COMISIA EUROPEANĂ

Bruxelles, 25.1.2012
COM(2012) 11 final

2012/0011 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ŞI AL CONSILIULUI

privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal și libera circulație a acestor date (Regulament general privind protecția datelor)

(Text cu relevanță pentru SEE)

{SEC(2012) 72 final}
{SEC(2012) 73 final}

EXPUNERE DE MOTIVE

1. CONTEXTUL PROPUNERII

Prezenta expunere de motive descrie în detaliu noua propunere de cadru juridic privind protecția datelor cu caracter personal în UE, prevăzut în Comunicarea COM (2012) 9 final[1]. Noul cadru legislativ propus 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[2].

Prezenta expunere de motive se referă la propunerea de regulament general privind protecția datelor.

Documentul care stă la baza legislației UE existente privind protecția datelor cu caracter personal, Directiva 95/46/CE[3], a fost adoptat în 1995, aceasta având două obiective: protejarea dreptului fundamental la protecția datelor și garantarea liberei circulații a datelor cu caracter personal între statele membre. Aceasta a fost completată de Decizia-cadru 2008/977/JAI, un instrument general, la nivelul Uniunii, în scopul protecției datelor cu caracter personal în domeniul cooperării polițienești și judiciare în materie penală[4].

Evoluțiile tehnologice rapide au generat noi provocări în domeniul protecției datelor cu caracter personal. Amploarea schimbului și a colectării de date a crescut spectaculos. Tehnologia permite atât societăților private, cât și autorităților publice să utilizeze date cu caracter personal la un nivel fără precedent în cadrul activităților desfășurate. Din ce în ce mai multe persoane fizice la nivel mondial fac publice informații cu caracter personal. Tehnologia a transformat atât economia, cât și viața socială.

Consolidarea încrederii în mediul online este esențială pentru dezvoltarea economică. Lipsa de încredere îi determină pe consumatori să ezită să cumpere online și să apeleze la noi servicii. Aceasta poate conduce la încetinirea dezvoltării utilizărilor inovatoare ale noilor tehnologii. Prin urmare, protecția datelor cu caracter personal joacă un rol central în cadrul Agendei digitale pentru Europa[5] și, în mod mai general, în cadrul Strategiei Europa 2020[6].

---

1 „Protecția vieții private într-o lume interconectată - Un cadru european privind protecția datelor pentru secolul 21”, COM (2012) 9 final.

2 COM(2012) 10 final.

3 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, 23.11.1995, p. 31.

4 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 (denumită în continuare „decizia-cadru”).

5 COM(2010) 245 final.

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

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[7]. În rezoluția sa privind Programul de la Stockholm, Parlamentul European[8] a salutat inițiativa unui regim cuprinzător de protecție a datelor în UE și, printre altele, a făcut apel la revizuirea deciziei-cadru. Comisia a subliniat în planul său de acțiune pentru punerea în aplicare a programului de la Stockholm[9], necesitatea de a se asigura că dreptul fundamental la protecția datelor cu caracter personal este aplicat în mod consecvent în contextul tuturor politicilor UE.

În comunicarea sa privind „O abordare globală a protecției datelor cu caracter personal în Uniunea Europeană”[10], Comisia a concluzionat că UE are nevoie de o politică mai cuprinzătoare și mai coerentă privind dreptul fundamental la protecția datelor cu caracter personal.

Cadrul actual rămâne în continuare satisfăcător în ceea ce privește obiectivele și principiile, însă acesta nu a împiedicat fragmentarea modului în care protecția datelor cu caracter personal este pusă în aplicare pe întreg teritoriul Uniunii, incertitudinea juridică și percepția publică larg răspândită conform căreia există riscuri semnificative, în special asociate cu activitatea online[11]. Din acest motiv, ar trebui elaborat un cadru mai solid și mai coerent privind protecția datelor în UE, care, împreună cu o aplicare riguroasă a normelor în acest domeniu, vor permite economiei digitale să se dezvolte pe tot cuprinsul pieței interne, vor facilita deținerea controlului de către persoane asupra propriilor date și vor consolida securitatea juridică și practică pentru operatorii economici și autoritățile publice.

2. REZULTATELE CONSULTĂRILOR CU PĂRȚILE INTERESATE ȘI ALE EVALUĂRII IMPACTULUI

Prezenta inițiativă este rezultatul unor ample consultări cu principalele părți interesate privind o revizuire a actualului cadru juridic privind protecția datelor cu caracter personal, care au durat peste doi ani, incluzând o conferință la nivel înalt desfășurată în mai 2009[12] și două faze ale consultării publice:

---

6 COM(2010) 2020 final.

7 „Programul de la Stockholm — O Europă deschisă și sigură în serviciul cetățenilor și pentru protecția acestora”, JO C 115, 4.5.2010, p. 1.

