COMISIA EUROPEANĂ

Bruxelles, 25.1.2012
COM(2012) 10 final

2012/0010 (COD)

Propunere de

DIRECTIVĂ A PARLAMENTULUI EUROPEAN ŞI A CONSILIULUI

privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și la libera circulație a acestor date

[…]

EXPUNERE DE MOTIVE

1. CONTEXTUL PROPUNERII

Prezenta expunere de motive descrie în detaliu abordarea privind noul cadru juridic referitor la protecția datelor cu caracter personal în UE, prevăzut în Comunicarea COM (2012) 9 final. Cadrul legislativ constă în două propuneri legislative:

– o propunere de regulament al Parlamentului European și al Consiliului privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal și libera circulație a acestor date (Regulament general privind protecția datelor) și

– o propunere de directivă a Parlamentului European și a Consiliului privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și libera circulație a acestor date.

Prezenta expunere de motive se referă la cea din urmă propunere legislativă.

Documentul care stă la baza legislației UE existente privind protecția datelor cu caracter personal, Directiva 95/46/CE[1], a fost adoptat în 1995, având două obiective: protejarea dreptului fundamental la protecția datelor și garantarea liberei circulații a datelor cu caracter personal între statele membre. Directiva a fost completată de o serie de instrumente care prevăd norme specifice privind protecția datelor în domeniul cooperării polițienești și judiciare în materie penală[2] (fostul al treilea pilon), inclusiv Decizia-cadru 2008/977/JAI[3].

Consiliul European a invitat Comisia să evalueze funcționarea instrumentelor UE privind protecția datelor și să prezinte, dacă este cazul, alte inițiative legislative și fără caracter legislativ[4]. În rezoluția sa privind Programul de la Stockholm, Parlamentul European[5] a salutat inițiativa unui regim cuprinzător de protecție a datelor în UE și, printre altele, a solicitat revizuirea deciziei-cadru. Comisia a subliniat în planul său de acțiune pentru punerea în aplicare a programului de la Stockholm[6], necesitatea de a se asigura că dreptul fundamental la protecția datelor cu caracter personal este aplicat în mod coerent în contextul tuturor politicilor UE. Planul de acțiune a subliniat că „*într-o societate globală caracterizată de schimbări tehnologice rapide, în care schimbul de informații nu cunoaște limite, este deosebit de important ca viața privată să fie protejată. Uniunea trebuie să se asigure că dreptul fundamental la protecția datelor este aplicat în mod coerent. Trebuie să consolidăm poziția UE cu privire la protecția datelor cu caracter personal ale persoanelor în contextul tuturor*

---

1 Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, JO L 281/95, p. 31.

2 A se vedea lista completă în anexa 3 la evaluarea impactului [SEC (2012) 72].

3 Decizia-cadru 2008/977/JAI a Consiliului din 27 noiembrie 2008 privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală, JO L 350, 30.12.2008, p. 60.

4 În conformitate cu Programul de la Stockholm, JO C 115, 4.5.2010, p. 1.

5 A se vedea rezoluția Parlamentului European privind Programul de la Stockholm, adoptată la 25 noiembrie 2009.

6 COM (2010) 171 final.

politicilor UE, inclusiv în contextul aplicării legii și al prevenirii criminalității, precum și în relațiile noastre internaționale."

În comunicarea sa privind „O abordare globală a protecției datelor cu caracter personal în Uniunea Europeană"[7], Comisia a concluzionat că UE are nevoie de o politică mai cuprinzătoare și mai coerentă privind dreptul fundamental la protecția datelor cu caracter personal.

Decizia-cadru 2008/977/JAI are un domeniu de aplicare limitat, deoarece se aplică doar în cazul prelucrării datelor la nivel transfrontalier și nu în cazul activităților de prelucrare realizate de către poliție și autoritățile judiciare exclusiv la nivel național. Acest fapt poate crea dificultăți pentru poliție și alte autorități competente în domeniul cooperării judiciare în materie penală și al cooperării polițienești. Acestea nu reușesc întotdeauna să facă distincție cu ușurință între prelucrarea exclusiv la nivel național și cea la nivel transfrontalier sau să prevadă dacă anumite date personale pot face obiectul unui schimb transfrontalier într-o etapă ulterioară (a se vedea punctul 2 de mai jos). În plus, ca urmare a naturii și conținutului său, decizia-cadru lasă legislațiilor naționale ale statelor membre o amplă marjă de manevră privind punerea în aplicare a dispozițiile sale. De asemenea, decizia-cadru nu include niciun mecanism sau grup consultativ similar Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal care să sprijine interpretarea comună a dispozițiilor sale, și nici nu prevede competențe de executare pentru Comisie în vederea asigurării unei abordări comune în punerea sa în aplicare.

Articolul 16 alineatul (1) din Tratatul privind funcționarea Uniunii Europene (TFUE) stabilește principiul conform căruia orice persoană are dreptul la protecția datelor cu caracter personal. Mai mult, prin articolul 16 alineatul (2) din TFUE, Tratatul de la Lisabona introduce un temei juridic specific pentru adoptarea de norme în materie de protecție a datelor cu caracter personal care se aplică, de asemenea, cooperării judiciare în materie penală și cooperării polițienești. Articolul 8 din Carta drepturilor fundamentale a Uniunii Europene consacră protecția datelor cu caracter personal ca drept fundamental. Articolul 16 din TFUE impune legiuitorului să prevadă norme privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal și în domeniul cooperării judiciare în materie penală și al cooperării polițienești, care să acopere atât prelucrarea datelor cu caracter personal la nivel transfrontalier, cât și cea la nivel național. Acest lucru va permite protejarea drepturilor și a libertăților fundamentale ale persoanelor fizice și, în special, al dreptului acestora la protecția datelor cu caracter personal, asigurând, în același timp, schimbul de date cu caracter personal în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și contribuind la facilitarea cooperării în lupta împotriva criminalității în Europa.

Ca urmare a naturii specifice a domeniului cooperării polițienești și judiciare în materie penală, Declarația 21[8] precizează că ar putea fi necesară elaborarea unor norme specifice privind protecția datelor cu caracter personal și libera circulație a acestor date în domeniul cooperării judiciare în materie penală și al cooperării polițienești în temeiul articolului 16 din TFUE.

---

7 Comisia Europeană, Comunicarea privind „O abordare globală a protecției datelor cu caracter personal în Uniunea Europeană", COM (2010) 609 final, 4 noiembrie 2010.

8 Declarația 21 privind 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, 13.12.2007).

2. REZULTATELE CONSULTĂRILOR CU PĂRȚILE INTERESATE ȘI ALE EVALUĂRII IMPACTULUI

Prezenta inițiativă este rezultatul unor ample consultări cu principalele părți interesate referitoare la o revizuire a cadrului juridic existent privind protecția datelor cu caracter personal, care a inclus două faze ale consultării publice:

– în perioada 9 iulie - 31 decembrie 2009, *consultarea referitoare la cadrul juridic privind dreptul fundamental la protecția datelor cu caracter personal.* Comisia a primit 168 de răspunsuri, din care 127 de la persoane fizice, organizații și asociații profesionale și 12 de la autoritățile publice. Contribuțiile care nu au caracter confidențial pot fi consultate pe site-ul internet al Comisiei[9];

– în perioada 4 noiembrie 2010 - 15 ianuarie 2011, *consultarea privind abordarea cuprinzătoare a Comisiei cu privire la protecția datelor cu caracter personal în Uniunea Europeană*. Comisia a primit 305 de răspunsuri, din care 54 de la cetățeni, 31 de la autoritățile publice și 220 de la organizațiile private, în special asociații de afaceri și organizații neguvernamentale. Contribuțiile care nu au caracter confidențial pot fi consultate pe site-ul internet al Comisiei[10].

Întrucât aceste consultări s-au axat, în mare parte, pe revizuirea Directivei 95/46/CE, au avut loc consultări specifice cu părțile interesate din domeniul aplicării legii; în special, la 29 iunie 2010, a fost organizat un atelier cu autoritățile statelor membre privind aplicarea normelor în materie de protecție a datelor, inclusiv în domeniul cooperării polițienești și judiciare în materie penală. Mai mult, la 2 februarie 2011, Comisia a organizat un atelier cu autoritățile statelor membre pentru a discuta punerea în aplicare a Deciziei-cadru 2008/977/JAI și, în sens mai general, aspecte legate de protecția datelor în domeniul cooperării polițienești și judiciare în materie penală.

Cetățenii UE au fost consultați prin intermediul unui sondaj Eurobarometru organizat în perioada noiembrie-decembrie 2010[11]. De asemenea, a fost lansată a serie de studii[12]. Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal[13] a furnizat mai multe avize și informații utile Comisiei[14]. De asemenea, Autoritatea

---

9 http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm.

10 http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104_en.htm.

11 Eurobarometrul special (EB) 359 - *Protecția datelor și identitatea electronică în UE* (2011): http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

12 A se vedea *Study on the economic benefits of privacy enhancing technologies* (Studiu privind beneficiile economice ale tehnologiilor de consolidare a protecției vieții private) și *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments* (Studiu comparativ privind diversele abordări ale noilor provocări din domeniul protecției vieții private, în special în lumina noilor dezvoltări tehnologice), ianuarie 2010. (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf)..

13 Grupul de lucru a fost înființat în 1996 (prin articolul 29 din directivă), având un caracter consultativ și fiind format din reprezentanți ai autorităților naționale de supraveghere a protecției datelor (DPA), ai Autorității Europene pentru Protecția Datelor (AEPD) și ai Comisiei. Pentru mai multe informații cu privire la activitățile grupului de lucru, a se vedea http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

14 A se vedea, în special, următoarele avize: cel privind „Viitorul protecției vieții private” [2009, Grupul de lucru (GL) 168]; cel privind conceptele de „operator” și „persoana împuternicită de către operator” (1/2010, GL 169); cel privind publicitatea comportamentală online (2/2010, GL 171); cel privind principiul responsabilității (3/2010, GL 173); cel privind dreptul aplicabil (8/2010, GL 179) și cel

Europeană pentru Protecția Datelor a emis un aviz cuprinzător privind problemele ridicate în comunicarea Comisiei din noiembrie 2010[15].

Parlamentul European a aprobat, prin rezoluția sa din 6 iulie 2011, un raport care susținea abordarea Comisiei în legătură cu reforma cadrului privind protecția datelor[16]. La 24 februarie 2011, Consiliul Uniunii Europene a adoptat concluzii în care susține în mare măsură intenția Comisiei de a reforma cadrul privind protecția datelor și aprobă numeroase elemente ale abordării Comisiei. De asemenea, Comitetul Economic și Social European s-a declarat în favoarea unei revizuiri corespunzătoare a Directivei 95/46/CE[17], sprijinind obiectivul general al Comisiei de a asigura o aplicare mai coerentă a normelor UE în materie de protecție a datelor în toate statele membre.

În conformitate cu politica sa privind „o mai bună legiferare", Comisia a realizat o evaluare a impactului privind politicile alternative[18]. Studiul a avut la bază trei obiective de politică: îmbunătățirea dimensiunii privind piața internă a protecției datelor, o exercitare mai eficientă de către persoanele fizice a drepturilor pe care le au în materie de protecție a datelor și elaborarea unui cadru cuprinzător și coerent care acoperă toate domeniile de competență ale Uniunii, inclusiv cooperarea polițienească și judiciară în materie penală. În special, în ceea ce privește ultimul obiectiv, au fost evaluate două opțiuni de politică: o primă opțiune care, în principal, extinde domeniul de aplicare a normelor în materie de protecție a datelor în acest domeniu și abordează neajunsurile și alte probleme ridicate de decizia-cadru; și o a doua opțiune, mai cuprinzătoare, cu norme foarte riguroase și stricte, care ar conduce, de asemenea, la modificări imediate ale tuturor celorlalte instrumente din cadrul „fostului al treilea pilon". O a treia opțiune „minimală", în mare parte bazată pe comunicări interpretative și pe măsuri de sprijin în materie de politici, cum ar fi programele de finanțare și instrumentele tehnice, însoțită de o intervenție legislativă minimă, nu a fost considerată ca fiind corespunzătoare în vederea abordării problemelor identificate în acest domeniu, în ceea ce privește protecția datelor.

În conformitate cu metodologia consacrată a Comisiei, fiecare opțiune de politică a fost evaluată cu ajutorul unui grup de coordonare interservicii în ceea ce privește eficiența acesteia în vederea îndeplinirii obiectivelor de politică, impactul său economic asupra părților interesate (inclusiv asupra bugetului instituțiilor UE), impactul său social și efectele acesteia asupra drepturilor fundamentale. Nu a fost analizat impactul asupra mediului.

Analiza impactului global a condus la elaborarea opțiunii de politică preferate care este încorporată în prezenta propunere. În conformitate cu evaluarea, punerea în aplicare a opțiunii menționate anterior va duce la consolidarea în continuare a protecției datelor în acest domeniu de politică, în special prin includerea prelucrării datelor la nivel național, contribuind astfel la

---

privind consimțământul (15/2011, GL 187). La cererea Comisiei, Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal a adoptat, de asemenea, următoarele trei recomandări: cea privind notificările, cea privind datele sensibile și cea privind punerea concretă în aplicare a articolului 28 alineatul (6) din Directiva 95/46/CE. Documentele pot fi consultate la adresa: http://ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm.

15 Aceasta este disponibilă pe website-ul AEPD: http://www.edps.europa.eu/EDPSWEB.

16 Rezoluția PE din 6 iulie 2011 referitoare la o abordare globală a protecției datelor cu caracter personal în Uniunea Europeană [2011/2025 (INI), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0323+0+DOC+XML+V0//RO (raportor: MP Axel Voss (DE/PPE)].

17 CESE 999/2011.

18 SEC (2012) 72.

consolidarea securității juridice pentru autoritățile competente în domeniul cooperării judiciare în materie penală și al cooperării polițienești.

Comitetul de evaluare a impactului (IAB) a emis, la 9 septembrie 2011, un aviz cu privire la proiectul de evaluare a impactului, pe baza căruia i-au fost aduse proiectului, în special, următoarele modificări:

– au fost clarificate obiectivele cadrului juridic actual (măsura în care au fost atinse sau nu), precum și obiectivele reformei preconizate;

– au fost adăugate mai multe dovezi și explicații/clarificări suplimentare la secțiunea privind definirea problemelor.

De asemenea, Comisia a pregătit un raport privind punerea în aplicare a Deciziei-cadru 2008/977/JAI, pe baza articolului 29 alineatul (2), care urmează să fie adoptat ca parte a prezentului pachet legislativ privind protecția datelor[19]. Concluziile prezentate în raport pe baza informațiilor transmise de statele membre au fost, de asemenea, luate în considerare la elaborarea evaluării impactului.

3. ELEMENTELE JURIDICE ALE PROPUNERII

3.1. Temei juridic

Propunerea se bazează pe articolul 16 alineatul (2) din TFUE, care constituie un nou temei juridic specific, introdus prin Tratatul de la Lisabona, pentru adoptarea normelor privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către instituțiile, organismele, oficiile și agențiile Uniunii, precum și de către statele membre atunci când desfășoară activități care intră în domeniul de aplicare a dreptului Uniunii, și normele privind libera circulație a acestor date.

Scopul propunerii este acela de a asigura un nivel ridicat și coerent de protecție a datelor în acest domeniu, sporind astfel încrederea reciprocă între autoritățile polițienești și cele judiciare din diferitele state membre și facilitând libera circulație a datelor și cooperarea între aceste autorități.

3.2. Subsidiaritate și proporționalitate

În conformitate cu principiului subsidiarității [articolul 5 alineatul (3) din TUE], se iau măsuri la nivelul Uniunii numai dacă obiectivele urmărite nu pot fi realizate suficient de bine de către statele membre și, prin urmare, având în vedere amploarea și efectele măsurilor propuse, obiectivele pot fi realizate mai bine la nivelul Uniunii. În lumina problemelor subliniate mai sus, analiza principiului subsidiarității indică necesitatea unor măsuri la nivelul UE în domenii precum poliția și justiția penală, pe baza următoarelor motive:

– dreptul la protecția datelor cu caracter personal, prevăzut la articolul 8 din Carta drepturilor fundamentale a Uniunii Europene și la articolul 16 alineatul (1) din TFUE, necesită același nivel de protecție a datelor pe tot cuprinsul Uniunii. De asemenea, necesită același nivel de protecție în ceea ce privește datele schimbate și datele prelucrate la nivel național.

[19] COM (2012) 12.

– este din ce în ce mai important ca autoritățile de aplicare a legii din statele membre să prelucreze și să facă schimb de date în mod tot mai rapid, în scopul prevenirii și al combaterii criminalității transfrontaliere și a terorismului. În acest context, existența unor norme clare și coerente privind protecția datelor la nivelul UE va contribui la încurajarea cooperării între astfel de autorități.

– în plus, există dificultăți practice în aplicarea legislației privind protecția datelor, fiind necesară o mai bună cooperare între statele membre și autoritățile acestora, care trebuie organizată la nivelul UE pentru a se asigura aplicarea uniformă a dreptului Uniunii. În anumite situații, UE este cea mai în măsură să asigure în mod efectiv și consecvent același nivel de protecție a persoanelor atunci când datele lor cu caracter personal sunt transferate către țări terțe.

– statele membre nu pot atenua în mod individual problemele care apar în situația actuală, în special cele legate de fragmentarea legislațiilor naționale. Prin urmare, apare necesitatea specifică de a institui un cadru armonizat și coerent, care să permită transferarea cu ușurință a datelor cu caracter personal dintr-un stat membru în altul, în cadrul UE, asigurându-se în același timp o protecție eficientă pentru toate persoanele fizice pe întreg teritoriul UE;

– acțiunile legislative propuse la nivelul UE pot fi mai eficace decât acțiuni similare la nivelul statelor membre, datorită naturii și amplorii problemelor, care nu sunt limitate la unul sau mai multe state membre.

Principiul proporționalității prevede ca fiecare intervenție să vizeze un obiectiv și să nu depășească ceea ce este necesar pentru îndeplinirea sa. Acest principiu a stat la baza elaborării prezentei propuneri, începând cu identificarea și evaluarea opțiunilor de politică alternative și până la redactarea propunerii legislative.

