57
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 58
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 și a oricărui alt act al Uniunii referitor la protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către o instituție sau un organ al Uniunii, cu excepția prelucrării de date cu caracter personal de către Curtea de Justiție a Uniunii Europene 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 de supraveghere din statele membre 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 consultanță 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 49 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, înființat prin articolul 68 din Regulamentul (UE) 2016/679;

(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 49 alineatul (3);

(o) menține la zi evidențe interne privind încălcările prezentului regulament și măsurile luate în conformitate cu articolul 59 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 59
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 sau cu dreptul procesual intern.

(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 instituția sau organul Uniunii nu respectă una dintre măsurile menționate 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;

(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 49 alineatul (2) litera (c);

(e) de a autoriza clauzele contractuale menționate la articolul 49 alineatul (3) litera (a);

(f) de a autoriza acordurile administrative menționate la articolul 49 alineatul (3) litera (b).

(4) 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.

(5) Autoritatea Europeană pentru Protecția Datelor are competența de a sesiza Curtea de Justiție a Uniunii Europene în condițiile prevăzute de tratat și de a interveni în acțiunile introduse la Curtea de Justiție a Uniunii Europene.

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 de activitate 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 cu autoritățile naționale de supraveghere

Autoritatea Europeană pentru Protecția Datelor cooperează cu autoritățile de supraveghere instituite în temeiul articolului 41 din Regulamentul (UE) 2016/679 și al articolului 51 din Directiva (UE) 2016/680 (denumite în continuare „autorități naționale de supraveghere”) și cu autoritatea comună de control instituită în temeiul articolului 25 din Decizia 2009/917/JAI a Consiliului[21], în măsura în care este necesar pentru îndeplinirea atribuțiilor care revin fiecăreia, în special transmițându-și reciproc informații relevante, solicitând autorităților naționale de supraveghere să își exercite competențele sau ca răspuns la o cerere din partea acestor autorități.

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 cooperează în mod activ cu autoritățile de supraveghere naționale pentru a asigura o supraveghere eficace a sistemelor IT de mari dimensiuni sau a agențiilor Uniunii.

(2) Autoritatea Europeană pentru Protecția Datelor, acționând în cadrul propriilor competențe și responsabilități, face schimb de informații relevante, acordă asistență în efectuarea de audituri și de inspecții, examinează dificultățile de interpretare sau

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

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 de soluții la eventualele probleme și promovează sensibilizarea cu privire la drepturile privind protecția datelor, dacă este necesar, împreună cu autoritățile naționale de supraveghere.

(3) În scopurile enunțate la alineatul (2), Autoritatea Europeană pentru Protecția Datelor se întâlnește cu autoritățile naționale de supraveghere cel puțin de două ori pe an în cadrul Comitetului european pentru protecția datelor. Costurile acestor reuniuni și serviciile aferente sunt suportate de Comitetul european pentru protecția datelor. Regulamentul de procedură se adoptă cu ocazia primei reuniuni. Alte metodele de lucru sunt adoptate de comun acord, 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.

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 persoana vizată 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 plângerea a fost respinsă.

Articolul 64
Dreptul la o cale de atac judiciară eficientă

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

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 operator sau de la persoana împuternicită de operator 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 59 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) în cazul în care au fost luate anterior măsuri dintre cele menționate la articolul 59 împotriva instituției sau a organului Uniunii cu privire la aceeași chestiune, respectarea măsurilor în cauză.

Procedurile care conduc la aplicarea acestor amenzi ar trebui să se desfășoare 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, 28, 29, 30, 31, 32, 33, 37, 38, 39, 40, 44, 45 și 46, săvârșite de către instituția sau organul Uniunii fac, în

conformitate cu alineatul (1), 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 47 - 51.

(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 autoritate posibilitatea de a se exprima în cadrul unei audieri în legătură cu aspectele cu privire la care autoritatea 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 Europene.

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 articolul 63, 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, fără a acționa pe căi oficiale. Nimeni nu poate să sufere prejudicii din cauza unei plângeri depuse la Autoritatea Europeană pentru Protecția Datelor care susține existența unei astfel de încălcări.

Articolul 69
Sancțiuni

Orice neîndeplinire a obligațiilor prevăzute de prezentul regulament, fie aceasta intenționată sau din neglijență, atrage după sine sancțiuni disciplinare sau alte măsuri asupra funcționarului sau agentului Uniunii Europene, conform normelor și procedurilor prevăzute de Statutul funcționarilor Uniunii Europene sau de Regimul aplicabil celorlalți agenți.