Prin urmare, directiva este instrumentul cel mai potrivit pentru asigurarea armonizării la nivelul UE în acest domeniu, acordând, în același timp, statelor membre flexibilitatea necesară atunci când pun în aplicare principiile, normele și derogările la nivel național. Având în vedere complexitatea normelor naționale în vigoare privind protecția datelor cu caracter personal în domeniul cooperării polițienești și judiciare în materie penală, precum și obiectivul armonizării globale a acestor norme prin intermediul prezentei directive, Comisia va trebui să solicite statelor membre să furnizeze documente care să explice relația dintre componentele directivei și părțile corespondente din instrumente naționale de transpunere, pentru a fi în măsură să își îndeplinească sarcina de a monitoriza transpunerea prezentei directive.

3.3. Rezumat al aspectelor legate de drepturile fundamentale

Dreptul la protecția datelor cu caracter personal este prevăzut la articolul 8 din Carta drepturilor fundamentale a Uniunii Europene, articolul 16 din TFUE și articolul 8 din Convenția europeană a drepturilor omului. Așa cum subliniază Curtea de Justiție a UE[20], dreptul la protecția datelor cu caracter personal nu este, totuși, un drept absolut, ci trebuie să

[20] Curtea de Justiție a UE, hotărârea din 9.11.2010 în cauzele conexate C-92/09 și C-93/09 Volker und Markus Schecke și Eifert, Rep., 2010, p. I-0000.

fie luat în considerare în raport cu funcția sa în societate[21]. Protecția datelor este strâns legată de respectarea vieții private și a celei de familie, protejate prin articolul 7 din cartă. Acest lucru este reflectat în articolul 1 alineatul (1) din Directiva 95/46/CE care prevede că statele membre trebuie să protejeze drepturile și libertățile fundamentale ale persoanelor fizice și, în special, dreptul acestora la respectarea vieții private cu privire la prelucrarea datelor cu caracter personal.

Alte drepturi fundamentale consacrate în cartă, care ar putea fi potențial afectate, sunt interzicerea oricărei discriminări bazate, printre altele, 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 o cale de atac eficientă în fața unei instanțe judecătorești și la un proces echitabil (articolul 47).

3.4. Explicarea detaliată a propunerii

3.4.1. CAPITOLUL I - DISPOZIȚII GENERALE

Articolul 1 definește obiectul directivei, și anume prevederea de norme referitoare la prelucrarea datelor cu caracter personal în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, și stabilește dublul obiectiv al directivei, și anume protecția drepturilor și a libertăților fundamentale ale persoanelor fizice și, în special, a dreptului acestora la protecția datelor cu caracter personal, garantând în același timp un nivel ridicat de siguranță publică, și asigurarea schimbului de date cu caracter personal între autoritățile competente în cadrul Uniunii.

Articolul 2 definește domeniul de aplicare a directivei. Domeniul de aplicare a directivei nu este limitat la prelucrarea datelor la nivel transfrontalier, însă se aplică tuturor activităților de prelucrare efectuate de „autoritățile competente” [astfel cum sunt definite la articolul 3 alineatul (14)], în sensul directivei. Directiva nu se aplică nici în cazul prelucrării în cadrul unei activități care nu intră în domeniul de aplicare a dreptului Uniunii, nici în cazul prelucrării de către instituțiile, organele, oficiile și agențiile Uniunii, care intră sub incidența Regulamentului (CE) nr. 45/2001 și a altor norme specifice.

Articolul 3 conține definițiile termenilor utilizați în directivă. În timp ce unele definiții sunt preluate din Directiva 95/46/CE și din Decizia-cadru 2008/977/JAI, altele sunt modificate, completate cu elemente suplimentare sau nou introduse. Noile definiții introduse sunt cele privind „încălcarea securității datelor cu caracter personal”, „datele genetice”, „datele biometrice”, „autoritățile competente” [bazată pe articolul 87 din TFUE și pe articolul 2 litera (h) din Decizia-cadru 2008/977/JAI] și „copilul”, bazată pe Convenția ONU privind drepturile copilului[22].

---

[21] 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.

[22] De asemenea, menționată la articolul 2(a) din Directiva 2011/92/UE a Parlamentului European și a Consiliului din 13 decembrie 2011 privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile și de înlocuire a Deciziei-cadru 2004/68/JAI a Consiliului, JO L 335, 17.12.2011, p. 1.

3.4.2. CAPITOLUL II – PRINCIPII

Articolul 4 stabilește principiile cu privire la prelucrarea datelor cu caracter personal, pe baza articolului 6 din Directiva 95/46/CE și a articolului 3 din Decizia-cadru 2008/977/JAI, adaptând dispozițiile acestora la contextul specific al prezentei directive.

Articolul 5 prevede necesitatea unei distincții cât mai clare între datele cu caracter personal ale diferitelor categorii de persoane vizate. Aceasta este o nouă dispoziție, care nu este inclusă nici în Directiva 95/46/CE, nici în Decizia-cadru 2008/977/JAI, dar care a fost propusă de Comisie în propunerea sa inițială de decizie-cadru[23]. Prevederile articolului se inspiră din Recomandarea Consiliului Europei nr. R (87)15. Există deja norme similare pentru Europol[24] și Eurojust[25].

Articolul 6 privind gradele diferite de precizie și de fiabilitate a datelor reflectă principiul 3.2 din Recomandarea Consiliului Europei nr. R (87)15. Norme similare, incluse, de asemenea, în propunerea de decizie-cadru a Comisiei, există pentru Europol[26].

Articolul 7 stabilește criteriile privind prelucrarea legală, în cazul în care este necesară pentru îndeplinirea unei sarcini de către o autoritate competentă, în temeiul legislației naționale, pentru a respecta o obligație legală pe care o are operatorul de date, în scopul protejării intereselor vitale ale persoanei vizate sau ale unei alte persoane sau în scopul prevenirii unei amenințări imediate și grave la adresa securității publice. Celelalte motive pentru prelucrarea legală prevăzute la articolul 7 din Directiva 95/46/CE nu sunt adecvate pentru prelucrarea datelor în domeniul poliției și al justiției penale.

Articolul 8 prevede, pe baza articolului 8 din Directiva 95/46/CE, interdicția generală privind prelucrarea categoriilor speciale de date cu caracter personal și excepțiile de la această regulă generală, la care se adaugă datele genetice, în conformitate cu jurisprudența CEDO[27].

Articolul 9 prevede o interdicție a măsurilor care se bazează exclusiv pe prelucrarea automată a datelor cu caracter personal în cazul în care aceasta nu este autorizată printr-o prevedere legală care oferă garanții corespunzătoare, în conformitate cu articolul 7 din Decizia-cadru 2008/977/JAI.

3.4.3. CAPITOLUL III - DREPTURILE PERSOANEI VIZATE

Articolul 10 introduce obligația statelor membre de a furniza informații ușor accesibile și inteligibile, această dispoziție fiind inspirată, în special, de principiul numărul 10 prevăzut în Rezoluția de la Madrid privind standardele internaționale în materie de protecție a datelor cu caracter personal și a vieții private[28], precum și de a impune operatorilor să prevadă proceduri și mecanisme pentru facilitarea exercitării de către persoana vizată a drepturile sale. Aceasta include cerința ca exercitarea drepturilor să fie, în principiu, gratuită.

---

23 COM(2005) 475 final.

24 Articolul 14 din Decizia 2009/371/JAI privind Europol.

25 Articolul 15 din Decizia 2009/426/JAI privind Eurojust.

26 Articolul 14 din Decizia 2009/371/JAI privind Europol.

27 CEDO, hotărârea din 4.12.2008, S. și Marper V. Unit (cererea nr. 30562/04 și 30566/04).

28 Adoptată în cadrul Conferinței internaționale a comisarilor pentru protecția datelor și a vieții private din 5.11.2009.

Articolul 11 prevede obligația statelor membre de a asigura informarea persoanei vizate. Aceste obligații sunt întemeiate pe articolele 10 și 11 din Directiva 95/46/CE, fără să fie prevăzute articole separate care să precizeze dacă informațiile sunt colectate sau nu de la persoana vizată, articolul extinzând informațiile care trebuie furnizate. Articolul prevede excepții de la obligația de informare, în cazul în care acestea sunt proporționale și necesare într-o societate democratică pentru exercitarea sarcinilor de către autoritățile competente (fiind bazate pe articolul 13 din Directiva 95/46/CE și pe articolul 17 din Decizia-cadru 2008/977/JAI).

Articolul 12 prevede obligația statelor membre de a asigura dreptul persoanei vizate de a avea acces la datele sale cu caracter personal. Acesta se bazează pe articolul 12 litera (a) din Directiva 95/46/CE, la care adaugă noi elemente de informare a persoanei vizate (privind perioada de stocare a datelor, drepturile persoanelor privind rectificarea, ștergerea sau restricționarea și dreptul de a depune o plângere).

Articolul 13 prevede, pe baza articolului 17 alineatele (2) și (3) din Decizia-cadru 2008/977/JAI, că statele membre pot adopta măsuri legislative care limitează dreptul de acces în cazul în care acest lucru este necesar datorită naturii specifice a prelucrării datelor în domeniul poliției și al justiției penale, precum și cu privire la informarea persoanei vizate cu privire la o limitare a accesului.

Articolul 14 introduce dispoziția conform căreia, în cazurile în care accesul direct este restricționat, persoana vizată trebuie să fie informată cu privire la posibilitățile de acces indirect, prin intermediul autorității de supraveghere care ar trebui să exercite acest drept în numele persoanei vizate și să o informeze cu privire la rezultatul verificărilor sale.

Articolul 15 privind dreptul la rectificare se bazează pe articolul 12 litera (b) din Directiva 95/46/CE și, în ceea ce privește obligațiile în cazul unui refuz, pe articolul 18 alineatul (1) din Decizia-cadru 2008/977/JAI.

Articolul 16 privind dreptul la ștergerea datelor se bazează pe articolul 12 litera (b) din Directiva 95/46/CE și, în ceea ce privește obligațiile în cazul unui refuz, pe articolul 18 alineatul (1) din Decizia-cadru 2008/977/JAI. De asemenea, acesta include dreptul de marcare a datelor în anumite cazuri, evitând termenul echivoc de „blocare” utilizat la articolul 12 litera (b) din Directiva 95/46/CE și la articolul 18 alineatul (1) din Decizia-cadru 2008/977/JAI.

Articolul 17 cu privire la rectificarea, ștergerea și restricționarea prelucrării datelor în cadrul procedurilor judiciare oferă clarificări pe baza articolului 4 alineatul (4) din Decizia-cadru 2008/977/JAI.

3.4.4. CAPITOLUL IV - OPERATORUL ȘI PERSOANA ÎMPUTERNICITĂ DE CĂTRE OPERATOR

3.4.4.1. SECȚIUNEA 1 - OBLIGAȚII GENERALE

Articolul 18 descrie responsabilitatea operatorului de a respecta dispozițiile prezentei directive și de a asigura conformitatea cu aceasta, inclusiv adoptarea de politici și mecanisme în acest scop.

Articolul 19 prevede că statele membre trebuie să asigure respectarea de către operator a obligațiilor care rezultă din principiile protecției datelor începând cu momentul conceperii și protecției implicite a datelor.

Articolul 20 privind operatorii asociați clarifică statutul acestora în ceea ce privește relațiile lor interne.

Articolul 21 clarifică poziția și obligațiile persoanelor împuternicite de către operator, reluând, în parte, prevederile articolului 17 alineatul (2) din Directiva 95/46/CE, la care adaugă elemente noi, inclusiv faptul că o persoană împuternicită de către operator care prelucrează date într-un alt mod decât cel prevăzut în instrucțiunile date de operator trebuie considerată ca fiind un operator asociat.

Articolul 22 privind prelucrarea sub autoritatea operatorului și a persoanei împuternicite de către operator reia articolul 16 din Directiva 95/46/CE.

Articolul 23 introduce obligația pentru operatori și persoanele împuternicite de către operator de a păstra documentația referitoare la toate sistemele și procedurile de prelucrare aflate în responsabilitatea lor.

Articolul 24 se referă la păstrarea evidențelor, în conformitate cu articolul 10 alineatul (1) din Decizia-cadru 2008/977, oferind, totodată, clarificări suplimentare.

Articolul 25 clarifică obligațiile operatorului și ale persoanei împuternicite de către operator în ceea ce privește cooperarea cu autoritatea de supraveghere.

Articolul 26 se referă la cazurile în care consultarea cu autoritatea de supraveghere este obligatorie înainte de prelucrare, în baza articolului 23 din Decizia-cadru 2008/977/JAI.

3.4.4.2. SECȚIUNEA 2 - SECURITATEA DATELOR

Articolul 27 privind securitatea prelucrării se bazează pe actualul articol 17 alineatul (1) din Directiva 95/46, care se referă la securitatea prelucrării, și pe articolul 22 din Decizia-cadru 2008/977/JAI, care extinde obligațiile aferente la persoanele împuternicite de către operator, indiferent de tipul de contract încheiat cu operatorul.

Articolele 28 și 29 introduc obligația de a notifica încălcarea securității datelor cu caracter personal, inspirată de notificarea încălcării securității datelor cu caracter personal prevăzută la articolul 4 alineatul (3) din Directiva 2002/58/CE asupra confidențialității și comunicațiilor electronice, care clarifică și separă obligațiile de a notifica autoritatea de supraveghere (articolul 28) și de a informa, în anumite circumstanțe, persoana vizată (articolul 29). Articolul 29 prevede, de asemenea, derogări, făcându-se referire la articolul 11 alineatul (4).

3.4.4.3. SECȚIUNEA 3 - RESPONSABILUL CU PROTECȚIA DATELOR

Articolul 30 introduce obligația operatorului de a desemna un responsabil cu protecția datelor care ar trebui să îndeplinească sarcinile enumerate la articolul 32. În cazul în care mai multe autorități competente acționează sub supravegherea unei autorități centrale, care are calitatea de operator, cel puțin această autoritate centrală ar trebui să desemneze un astfel de responsabil cu protecția datelor. Articolul 18 alineatul (2) din Directiva 95/46/CE prevedea posibilitatea ca statele membre să introducă o astfel de cerință în locul obligației de notificare generală prevăzută de directiva menționată.

Articolul 31 stabilește statutul responsabilului cu protecția datelor.

Articolul 32 prevede sarcinile responsabilului cu protecția datelor.

3.4.5. CAPITOLUL V - TRANSFERUL DATELOR CU CARACTER PERSONAL CĂTRE ȚĂRI TERȚE SAU ORGANIZAȚII INTERNAȚIONALE

Articolul 33 stabilește principiile generale pentru transferurile de date către țări terțe sau organizații internaționale în domeniul cooperării polițienești și judiciare în materie penală, inclusiv transferurile ulterioare. Articolul clarifică faptul că transferurile către țările terțe nu pot avea loc decât dacă acestea sunt necesare în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor.

Articolul 34 autorizează transferurile către o țară terță în privința căreia Comisia a adoptat o decizie privind caracterul adecvat al nivelului de protecție în temeiul Regulamentului …./../201X sau, în mod specific, în domeniul cooperării polițienești și judiciare în materie penală sau, în absența unei astfel de decizii, în cazul instituirii unor garanții corespunzătoare. Atât timp cât nu există decizii privind caracterul adecvat al nivelului de protecție, directiva asigură că transferurile pot continua să aibă loc pe baza unor garanții și derogări corespunzătoare. În plus, articolul stabilește criteriile pentru evaluarea Comisiei cu privire la caracterul adecvat sau neadecvat al nivelului de protecție și include, în mod expres, statul de drept, accesul la justiție și supravegherea independentă. Articolul prevede, de asemenea, posibilitatea Comisiei de a evalua nivelul de protecție asigurat de un teritoriu sau de un sector de prelucrare a datelor într-o țară terță. Acesta introduce dispoziția conform căreia o decizie generală privind caracterul adecvat al nivelului de protecție, adoptată în conformitate cu procedurile prevăzute la articolul 38 din Regulamentul general privind protecția datelor, este aplicabilă în cadrul domeniului de acțiune a prezentei directive. Alternativ, o decizie privind caracterul adecvat al nivelului de protecție poate fi adoptată de către Comisie doar în sensul prezentei directive.

Articolul 35 definește garanțiile corespunzătoare necesare înainte de efectuarea transferurilor internaționale, în absența unei decizii a Comisiei privind caracterul adecvat al nivelului de protecție. Aceste garanții pot fi asigurate printr-un instrument cu forță juridică obligatorie, cum ar fi un acord internațional. Alternativ, operatorul de date poate concluziona că acestea există pe baza unei evaluări a circumstanțelor aferente transferului.

Articolul 36 definește derogările pentru transferul de date efectuat în baza articolului 26 din Directiva 95/46/CE și a articolului 13 din Decizia-cadru 2008/977/JAI.

Articolul 37 obligă statele membre să prevadă că operatorul informează destinatarul cu privire la orice restricții de prelucrare și ia toate măsurile rezonabile pentru a se asigura că aceste restricții sunt respectate de către destinatarii datelor cu caracter personal în țara terță sau organizația internațională.

Articolul 38 prevede în mod explicit instituirea unor mecanisme de cooperare internațională pentru protecția datelor cu caracter personal între Comisie și autoritățile de supraveghere ale țărilor terțe, în special cele considerate ca asigurând un nivel adecvat de protecție, luând în considerare recomandarea din 12 iunie 2007 a Organizației pentru Cooperare și Dezvoltare Economică (OCDE) privind cooperarea transfrontalieră în aplicarea legislației privind protejarea confidențialității.

CAPITOLUL VI - AUTORITĂȚILE NAȚIONALE DE SUPRAVEGHERE

3.4.5.1. SECȚIUNEA 1 - STATUTUL INDEPENDENT

Articolul 39 prevede obligația statelor membre de a institui autorități de supraveghere, în conformitate cu articolul 28 alineatul (1) din Directiva 95/46/CE și cu articolul 25 din Decizia-cadru 2008/977/JAI, extinzând misiunea acestora pentru a contribui la aplicarea uniformă a directivei în întreaga Uniune; această autoritate de supraveghere poate fi cea instituită în temeiul Regulamentului general privind protecția datelor.

Articolul 40 aduce clarificări cu privire la condițiile de garantare a independenței autorităților de supraveghere, prin aplicarea jurisprudenței Curții de Justiție a UE[29] și inspirându-se, de asemenea, din articolul 44 din Regulamentul (CE) nr. 45/2001[30].

Articolul 41 prevede condițiile generale aplicabile membrilor autorității de supraveghere, prin aplicarea jurisprudenței relevante[31] și inspirându-se, de asemenea, din articolul 42 alineatele (2) - (6) din Regulamentul (CE) nr. 45/2001.

Articolul 42 stabilește norme privind instituirea autorității de supraveghere, inclusiv privind condițiile aplicabile membrilor săi, pe care statele membre trebuie să le prevadă pe cale legislativă.

Articolul 43 privind păstrarea secretului profesional de către membrii și personalul autorității de supraveghere se inspiră din articolul 28 alineatul (7) din Directiva 95/46/CE și din articolul 25 alineatul (4) Decizia-cadru 2008/977/JAI.

3.4.5.2. SECȚIUNEA 2 - ATRIBUȚII ȘI COMPETENȚE

Articolul 44 definește competența autorităților de supraveghere, în baza articolului 28 alineatul (6) din Directiva 95/46/CE și a articolului 25 alineatul (1) din Decizia-cadru 2008/977/JAI. Atunci când acționează în capacitatea lor judiciară, instanțele sunt exceptate de la monitorizarea exercitată de către autoritatea de supraveghere, însă nu de aplicarea normelor de fond în materie de protecție a datelor.

Articolul 45 prevede obligația statelor membre de a defini atribuțiile autorității de supraveghere, inclusiv primirea de plângeri și investigarea acestora, precum și promovarea unor acțiuni de sensibilizare a publicului cu privire la riscuri, norme, garanții și drepturi. O atribuție specială a autorităților de supraveghere în contextul prezentei directive este aceea conform căreia, în cazul în care accesul direct este refuzat sau restricționat, exercită dreptul de acces în numele persoanelor vizate și verifică legalitatea prelucrării datelor.

Articolul 46 prevede competențele autorității de supraveghere, în baza articolului 28 alineatul (3) din Directiva 95/46/CE, a articolului 25 alineatele (2) și (3) din Decizia-cadru 2008/977JAI. Articolul 47 prevede obligația autorităților de supraveghere de a

---

29 Curtea de Justiție a UE, hotărârea din 9.3.2010, Comisia/Germania (C-518/07, Rep., 2010, p. I-1885).

30 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 008, 12.1.2001, p. 1.

31 *Op. cit*, nota de subsol 27.

elabora rapoarte anuale de activitate, în baza articolului 28 alineatul (5) din Directiva 95/46/CE.

3.4.6. CAPITOLUL VII - COOPERAREA

Articolul 48 introduce norme privind asistența reciprocă obligatorie, în timp ce articolul 28 alineatul (6) paragraful al doilea din Directiva 95/46/CE prevedea doar o obligație generală de a coopera, fără a se aduce alte precizări.

Conform articolului 49, Comitetul european pentru protecția datelor, instituit prin Regulamentul general privind protecția datelor, își exercită, de asemenea, sarcinile în ceea ce privește activitățile de prelucrare care intră în domeniul de aplicare a prezentei directive. În vederea asigurării unui sprijin complementar, Comisia se va consulta cu reprezentanți ai autorităților competente în materie de prevenire, detectare, investigare și urmărire penală a infracțiunilor din statele membre, precum și cu reprezentanți ai Europol și Eurojust, prin intermediul unui grup de experți privind aspecte referitoare la aplicarea legii în domeniul protecției datelor.

3.4.7. CAPITOLUL VIII - CĂI DE ATAC, RĂSPUNDERE ȘI SANCȚIUNI

Articolul 50 prevede dreptul oricărei persoane vizate de a depune o plângere la o autoritate de supraveghere, în baza articolului 28 alineatul (4) din Directiva 95/46/CE, și se referă la orice încălcare a directivei în raport cu reclamantul. De asemenea, acest articol specifică organismele, organizațiile sau asociațiile care pot depune o plângere în numele persoanei vizate și, de asemenea, în cazul unei încălcări a securității datelor cu caracter personal, independent de plângerea înaintată de o persoană vizată.

Articolul 51 se referă la dreptul la o cale de atac împotriva unei autorități de supraveghere. Acesta se bazează pe dispoziția generală prevăzută la articolul 28 alineatul (3) din Directiva 95/46/CE și prevede, în mod specific, că persoana vizată poate iniția o acțiune judiciară pentru a obliga autoritatea de supraveghere să dea curs unei plângeri.

Articolul 52 se referă la dreptul la o cale de atac împotriva unui operator sau unei persoane împuternicite de către operator, în baza articolului 22 din Directiva 95/46/CE și a articolului 20 din Decizia-cadru 2008/977/JAI.

Articolul 53 introduce norme comune aplicabile acțiunilor în instanță, inclusiv dreptul organismelor, organizațiilor sau asociațiilor de a reprezenta persoanele vizate în fața instanțelor și dreptul autorităților de supraveghere de a acționa în justiție. Obligația statelor membre de a asigura o soluționare rapidă a acțiunilor în justiție este inspirată de articolul 18 alineatul (1) din Directiva 2000/31/CE privind comerțul electronic[32].

Articolul 54 obligă statele membre să prevadă dreptul la despăgubiri. Acesta se bazează pe articolul 23 din Directiva 95/46/CE și pe articolul 19 alineatul (1) din Decizia-cadru 2008/977/JAI, extinzând acest drept pentru a cuprinde prejudiciile cauzate de operatori și clarifică responsabilitatea operatorilor asociați și a persoanelor asociate împuternicite de către operator.

---

[32] Directiva 2000/31/CE a Parlamentului European și a Consiliului din 8 iunie 2000 privind anumite aspecte juridice ale serviciilor societății informaționale, în special ale comerțului electronic, pe piața internă („Directiva privind comerțul electronic”); JO L 178, 17.7.2000, p. 1.

Articolul 55 prevede obligația statelor membre de a stabili norme privind sancțiunile aplicabile în cazul încălcării dispozițiilor directivei și de a se asigura că acestea sunt puse în aplicare.

3.4.8. CAPITOLUL IX - ACTE DELEGATE ŞI ACTE DE PUNERE ÎN APLICARE

Articolul 56 conține dispoziții standard privind exercitarea delegării în conformitate cu articolul 290 din TFUE. Acesta din urmă autorizează legiuitorul să delege Comisiei competența de a adopta acte fără caracter legislativ și cu domeniu de aplicare general, care completează sau modifică anumite elemente neesențiale ale unui act legislativ (acte „cvasilegislative").

Articolul 57 cuprinde dispoziții privind procedura comitetului necesară pentru a se acorda Comisiei competențe de executare, în cazurile în care, în conformitate cu articolul 291 din TFUE, sunt necesare condiții unitare de punere în aplicare a actelor obligatorii din punct de vedere juridic ale Uniunii. În acest caz, se aplică procedura de examinare.

3.4.9. CAPITOLUL X - DISPOZIȚII FINALE

Articolul 58 abrogă Decizia-cadru 2008/977/JAI.

Articolul 59 prevede că dispozițiile specifice cu privire la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, prevăzute în acte ale Uniunii, care reglementează prelucrarea datelor cu caracter personal sau accesul la sisteme de informații care intră în domeniul de aplicare a prezentei directive, și care au fost adoptate înainte de adoptarea prezentei directive, rămân neschimbate.

Articolul 60 clarifică relația dintre prezenta directivă și acordurile internaționale încheiate anterior cu statele membre în domeniul cooperării judiciare în materie penală și al cooperării polițienești.

Articolul 61 prevede obligația Comisiei de a evalua punerea în aplicare a directivei și de a prezenta rapoarte cu privire la aceasta, în vederea evaluării necesității de a alinia dispozițiile specifice adoptate anterior, menționate la articolul 59, la prezenta directivă.

Articolul 62 prevede obligația statelor membre de a transpune directiva în legislația lor națională și de a informa Comisia cu privire la dispozițiile adoptate în temeiul directivei.

Articolul 63 stabilește data intrării în vigoare a directivei.

Articolul 64 desemnează destinatarii prezentei directive.

4. IMPLICAȚII BUGETARE

Fișa financiară legislativă care însoțește propunerea de regulament general privind protecția datelor acoperă impacturile bugetare ale regulamentului și ale prezentei directive.

2012/0010 (COD)

Propunere de

DIRECTIVĂ A PARLAMENTULUI EUROPEAN ŞI A CONSILIULUI

privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și la libera circulație a acestor date

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,

după consultarea Autorității Europene pentru Protecția Datelor[33],

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 și articolul 16 alineatul (1) din Tratatul privind funcționarea Uniunii Europene prevăd că orice persoană are dreptul la protecția datelor cu caracter personal care o privesc.

(2) Prelucrarea datelor cu caracter personal este în serviciul cetățeanului; principiile și normele privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal ar trebui, indiferent de cetățenia sau de locul de reședință al persoanelor fizice, să respecte drepturile și libertățile fundamentale ale acestora, în special dreptul la protecția datelor cu caracter personal. Aceasta ar trebui să contribuie la realizarea unui spațiu de libertate, securitate și justiție.

(3) Evoluțiile tehnologice rapide și globalizarea au generat noi provocări pentru protecția datelor cu caracter personal. Amploarea colectării și a schimbului și de date a crescut spectaculos. Tehnologia permite autorităților competente să utilizeze date cu caracter personal la un nivel fără precedent în cadrul activităților lor.

[33] JO C… , p. .

(4) Această evoluție necesită facilitarea liberei circulații a datelor între autoritățile competente în cadrul Uniunii și a transferului către țări terțe și organizații internaționale, asigurând, totodată, un nivel ridicat de protecție a datelor cu caracter personal. Aceste evoluții impun construirea unui cadru solid și mai coerent în materie de protecție a datelor în Uniune, însoțit de o aplicare riguroasă a normelor.

(5) Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date[34] se aplică tuturor activităților de prelucrare a datelor cu caracter personal în statele membre, atât în sectorul public, cât și în cel privat. Cu toate acestea, directiva menționată nu se aplică prelucrării datelor cu caracter personal „puse în practică pentru exercitarea activităților din afara domeniului de aplicare a dreptului comunitar", cum ar fi activitățile în domeniul cooperării judiciare în materie penală și al cooperării polițienești.

(6) Decizia-cadru 2008/977/JAI a Consiliului din 27 noiembrie 2008 privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală[35] se aplică în domeniul cooperării judiciare în materie penală și al cooperării polițienești. Domeniul de aplicare a prezentei decizii-cadru este limitat la prelucrarea datelor cu caracter personal transmise sau puse la dispoziție între statele membre.

(7) Asigurarea unui nivel omogen și ridicat de protecție a datelor cu caracter personal ale persoanelor fizice și facilitarea schimbului de date cu caracter personal între autoritățile competente ale statelor membre sunt esențiale pentru a se garanta eficacitatea cooperării judiciare în materie penală și a cooperării polițienești. În acest scop, nivelul de protecție a drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor trebuie să fie echivalent în toate statele membre. Protecția efectivă a datelor cu caracter personal în întreaga Uniune necesită nu numai consolidarea drepturilor persoanelor vizate și a obligațiilor celor care prelucrează date cu caracter personal, ci și competențe echivalente pentru monitorizarea și asigurarea conformității cu normele în materie de protecție a datelor cu caracter personal în statele membre.

(8) Articolul 16 alineatul (2) din Tratatul privind funcționarea Uniunii Europene prevede că Parlamentul European și Consiliul ar trebui să stabilească normele privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal, precum și normele privind libera circulație a acestor date.

(9) Pe această bază, Regulamentul UE …../2012 al Parlamentului European și al Consiliului privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal și libera circulație a acestor date (Regulament general privind protecția datelor) stabilește normele generale pentru protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și garantarea liberei circulații a acestor date în cadrul Uniunii.

---

[34] JO L 281, 23.11.1995, p. 31.
[35] JO L 350, 30.12.2008, p. 60.

(10) În Declarația 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 normele specifice privind protecția datelor cu caracter personal și libera circulație a acestor date în domeniul cooperării judiciare în materie penală și al cooperării polițienești în temeiul articolului 16 din Tratatul privind funcționarea Uniunii Europene s-ar putea dovedi necesare, având în vedere natura specifică a acestor domenii.

(11) Prin urmare, o directivă distinctă ar trebui să fie adaptată naturii specifice a acestor domenii și să stabilească normele privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal, de către autoritățile competente în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor.

(12) În vederea asigurării aceluiași nivel de protecție pentru persoanele fizice prin drepturi garantate din punct de vedere juridic în întreaga Uniune și a preîntâmpinării discrepanțelor care împiedică schimbul de date cu caracter personal între autoritățile competente, directiva ar trebui să prevadă norme armonizate pentru protecția și libera circulație a datelor cu caracter personal în domeniul cooperării judiciare în materie penală și al cooperării polițienești.

(13) Prezenta directivă permite luarea în considerare a principiului accesului publicului la documentele oficiale, în aplicarea dispozițiilor prevăzute de aceasta.

(14) Protecția conferită de prezenta directivă ar trebui să vizeze persoanele fizice, indiferent de cetățenia sau de locul de reședință al acestora, în ceea ce privește prelucrarea datelor cu caracter personal.

(15) Protecția persoanelor fizice ar trebui să fie neutră din punct de vedere tehnologic și să nu depindă de tehnicile utilizate, în caz contrar, creându-se un risc serios de eludare. Protecția persoanelor fizice ar trebui să se aplice prelucrării datelor cu caracter personal prin mijloace automate, precum și prelucrării manuale, în cazul în care datele 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 a prezentei directive. Aceasta nu ar trebui să se aplice prelucrării datelor cu caracter personal în cadrul unei activități care nu intră în domeniul de aplicare a dreptului Uniunii, în special privind securitatea națională, nici prelucrării datelor efectuate de către instituțiile, organismele, oficiile și agențiile Uniunii, cum ar fi Europol sau Eurojust.

(16) Principiile protecției ar trebui să se aplice oricărei informații referitoare la o persoană identificată sau identificabilă. Pentru a se stabili dacă o persoană fizică este identificabilă, ar trebui să se ia în considerare toate mijloacele care pot fi utilizate în mod rezonabil fie de către operator, fie de către orice altă persoană în scopul identificării persoanei fizice respective. Principiile protecției datelor nu ar trebui să se aplice datelor anonimizate astfel încât persoana vizată să nu mai fie identificabilă.

(17) Datele cu caracter personal referitoare la sănătate ar trebui să includă, în special, toate datele având legătură cu starea de sănătate a persoanei vizate; informații privind

înscrierea persoanei pentru acordarea de servicii medicale; informații privind plățile pentru asistență medicală efectuate de persoana fizică sau privind eligibilitatea acesteia pentru acordarea de asistență medicală; un număr, simbol sau semn distinctiv atribuit unei persoane fizice pentru identificarea unică a acesteia în scopuri medicale; orice informații privind persoana fizică respectivă colectate în cadrul furnizării de servicii de sănătate pentru aceasta; informații rezultate din testarea sau examinarea unei părți a corpului sau a unei substanțe corporale, inclusiv eșantioane de material biologic; identificarea unei persoane ca furnizor de asistență medicală pentru persoana fizică respectivă sau orice informații privind, de exemplu, o boală, un handicap, un risc de îmbolnăvire, un tratament clinic sau o boală, istoricul medical, tratamentul clinic sau starea psihologică sau biomedicală efectivă a persoanei vizate, indiferent de sursa acestora, cum ar fi de exemplu, un medic sau un alt cadru medical, un spital, un dispozitiv medical sau un test de diagnostic in vitro.

(18) Orice prelucrare a datelor cu caracter personal trebuie să fie echitabilă și legală în raport cu persoanele vizate. În special, scopul specific pentru care sunt prelucrate datele ar trebui să fie explicit.

(19) Pentru prevenirea, cercetarea și urmărirea penală a infracțiunilor, autoritățile competente trebuie să păstreze și să prelucreze datele cu caracter personal colectate în contextul prevenirii, identificării, investigării sau urmăririi penale a anumitor infracțiuni penale dincolo de acest context pentru a înțelege mai bine fenomenele și tendințele infracționale, pentru a culege informații despre rețelele de crimă organizată și pentru a face legături între diferitele infracțiuni constatate.

(20) Datele cu caracter personal nu ar trebui prelucrate în scopuri considerate incompatibile cu scopul în care au fost colectate. Datele cu caracter personal ar trebui să fie adecvate, relevante și neexcesive în ceea ce privește scopurile în care sunt prelucrate datele cu caracter personal. Ar trebui luate toate măsurile rezonabile pentru a se asigura rectificarea sau ștergerea datelor cu caracter personal care sunt inexacte.

(21) Principiul exactității datelor ar trebui aplicat luând în considerare natura și scopul prelucrării în cauză. În special în cadrul procedurilor judiciare, declarațiile care conțin date cu caracter personal se bazează pe o percepție subiectivă a persoanelor fizice și nu sunt întotdeauna verificabile. În consecință, acest principiu nu ar trebui să se aplice exactității unei declarații, ci doar faptului că o anumită declarație a fost făcută.

(22) În interpretarea și aplicarea principiilor generale referitoare la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, ar trebui să se țină seama de specificul sectorului, inclusiv de obiectivele specifice urmărite.

(23) Prelucrarea datelor cu caracter personal în domeniul cooperării judiciare în materie penală și al cooperării polițienești presupune prelucrarea datelor cu caracter personal referitoare la diferite categorii de persoane. Prin urmare, ar trebui să se facă o distincție cât mai clară între datele cu caracter personal ale diferitelor categorii de persoane vizate, cum ar fi suspecții, persoanele condamnate pentru comiterea unei infracțiuni, victimele și părțile terțe, cum ar fi martorii, persoanele care dețin informații sau contacte relevante și complicii suspecților și ai infractorilor condamnați.

(24) Pe cât posibil, datele cu caracter personal ar trebui diferențiate în funcție de gradul de exactitate și fiabilitate. Ar trebui să se facă diferența între fapte și evaluări cu caracter personal, pentru a garanta atât protecția persoanelor fizice, cât și calitatea și fiabilitatea informațiilor prelucrate de autoritățile competente.

(25) Pentru a fi legală, prelucrarea datelor cu caracter personal ar trebui să fie necesară pentru respectarea unei obligații legale care incumbă operatorului, pentru îndeplinirea unei sarcini de interes public de către o autoritate competentă în temeiul legii sau în scopul protejării intereselor vitale ale persoanei vizate sau ale unei alte persoane, sau în scopul prevenirii unei amenințări imediate și grave la adresa securității publice.