CAPITOLUL IX

ACTE DE PUNERE ÎN APLICARE

Articolul 70
Procedura comitetului

(1) Comisia este asistată de comitetul înființat prin articolul 93 din Regulamentul (UE) 2016/679. Acesta este un comitet în sensul 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 X

DISPOZIȚII FINALE

Articolul 71
Abrogarea Regulamentului (CE) nr. 45/2001 și a Deciziei 1247/2002/CE

Regulamentul (CE) nr. 45/2001[22] și Decizia 1247/2002/CE[23] se abrogă cu efect de la 25 mai 2018. Trimiterile la regulamentul și la decizia abrogată se interpretează ca trimiteri la

[22] 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).

[23] Decizia nr. 1247/2002/CE 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.

prezentul regulament. Trimiterile la regulamentul și decizia abrogate se interpretează ca trimiteri la prezentul regulament.

Articolul 72
Măsuri tranzitorii

(1) Decizia 2014/886/UE a Parlamentului European și a Consiliului[24] și actualul mandat al Autorității Europene pentru Protecția Datelor și al adjunctului acesteia nu sunt afectate de prezentul regulament.

(2) Adjunctul autorității este asimilat grefierului Curții de Justiție a Uniunii Europene 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 54 alineatele (4), (5) și (7), precum și articolele 56 și 57 din prezentul regulament se aplică adjunctului actual al autorității până la sfârșitul mandatului său – la 5 decembrie 2019.

(4) Adjunctul autorității asistă Autoritatea Europeană pentru Protecția Datelor în toate atribuțiile acesteia din urmă și o înlocuiește atunci când este absentă sau nu își poate îndeplini atribuțiile respective, până la sfârșitul mandatului adjunctului autorității – la 5 decembrie 2019.

Articolul 73
Intrare în vigoare și aplicare

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

(2) Prezentul regulament se aplică de la 25 mai 2018.

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

Adoptat la Bruxelles,

Pentru Parlamentul European,	*Pentru Consiliu,*
Președintele	*Președintele*

[24] 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.

FIȘĂ FINANCIARĂ LEGISLATIVĂ

1. CADRUL PROPUNERII/INIȚIATIVEI

1.1. Denumirea propunerii/inițiativei

1.2. Domeniul (domeniile) de politică în cauză în structura ABM/ABB

1.3. Tipul propunerii/inițiativei

1.4. Obiectiv(e)

1.5. Motivele propunerii/inițiativei

1.6. Durata și impactul financiar

1.7. Modul (modurile) de gestiune preconizat(e)

2. MĂSURI DE GESTIONARE

2.1. Dispoziții în materie de monitorizare și de raportare

2.2. Sistemul de gestiune și de control

2.3. Măsuri de prevenire a fraudelor și a neregulilor

3. IMPACTUL FINANCIAR ESTIMAT AL PROPUNERII/INIȚIATIVEI

3.1. Rubrica (rubricile) din cadrul financiar multianual și linia (liniile) bugetară (bugetare) de cheltuieli afectată (afectate)

3.2. Impactul estimat asupra cheltuielilor

3.2.1. Sinteza impactului estimat asupra cheltuielilor

3.2.2. Impactul estimat asupra creditelor operaționale

3.2.3. Impactul estimat asupra creditelor cu caracter administrativ

3.2.4. Compatibilitatea cu actualul cadru financiar multianual

3.2.5. Contribuția terților

3.3. Impactul estimat asupra veniturilor

FIȘĂ FINANCIARĂ LEGISLATIVĂ

1. CADRUL PROPUNERII/INIȚIATIVEI

1.1. Denumirea propunerii/inițiativei

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

1.2. Domeniul (domeniile) de politică în cauză în structura ABM/ABB[25]

Justiție – protecția datelor cu caracter personal

1.3. Tipul propunerii/inițiativei

☐ Propunerea/inițiativa se referă la **o acțiune nouă**

☐ Propunerea/inițiativa se referă la **o acțiune nouă ca urmare a unui proiect-pilot/a unei acțiuni pregătitoare**[26]

– Propunerea/inițiativa se referă la **prelungirea unei acțiuni existente**

☐ Propunerea/inițiativa se referă la **o acțiune reorientată către o acțiune nouă**

1.4. Obiectiv(e)

1.4.1. Obiectiv(e) strategic(e) multianual(e) al(e) Comisiei vizat(e) de propunere/inițiativă

Intrarea în vigoare a Tratatului de la Lisabona - și în special introducerea unui nou temei juridic (articolul 16 din TFUE) - oferă oportunitatea stabilirii unui cadru cuprinzător pentru protecția datelor, care să acopere toate domeniile.

În data de 27 aprilie 2016, Uniunea a adoptat 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) (Text cu relevanță pentru SEE), JO L 119, 4.5.2016, p. 1- 88.

În aceeași zi, Uniunea a adoptat Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la

[25] ABM: gestionarea pe activități; ABB: întocmirea bugetului pe activități.

[26] Astfel cum sunt menționate la articolul 54 alineatul (2) litera (a) sau (b) din Regulamentul financiar.

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 -131.

Prezenta propunere vizează finalizarea procesului de stabilire a unui cadru cuprinzător pentru protecția datelor în Uniune, prin alinierea normelor de protecție a datelor aplicabile instituțiilor și organelor Uniunii la normele de protecție a datelor din Regulamentul (UE) 2016/679. Din motive de consecvență și coerență, instituțiile și organele Uniunii ar trebui să aplice un set de norme privind protecția datelor similar cu cel al sectorului public din statele membre.

1.4.2. Obiectiv(e) specific(e) și activitatea (activitățile) ABM/ABB în cauză

Obiectivul specific nr. 1:

asigurarea unei aplicări consecvente a normelor privind protecția datelor în întreaga Uniune.

Obiectivul specific nr. 2:

raționalizarea modelului actual de guvernanță în ceea ce privește protecția datelor în instituțiile și organele Uniunii.

Obiectivul specific nr. 3:

asigurarea unei mai stricte respectări și aplicări a normelor de protecție a datelor în cadrul instituțiilor și organelor Uniunii.

1.4.3. Rezultatul (rezultatele) și impactul preconizate

A se preciza efectele pe care propunerea/inițiativa ar trebui să le aibă asupra beneficiarilor vizați/ grupurilor vizate.

În ceea ce privește instituțiile și organele Uniunii în calitatea lor de operatori de date, acestea ar trebui să beneficieze de trecerea de la procesele administrative actuale (abordarea *ex ante*) legate de protecția datelor la respectarea efectivă și un control mai strict al respectării normelor de fond privind protecția datelor și a noilor principii și concepte de protecție a datelor introduse de Regulamentul (UE) 2016/679 (abordarea *ex post*), care vor fi aplicabile în întreaga Uniune. Persoanele ale căror date sunt prelucrate de instituțiile și organele Uniunii vor beneficia de un control mai bun al datelor lor cu caracter personal și vor avea încredere în mediul digital. De asemenea, vor constata o creștere a responsabilității instituțiilor și organelor Uniunii. Autoritatea Europeană pentru Protecția Datelor va putea să se concentreze mai mult asupra rolului său de supraveghere. Distribuirea sarcinii de a oferi consiliere Comisiei între Comitetul european pentru protecția datelor instituit prin Regulamentul (UE) 2016/679 și Autoritatea Europeană pentru Protecția Datelor va fi clarificată, iar suprapunerile vor fi evitate.

1.4.4. Indicatori de rezultat și de impact

A se preciza indicatorii care permit monitorizarea punerii în aplicare a propunerii/inițiativei.

Indicatorii includ următoarele elemente: numărul avizelor emise de Comitetul european pentru protecția datelor și de Autoritatea Europeană pentru Protecția Datelor; defalcarea activităților responsabililor cu protecția datelor; utilizarea de evaluări ale impactului asupra protecției datelor; numărul de plângeri depuse de persoane vizate; amenzile aplicate operatorilor de date care au încălcat protecția datelor.

1.5. Motivele propunerii/inițiativei

1.5.1. Cerință (cerințe) de îndeplinit pe termen scurt sau lung

În Regulamentul (UE) 2016/679 [articolul 2 alineatul (3), articolul 98 și considerentul (17)], colegiuitorii Uniunii au cerut adaptarea Regulamentului (CE) nr. 45/2001 la principiile și normele stabilite prin Regulamentul (UE) 2016/679, cu scopul de a oferi un cadru solid și coerent în materie de protecție a datelor în Uniune și de a permite aplicarea ambelor instrumente în același timp, și anume la 25 mai 2018.

1.5.2. Valoarea adăugată a implicării UE

Normele de protecție a datelor aplicabile instituțiilor și organelor Uniunii pot fi instituite doar prin intermediul unui act al UE.

1.5.3. Învățăminte desprinse din experiențe anterioare similare

Prezenta propunere se bazează pe experiența dobândită datorită Regulamentului (CE) nr. 45/2001 și pe evaluarea aplicării acestuia, efectuată în cadrul unui studiu de evaluare (realizat de un contractant extern între septembrie 2014 și iunie 2015)[27].