(26) Datele cu caracter personal care sunt, prin natura lor, deosebit de sensibile în ceea ce privește drepturile fundamentale sau viața privată, inclusiv datele genetice, necesită o protecție specifică. Astfel de date nu ar trebui prelucrate, cu excepția cazului în care prelucrarea este în mod expres permisă de o lege care prevede măsuri corespunzătoare pentru protejarea intereselor legitime ale persoanei vizate; sau prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale altei persoane; sau prelucrarea se referă la date care sunt făcute publice în mod manifest de persoana vizată.

(27) Fiecare persoană fizică ar trebui să aibă dreptul de a nu face obiectul unei măsuri care se bazează exclusiv pe prelucrarea automată dacă aceasta aduce prejudicii în plan juridic pentru persoana respectivă, cu excepția cazului în care respectiva măsură este permisă de lege și sub rezerva unor măsuri adecvate de protejare a intereselor legitime ale persoanei vizate.

(28) Pentru ca persoanele vizate să își poată exercita drepturile, toate informațiile care le sunt adresate trebuie să fie ușor accesibile și ușor de înțeles, limbajul folosit fiind simplu și clar.

(29) Ar trebui prevăzute modalități pentru a facilita exercitarea, de către persoana vizată, a drepturilor pe care i le conferă prezenta directivă, printre care se numără în special mecanismele prin care poate solicita, în mod gratuit, accesul la date, rectificarea și ștergerea acestora. Operatorul ar trebui să fie obligat să răspundă cererilor persoanei vizate fără întârzieri nejustificate.

(30) Conform principiului prelucrării echitabile, persoanele vizate ar trebui să fie informate, în special, cu privire la existența unei operațiuni de prelucrare și la scopurile acesteia, la durata stocării datelor, la existența dreptului de acces, de rectificare sau ștergere a datelor și la dreptul de a înainta o plângere. Atunci când datele sunt colectate de la persoana vizată, aceasta ar trebui informată, de asemenea, dacă are obligația de a furniza datele și care sunt consecințele în cazul unui refuz.

(31) Informațiile în legătură cu prelucrarea datelor cu caracter personal ar trebui oferite persoanei vizate în momentul colectării acestor date, sau, în cazul în care datele nu sunt obținute de la persoana vizată, în momentul în care sunt înregistrate sau într-o perioadă de timp rezonabilă după colectare, având în vedere circumstanțele specifice ale prelucrării datelor.

(32) Orice persoană ar trebui să aibă drept de acces la datele colectate care o privesc și ar trebui să își exercite acest drept cu ușurință, pentru a fi informată cu privire la

prelucrare și pentru a verifica legalitatea acesteia. Orice persoană vizată ar trebui, prin urmare, să aibă dreptul de a cunoaște și de a i se comunica, în special, în ce scopuri sunt prelucrate datele, pentru ce perioadă, care este identitatea destinatarilor datelor, inclusiv în țările terțe. Persoanele vizate ar trebui să aibă dreptul de a primi o copie a datelor lor cu caracter personal care sunt prelucrate.

(33) Statele membre ar trebui să aibă posibilitatea de a adopta măsuri legislative în vederea amânării, a restricționării parțiale sau totale a informării persoanelor vizate sau a accesului la datele lor cu caracter personal în măsura în care o astfel de restricționare parțială sau totală constituie o măsură necesară și proporțională într-o societate democratică, ținând seama de interesele legitime ale persoanei vizate, pentru a se evita obstrucționarea cercetărilor, a anchetelor sau a procedurilor oficiale sau judiciare, pentru a nu se afecta măsurile de prevenire, identificare, investigare sau urmărire penală a infracțiunilor sau executarea pedepselor, pentru a se proteja securitatea publică sau securitatea națională ori pentru a se proteja persoana vizată sau drepturile și libertățile altor persoane.

(34) Orice refuz sau restricționare a accesului ar trebui prezentat în scris persoanei vizate, precizându-se motivele de fapt și de drept pe care se bazează decizia.

(35) În cazul în care statele membre au adoptat măsuri legislative care limitează total sau parțial dreptul de acces, persoana vizată ar trebui să aibă dreptul de a solicita autorității naționale de supraveghere competente să verifice legalitatea prelucrării datelor. Persoana vizată trebuie să fie informată cu privire la acest drept. Atunci când dreptul de acces este exercitat de către autoritatea de supraveghere în numele persoanei vizate, autoritatea de supraveghere ar trebui cel puțin să informeze persoana vizată că toate verificările necesare au avut loc și să îi comunice dacă prelucrarea respectivă este legală sau nu.

(36) Orice persoană ar trebui să aibă dreptul de a obține rectificarea datelor cu caracter personal inexacte care o privesc și dreptul de eliminare a datelor în cazul în care prelucrarea datelor respective nu este în conformitate cu principiile de bază prevăzute în prezenta directivă. În cazul în care datele cu caracter personal sunt prelucrate în cadrul unei anchete și a unor proceduri judiciare, rectificarea, dreptul la informare, dreptul de acces, dreptul de ștergere și de restricționare a prelucrării pot fi exercitate în conformitate cu normele naționale privind procedurile judiciare.

(37) Ar trebui prevăzută responsabilitatea și răspunderea generală a operatorului pentru orice prelucrare a datelor cu caracter personal efectuată de către acesta sau în numele său. În special, operatorul ar trebui să asigure conformitatea operațiunilor de prelucrare cu normele adoptate în conformitate cu prezenta directivă.

(38) Protecția drepturilor și libertăților persoanelor vizate în ceea ce privește prelucrarea datelor cu caracter personal necesită adoptarea de măsuri tehnice și organizatorice corespunzătoare pentru a se asigura îndeplinirea cerințelor din prezenta directivă. Pentru a asigura respectarea dispozițiilor adoptate în conformitate cu prezenta directivă, controlorul ar trebui să adopte politici și să pună în aplicare măsuri adecvate, care respectă, în special, principiile de protecție a datelor începând cu momentul conceperii și protecție implicită a datelor.

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

(40) Activitățile de prelucrare ar trebui să fie înregistrate de către operator sau de către persoana împuternicită de către operator, în scopul de a monitoriza conformitatea cu prezenta directivă. Fiecare operator și fiecare persoană împuternicită de către operator ar trebui să aibă obligația de a coopera cu autoritatea de supraveghere și de a pune la dispoziția acesteia, la cerere, documentația disponibilă, pentru a putea fi utilizată în scopul monitorizării operațiunilor de prelucrare.

(41) Pentru a garanta protecția eficientă a drepturilor și libertăților persoanelor vizate prin intermediul unor acțiuni preventive, operatorul sau persoana împuternicită de către operator ar trebui să se consulte cu autoritatea de supraveghere în anumite cazuri înainte de prelucrare.

(42) Dacă nu este soluționată la timp și într-un mod adecvat, o încălcare a securității datelor cu caracter personal poate produce efecte negative, inclusiv asupra reputației persoanei fizice vizate. Prin urmare, de îndată ce un operator află că a avut loc o astfel de încălcare, aceasta ar trebui să notifice respectiva încălcare autorității naționale competente. Persoanele fizice ale căror date cu caracter personal sau a căror viață privată ar putea fi afectate negativ de încălcare ar trebui să fie înștiințate fără întârzieri nejustificate, pentru a putea să ia măsurile de precauție necesare. Ar trebui să se considere că o încălcare afectează în mod negativ datele cu caracter personal sau viața privată a unei persoane vizate în cazul în care aceasta ar putea avea drept rezultat, de exemplu, furtul sau fraudarea identității, vătămarea corporală, umilirea gravă sau afectarea reputației în legătură cu prelucrarea datelor cu caracter personal.

(43) La stabilirea de norme detaliate privind formatul și procedurile aplicabile notificării referitoare la încălcările securității datelor cu caracter personal, ar trebui să se acorde atenția cuvenită circumstanțelor în care a avut loc încălcarea, stabilindu-se inclusiv dacă protecția datelor cu caracter personal a fost sau nu a fost asigurată prin măsuri tehnice de protecție corespunzătoare, care să limiteze efectiv probabilitatea utilizării incorecte. În plus, astfel de norme și proceduri ar trebui să țină cont de interesele legitime ale autorităților competente în cazurile în care divulgarea timpurie ar putea îngreuna în mod inutil investigarea circumstanțelor în care a avut loc o încălcare.

(44) Operatorul sau persoana împuternicită de către operator ar trebui să desemneze o persoană care să ajute operatorul sau persoana împuternicită de către operator să monitorizeze respectarea dispozițiilor adoptate în temeiul prezentei directive. Un responsabil cu protecția datelor poate fi numit în comun de mai multe entități ale autorității competente. Responsabilii cu protecția datelor trebuie să fie în măsură să își îndeplinească îndatoririle și sarcinile în mod independent și eficient.

(45) Statele membre ar trebui să asigure că transferul către o țară terță nu are loc decât în cazul în care acesta este necesar pentru prevenirea, investigarea, identificarea sau urmărirea penală a infracțiunilor sau pentru executarea pedepselor, iar autoritatea de control din țara terță sau dintr-o organizație internațională competentă este o autoritate

competentă în sensul prezentei directive. Un transfer poate avea loc în cazul în care Comisia decide că țara terță sau organizația internațională în cauză asigură un nivel adecvat de protecție sau că oferă garanții corespunzătoare.

(46) Comisia poate decide, cu efect în întreaga Uniune, că anumite țări terțe sau un teritoriu ori un sector de prelucrare dintr-o țară terță sau o organizație internațională oferă un nivel adecvat de protecție a datelor, furnizând astfel securitate juridică și uniformitate în Uniune în ceea ce privește țările terțe sau organizațiile internaționale care sunt considerate a furniza un astfel de nivel de protecție. În aceste cazuri, transferurile de date cu caracter personal către țările respective pot avea loc fără a fi necesar să se obțină o autorizație suplimentară.

(47) În conformitate cu valorile fundamentale pe care se întemeiază Uniunea, în special protecția drepturilor omului, Comisia ar trebui să ia în considerare modul în care aceasta respectă statul de drept, accesul la justiție, precum și normele și standardele internaționale în materie de drepturi ale omului.

(48) Comisia ar trebui, de asemenea, să poată recunoaște că o țară terță, un teritoriu sau un sector de prelucrare a datelor dintr-o țară terță ori o organizație internațională nu oferă un nivel corespunzător de protecție a datelor. În acest caz, transferul de date cu caracter personal către țări terțe ar trebui interzis, cu excepția cazurilor în care acesta se bazează pe un acord internațional, garanții corespunzătoare sau o derogare. Ar trebui să se prevadă proceduri de consultare între Comisie și astfel de țări terțe sau organizații internaționale. Cu toate acestea, o astfel de decizie a Comisiei nu trebuie să aducă atingere posibilității de a efectua transferuri pe baza unor garanții adecvate sau a unei derogări prevăzute în directivă.

(49) Transferurile care nu se bazează pe o decizie privind caracterul adecvat al nivelului de protecție ar trebui să fie permise numai în cazul în care au fost prezentate garanții corespunzătoare într-un instrument obligatoriu din punct de vedere juridic, care asigură protecția datelor cu caracter personal în cazul în care operatorul sau persoana împuternicită de către operator a evaluat toate condițiile legate de operațiunea de transfer de date sau de setul de operațiuni de transfer de date și, pe baza acestei evaluări, consideră că există garanții adecvate în ceea ce privește protecția datelor cu caracter personal. În cazul în care nu există motive pentru autorizarea transferului, ar trebui să se permită derogări, dacă este necesar, în vederea protejării intereselor vitale ale persoanei în cauză sau ale unei alte persoane, sau în vederea protejării intereselor legitime ale persoanei vizate, în cazul în care legislația statului membru care transferă datele cu caracter personal prevede acest lucru, sau în cazul în care acestea sunt indispensabile pentru prevenirea unei amenințări imediate și grave la adresa siguranței publice a unui stat membru sau a unei țări terțe, sau în cazuri specifice, în scopul prevenirii, investigării, identificării sau urmăririi penale a infracțiunilor sau al executării pedepselor sau, în anumite cazuri, pentru constatarea, exercitarea sau apărarea unui drept în instanță.

(50) Fluxul transfrontalier de date cu caracter personal poate expune unui risc sporit capacitatea persoanelor fizice de a-și exercita drepturile în materie de protecție a datelor, pentru a-și asigura protecția împotriva utilizării sau a divulgării ilegale a acestor date. În același timp, autoritățile de supraveghere pot constata că se află în imposibilitatea de a trata plângeri sau de a efectua investigații referitoare la activitățile desfășurate în afara frontierelor lor. Eforturile lor de a conlucra în context

transfrontalier pot fi, de asemenea, îngreunate de insuficiența competențelor de prevenire sau remediere ori de caracterul eterogen al regimurilor juridice. Prin urmare, este necesar să se promoveze o cooperare mai strânsă între autoritățile de supraveghere a protecției datelor pentru a putea face schimb de informații cu omologii lor străini.

(51) Instituirea în statele membre a unor autorități de supraveghere care să își exercite atribuțiile în deplină independență este un element esențial al protecției persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal. Autoritățile de supraveghere ar trebui să monitorizeze aplicarea dispozițiilor prevăzute de prezenta directivă și să contribuie la aplicarea consecventă a acesteia în întreaga Uniune, în scopul asigurării protecției persoanele fizice în ceea ce privește prelucrarea datelor lor cu caracter personal. În acest sens, autoritățile de supraveghere ar trebui să coopereze între ele și cu Comisia.

(52) Statele membre pot încredința unei autorități de supraveghere deja existente din statele membre, în conformitate cu Regulamentul (CE) …./2012, responsabilitatea pentru sarcinile care urmează să fie îndeplinite de către autoritățile naționale de supraveghere care urmează a fi înființate în temeiul prezentei directive.

(53) Statele membre ar trebui să aibă posibilitatea de a institui mai multe autorități de supraveghere, pentru a reflecta structura lor constituțională, organizatorică și administrativă. Fiecare autoritate de supraveghere ar trebui să beneficieze de resurse financiare și umane adecvate, de localuri și de infrastructura necesară pentru îndeplinirea cu eficacitate a sarcinilor lor, inclusiv a celor legate de asistența reciprocă și cooperarea cu alte autorități de supraveghere în întreaga Uniune.

(54) Condițiile generale pentru membrii autorității de supraveghere ar trebui stabilite prin lege în fiecare stat membru și ar trebui, în special, să prevadă condiția ca acești membri să fie numiți de parlamentul sau de guvernul statului membru și să includă dispoziții privind calificarea personală și funcția membrilor respectivi.

(55) Cu toate că prezenta directivă se aplică, de asemenea, activităților instanțelor naționale, prelucrarea datelor cu caracter personal nu ar trebui să fie de competența autorităților de supraveghere atunci când instanțele își exercită atribuțiile judiciare, în scopul asigurării independenței judecătorilor în îndeplinirea sarcinilor lor judiciare. Cu toate acestea, derogarea ar trebui să se limiteze la activități pur judiciare în cadrul acțiunilor în instanță și să nu se aplice altor activități în care judecătorii ar putea fi implicați, în conformitate cu legislația națională.

(56) Pentru a se asigura consecvența monitorizării și a aplicării prezentei directive în întreaga Uniune, autoritățile de supraveghere ar trebui să aibă aceleași atribuții și competențe efective în fiecare stat membru, inclusiv competențe de investigare, de intervenție obligatorie conform legii, de decizie și sancționare, în special în cazul plângerilor înaintate de persoane fizice, precum și de acționare în justiție.

(57) Fiecare autoritate de supraveghere ar trebui să răspundă plângerilor depuse de orice persoană vizată și ar trebui să investigheze cazul. Investigația în urma unei plângeri ar trebui să fie efectuată doar dacă se dovedește necesară în respectivul caz și trebuie să poată face obiectul căilor de atac judiciare. Autoritatea de supraveghere ar trebui să informeze persoana vizată cu privire la evoluția și soluționarea plângerii într-un termen rezonabil. În eventualitatea în care cazul necesită o investigare suplimentară

sau coordonarea cu o altă autoritate de supraveghere, ar trebui să se furnizeze informații intermediare persoanei vizate.

(58) Autoritățile de supraveghere ar trebui să își acorde reciproc asistență în îndeplinirea atribuțiilor care le revin, pentru a se asigura coerența aplicării și a asigurării aplicării dispozițiilor adoptate în temeiul prezentei directive.

(59) Comitetul european pentru protecția datelor, instituit prin Regulamentul (UE) …/2012, ar trebui să contribuie la aplicarea coerentă a prezentei directive în întreaga Uniune, inclusiv prin oferirea de consultanță Comisiei și prin promovarea cooperării autorităților de supraveghere în întreaga Uniune.

(60) Orice persoană vizată ar trebui să aibă dreptul de a depune o plângere la o autoritate de supraveghere în orice stat membru și dreptul la exercitarea unei căi de atac, în cazul în care consideră că drepturile pe care i le conferă prezenta directivă sunt încălcate sau în cazul în care autoritatea de supraveghere nu reacționează la o plângere sau nu acționează atunci când o astfel de acțiune este necesară pentru asigurarea protecției drepturilor persoanei vizate.

(61) Orice organism, organizație sau asociație care are drept obiectiv asigurarea protecției drepturilor și a intereselor persoanelor vizate în ceea ce privește protecția datelor acestora și este constituit(ă) în conformitate cu legislația unui stat membru ar trebui să aibă dreptul să depună o plângere, să își exercite dreptul la o cale de atac în numele persoanelor vizate, dacă au primit mandat corespunzător din partea acestora, sau să depună, independent de plângerea înaintată de o persoană vizată, o plângere în nume propriu în cazul în care consideră că a avut loc o încălcare a securității datelor cu caracter personal.

(62) Orice persoană fizică sau juridică ar trebui să aibă dreptul la exercitarea unei căi de atac împotriva deciziilor unei autorități de supraveghere care o privesc. Acțiunile inițiate împotriva unei autorități de supraveghere ar trebui să fie înaintate instanțelor statului membru în care se află autoritatea de supraveghere.

(63) Statele membre ar trebui să se asigure că acțiunile în justiție, pentru a fi eficiente, permit adoptarea rapidă de măsuri în scopul remedierii sau al prevenirii încălcării prezentei directive.

(64) Orice daună pe care o persoană o poate suferi ca urmare a unei prelucrări ilegale ar trebui să fie despăgubită de operator sau de persoana împuternicită de către operator, care pot fi exonerați de răspundere dacă dovedesc că nu sunt răspunzători pentru prejudiciu, în special în cazul în care aceștia dovedesc că s-a produs din culpa persoanei vizate sau este rezultatul unui caz de forță majoră.

(65) Ar trebui impuse sancțiuni oricărei persoane fizice sau juridice, de drept privat sau public, care nu respectă prezenta directivă. Statele membre ar trebui să se asigure că sancțiunile sunt eficace, proporționale și cu efect de descurajare și ar trebui să adopte toate măsurile pentru punerea în aplicare a sancțiunilor.

(66) Pentru a se realiza obiectivele prezentei directive, și anume protejarea drepturilor și libertăților fundamentale ale persoanelor fizice și, în special, dreptul acestora la protecția datelor cu caracter personal, și pentru a se garanta liberul schimb de date cu

caracter personal de către autoritățile competente pe teritoriul Uniunii, competența de a adopta acte în conformitate cu articolul 290 din Tratatul privind funcționarea Uniunii Europene ar trebui să fie delegată Comisiei. Ar trebui adoptate în special acte delegate în ceea ce privește notificarea autorității de supraveghere în cazul încălcării securității datelor cu caracter personal. Este deosebit de important ca, pe durata activităților pregătitoare, Comisia să desfășoare consultări adecvate, inclusiv la nivel de experți. Atunci când pregătește și elaborează acte delegate, Comisia trebuie să asigure transmiterea simultană, la timp și în mod corespunzător a documentelor relevante către Parlamentul European și către Consiliu.

(67) Pentru a se asigura condiții uniforme de punere în aplicare a prezentei directive în ceea ce privește documentația deținută de operatori și de persoanele împuternicite de către operatori, securitatea prelucrării, în special în ceea ce privește standardele de criptare, notificarea autorității de supraveghere în cazul încălcării securității datelor cu caracter personal și nivelul adecvat de protecție oferit de o țară terță, un teritoriu sau un sector de prelucrare în țara terță respectivă sau de o organizație internațională, ar trebui să i se confere Comisiei competențe de executare. Competențele respective ar trebui să fie exercitate în conformitate cu 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[36].

(68) Procedura de examinare ar trebui să fie utilizată pentru adoptarea de măsuri în ceea ce privește documentația deținută de operatori și de persoane împuternicite de către operatori, securitatea prelucrării, notificarea autorității de supraveghere în cazul încălcării securității datelor cu caracter personal și nivelul adecvat de protecție oferit de o țară terță, un teritoriu sau un sector de prelucrare în țara terță respectivă sau de o organizație internațională, ținând seama de faptul că actele respective au un caracter general.

(69) Comisia ar trebui să adopte acte de punere în aplicare imediat aplicabile atunci când acest lucru se impune din motive imperative de urgență, în cazuri justificate în mod corespunzător referitoare la o țară terță, un teritoriu sau un sector de prelucrare din țara terță respectivă sau o organizație internațională care nu asigură un nivel de protecție adecvat.

(70) Întrucât obiectivele prezentei directive, și anume protejarea drepturilor și a libertăților fundamentale ale persoanelor fizice, în special dreptul acestora la protecția datelor cu caracter personal și asigurarea liberului schimb de date cu caracter personal de către autoritățile competente în cadrul Uniunii, nu pot fi realizate în mod satisfăcător de către statele membre și, prin urmare, din cauza dimensiunilor sau a efectelor acțiunii, pot fi realizate mai bine la nivelul Uniunii, Uniunea poate adopta măsuri, în conformitate cu principiul subsidiarității, astfel cum se prevede la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, astfel cum este enunțat la articolul respectiv, prezenta directivă nu depășește ceea ce este necesar pentru atingerea acestui obiectiv.

(71) Decizia-cadru 2008/977/JAI a Consiliului ar trebui abrogată prin prezenta directivă.

---

[36] JO L 55, 28.2.2011, p. 13.

(72) Dispoziții specifice cu privire la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor în actele Uniunii adoptate înainte de data adoptării prezentei directive, care reglementează prelucrarea datelor cu caracter personal între statele membre și accesul autorităților desemnate de statele membre la sistemele informatizate instituite în temeiul tratatelor, ar trebui să rămână neschimbate. Comisia ar trebui să evalueze situația în ceea ce privește relația dintre prezenta directivă și actele adoptate înainte de data adoptării prezentei directive care reglementează prelucrarea datelor cu caracter personal între statele membre și accesul autorităților desemnate de statele membre la sistemele informatizate instituite în conformitate cu tratatele, pentru a evalua necesitatea alinierii acestor dispoziții specifice cu prezenta directivă.

(73) În vederea asigurării unei protecții globale și coerente a datelor cu caracter personal în cadrul Uniunii, ar trebui modificate acordurile internaționale încheiate de statele membre înainte de intrarea în vigoare a prezentei directive în vederea armonizării cu prezenta directivă.

(74) Prezenta directivă se aplică fără a aduce atingere normelor privind combaterea abuzului sexual, a exploatării sexuale a copiilor și a pornografiei infantile, astfel cum se prevede în Directiva 2011/92/UE a Parlamentului European și a Consiliului din 13 decembrie 2011[37].

(75) În conformitate cu articolul 6a din Protocolul privind poziția Regatului Unit și a Irlandei în ceea ce privește spațiul de libertate, securitate și justiție, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, Regatul Unit și Irlanda nu sunt obligate să aplice normele stabilite în prezenta directivă întrucât Regatul Unit și Irlanda nu sunt obligate să aplice normele care reglementează formele de cooperare judiciară în materie penală sau de cooperare polițienească, care necesită respectarea dispozițiilor stabilite pe baza articolului 16 din Tratatul privind funcționarea Uniunii Europene.

(76) În conformitate cu articolele 2 și 2a din Protocolul privind poziția Danemarcei, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, Danemarca nu este obligată de prezenta directivă și nici nu face obiectul aplicării acesteia. Având în vedere faptul că prezenta directivă reprezintă o completare a acquis-ului Schengen, în temeiul titlului V partea a treia din Tratatul privind funcționarea Uniunii Europene, Danemarca, în conformitate cu articolul 4 din protocolul menționat, decide, în termen de șase luni de la adoptarea prezentei directive, dacă o va transpune în legislația sa națională.

(77) În ceea ce privește Islanda și Norvegia, prezenta directivă constituie o dezvoltare a dispozițiilor acquis-ului Schengen, în conformitate cu acordul încheiat de Consiliul Uniunii Europene și de Republica Islanda și Regatul Norvegiei privind asocierea acestor două state la implementarea, aplicarea și dezvoltarea acquis-ului Schengen[38].

---

37 JO L 335 17.12.2011, p. 1.

38 JO L 176, 10.7.1999, p. 36.

(78) În ceea ce privește Elveția, prezenta directivă constituie o dezvoltare a dispozițiilor acquis-ului Schengen, în conformitate cu Acordul dintre Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană privind asocierea Confederației Elvețiene la punerea în aplicare, respectarea și dezvoltarea acquis-ului Schengen[39].

(79) În ceea ce privește Liechtenstein, prezenta directivă reprezintă o dezvoltare a dispozițiilor acquis-ului Schengen, astfel cum se prevede în Protocolul dintre Uniunea Europeană, Comunitatea Europeană, Confederația Elvețiană și Principatul Liechtenstein privind aderarea Principatului Liechtenstein la Acordul dintre Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană privind asocierea Confederației Elvețiene la punerea în aplicare, respectarea și dezvoltarea acquis-ului Schengen[40].

(80) Prezenta directivă respectă drepturile fundamentale și principiile recunoscute de Carta drepturilor fundamentale a Uniunii Europene, astfel cum sunt consacrate în tratat, în special dreptul la respectarea vieții private și de familie, dreptul la protecția datelor cu caracter personal, dreptul la o cale de atac eficientă și la un proces echitabil. Limitările aduse acestor drepturi sunt în conformitate cu articolul 52 alineatul (1) din cartă întrucât sunt necesare pentru atingerea obiectivelor de interes general recunoscute de Uniune sau pentru a proteja drepturile și libertățile celorlalți.

(81) În conformitate cu declarația politică comună a statelor membre și a Comisiei privind documentele explicative din 28 septembrie 2011, statele membre s-au angajat să atașeze la notificarea măsurilor de transpunere, în cazuri justificate, unul sau mai multe documente care explică relația dintre elementele unei directive și părțile corespunzătoare ale instrumentelor naționale de transpunere. În ceea ce privește această directivă, legiuitorul consideră că transmiterea unor astfel de documente este justificată.

(82) Prezenta directivă nu ar trebui să împiedice statele membre să pună în aplicare exercitarea drepturilor persoanelor vizate cu privire la informare, acces, rectificare, ștergere și limitarea prelucrării datelor lor cu caracter personal în cadrul procedurilor penale, precum și eventualele limitări ale acestor drepturi în normele naționale privind procedura penală,

ADOPTĂ PREZENTA DIRECTIVĂ:

CAPITOLUL I
DISPOZIȚII GENERALE

Articolul 1
Obiect și obiective

1. Prezenta directivă stabilește normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile competente în

[39] JO L 53, 27.2.2008, p. 52.
[40] JO L 160, 18.6.2011, p. 19.

scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor.

2. În conformitate cu prezenta directivă, statele membre:

(a) protejează drepturile și libertățile fundamentale ale persoanelor fizice, în special dreptul acestora la protecția datelor cu caracter personal; și

(b) se asigură că schimbul de date cu caracter personal de către autoritățile competente în cadrul Uniunii nu este limitat sau interzis din motive legate de protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.

Articolul 2
Domeniu de aplicare

1. Prezenta directivă se aplică prelucrării datelor cu caracter personal de către autoritățile competente în scopurile prevăzute la articolul 1 alineatul (1).

2. Prezenta directivă se aplică prelucrării datelor cu caracter personal, realizate integral 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 a datelor sau care urmează să facă parte dintr-un sistem de evidență a datelor.

3. Prezenta directivă nu se aplică prelucrării datelor cu caracter personal:

(a) în cadrul unei activități care nu intră în sfera dreptului Uniunii, în ceea ce privește, mai ales, securitatea națională;

(b) de către instituțiile, organele, oficiile și agențiile Uniunii.

Articolul 3
Definiții

În sensul prezentei directive:

(1) „persoană vizată” înseamnă o persoană fizică identificată sau o persoană fizică ce poate fi identificată, în mod direct sau indirect, prin mijloace care pot fi utilizate, cu o probabilitate rezonabilă, de operator sau de orice altă persoană fizică sau juridică, în special prin referire la un număr de identificare, la date de localizare, la identificatori online sau la unul sau mai mulți factori specifici identității fizice, fiziologice, genetice, psihice, economice, culturale sau sociale a persoanei respective;

(2) „date cu caracter personal” înseamnă orice informație privind o persoană vizată;

(3) „prelucrare” înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi culegerea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea,

dezvăluirea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;

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

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

(6) „operator” înseamnă autoritatea publică competentă care, singură sau împreună cu alte autorități, stabilește scopurile, condițiile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile, condițiile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau prin legislația unui stat membru, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi stabilite prin dreptul Uniunii sau prin legislația unui stat membru;

(7) „persoana împuternicită de către operator” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau orice alt organism care prelucrează datele cu caracter personal în numele operatorului;

(8) „destinatar” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau orice alt organism căruia îi sunt transmise datele cu caracter personal;

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

(10) „date genetice” înseamnă toate datele, indiferent de tipul acestora, referitoare la caracteristicile unei persoane, care sunt moștenite sau dobândite într-un stadiu precoce de dezvoltare prenatală;

(11) „date biometrice” înseamnă orice date referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane, care permit identificarea unică a acesteia, cum ar fi imaginile faciale sau datele dactiloscopice;

(12) „date privind sănătatea” înseamnă orice informații legate de sănătatea fizică sau mentală a unei persoane sau de acordarea de servicii medicale persoanei respective;

(13) „minor” înseamnă orice persoană cu vârsta sub 18 ani;

(14) „autorități competente” înseamnă orice autoritate publică abilitată în vederea prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor;

(15) „autoritate de supraveghere” înseamnă o autoritate publică instituită de un stat membru în conformitate cu articolul 39.

CAPITOLUL II
PRINCIPII

Articolul 4
Principii legate de prelucrarea datelor cu caracter personal

Statele membre prevăd dispoziții potrivit cărora datele cu caracter personal trebuie:

(a) prelucrate în mod corect și în conformitate cu dispozițiile legale;

(b) colectate în scopuri determinate, explicite și legitime și nu trebuie prelucrate ulterior într-un mod incompatibil cu aceste scopuri;

(c) să fie adecvate, relevante și neexcesive în ceea ce privește scopurile în care sunt prelucrate;

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

(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;

(f) prelucrate sub responsabilitatea și răspunderea operatorului, care asigură respectarea dispozițiilor adoptate în conformitate cu prezenta directivă.

.

Articolul 5
Distincția între diferitele categorii de persoane vizate

1. Statele membre prevăd dispoziții potrivit cărora, în măsura posibilului, operatorul face distincție clară între datele cu caracter personal ale diferitelor categorii de persoane vizate, precum:

(a) persoane în privința cărora există motive serioase să se creadă că au săvârșit sau că urmează să săvârșească o infracțiune;

(b) persoane condamnate pentru comiterea unei infracțiuni;

(c) victime ale unei infracțiuni sau persoane în privința cărora, în baza anumitor fapte, există motive să se creadă că persoanele respective ar putea fi victimele unei infracțiuni;

(d) părți terțe la infracțiune, ca de exemplu persoane care ar putea fi chemate să depună mărturie în cadrul anchetelor legate de infracțiuni sau în cadrul

procedurilor penale ulterioare sau persoane care pot oferi informații cu privire la infracțiuni sau persoane care sunt în legătură sau asociate cu persoanele menționate la literele (a) și (b); și

(e) persoane care nu se încadrează în niciuna dintre categoriile menționate mai sus.

Articolul 6

Grade diferite de precizie și de fiabilitate a datelor cu caracter personal

1. Statele membre se asigură că, pe cât posibil, se face distincție între diferitele categorii de date cu caracter personal care fac obiectul prelucrării în funcție de gradul de precizie și de fiabilitate.

2. Statele membre se asigură că, pe cât posibil, se face distincție între datele cu caracter personal bazate pe fapte și datele cu caracter personal bazate pe evaluări personale.

Articolul 7

Legalitatea prelucrării

Statele membre prevăd dispoziții potrivit cărora prelucrarea datelor cu caracter personal este conformă dispozițiilor legale doar în cazul în care și în măsura în care prelucrarea este necesară:

(a) pentru executarea unei sarcini de către o autoritate competentă, conform legislației, în scopurile prevăzute la articolul 1 alineatul (1); sau

(b) pentru respectarea unei obligații legale care revine operatorului; sau

(c) pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane; sau

(d) pentru prevenirea unei amenințări imediate și grave la adresa siguranței publice.

Articolul 8

Prelucrarea categoriilor speciale de date cu caracter personal

1. Statele membre interzic prelucrarea datelor cu caracter personal care dezvăluie rasa sau originea etnică, opiniile politice, religia sau convingerile, apartenența la un sindicat, a datelor genetice sau a datelor privind sănătatea sau viața sexuală.

2. Alineatul (1) nu se aplică atunci când:

(a) prelucrarea este permisă printr-o lege care oferă garanții adecvate; sau

(b) prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale altei persoane; sau

(c) prelucrarea se referă la date care sunt făcute publice în mod manifest de persoana vizată.

Articolul 9

Măsuri bazate pe crearea de profiluri și pe prelucrarea automată

1. Statele membre prevăd dispoziții potrivit cărora sunt interzise măsurile care au efect juridic negativ pentru persoana vizată sau care afectează în mod semnificativ persoana vizată și care se bazează exclusiv pe prelucrarea automată a datelor cu caracter personal care au ca scop evaluarea anumitor aspecte personale privind persoana vizată, cu excepția cazului în care acest lucru este permis de un act legislativ care prevede, de asemenea, măsuri de protejare a intereselor legitime ale persoanei vizate.

2. Prelucrarea automată a datelor cu caracter personal, menite să evalueze anumite aspecte personale privind persoana vizată nu se bazează exclusiv pe categoriile speciale de date cu caracter personal prevăzute la articolul 8.

CAPITOLUL III

DREPTURILE PERSOANEI VIZATE

Articolul 10

Modalități de exercitare a drepturilor persoanei vizate

1. Statele membre prevăd dispoziții potrivit cărora operatorul ia toate măsurile rezonabile pentru a aplica politici transparente și ușor accesibile în ceea ce privește prelucrarea datelor cu caracter personal și exercitarea drepturilor persoanelor vizate.

2. Statele membre prevăd dispoziții potrivit cărora operatorul pune la dispoziția persoanei vizate orice informație și orice comunicare referitoare la prelucrarea datelor cu caracter personal, într-o formă inteligibilă, folosind un limbaj simplu și clar.

3. Statele membre prevăd dispoziții potrivit cărora operatorul ia toate măsurile rezonabile pentru stabilirea procedurilor de furnizare a informațiilor prevăzute la articolul 11 și de exercitare a drepturilor persoanelor vizate prevăzute la articolele 12 - 17.

4. Statele membre prevăd dispoziții potrivit cărora operatorul informează persoana vizată cu privire la modul în care a dat curs cererii, fără întârzieri nejustificate.

5. Statele membre prevăd dispoziții potrivit cărora informațiile și orice acțiune întreprinsă de către operator în urma unei cereri prevăzute la alineatele (3) și (4) nu se taxează. În cazul în care cererile sunt ofensatoare, în special, din cauza caracterului repetitiv sau al mărimii ori volumului cererii, operatorul poate percepe o taxă pentru furnizarea informațiilor sau întreprinderea acțiunii solicitate sau operatorul poate să nu întreprindă acțiunea cerută. În acest caz, sarcina probei în ceea ce privește caracterul vădit ofensator al cererii revine operatorului.