1.5.4. Compatibilitatea și posibila sinergie cu alte instrumente corespunzătoare:

Prezenta propunere se bazează pe Regulamentul (UE) 2016/679 și finalizează construirea unui cadru solid, coerent și modern de protecție a datelor în Uniune, neutru din punct de vedere tehnologic și capabil să facă față viitorului.

[27] JUST/2013/FRAC/FW/0157/A4 în contextul contractului-cadru multiplu JUST/2011/EVAL/01 (RS 2013/05) - Studiu de evaluare privind Regulamentul (CE) nr. 45/2001, de *Ernst and Young*

1.6. Durata și impactul financiar

☐ Propunere/inițiativă pe **durată determinată**

– ☐ Propunere/inițiativă în vigoare de la [ZZ/LL]AAAA până la [ZZ/LL]AAAA

– ☐ Impact financiar din AAAA până în AAAA

- Propunere/inițiativă pe **durată nedeterminată**
- Punere în aplicare cu o perioadă de creștere în intensitate din [2017] până la 25 mai 2018, urmată de funcționare în regim de croazieră.

1.7. Modul (modurile) de gestiune preconizat(e)[28]

- Gestiune directă asigurată de către Comisie

– ☐prin intermediul serviciilor sale, inclusiv al personalului din delegațiile Uniunii;

– ☐ prin intermediul agențiilor executive;

☐ **Gestiune partajată** cu statele membre

☐ **Gestiune indirectă**, cu delegarea sarcinilor de execuție bugetară:

– ☐țărilor terțe sau organismelor pe care le-au desemnat acestea;

– ☐organizațiilor internaționale și agențiilor acestora (a se preciza);

– ☐BEI și Fondului european de investiții;

– ☐ organismelor menționate la articolele 208 și 209 din Regulamentul financiar;

– ☐ organismelor de drept public;

– ☐ organismelor de drept privat cu misiune de serviciu public, cu condiția să prezinte garanții financiare adecvate;

– ☐ organismelor de drept privat dintr-un stat membru care sunt responsabile cu punerea în aplicare a unui parteneriat public-privat și care prezintă garanții financiare adecvate;

– ☐ persoanelor cărora li se încredințează executarea unor acțiuni specifice în cadrul PESC, în temeiul titlului V din TUE, identificate în actul de bază relevant.

– *Dacă se indică mai multe moduri de gestiune, a se furniza detalii suplimentare în secțiunea „Observații".*

Observații

[28] Explicațiile privind modurile de gestiune, precum și trimiterile la Regulamentul financiar sunt disponibile pe site-ul BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

Prezenta propunere se limitează la instituțiile și organele Uniunii și are efecte asupra tuturor acestora.

2. MĂSURI DE GESTIONARE

2.1. Dispoziții în materie de monitorizare și de raportare

A se preciza frecvența și condițiile aferente acestor dispoziții.

Prezenta propunere se limitează la aplicarea normelor de protecție a datelor de către instituțiile și organele Uniunii. Supravegherea și asigurarea respectării acestor norme este o sarcină efectuată de Autoritatea Europeană pentru Protecția Datelor. Activitățile de monitorizare și raportare sunt, prin urmare, asigurate de Autoritatea Europeană pentru Protecția Datelor. În temeiul articolului 60 din prezenta propunere, Autoritatea Europeană pentru Protecția Datelor are în special obligația de a prezenta Parlamentului European, Consiliului și Comisiei un raport anual privind activitățile din sfera sa de competență și de a-l publica în același timp.

2.2. Sistemul de gestiune și de control

2.2.1. Riscul (riscurile) identificat(e)

Un studiu de evaluare a punerii în aplicare a dispozițiilor din Regulamentul (CE) nr. 45/2001 a fost efectuat de un contractant extern între septembrie 2014 și iunie 2015. Acesta analizează, de asemenea, impactul introducerii principalelor concepte și principii ale Regulamentului (UE) 2016/679 în instituțiile și organele Uniunii. Noul model de protecție a datelor se va concentra pe respectarea efectivă a normelor privind protecția datelor și pe supravegherea și aplicarea efectivă a acestor norme. Aceasta va necesita o schimbare a culturii protecției datelor în instituțiile și organele Uniunii, trecându-se de la abordarea administrativă *ex ante* la abordarea *ex post* eficace.

2.2.2. Informații privind sistemul de control intern instituit.

Metodele de control existente aplicate de către instituțiile și organele Uniunii.

2.2.3. Estimarea costurilor și a beneficiilor controalelor și evaluarea nivelului prevăzut de risc de eroare.

Metodele de control existente aplicate de către instituțiile și organele Uniunii.

2.3. Măsuri de prevenire a fraudelor și a neregulilor

A se preciza măsurile de prevenire și de protecție existente sau preconizate.

Metodele existente de prevenire a fraudelor aplicate de către instituțiile și organele Uniunii.

3. IMPACTUL FINANCIAR ESTIMAT AL PROPUNERII/INIȚIATIVEI

3.1. Rubrica (rubricile) din cadrul financiar multianual și linia (liniile) bugetară (bugetare) de cheltuieli afectată (afectate)

- Linii bugetare existente

În ordinea rubricilor din cadrul financiar multianual și a liniilor bugetare.

Rubrica din cadrul financiar multianual	Linia bugetară	Tip de cheltuieli	Contribuție			
	Număr [Rubrica……...……]	Dif./ Nedif.[29].	Țări AELS[30]	Țări candidate[31]	Țări terțe	În sensul articolului 21 alineatul (2) litera (b) din Regulamentul financiar
	[XX.YY.YY.YY]	Dif./ Nedif.	DA/NU	DA/NU	DA/NU	DA/NU

- Noile linii bugetare solicitate

În ordinea rubricilor din cadrul financiar multianual şi a liniilor bugetare.

Rubrica din cadrul financiar multianual	Linia bugetară	Tip de cheltuieli	Contribuție			
	Număr [Rubrica……]	Dif./ Nedif.	Țări AELS	Țări candidate	Țări terțe	În sensul articolului 21 alineatul (2) litera (b) din Regulamentul financiar
	[XX.YY.YY.YY]		DA/NU	DA/NU	DA/NU	DA/NU

[29] Dif.= credite diferențiate / Nedif. = credite nediferențiate.
[30] AELS: Asociația Europeană a Liberului Schimb.
[31] Țările candidate și, după caz, țările potențial candidate din Balcanii de Vest.

3.2. Impactul estimat asupra cheltuielilor

Impactul prezentei propuneri asupra cheltuielilor este limitat la cheltuielile efectuate de instituțiile și organele Uniunii. Cu toate acestea, evaluarea costurilor legate de prezenta propunere demonstrează că aceasta nu creează cheltuieli suplimentare considerabile pentru instituțiile și organele Uniunii.

În ceea ce privește operatorii de date din instituțiile și organele Uniunii, studiul de evaluare a Regulamentului (CE) nr. 45/2001 arată că activitățile lor în materie de protecție a datelor corespund unui număr de aproximativ 70 de unități echivalente cu o normă întreagă (ENI), adică aproximativ 9,3 milioane EUR pe an. Aproximativ 20 % din activitățile lor în materie de protecție a datelor sunt destinate în prezent notificărilor privind prelucrarea datelor. Această activitate este eliminată în prezentul regulament, ceea ce corespunde unor economii anuale în valoare de 1,922 de milioane EUR pentru operatorii de date din instituțiile și organele Uniunii. Se preconizează că aceste economii vor fi compensate prin implicarea tot mai mare a operatorilor de date în punerea în aplicare a noilor principii și concepte introduse prin prezentul regulament.

Mai exact, sondajul realizat în cadrul studiului de evaluare a arătat că:

a) introducerea principiului reducerii la minimum a datelor ar avea un impact minim sau inexistent asupra instituțiilor și organelor Uniunii;

b) introducerea principiului transparenței nu ar avea un impact semnificativ asupra instituțiilor și organelor Uniunii;

c) sporirea obligațiilor de informare ar duce la creșterea volumului de lucru al operatorilor de date și al responsabililor cu protecția datelor;

d) dreptul de a fi uitat nu ar avea un impact semnificativ asupra instituțiilor și organelor Uniunii;

e) dreptul la portabilitatea datelor ar avea un impact minim sau inexistent asupra instituțiilor și organelor Uniunii;

f) evaluările impactului asupra protecției datelor ar avea un efect relativ important asupra volumului de lucru al operatorilor de date și al responsabililor cu protecția datelor, deoarece unele dintre instituțiile și organele Uniunii efectuează deja evaluări ale impactului asupra protecției datelor, iar situațiile în care astfel de evaluări ale impactului asupra protecției datelor vor trebui realizate sunt limitate;

g) notificările încălcării securității datelor cu caracter personal ar duce la creșterea volumului de lucru al operatorilor de date, dar astfel de încălcări nu sunt frecvente;

h) protecția datelor începând cu momentul conceperii și protecția implicită a datelor sunt deja utilizate în mai multe instituții și organe ale Uniunii.