Articolul 11
Informații pentru persoana vizată

1. În cazul în care se colectează date cu caracter personal referitoare la o persoană vizată, statele membre se asigură că operatorul ia toate măsurile necesare pentru a furniza persoanei vizate cel puțin următoarele informații:

   (a) identitatea și datele de contact ale operatorului și ale responsabilului cu protecția datelor;

   (b) scopurile în care sunt prelucrate datele cu caracter personal;

   (c) perioada de stocare a datelor cu caracter personal;

   (d) existența dreptului de a solicita operatorului accesul și rectificarea, ștergerea sau limitarea prelucrării datelor cu caracter personal referitoare la persoana vizată;

   (e) dreptul de a depune o plângere la autoritatea de supraveghere prevăzută la articolul 39 și datele de contact ale acestei autorități;

   (f) destinatarii sau categoriile de destinatari ai datelor cu caracter personal, inclusiv în țări terțe sau organizații internaționale;

   (g) orice alte informații suplimentare, în măsura în care astfel de informații suplimentare sunt necesare pentru garantarea prelucrării echitabile în ceea ce privește persoana vizată, având în vedere circumstanțele specifice în care sunt prelucrate datele cu caracter personal.

2. În cazul în care datele cu caracter personal sunt colectate de la persoana vizată, operatorul transmite persoanei vizate, în plus față de informațiile menționate la alineatul (1), informații cu privire la caracterul obligatoriu sau voluntar al furnizării datelor cu caracter personal, precum și la eventualele consecințe ale refuzului de a furniza aceste date.

3. Operatorul furnizează informațiile prevăzute la alineatul (1):

   (a) în momentul obținerii datelor cu caracter personal de la persoana vizată; sau

   (b) în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, în momentul în care sunt înregistrate sau într-o perioadă de timp rezonabilă după colectare, având în vedere circumstanțele specifice ale prelucrării datelor.

4. Statele membre pot adopta măsuri legislative de amânare, restricționare sau omitere a dispoziției privind informațiile pentru persoana vizată în măsura în care și atât timp cât o astfel de restricționare parțială sau totală constituie o măsură necesară și proporțională într-o societate democratică, ținând seama de interesele legitime ale persoanei vizate:

   (a) pentru evitarea obstrucționării cercetărilor, anchetelor sau procedurilor oficiale sau juridice;

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

(c) pentru protejarea siguranței publice;

(d) pentru protejarea securității naționale;

(e) pentru protejarea drepturilor și libertăților celorlalți.

5. Statele membre pot stabili categoriile de prelucrare a datelor care se pot încadra, integral sau parțial, la excepțiile de la alineatul (4).

Articolul 12
Dreptul de acces al persoanei vizate

1. Statele membre prevăd dispoziții potrivit cărora persoana vizată are dreptul de a obține de la operator confirmarea cu privire la prelucrarea datelor sale cu caracter personal. În cazul în care aceste date cu caracter personal sunt prelucrate, operatorul furnizează următoarele informații:

(a) scopurile prelucrării;

(b) categoriile de date cu caracter personal vizate;

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

(d) perioada de stocare a datelor cu caracter personal;

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

(f) dreptul de a depune o plângere în fața autorității de supraveghere și datele de contact ale autorității de supraveghere;

(g) comunicarea datelor cu caracter personal care fac obiectul prelucrării și a oricărei informații disponibile cu privire la originea datelor.

2. Statele membre prevăd dispoziții potrivit cărora persoana vizată are dreptul de a obține de la operator o copie a datelor cu caracter personal care fac obiectul prelucrării.

Articolul 13
Limitarea dreptului de acces

1. Statele membre pot adopta măsuri legislative care limitează, integral sau parțial, dreptul de acces al persoanei vizate în măsura în care o astfel de limitare, parțială sau totală, constituie o măsură necesară și proporțională într-o societate democratică, ținându-se seama de interesele legitime ale persoanei în cauză:

(a) pentru evitarea obstrucționării cercetărilor, anchetelor sau procedurilor oficiale sau juridice;

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

(c) pentru protejarea siguranței publice;

(d) pentru protejarea securității naționale;

(e) pentru protejarea drepturilor și libertăților celorlalți.

2. Statele membre pot stabili prin lege categoriile de prelucrare a datelor care se pot încadra, integral sau parțial, la excepțiile de la alineatul (1).

3. În cazurile prevăzute la alineatele (1) și (2), statele membre prevăd dispoziții potrivit cărora operatorul informează în scris persoana vizată cu privire la refuzarea sau limitarea accesului, cu privire la motivele refuzului și cu privire la posibilitățile de a depune o plângere la autoritatea de supraveghere și de a introduce o cale de atac în justiție. Informațiile cu privire la motivele de fapt și de drept care stau la baza deciziei pot fi omise în cazul în care furnizarea acestor informații ar contraveni unuia dintre obiectivele de la alineatul (1).

4. Statele membre se asigură că operatorul justifică motivele pentru omiterea comunicării motivelor de fapt și de drept care stau la baza deciziei.

Articolul 14
Modalitățile de exercitare a dreptului de acces

1. Statele membre prevăd dispoziții potrivit cărora persoana vizată are dreptul de a solicita, în special în cazurile menționate la articolul 13, verificarea legalității prelucrării datelor de către autoritatea de supraveghere.

2. Statul membru prevede dispoziții potrivit cărora operatorul informează persoana vizată cu privire la dreptul de a solicita intervenția autorității de supraveghere în temeiul alineatului (1).

3. Atunci când este exercitat dreptul menționat la alineatul (1), autoritatea de supraveghere informează persoana vizată, cel puțin că au fost realizate toate verificările necesare de către autoritatea de supraveghere, precum și cu privire la rezultatul legalității prelucrării respective.

Articolul 15
Dreptul la rectificare

1. Statele membre prevăd dispoziții potrivit cărora persoana vizată are dreptul de a obține de la operator rectificarea datelor cu caracter personal inexacte care o privesc. Persoana vizată are dreptul de a obține completarea datelor cu caracter personal care sunt incomplete, în special prin furnizarea unei declarații corective suplimentare.

2. Statele membre prevăd dispoziții potrivit cărora operatorul informează în scris persoana vizată cu privire la orice refuz de rectificare, cu privire la motivele refuzului și cu privire la posibilitățile de a depune o plângere la autoritatea de supraveghere și de a introduce o cale de atac în justiție.

Articolul 16
Dreptul de a șterge

1. Statele membre prevăd dispoziții potrivit cărora persoana vizată are dreptul de a obține din partea operatorului ștergerea datelor cu caracter personal referitoare la aceasta, în cazul în care prelucrarea nu este în conformitate cu dispozițiile adoptate în temeiul articolului 4 literele (a) – (e) și al articolelor 7 și 8 din prezenta directivă.

2. Operatorul efectuează ștergerea fără întârziere.

3. În loc de ștergere, operatorul marchează datele cu caracter personal în cazul în care:

   (a) persoana vizată contestă exactitatea acestor date, pentru o perioadă care să îi permită operatorului să verifice exactitatea datelor;

   (b) datele cu caracter personal trebuie să fie păstrate ca dovadă;

   (c) persoana vizată se opune ștergerii și solicită în schimb restricționarea utilizării acestora.

4. Statele membre prevăd dispoziții potrivit cărora operatorul informează persoana vizată, în scris, cu privire la orice refuz de ștergere sau de marcare a prelucrării, cu privire la motivele refuzului și cu privire la posibilitățile de a depune o plângere la autoritatea de supraveghere și de a introduce o cale de atac în justiție.

Articolul 17
Drepturile persoanelor vizate în cadrul investigațiilor și procedurilor penale

Statele membre pot prevedea dispoziții potrivit cărora drepturile la informare, acces, rectificare, ștergere și la restricționarea prelucrării menționate la articolele 11 - 16 sunt exercitate în conformitate cu normele naționale privind procedurile judiciare în cazul în care datele cu caracter personal sunt conținute într-o hotărâre sau înregistrare judecătorească prelucrată în cursul unor investigații și al unor proceduri penale.

CAPITOLUL IV
OPERATORUL ȘI PERSOANA ÎMPUTERNICITĂ DE CĂTRE OPERATOR

SECȚIUNEA 1
OBLIGAȚII GENERALE

Articolul 18
Responsabilitatea operatorului

1. Statele membre prevăd dispoziții potrivit cărora operatorul adoptă norme interne și pune în aplicare măsuri adecvate pentru a se asigura că prelucrarea datelor cu caracter personal este realizată în conformitate cu dispozițiile adoptate în temeiul prezentei directive.

2. Măsurile menționate la alineatul (1) cuprind în special:

   (a) păstrarea documentației menționate la articolul 23;

   (b) respectarea cerințelor privind consultarea prealabilă, în temeiul articolului 26;

   (c) punerea în aplicare a cerințelor privind securitatea datelor prevăzute la articolul 27;

   (d) desemnarea unui responsabil cu protecția datelor, în temeiul articolului 30.

3. Operatorul pune în aplicare mecanisme pentru a asigura verificarea eficacității măsurilor menționate la alineatele (1) și (2) ale prezentului articol. Dacă se dovedește a fi proporțională, această verificare va fi efectuată de auditori interni sau externi independenți.

Articolul 19
Protecția datelor începând cu momentul conceperii și protecția implicită a datelor

1. Statele membre prevăd dispoziții potrivit cărora, având în vedere stadiul actual al tehnicii și costurile de implementare, operatorul pune în aplicare măsuri și proceduri tehnice și organizatorice corespunzătoare astfel încât prelucrarea să îndeplinească cerințele dispozițiilor adoptate în temeiul prezentei directive și să asigure protecția drepturilor persoanei vizate.

2. Operatorul pune în aplicare mecanisme care garantează că, în mod implicit, sunt prelucrate numai acele date cu caracter personal care sunt necesare pentru scopurile prelucrării.

Articolul 20
Operatorii asociați

Statele membre prevăd dispoziții potrivit cărora, în cazul în care un operator stabilește scopul, condițiile și mijloacele de prelucrare a datelor cu caracter personal împreună cu alții,

operatorii asociați trebuie să stabilească responsabilitățile care revin fiecăruia pentru respectarea dispozițiilor adoptate în temeiul prezentei directive, în special în ceea ce privește procedurile și mecanismele pentru exercitarea drepturilor persoanelor vizate, prin intermediul unui acord între aceștia.

Articolul 21
Persoana împuternicită de către operator

1. Statele membre prevăd dispoziții potrivit cărora, atunci când o operațiune de prelucrare este realizată în numele unui operator, operatorul trebuie să aleagă o persoană împuternicită care să ofere garanții suficiente pentru punerea în aplicare a măsurilor tehnice și organizatorice adecvate și a procedurilor, astfel încât prelucrarea să îndeplinească cerințele prevăzute în dispozițiile adoptate în temeiul prezentei directive și să asigure protecția drepturilor persoanei vizate.

2. Statele membre prevăd dispoziții potrivit cărora realizarea prelucrării de către o persoană împuternicită de către operator trebuie să fie reglementată printr-un act juridic care obligă persoana împuternicită de către operator în raport cu operatorul și care prevede, în special, că persoana împuternicită de către operator acționează numai la instrucțiunile operatorului; în special, în cazul în care transferul datelor cu caracter personal utilizate este interzis.

3. În cazul în care o persoană împuternicită de către operator prelucrează date cu caracter personal într-un alt mod decât cel prevăzut în instrucțiunile date de operator, persoana împuternicită de către operator este considerată operator pentru prelucrarea respectivă și face obiectul dispozițiilor privind operatorii asociați prevăzute la articolul 20.

Articolul 22
Desfășurarea activității de prelucrare sub autoritatea operatorului și a persoanei împuternicite de către operator

Statele membre prevăd dispoziții potrivit cărora orice persoană acționând sub autoritatea operatorului sau a persoanei împuternicite, care are acces la date cu caracter personal, nu le poate prelucra decât pe baza instrucțiunilor operatorului sau dacă acest lucru este impus de legislația Uniunii sau a unui stat membru.

Articolul 23
Documentația

1. Statele membre prevăd dispoziții potrivit cărora fiecare operator și persoană împuternicită de către operator păstrează documentația referitoare la toate sistemele și procedurile de prelucrare aflate în responsabilitatea lor.

2. Această documentație cuprinde cel puțin următoarele informații:

   (a) numele și datele de contact ale operatorului, sau ale oricărui operator asociat sau persoane împuternicite de către operator;

(b) scopurile prelucrării;

(c) destinatarii sau categoriile de destinatari ai datelor cu caracter personal;

(d) transferurile de date către o țară terță sau către o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective.

3. Operatorul și persoana împuternicită de către operator pun documentația la dispoziția autorității de supraveghere, la cererea acesteia.

Articolul 24
Păstrarea înregistrărilor

1. Statele membre prevăd dispoziții potrivit cărora se înregistrează următoarele operațiuni de prelucrare: colectare, modificare, consultare, divulgare, combinare sau ștergere. Înregistrările consultărilor sau ale divulgărilor indică, în special, scopul, data și momentul acestor operațiuni și, în măsura în care este posibil, identificarea persoanei ale cărei date cu caracter personal au fost consultate sau divulgate.

2. Înregistrările sunt utilizate exclusiv în scopul verificării legalității prelucrării datelor, al monitorizării proprii și al asigurării integrității și securității datelor.

Articolul 25
Cooperarea cu autoritatea de supraveghere

1. Statele membre prevăd dispoziții potrivit cărora operatorul și persoana împuternicită de operator cooperează cu autoritatea de supraveghere, la cererea acesteia, în îndeplinirea îndatoririlor sale, în special prin furnizarea tuturor informațiilor necesare autorității de supraveghere pentru a-și îndeplini sarcinile.

2. În urma exercitării de către autoritatea de supraveghere a competențelor sale prevăzute la articolul 46 literele (a) și (b), operatorul și persoana împuternicită de către operator răspund autorității de supraveghere într-un termen rezonabil. Răspunsul include o descriere a măsurilor adoptate și a rezultatelor obținute în urma observațiilor autorității de supraveghere.

Articolul 26
Consultarea prealabilă a autorității de supraveghere

1. Statele membre se asigură că operatorul sau persoana împuternicită consultă autoritatea de supraveghere înainte de prelucrarea datelor cu caracter personal care fac parte dintr-un sistem nou de evidență a datelor care urmează a fi creat, în cazul în care:

(a) urmează a fi prelucrate categorii speciale de date, menționate la articolul 8;

(b) tipul prelucrării, în special prin utilizarea de tehnologii, mecanisme sau proceduri noi prezintă riscuri specifice pentru drepturile și libertățile

fundamentale, în special pentru protecția datelor cu caracter personal ale persoanelor vizate.

2. Statele membre pot prevedea dispoziții potrivit cărora autoritatea de supraveghere stabilește o listă a operațiunilor de prelucrare care fac obiectul consultării prealabile, în conformitate cu alineatul (1).

SECȚIUNEA 2
SECURITATEA DATELOR

Articolul 27
Securitatea prelucrării

1. Statele membre prevăd dispoziții potrivit cărora operatorul și persoana împuternicită de către operator pun în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura un nivel de securitate corespunzător riscurilor pe care le presupune prelucrarea și naturii datelor care trebuie protejate, având în vedere stadiul actual al tehnologiei și costurile punerii lor în aplicare.

2. În ceea ce privește prelucrarea automată a datelor, fiecare stat membru prevede dispoziții potrivit cărora operatorul sau persoana împuternicită de către operator, în urma unei evaluări a riscurilor, pune în aplicare măsuri menite:

   (a) să împiedice accesul persoanelor neautorizate la echipamentele de prelucrare a datelor utilizate pentru prelucrarea datelor cu caracter personal (controlul accesului la echipamente);

   (b) să împiedice orice citire, copiere, modificare sau eliminare neautorizată a suporturilor de date (controlul suporturilor de date);

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

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

   (e) să asigure faptul că persoanele autorizate să utilizeze un sistem de prelucrare automată a datelor au acces numai la datele pentru care au autorizare (controlul accesului la date);

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

   (g) să asigure că este posibil ulterior să se verifice și să se identifice datele cu caracter personal introduse în sistemele de prelucrare automată a datelor, momentul introducerii acestora și entitatea care le-a introdus (controlul introducerii datelor);

(h) să împiedice citirea, copierea, modificarea sau ștergerea neautorizată a datelor cu caracter personal în timpul transferurilor de date cu caracter personal sau în timpul transportării suporturilor de date (controlul transportării);

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

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

3. Comisia poate adopta, după caz, acte de punere în aplicare pentru specificarea cerințelor prevăzute la alineatele (1) și (2) în diverse situații, în special a standardelor de codificare. Actele de punere în aplicare respective sunt adoptate în conformitate cu procedura de examinare menționată la articolul 57 alineatul (2).

Articolul 28

Notificarea autorității de supraveghere în cazul încălcării securității datelor cu caracter personal

1. Statele membre prevăd dispoziții potrivit cărora, în cazul în care are loc o încălcare a securității datelor cu caracter personal, operatorul notifică acest lucru autorității de supraveghere fără întârzieri nejustificate și, în cazul în care este posibil, în termen de cel mult 24 de ore de la data la care a luat cunoștință de aceasta. Operatorul transmite autorității de supraveghere, la cerere, o explicație motivată în cazurile în care notificarea nu este efectuată în termen de 24 de ore.

2. Persoana împuternicită de către operator alertează și informează operatorul, imediat după ce ia cunoștință de o încălcare a securității datelor cu caracter personal.

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

(a) să descrie caracterul încălcării securității datelor cu caracter personal, inclusiv categoriile și numărul persoanelor vizate în cauză, precum și categoriile și numărul de înregistrări de date în cauză;

(b) să comunice identitatea și datele de contact ale responsabilului cu protecția datelor menționat la articolul 30 sau alt punct de contact unde pot fi obținute mai multe informații;

(c) să recomande măsuri de atenuare a eventualelor efecte negative ale încălcării securității datelor cu caracter personal;

(d) să descrie consecințele posibile ale încălcării securității datelor cu caracter personal;

(e) să descrie măsurile propuse sau adoptate de operator pentru a remedia problema încălcării securității datelor cu caracter personal.

4. Statele membre prevăd dispoziții potrivit cărora operatorul păstrează documente referitoare la toate cazurile de încălcare a securității datelor cu caracter personal, care

cuprind o descriere a situației în care a avut loc încălcarea, a efectelor acesteia și a măsurilor de remediere întreprinse. Aceste documente trebuie să permită autorității de supraveghere să verifice conformitatea cu prezentul articol. Documentele respective includ numai informațiile necesare în acest scop.

5. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 56 în scopul detalierii criteriilor și cerințelor necesare pentru stabilirea încălcării menționate la alineatele (1) și (2) și pentru circumstanțele speciale în care un operator și o persoană împuternicită de către operator au obligația de a notifica încălcarea securității datelor cu caracter personal.

6. Comisia poate stabili formatul standard al notificării adresate autorității de supraveghere, procedurile aplicabile în cazul obligației de notificare și forma și modalitățile de întocmire a documentelor menționate la alineatul (4), inclusiv termenele pentru ștergerea informațiilor conținute în acestea. Actele de punere în aplicare respective sunt adoptate în conformitate cu procedura de examinare menționată la articolul 57 alineatul (2).

Articolul 29

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

1. Statele membre prevăd dispoziții potrivit cărora, atunci când încălcarea securității datelor cu caracter personal afectează protecția datelor cu caracter personal și a vieții private a persoanei vizate, operatorul, după notificarea prevăzută la articolul 28, informează persoana vizată, fără întârzieri nejustificate, cu privire la încălcarea securității datelor cu caracter personal.

2. Informarea persoanei vizate prevăzută la alineatul (1) cuprinde o descriere a caracterului încălcării securității datelor cu caracter personal și conține cel puțin informațiile și recomandările prevăzute la articolul 28 alineatul (3) literele (b) și (c).

3. Informarea persoanei vizate cu privire la încălcarea securității datelor cu caracter personal ale acesteia nu este necesară în cazul în care operatorul demonstrează într-un mod satisfăcător autorității de supraveghere că a pus în aplicare măsuri tehnologice adecvate de protecție și că respectivele măsuri au fost aplicate în cazul datelor afectate de încălcarea securității datelor cu caracter personal. Astfel de măsuri tehnologice de protecție asigură faptul că datele devin neinteligibile persoanelor care nu sunt autorizate să le acceseze.

4. Informarea persoanei vizate poate fi întârziată, restricționată sau omisă din motivele menționate la articolul 11 alineatul (4).

SECȚIUNEA 3
RESPONSABILUL CU PROTECȚIA DATELOR

Articolul 30

Desemnarea responsabilului cu protecția datelor

1. Statele membre prevăd dispoziții potrivit cărora operatorul sau persoana împuternicită de către operator desemnează un responsabil cu protecția datelor.

2. Responsabilul cu protecția datelor este desemnat pe baza calităților profesionale și, în special, a cunoștințelor de specialitate în domeniul legislației și practicilor privind protecția datelor, precum și pe baza capacității de a îndeplini sarcinile prevăzute la articolul 32.

3. Responsabilul cu protecția datelor poate fi desemnat pentru mai multe entități, ținându-se seama de structura organizatorică a autorității competente.

Articolul 31
Funcția responsabilului cu protecția datelor

1. Statele membre prevăd dispoziții potrivit cărora operatorul sau persoana împuternicită de către operator 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. Operatorul sau persoana împuternicită de către operator se asigură că responsabilul cu protecția datelor are la dispoziție mijloacele pentru îndeplinirea cu eficacitate și în mod independent a funcțiilor și sarcinilor menționate la articolul 32 și că nu primește instrucțiuni în ceea ce privește exercitarea funcției sale.

Articolul 32
Sarcinile responsabilului cu protecția datelor

Statele membre prevăd dispoziții potrivit cărora operatorul sau persoana împuternicită de către operator încredințează responsabilului cu protecția datelor cel puțin următoarele sarcini:

(a) informarea și consilierea operatorului sau a persoanei împuternicite de către operator cu privire la obligațiile care îi revin în conformitate cu dispozițiile adoptate în temeiul prezentei directive și păstrarea documentelor referitoare la această activitate și la răspunsurile primite;

(b) monitorizarea aplicării politicilor în ceea ce privește protecția datelor cu caracter personal, inclusiv alocarea responsabilităților, formarea personalului implicat în operațiunile de prelucrare și auditurile aferente;

(c) monitorizarea punerii în aplicare și aplicarea dispozițiilor adoptate în temeiul prezentei directive, în special cu privire la cerințele legate de protecția datelor începând cu momentul conceperii, de protecția implicită a datelor, securitatea datelor și de informarea persoanelor vizate, precum și de solicitările acestora în exercitarea drepturilor lor prevăzute de dispozițiile adoptate în temeiul prezentei directive;

(d) asigurarea păstrării documentației, prevăzute la articolul 23;

(e) monitorizarea documentației, a notificării și a comunicării cazurilor de încălcare a securității datelor cu caracter personal, în temeiul articolelor 28 și 29;

(f) monitorizarea cererii de consultare prealabilă adresată autorității de supraveghere, în cazul în care este necesar, în conformitate cu articolul 26;

(g) monitorizarea răspunsului la solicitările autorității de supraveghere și, în limitele ariei de competență a responsabilului cu protecția datelor, cooperarea cu autoritatea de supraveghere, la cererea acesteia sau din proprie inițiativă;

(h) asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare și, dacă este cazul, de consultare a autorității de supraveghere, din propria inițiativă a responsabilului cu protecția datelor.

CAPITOLUL V
TRANSFERUL DATELOR CU CARACTER PERSONAL CĂTRE ȚĂRI TERȚE SAU ORGANIZAȚII INTERNAȚIONALE

Articolul 33

Principii generale pentru transferurile de date cu caracter personal

Statele membre prevăd dispoziții potrivit cărora orice transfer de date cu caracter personal de către autoritățile competente, care sunt prelucrate sau care sunt destinate prelucrării după transferul către o țară terță sau către o organizație internațională, inclusiv, ulterior, transferul în continuare către o altă țară terță sau organizație internațională, poate avea loc numai dacă:

(a) transferul este necesar pentru prevenirea, investigarea, identificarea sau urmărirea penală a infracțiunilor sau pentru executarea pedepselor și

(b) condițiile prevăzute în prezentul capitol sunt respectate de operator și de persoana împuternicită de către operator.

Articolul 34

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

1. Statele membre prevăd dispoziții potrivit cărora un transfer de date cu caracter personal către o țară terță sau către o organizație internațională poate avea loc în cazul în care Comisia a decis, în conformitate cu articolul 41 din Regulamentul (CE) …./2012 sau în conformitate cu alineatul (3) din prezentul articol, că țara terță sau un teritoriu sau un sector de prelucrare din acea țară terță sau organizația internațională respectivă asigură un nivel adecvat de protecție. Transferurile realizate în aceste condiții nu necesită alte autorizări suplimentare.

2. În cazul în care nu există nici decizie adoptată în conformitate cu articolul 41 din Regulamentul (CE) …./2012, Comisia evaluează caracterul adecvat al nivelului de protecție, luând în considerare următoarele elemente:

(a) statul de drept, legislația relevantă în vigoare, atât generală, cât și sectorială, inclusiv cea referitoare la securitatea publică, la apărare, la securitatea națională și la dreptul penal, măsurile de securitate respectate în țara respectivă sau de respectiva organizație internațională, precum și drepturile efective și opozabile, inclusiv căile de atac administrative și judiciare efective ale persoanelor vizate, în special în cazul persoanelor vizate care au reședința în Uniune și ale căror date cu caracter personal sunt transferate;

(b) existența și funcționarea efectivă a uneia sau a mai multor autorități de supraveghere independente în țara terță sau în cadrul organizației internaționale în cauză, care are responsabilitatea de a asigura respectarea normelor în materie de protecție a datelor, de a asista și de a consilia persoana vizată în ceea ce privește exercitarea drepturilor sale și de a coopera cu autoritățile de supraveghere din statele membre și din Uniune și

(c) angajamentele internaționale la care a aderat țara terță sau organizația internațională în cauză.

3. Comisia poate decide, în limitele prezentei directive, că o țară terță, un teritoriu sau un sector de prelucrare din acea țară terță sau o organizație internațională asigură un nivel de protecție adecvat în sensul alineatului (2). Actele de punere în aplicare respective sunt adoptate în conformitate cu procedura de examinare menționată la articolul 57 alineatul (2).

4. Actul de punere aplicare menționează aplicarea geografică și sectorială, și, după caz, identifică autoritatea de supraveghere menționată la alineatul (2) litera (b).

5. Comisia poate decide, în limitele prezentei directive, că o țară terță, un teritoriu sau un sector de prelucrare din acea țară terță, sau o organizație internațională nu asigură un nivel de protecție adecvat în sensul alineatului (2), în special în cazurile în care legislația relevantă, atât cea generală, cât și cea sectorială, în vigoare în țara terță sau în organizația internațională, nu garantează drepturi efective și opozabile, inclusiv căi de atac administrative și judiciare efective pentru persoanele vizate, în special pentru acele persoanele vizate care își au reședința în Uniune și ale căror date cu caracter personal sunt transferate. Actele de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 57 alineatul (2), sau, în cazuri de extremă urgență pentru persoanele fizice în ceea ce privește dreptul la protecția datelor cu caracter personal, în conformitate cu procedura menționată la articolul 57 alineatul (3).

6. Statele membre asigură că, atunci când Comisia ia o decizie în temeiul alineatului (5), potrivit căreia transferurile de date cu caracter personal către țara terță, un teritoriu sau un sector de prelucrare din acea țară terță sau către organizația internațională în cauză sunt interzise, decizia respectivă nu aduce atingere transferurilor efectuate în temeiul articolului 35 alineatul (1) sau în conformitate cu articolul 36. La momentul oportun, Comisia efectuează consultări cu țara terță sau organizația internațională în vederea remedierii situației apărute în urma deciziei luate în conformitate cu alineatul (5) al prezentului articol.

7. Comisia publică în *Jurnalul Oficial al Uniunii Europene* o listă a țărilor terțe, a teritoriilor și sectoarelor de prelucrare din țările terțe și a organizațiilor internaționale în cazul cărora a decis că nivelul de protecție adecvat este asigurat sau nu este asigurat.

8. Comisia monitorizează aplicarea actelor de punere în aplicare la care se face referire la alineatele (3) și (5).

Articolul 35
Transferurile în baza unor garanții adecvate

1. În cazul în care Comisia nu a luat o decizie în temeiul articolului 34, statele membre prevăd dispoziții potrivit cărora un transfer de date cu caracter personal către un destinatar dintr-o țară terță sau o organizație internațională poate avea loc în condițiile în care:

   (a) s-au prezentat garanții corespunzătoare în ceea ce privește protecția datelor cu caracter personal printr-un instrument cu forță juridică obligatorie sau

   (b) operatorul sau persoana împuternicită de către operator a evaluat toate circumstanțele aferente transferului de date cu caracter personal și a concluzionat că există garanții corespunzătoare în ceea ce privește protecția datelor cu caracter personal.

1. Decizia privind transferurile în temeiul alineatului (1) litera (b) trebuie să fie luată de personalul autorizat în acest sens. Aceste transferuri trebuie să fie documentate, iar documentele trebuie să fie puse la dispoziția autorității de supraveghere, la cerere.

Articolul 36
Derogări

Prin derogare de la articolele 34 și 35, statele membre prevăd dispoziții potrivit cărora un transfer de date cu caracter personal către o țară terță sau o organizație internațională poate avea loc numai în condițiile în care:

(a) transferul este necesar pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane sau

(b) transferul este necesar pentru protejarea intereselor legitime ale persoanei vizate, în cazul în care legea statului membru care transferă datele cu caracter personal prevede acest lucru sau

(c) transferul datelor este esențial pentru prevenirea unei amenințări imediate și grave la adresa siguranței publice a unui stat membru sau a unei țări terțe sau

(d) transferul este necesar, în cazuri individuale, în scopul prevenirii, investigării, identificării sau urmăririi penale a infracțiunilor sau al executării sancțiunilor penale sau

(e) transferul este necesar, în cazuri individuale, pentru constatarea, exercitarea sau apărarea unui drept în instanță legat de prevenirea, investigarea, identificarea sau urmărirea penală a infracțiunilor sau de executarea unei anumite sancțiuni penale.

Articolul 37

Condiții specifice pentru transferul datelor cu caracter personal

Statele membre prevăd dispoziții potrivit cărora operatorul informează destinatarul cu privire la orice restricție privind prelucrarea datelor cu caracter personal și ia toate măsurile rezonabile pentru a asigura respectarea acestor restricții.

Articolul 38

Cooperarea internațională în domeniul protecției datelor cu caracter personal

1. În ceea ce privește țările terțe și organizațiile internaționale, Comisia și statele membre iau măsurile corespunzătoare pentru:

   (a) elaborarea de mecanisme eficiente de cooperare internațională pentru a facilita asigurarea aplicării 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 reclamațiilor, asistență în anchete 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 lărgirea cooperării internaționale în vederea asigurarea aplicării legislației din domeniul protecției datelor cu caracter personal;

   (d) promovarea schimbului și a documentației cu privire la legislația și practicile în materie de protecție a datelor cu caracter personal.

2. În sensul alineatului (1), Comisia ia măsurile necesare pentru a consolida relațiile cu țările terțe sau cu organizațiile internaționale, în special cu autoritățile lor de supraveghere, în cazul în care Comisia a decis că acestea asigură un nivel adecvat de protecție în sensul articolului 34 alineatul (3).

CAPITOLUL VI
AUTORITĂȚI DE SUPRAVEGHERE INDEPENDENTE

SECȚIUNEA 1
STATUT INDEPENDENT

Articolul 39

Autoritatea de supraveghere

1. Fiecare stat membru prevede dispoziții potrivit cărora una sau mai multe autorități publice sunt responsabile de monitorizarea aplicării dispozițiilor adoptate în temeiul prezentei directive și de contribuția la aplicarea uniformă a acesteia în întreaga Uniune, în vederea protejării drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal ale acestora și în

vederea facilitării liberei circulații a datelor cu caracter personal în cadrul Uniunii. În acest sens, autoritățile de supraveghere cooperează între ele și cu Comisia.

2. Statele membre pot prevedea că autoritatea de supraveghere instituită în statele membre în temeiul Regulamentului (UE) …./2012 își asumă responsabilitatea pentru sarcinile autorității de supraveghere care urmează să fie instituită în temeiul alineatului (1) din prezentul articol.

3. În cazul în care un stat membru instituie mai multe autorități de supraveghere, statul membru respectiv desemnează autoritatea de supraveghere care funcționează ca punct unic de contact pentru participarea efectivă a autorităților respective la Comitetul european pentru protecția datelor.

Articolul 40
Independență

1. Statele membre se asigură că autoritatea de supraveghere beneficiază de independență deplină în exercitarea îndatoririlor și competențelor care îi sunt încredințate.

2. Fiecare stat membru prevede dispoziții potrivit cărora, în îndeplinirea îndatoririlor lor, membrii autorității de supraveghere nu solicită și nici nu acceptă niciun fel de instrucțiuni.

3. Membrii autorității de supraveghere nu întreprind acțiuni incompatibile cu îndatoririle lor și, pe durata mandatului, nu desfășoară activități incompatibile, remunerate sau nu.

4. După încheierea mandatului, membrii autorității de supraveghere trebuie să dea dovadă de integritate și discreție în ceea ce privește acceptarea unor funcții sau beneficii.

5. Fiecare stat membru se asigură că autoritatea de supraveghere beneficiază de resurse umane, tehnice și financiare adecvate, de sediul și infrastructura necesare pentru buna executare a sarcinilor și a competențelor sale, inclusiv a celor care urmează să fie efectuate în contextul asistenței reciproce, al cooperării și al participării active la Comitetul european pentru protecția datelor.

6 Fiecare stat membru se asigură că autoritatea de supraveghere dispune de personal propriu, care este numit de șeful autorității de supraveghere și care răspunde în fața acestuia.

7. Statele membre se asigură că autoritatea de supraveghere face obiectul unui control financiar care nu aduce atingere independenței sale. Statele membre se asigură că autoritatea de supraveghere dispune de bugete anuale distincte. Bugetele se fac publice.

Articolul 41

Condiții generale aplicabile membrilor autorității de supraveghere

1. Statele membre prevăd dispoziții potrivit cărora membrii autorității de supraveghere trebuie numiți fie de parlament, fie de guvernul statului membru în cauză.

2. Membrii se aleg din rândul persoanelor care fac dovada independenței dincolo de orice îndoială, precum și a experienței și a competențelor necesare pentru îndeplinirea îndatoririlor lor.

3. Funcțiile unui membru încetează în cazul expirării mandatului, în cazul demisiei sau al destituirii conform dispozițiilor alineatului (5).

4. Un membru poate fi demis sau poate fi decăzut din dreptul la pensie sau la alte beneficii echivalente de către instanța națională competentă, în cazul în care membrul respectiv nu mai îndeplinește condițiile necesare pentru executarea funcțiilor sau este vinovat de comiterea unei abateri disciplinare grave.

5. În cazul expirării mandatului sau al demisiei membrului, acesta continuă să își exercite îndatoririle până la numirea unui nou membru.

Articolul 42

Norme privind instituirea autorității de supraveghere

Fiecare stat membru prevede, pe cale legislativă, următoarele:

(a) instituirea și statutul autorității de supraveghere în conformitate cu articolele 39 și 40;

(b) calificările, experiența și competențele necesare pentru exercitarea funcției de membru al autorității de supraveghere;

(c) normele și procedurile pentru numirea membrilor autorității de supraveghere, precum și normele privind acțiunile sau ocupațiile incompatibile cu funcțiile membrilor;

(d) durata mandatului membrilor autorității de supraveghere, care nu poate fi sub patru ani, cu excepția primului mandat după intrarea în vigoare a prezentei directive, care poate fi pe o perioadă mai scurtă;

(e) posibilitatea de reînnoire a mandatului membrilor autorității de supraveghere;

(f) regulile și condițiile comune care reglementează îndatoririle membrilor și ale personalului autorității de supraveghere;

(g) normele și procedurile privind încetarea funcțiilor asumate de membrii autorității de supraveghere, inclusiv în cazul în care nu mai îndeplinesc condițiile necesare pentru exercitarea atribuțiilor lor sau în cazul în care sunt vinovați de comiterea unei abateri disciplinare grave.

Articolul 43
Secretul profesional

Statele membre prevăd dispoziții potrivit cărora membrii și personalul autorității de supraveghere au obligația, atât în cursul mandatului, cât și după încetarea acestuia, de a respecta secretul profesional în ceea ce privește informațiile confidențiale de care au luat cunoștință în timpul exercitării sarcinilor lor oficiale.