În plus, studiul de evaluare a impactului efectuat înaintea adoptării propunerii de pachet de reforme privind protecția datelor a concluzionat că „nicio sarcină administrativă nu ar urma să fie suportată de autoritățile publice sau de operatorii de date prin introducerea principiului de protecție a datelor începând cu momentul conceperii”[32].

În ceea ce privește responsabilii cu protecția datelor, studiul de evaluare a estimat la 82,9 ENI sau 10,9 de milioane EUR anual costurile rețelei actuale a responsabililor cu protecția datelor și a coordonatorilor pentru protecția datelor din instituțiile și organele Uniunii. Aceștia își petrec 26 % din timpul lor de lucru dedicat protecției datelor cu activități desființate prin prezentul regulament, respectiv redactarea notificărilor (în locul operatorilor de date), evaluarea notificărilor primite și ținerea unei evidențe a înregistrărilor, precum și efectuarea de verificări prealabile. Acest lucru duce la economii suplimentare de 2,834 de milioane EUR anual pentru instituțiile și organele Uniunii. În plus, prezentul regulament prevede o marjă pentru eventuale economii suplimentare, permițând instituțiilor și organelor Uniunii să externalizeze activitățile specifice responsabililor cu protecția datelor, în loc să recurgă la personalul propriu.

Economiile realizate în ceea ce privește activitățile specifice responsabililor cu protecția datelor vor fi compensate prin implicarea lor în activități legate de creșterea obligațiilor de informare, de evaluările impactului asupra protecției datelor (în cazuri limitate, atunci când acestea vor fi necesare) și de consultarea prealabilă a Autorității Europene pentru Protecția Datelor (a cărei sferă de competențe va fi cu mult mai limitată decât în cazul actualei obligații de verificare prealabilă).

În ceea ce privește Autoritatea Europeană pentru Protecția Datelor, bugetul său anual este relativ stabil începând din 2011, fiind în jurul sumei de 8 milioane EUR. În prezent, unitatea sa de supraveghere și de asigurare a punerii în aplicare și unitatea sa de politici și consultanță au efective de personal similare, fiind stabile din 2008. Atenția sporită acordată de prezentul regulament rolului de supraveghere al Autorității Europene pentru Protecția Datelor va fi compensată de rolul consultativ mai bine orientat și de eliminarea suprapunerii sarcinilor cu cele ale Comitetului european pentru protecția datelor. O realocare a personalului Autorității Europene pentru Protecția Datelor poate fi, prin urmare, realizată pe plan intern.

[32] Document de lucru al serviciilor Comisiei, Evaluarea impactului, SEC (2012) 72 final, pagina 110.

Prezenta propunere prevede posibilitatea ca Autoritatea Europeană pentru Protecția Datelor să aplice amenzi administrative instituțiilor și organelor Uniunii. Fiecare instituție sau organ al Uniunii ar putea fi amendat cu până la cel mult 250 000 EUR pe an (25 000 EUR pentru fiecare încălcare) sau cu 500 000 EUR pe an (50 000 EUR pentru fiecare încălcare) pentru cele mai grave încălcări ale prezentului regulament. Se preconizează că aceste amenzi se vor aplica numai în cazurile cele mai grave, și ca urmare a unei nerespectări de către instituția sau organul Uniunii prin exercitarea altor competențe corective de către Autoritatea Europeană pentru Protecția Datelor. Prin urmare, se preconizează că impactul financiar al acestor amenzi este limitat.

3.2.1. Sinteza impactului estimat asupra cheltuielilor

milioane EUR (cu trei zecimale)

Rubrica din cadrul financiar multianual	Număr	[Rubrica……...…….]

DG: <…….>			Anul **N**[33]	Anul **N+1**	Anul **N+2**	Anul **N+3**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (cf. punctul 1.6)			**TOTAL**
• Credite operaționale										
Numărul liniei bugetare	Angajamente	(1)								
	Plăți	(2)								
Numărul liniei bugetare	Angajamente	(1a)								
	Plăți	(2a)								
Credite cu caracter administrativ finanțate din bugetul anumitor programe[34]										
Numărul liniei bugetare		(3)								

[33] Anul N este anul în care începe punerea în aplicare a propunerii/inițiativei.