SECȚIUNEA 2
ATRIBUȚII ȘI FUNCȚII

Articolul 44
Competență

1. Statele membre prevăd dispoziții potrivit cărora fiecare autoritate de supraveghere exercită, pe teritoriul statului membru de care aparține, funcțiile cu care este investită în conformitate cu prezenta directivă.

2. Statele membre prevăd dispoziții potrivit cărora autoritatea de supraveghere nu are competența de a supraveghea operațiunile de prelucrare ale instanțelor atunci când acestea acționează în exercițiul funcției lor jurisdicționale.

Articolul 45
Atribuții

1. Statele membre prevăd dispoziții potrivit cărora autoritatea de supraveghere:

   (a) monitorizează și asigură aplicarea dispozițiilor adoptate în temeiul prezentei directive, precum și a măsurilor de punere în aplicare aferente acesteia;

   (b) primește reclamațiile depuse de orice persoană vizată sau de o asociație care reprezintă persoana vizată respectivă și este împuternicită în mod corespunzător de aceasta, în conformitate cu articolul 50, investighează chestiunea, în măsura în care este adecvat, și informează, într-un termen rezonabil, persoana vizată sau asociația cu privire la evoluția și rezultatul reclamației, în special dacă este necesară efectuarea unei cercetări mai detaliate sau coordonarea cu o altă autoritate de supraveghere;

   (c) verifică legalitatea prelucrării datelor în conformitate cu articolul 14 și informează persoana vizată, într-un termen rezonabil, cu privire la rezultatul verificării sau la motivele pentru care nu a avut loc verificarea;

   (d) oferă asistență reciprocă altor autorități de supraveghere și asigură consecvența aplicării și a asigurării aplicării dispozițiilor adoptate în temeiul prezentei directive;

   (e) desfășoară anchete fie din proprie inițiativă, fie pe baza unei reclamații sau la cererea altei autorități de supraveghere și informează într-un termen rezonabil

persoana vizată cu privire la rezultatul anchetelor, în cazul în care persoana vizată a depus o reclamație;

(f) monitorizează evoluțiile relevante, în măsura în care acestea au impact asupra protecției datelor cu caracter personal, în special evoluția tehnologiilor informațiilor și comunicațiilor;

(g) este consultată de instituțiile și organele statului membru 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) este consultată cu privire la operațiunile de prelucrare prevăzute la articolul 26;

(i) participă la activitățile Comitetului european pentru protecția datelor.

2. Fiecare autoritate de supraveghere promovează acțiuni de sensibilizare a publicului cu privire la riscurile, normele, garanțiile și drepturile în materie de prelucrare a datelor cu caracter personal. Se acordă atenție specială activităților care se adresează în mod special minorilor.

3. La cerere, autoritatea de supraveghere oferă consiliere oricărei persoane vizate cu privire la exercitarea drepturilor de care beneficiază, în conformitate cu dispozițiile adoptate în temeiul prezentei directive și, dacă este cazul, cooperează cu autoritățile de supraveghere din alte state membre în acest scop.

4. Pentru reclamațiile prevăzute la alineatul (1) litera (b), autoritatea de supraveghere pune la dispoziție un formular de depunere a reclamației, care poate fi completat prin mijloace electronice, fără a exclude alte mijloace de comunicare.

5. Statele membre prevăd dispoziții potrivit cărora îndeplinirea funcțiilor autorității de supraveghere este gratuită pentru persoana vizată.

6. În cazul în care cererile sunt abuzive, în special din cauza caracterului repetitiv al acestora, autoritatea de supraveghere poate percepe o taxă sau poate să nu dea curs cererii persoanei vizate. Sarcina probei cu privire la caracterul abuziv al cererii revine autorității de supraveghere.

Articolul 46
Competențe

Statele membre prevăd dispoziții potrivit cărora fiecare autoritate de supraveghere trebuie investită, în special, cu următoarele competențe:

(a) competențe de investigare, cum ar fi competențe privind accesul la datele care fac obiectul operațiilor de prelucrare și competențe privind colectarea tuturor informațiilor necesare pentru îndeplinirea îndatoririlor sale de supraveghere;

(b) competențe efective de intervenție, cum ar fi competențe de a emite avize înainte ca operațiunile de prelucrare să fie efectuate și de a asigura publicarea corespunzătoare a acestor avize, de a ordona restricționarea, ștergerea sau distrugerea datelor, de a impune o interdicție temporară sau definitivă de

prelucrare, de a adresa operatorului un avertisment sau o mustrare sau de a sesiza parlamentele naționale sau alte instituții politice;

(c) competența de a acționa în justiție în cazul în care dispozițiile adoptate în temeiul prezentei directive au fost încălcate sau de a aduce aceste încălcări în atenția autorităților judiciare.

Articolul 47
Raport de activitate

Statele membre prevăd dispoziții potrivit cărora fiecare autoritate de supraveghere trebuie să întocmească un raport anual cu privire la activitățile sale. Acest raport este pus la dispoziția Comisiei și a Comitetului european pentru protecția datelor.

CAPITOLUL VII
COOPERARE

Articolul 48
Asistență reciprocă

1. Statele membre prevăd dispoziții potrivit cărora autoritățile de supraveghere își furnizează asistență reciprocă pentru a transpune și a pune în aplicare dispozițiile prezentei directive în mod coerent și instituie măsuri de cooperare eficace între ele. Asistența reciprocă se referă, în special, la cereri de informații și măsuri de control, cum ar fi cereri în vederea efectuării de consultări prealabile, inspecții și anchete.

2. Statele membre prevăd dispoziții potrivit cărora autoritatea de supraveghere ia toate măsurile corespunzătoare necesare pentru a răspunde solicitării formulate de o altă autoritate de supraveghere.

3. Autoritatea de supraveghere căreia i s-a adresat solicitarea informează autoritatea de supraveghere care a transmis solicitarea cu privire la rezultate sau, după caz, la progresele înregistrate ori măsurile întreprinse pentru a da curs solicitării respective.

Articolul 49
Sarcinile Comitetului european pentru protecția datelor

1. Comitetul european pentru protecția datelor instituit prin Regulamentul (UE) …./2012 exercită următoarele sarcini în ceea ce privește prelucrarea care intră sub incidența prezentei directive:

(a) să ofere Comisiei consiliere cu privire la orice aspect legat de protecția datelor cu caracter personal în cadrul Uniunii, inclusiv cu privire la orice propunere de modificare a prezentei directive;

(b) să analizeze, la cererea Comisiei, din proprie inițiativă sau la inițiativa unuia dintre membrii săi, orice chestiune referitoare la punerea în aplicare a dispozițiilor adoptate în temeiul prezentei directive și să emită orientări,

recomandări și bune practici adresate autorităților de supraveghere pentru a încuraja aplicarea uniformă a dispozițiilor respective;

(c) să revizuiască aplicarea practică a orientărilor, recomandărilor și bunelor practici menționate la litera (b) și să raporteze periodic Comisiei cu privire la acestea;

(d) să comunice Comisiei un aviz privind nivelul de protecție în țările terțe sau organizațiile internaționale;

(e) să promoveze cooperarea și schimbul eficient bilateral și multilateral de informații și practici între autoritățile de supraveghere;

(f) să promoveze programe comune de formare și să faciliteze schimburile de personal între autoritățile de supraveghere, precum și, după caz, cu autoritățile de supraveghere ale țărilor terțe sau organizațiilor internaționale;

(g) să promoveze schimbul de cunoștințe și de documente cu autoritățile de supraveghere a protecției datelor la nivel mondial, inclusiv privind legislația și practicile în materie de protecție a datelor.

2. În situațiile în care Comisia consultă Comitetul european pentru protecția datelor, aceasta poate stabili un termen în care Comitetul european pentru protecția datelor trebuie să comunice avizul său, ținând cont de caracterul urgent al chestiunii.

3. Comitetul european pentru protecția datelor își transmite avizele, orientările, recomandările și bunele practici Comisiei și comitetului menționat la articolul 57 alineatul (1) și le publică.

4. Comisia informează Comitetul european pentru protecția datelor cu privire la măsurile pe care le-a luat în urma avizelor, orientărilor, recomandărilor și bunelor practici emise de Comitetul european pentru protecția datelor.

CAPITOLUL VIII
CĂI DE ATAC, RĂSPUNDERE ȘI SANCȚIUNI

Articolul 50

Dreptul de a depune o plângere la o autoritate de supraveghere

1. Fără a aduce atingere oricăror alte căi de atac administrative sau judiciare, statele membre prevăd dispoziții potrivit cărora orice persoană vizată are dreptul de a depune o plângere la o autoritate de supraveghere în orice stat membru, în cazul în care consideră că prelucrarea datelor sale cu caracter personal nu respectă dispozițiile adoptate în temeiul prezentei directive.

2. Statele membre prevăd dispoziții potrivit cărora orice organism, organizație sau asociație a cărei activitate urmărește protecția drepturilor și intereselor persoanelor vizate cu privire la protecția datelor cu caracter personal ale acestora și care a fost constituită în mod adecvat, în conformitate cu legislația unui stat membru, are dreptul de a depune o plângere la o autoritate de supraveghere din orice stat membru în numele uneia sau mai multor persoane vizate, în cazul în care consideră că

drepturile de care persoanele vizate beneficiază în temeiul prezentei directive au fost încălcate ca urmare a prelucrării datelor cu caracter personal. Organizația sau asociația trebuie să fie mandatată în mod corespunzător de către persoana (persoanele) vizată(e).

3. Statele membre prevăd dispoziții potrivit cărora, independent de o plângere depusă de o persoană vizată, orice organism, organizație sau asociație menționată la alineatul (2) are dreptul de a depune o plângere la o autoritate de supraveghere din orice stat membru, în cazul în care consideră că a avut loc o încălcare a securității datelor cu caracter personal.

Articolul 51

Dreptul la o cale de atac judiciară împotriva unei autorități de supraveghere

1. Statele membre prevăd dreptul la o cale de atac judiciară împotriva deciziilor unei autorități de supraveghere.

2. Orice persoană vizată are dreptul de a exercita o cale de atac judiciară care să oblige autoritatea de supraveghere să dea curs unei plângeri, în absența unei decizii necesare pentru protejarea drepturilor sale sau în cazul în care autoritatea de supraveghere nu informează persoana vizată în termen de trei luni cu privire la progresele sau la soluționarea plângerii în temeiul articolului 45 alineatul (1) litera (b).

3. Statele membre prevăd dispoziții potrivit cărora acțiunile introduse împotriva unei autorități de supraveghere sunt înaintate instanțelor din statul membru în care este stabilită autoritatea de supraveghere.

Articolul 52

Dreptul la o cale de atac judiciară împotriva unui operator sau unei persoane împuternicite de operator

Fără a aduce atingere vreunei căi de atac administrative disponibile, inclusiv dreptului de a depune o plângere la o autoritate de supraveghere, statele membre prevăd dispoziții potrivit cărora orice persoană fizică are dreptul la exercitarea unei căi de atac judiciare, în cazul în care consideră că drepturile de care beneficiază conform dispozițiilor adoptate în temeiul prezentei directive au fost încălcate ca urmare a prelucrării datelor sale cu caracter personal efectuate încălcând dispozițiile respective.

Articolul 53

Norme comune aplicabile acțiunilor în instanță

1. Statele membre prevăd dispoziții potrivit cărora orice organism, organizație sau asociație menționată la articolul 50 alineatul (2) are dreptul de a exercita drepturile menționate la articolele 51 și 52 în numele uneia sau mai multor persoane vizate.

2. Fiecare autoritate de supraveghere are dreptul a participa la proceduri judiciare și de a sesiza o instanță, în scopul de a asigura aplicarea dispozițiilor adoptate în temeiul prezentei directive sau de a asigura coerența protecției datelor cu caracter personal în cadrul Uniunii.

3. Statele membre se asigură că acțiunile în justiție disponibile în dreptul intern permit adoptarea rapidă de măsuri, inclusiv măsuri provizorii, menite să ducă la încetarea oricărei încălcări presupuse și să prevină orice altă atingere adusă intereselor respective.

Articolul 54
Răspundere și dreptul la despăgubiri

1. Statele membre prevăd dispoziții potrivit cărora orice persoană care a suferit prejudicii ca urmare a unei operațiuni ilegale de prelucrare sau a unei acțiuni incompatibile cu dispozițiile adoptate în temeiul prezentei directive are dreptul să obțină despăgubiri de la operator sau de la persoana împuternicită de operator pentru prejudiciul suferit.

2. În cazul în care la prelucrare au participat mai mulți operatori sau persoane împuternicite de operator, fiecare operator sau persoană împuternicită de acesta sunt responsabile în mod solidar pentru întreaga valoare a prejudiciului.

3. Operatorul sau persoana împuternicită de operator poate fi total sau parțial exonerată de această răspundere, în cazul în care operatorul sau persoana împuternicită de acesta dovedește că nu este responsabilă pentru fapta care a provocat prejudiciul.

Articolul 55
Sancțiuni

Statele membre definesc normele privind sancțiunile aplicabile în cazul încălcării dispozițiilor adoptate în temeiul prezentei directive și iau toate măsurile necesare pentru a se asigura că acestea sunt puse în aplicare. Sancțiunile prevăzute trebuie să fie eficace, proporționale și disuasive.

CAPITOLUL IX
ACTE DELEGATE ȘI ACTE DE PUNERE ÎN APLICARE

Articolul 56
Exercitarea delegării de competențe

1. Competența de a adopta acte delegate este conferită Comisiei în condițiile prevăzute de prezentul articol.

2. Delegarea de competențe menționată la articolul 28 alineatul (5) îi este conferită Comisiei pentru o perioadă de timp nedeterminată, de la data intrării în vigoare a prezentei directive.

3. Delegarea de competențe menționată la articolul 28 alineatul (5) poate fi revocată în orice moment de către Parlamentul European sau de către Consiliu. O decizie de revocare pune capăt delegării de competențe precizată în decizia respectivă. Aceasta intră în vigoare în ziua următoare publicării deciziei în *Jurnalul Oficial al Uniunii Europene* sau la o dată ulterioară menționată în decizie. Aceasta nu aduce atingere validității actelor delegate aflate deja în vigoare.

4. De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului.

5. Un act delegat adoptat în temeiul articolului 28 alineatul (5) intră în vigoare numai în cazul în care nu a fost exprimată nicio obiecție din partea Parlamentului European sau Consiliului în termen de 2 luni de la notificarea acestui act Parlamentului European și Consiliului sau în cazul în care, înainte de expirarea acestei perioade, Parlamentul European și Consiliul informează Comisia că nu vor avea obiecții. Perioada se prelungește cu 2 luni, la inițiativa Parlamentului European sau a Consiliului.

Articolul 57
Procedura comitetului

1. Comisia este asistată de un comitet. 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.

3. Atunci când se face trimitere la prezentul alineat, se aplică articolul 8 din Regulamentul (UE) nr. 182/2011 coroborat cu articolul 5 din același regulament.

CAPITOLUL X
DISPOZIȚII FINALE

Articolul 58
Abrogări

1. Decizia-cadru 2008/977/JAI a Consiliului se abrogă.

2. Trimiterile la decizia-cadru abrogată menționată la alineatul (1) se interpretează ca trimiteri la prezenta directivă.

Articolul 59
Relația cu actele Uniunii adoptate anterior în domeniul cooperării judiciare în materie penală și al cooperării polițienești

Dispozițiile specifice referitoare la protecția datelor cu caracter personal cu privire la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, investigării, identificării sau urmăririi penale a infracțiunilor sau al executării pedepselor din actele Uniunii adoptate înainte de data adoptării prezentei directive, care reglementează prelucrarea datelor cu caracter personal între statele membre și accesul autorităților desemnate de statele membre la sistemele de informații instituite în temeiul tratatelor și care intră în domeniul de aplicare a prezentei directive nu sunt afectate.

Articolul 60

Relația cu acordurile internaționale încheiate anterior în domeniul cooperării judiciare în materie penală și al cooperării polițienești

Acordurile internaționale încheiate de către statele membre înainte de intrarea în vigoare a prezentei directive sunt modificate, dacă este necesar, în termen de cinci ani de la intrarea în vigoare a prezentei directive.

Articolul 61

Evaluare

1. Comisia evaluează punerea în aplicare a prezentei directive.

2. În termen de trei ani de la intrarea în vigoare a prezentei directive, Comisia revizuiește alte acte adoptate de Uniunea Europeană care reglementează prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, investigării, identificării sau urmăririi penale a infracțiunilor sau al executării pedepselor, în special a actelor adoptate de Uniune menționate la articolul 59, pentru a evalua necesitatea de a le alinia la prezenta directivă și prezintă, după caz, propunerile necesare de modificare a acestor acte pentru a asigura o abordare uniformă privind protecția datelor cu caracter personal care intră în domeniul de aplicare al prezentei directive.

3. Comisia transmite Parlamentului European și Consiliului, la intervale regulate, rapoarte privind evaluarea și revizuirea prezentei directive în temeiul alineatului (1). Primele rapoarte sunt transmise în termen de cel mult patru ani de la data intrării în vigoare a prezentei directive. Ulterior, următoarele rapoarte sunt transmise o dată la patru ani. Comisia transmite, dacă este necesar, propuneri corespunzătoare în vederea modificării prezentei directive, precum și a alinierii altor instrumente juridice. Raportul se publică.

Articolul 62

Punerea în aplicare

1. Statele membre adoptă și publică, până la cel târziu[data/doi ani de la intrarea în vigoare], actele cu putere de lege și actele administrative necesare pentru a se conforma prezentei directive. Statele membre notifică de îndată Comisiei textele acestor dispoziții.

   Statele membre aplică aceste dispoziții începând cu xx.xx.201x [data/doi ani de la intrarea în vigoare].

   Atunci când statele membre adoptă dispozițiile respective, acestea conțin o trimitere la prezenta directivă sau sunt însoțite de o astfel de trimitere la data publicării lor oficiale. Statele membre stabilesc modalitatea de efectuare a acestei trimiteri.

2. Statele membre comunică Comisiei textul principalelor dispoziții de drept intern pe care le adoptă în domeniul reglementat de prezenta directivă.

Articolul 63
Intrarea în vigoare și aplicarea

Prezenta directivă intră în vigoare în prima zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Articolul 64
Destinatari

Prezenta directivă se adresează statelor membre.

Adoptată la Bruxelles, 25.1.2012.

Pentru Parlamentul European	*Pentru Consiliu*
Președintele	*Președintele*