[34] Asistență tehnică și/sau administrativă și cheltuieli de sprijin pentru punerea în aplicare a programelor și/sau a acțiunilor UE (fostele linii „BA”), cercetare indirectă și cercetare directă.

TOTAL credite pentru DG<…….>	Angajamente	=1+1a +3								
	Plăți	=2+2a +3.								

•TOTAL credite operaționale	Angajamente	(4)								
	Plăți	(5)								
•TOTAL credite cu caracter administrativ finanțate din bugetul anumitor programe		(6)								
TOTAL credite în cadrul RUBRICII <….> din cadrul financiar multianual	Angajamente	=4+ 6								
	Plăți	=5+ 6								

<u>În cazul în care propunerea/inițiativa afectează mai multe rubrici:</u>

•TOTAL credite operaționale	Angajamente	(4)								
	Plăți	(5)								
•TOTAL credite cu caracter administrativ finanțate din bugetul anumitor programe		(6)								
TOTAL credite în cadrul RUBRICILOR 1 - 4 din cadrul financiar multianual (Suma de referință)	Angajamente	=4+ 6								
	Plăți	=5+ 6								

Rubrica din cadrul financiar multianual	**5.**	„Cheltuieli administrative”

milioane EUR (cu trei zecimale)

		Anul **N**	Anul **N+1**	Anul **N+2**	Anul **N+3**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (cf. punctul 1.6)			**TOTAL**
DG: <…….>									
•Resurse umane									
•Alte cheltuieli administrative									
TOTAL DG <…….>	Credite								

TOTAL credite în cadrul RUBRICII 5 din cadrul financiar multianual	(Total angajamente = Total plăți)								

milioane EUR (cu trei zecimale)

		Anul **N**[35]	Anul **N+1**	Anul **N+2**	Anul **N+3**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (cf. punctul 1.6)			**TOTAL**
TOTAL credite în cadrul RUBRICILOR 1 - 5 din cadrul financiar multianual	Angajamente								
	Plăți								

[35] Anul N este anul în care începe punerea în aplicare a propunerii/inițiativei.

3.2.2. Impactul estimat asupra creditelor operaționale

- Propunerea/inițiativa nu implică utilizarea de credite operaționale

☐Propunerea/inițiativa implică utilizarea de credite operaționale, conform explicațiilor de mai jos:

Credite de angajament în milioane EUR (cu trei zecimale)

Indicați obiectivele și realizările			Anul **N**		Anul **N+1**		Anul **N+2**		Anul **N+3**		A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (cf. punctul 1.6)						**TOTAL**	
	REALIZĂRI																	
⇩	Tip[36]	Costuri medii	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nu	Costuri	Nr. total	Costuri totale
OBIECTIVUL SPECIFIC NR. 1[37]…																		
- Realizare																		
- Realizare																		
- Realizare																		
Subtotal pentru obiectivul specific nr. 1																		
OBIECTIVUL SPECIFIC NR. 2…																		
- Realizare																		
Subtotal pentru obiectivul specific nr. 2																		

[36] Realizările se referă la produsele și serviciile care vor fi furnizate (de ex.: numărul de schimburi de studenți finanțate, numărul de km de străzi construiți etc.).

[37] Conform descrierii de la punctul 1.4.2. „Obiectiv(e) specific(e)…”

COSTURI TOTALE																

3.2.3. Impactul estimat asupra creditelor cu caracter administrativ

3.2.3.1. Sinteză

- Propunerea/inițiativa nu implică utilizarea de credite cu caracter administrativ

☐ Propunerea/inițiativa implică utilizarea de credite cu caracter administrativ, conform explicațiilor de mai jos:

milioane EUR (cu trei zecimale)

	Anul **N** [38]	Anul **N+1**	Anul **N+2**	Anul **N+3**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (cf. punctul 1.6)			**TOTAL**
RUBRICA 5din cadrul financiar multianual								
Resursele umane								
Alte cheltuieli administrative								
Subtotal RUBRICA 5 din cadrul financiar multianual								
în afara RUBRICII 5[39] **din cadrul financiar multianual**								
Resursele umane								
Alte cheltuieli cu caracter administrativ								
Subtotal în afara RUBRICII 5din cadrul financiar multianual								
TOTAL								

Necesarul de credite pentru resurse umane și alte cheltuieli cu caracter administrativ vor fi acoperite de creditele DG-ului care sunt deja alocate pentru gestionarea acțiunii și/sau realocate intern în cadrul DG-ului, completate, după caz, cu resurse suplimentare ce ar putea fi alocate DG-ului care gestionează acțiunea în cadrul procedurii de alocare anuală și în lumina constrângerilor bugetare.

[38] Anul N este anul în care începe punerea în aplicare a propunerii/inițiativei.

[39] Asistență tehnică și/sau administrativă și cheltuieli de sprijin pentru punerea în aplicare a programelor și/sau a acțiunilor UE (fostele linii „BA”), cercetare indirectă și cercetare directă.

3.2.3.2. Necesarul de resurse umane estimat

- Propunerea/inițiativa nu implică utilizarea de resurse umane.

☐ Propunerea/inițiativa implică utilizarea de resurse umane, conform explicațiilor de mai jos:

Estimarea trebuie exprimată în echivalent normă întreagă

	Anul **N**	Anul **N+1**	Anul **N+2**	Anul **N+3**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (cf. punctul 1.6)		
•Posturi din schema de personal (funcționari și agenți temporari)							
XX 01 01 01 (la sediu și în birourile de reprezentare ale Comisiei)							
XX 01 01 02 (în delegații)							
XX 01 05 01 (cercetare indirectă)							
10 01 05 01 (cercetare directă)							
•Personal extern (în echivalent normă întreagă: ENI)[40]							
XX 01 02 01 (AC, END, INT din „pachetul global")							
XX 01 02 02 (AC, AL, END, INT și JED în delegații)							
XX 01 04 **yy** [41] - la sediu							
XX 01 04 **yy** [41] - în delegații							
XX 01 05 02 (AC, END, INT - cercetare indirectă)							
10 01 05 02 (AC, END, INT - cercetare directă)							
Alte linii bugetare (a se preciza)							
TOTAL							

XX este domeniul de politică sau titlul din buget în cauză.

Necesarul de resurse umane va fi asigurat din efectivele de personal ale DG-ului în cauză alocate deja pentru gestionarea acțiunii și/sau realocate intern în cadrul DG-ului, completate, după caz, cu resurse suplimentare ce ar putea fi alocate DG-ului care gestionează acțiunea în cadrul procedurii de alocare anuală și în lumina constrângerilor bugetare.

Descrierea sarcinilor care trebuie efectuate:

Funcționari și personal temporar	

40 AC = agent contractual; AL = agent local; END= expert național detașat. INT = personal pus la dispoziție de agenții de muncă temporară; JED = expert tânăr în delegații.

41 Subplafonul pentru personal extern acoperit din creditele operaționale (fostele linii „BA").

Personal extern	

3.2.4. Compatibilitatea cu actualul cadru financiar multianual

- Propunerea/inițiativa este compatibilă cu cadrul financiar multianual existent.

☐ Propunerea/inițiativa necesită o reprogramare a rubricii corespunzătoare din cadrul financiar multianual.

A se explica reprogramarea necesară, precizându-se liniile bugetare în cauză și sumele aferente.

☐ Propunerea/inițiativa necesită recurgerea la instrumentul de flexibilitate sau la revizuirea cadrului financiar multianual.

A se explica necesitatea efectuării acestei acțiuni, precizând rubricile și liniile bugetare în cauză, precum și sumele aferente.

3.2.5. Contribuția terților

- Propunerea/inițiativa nu prevede cofinanțare din partea terților.

Propunerea/inițiativa prevede cofinanțare, estimată în cele ce urmează:

Credite de angajament în milioane EUR (cu 3 zecimale)

	Anul **N**	Anul **N+1**	Anul **N+2**	Anul **N+3**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (cf. punctul 1.6)			Total
A se preciza organismul care asigură cofinanțarea								
TOTAL credite cofinanțate								

3.3. Impactul estimat asupra veniturilor

- Propunerea/inițiativa nu are impact financiar asupra veniturilor.

☐ Propunerea/inițiativa are următorul impact financiar:

– ☐ asupra resurselor proprii

– ☐ asupra diverselor venituri

milioane EUR (cu trei zecimale)

Linia bugetară pentru venituri:	Credite disponibile pentru exercițiul financiar în curs	Impactul propunerii/inițiativei[42]						
		Anul **N**	Anul **N+1**	Anul **N+2**	Anul **N+3**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (cf. punctul 1.6)		
Articolul …..								

Pentru diversele venituri alocate, a se preciza linia bugetară (liniile bugetare) de cheltuieli afectată (afectate).

A se preciza metoda de calcul a impactului asupra veniturilor.

[42] În ceea ce privește resursele proprii tradiționale (taxe vamale, cotizații pentru zahăr), sumele indicate trebuie să fie sume nete, şi anume sume brute după deducerea unei cote de 25 % pentru costuri de colectare.