8 Rezoluția Parlamentului European privind Comunicarea Comisiei către Parlamentul European și Consiliu – Un spațiu de libertate, securitate și justiție în serviciul cetățenilor – Programul de la Stockholm, adoptat la 25 noiembrie 2009 [P7_TA (2009) 0090].

9 COM(2010) 171 final.

10 COM(2010) 609 final.

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 http://ec.europa.eu/justice/newsroom/data-protection/events/090519_en.htm.

– 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[13];

– 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[14].

De asemenea, s-au desfășurat consultări specifice cu principalele părți interesate; în iunie și iulie 2010, au fost organizate evenimente specifice cu autoritățile statelor membre și cu părțile interesate din sectorul privat, precum și cu organizații din domeniul protecției vieții private, a datelor și a consumatorilor[15]. În noiembrie 2010, vicepreședintele Comisiei Europene, Viviane Reding, a organizat o masă rotundă privind reforma în materie de protecție a datelor. La 28 ianuarie 2011 (Ziua protecției datelor), Comisia Europeană și Consiliul Europei au organizat o conferință comună la nivel înalt pentru a discuta aspecte referitoare la reforma cadrului juridic al UE, precum și la necesitatea unor standarde comune privind protecția datelor la nivel mondial[16]. Două conferințe privind protecția datelor au fost găzduite de președințiile ungară și poloneză ale Consiliului la 16-17 iunie 2011 și, respectiv, la 21 septembrie 2011.

Pe tot parcursul anului 2011, s-au organizat ateliere și seminarii pe teme specifice. În ianuarie, ENISA[17]a organizat un atelier privind notificările referitoare la încălcarea securității datelor în Europa[18]. În februarie, Comisia a organizat un atelier cu autoritățile din statele membre pentru a discuta aspecte legate de protecția datelor în domeniul cooperării polițienești și judiciare în materie penală, inclusiv punerea în aplicare a deciziei-cadru, iar Agenția pentru Drepturi Fundamentale a Uniunii Europene a organizat o reuniune de consultare cu părțile interesate privind „protecția datelor și a vieții private". La 13 iulie 2011, a avut loc o dezbatere cu autoritățile naționale pentru protecția datelor pe tema aspectelor-cheie ale reformei. Cetățenii UE au fost consultați prin intermediul unui sondaj Eurobarometru organizat în perioada noiembrie-decembrie 2010[19]. De asemenea, a fost lansată a serie de studii[20]. Grupul de lucru

---

13 Contribuțiile care nu au caracter confidențial pot fi consultate pe site-ul internet al Comisiei. http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm.

14 Contribuțiile care nu au caracter confidențial pot fi consultate pe site-ul internet al Comisiei. http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104_en.htm.

15 http://ec.europa.eu/justice/newsroom/data-protection/events/100701_en.htm.

16 http://www.coe.int/t/dghl/standardsetting/dataprotection/Data_protection_day2011_en.asp.

17 Agenția Europeană pentru Securitatea Rețelelor Informatice și a Datelor, care se ocupă cu chestiuni în materie de securitate legate de rețelele de comunicații și sistemele informatice.

18 A se vedea http://www.enisa.europa.eu/act/it/data-breach-notification.

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

20 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)..

pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal[21] a furnizat mai multe avize și informații utile Comisiei[22]. De asemenea, Autoritatea Europeană pentru Protecția Datelor a emis un aviz cuprinzător privind problemele ridicate în comunicarea Comisiei din noiembrie 2010[23].

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[24]. La 24 februarie 2011, Consiliul Uniunii Europene a adoptat concluzii în care sprijină 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 a Directivei 95/46/CE, sprijinind obiectivul Comisiei de a asigura o aplicare mai coerentă a normelor UE în materie de protecție a datelor[25] în toate statele membre[26].

Pe parcursul consultărilor privind abordarea globală, o mare majoritate a părților interesate au fost de acord că principiile generale rămân valabile, însă este necesară adaptarea cadrului actual pentru a răspunde mai bine provocărilor generate de dezvoltarea rapidă a noilor tehnologii (în special, cele online) și de globalizarea în continuă creștere, menținând totodată neutralitatea tehnologică a cadrului juridic. Fragmentarea actuală a protecției datelor cu caracter personal în Uniunea Europeană a făcut obiectul unor critici vehemente, în special din partea părților interesate din domeniul economic care au solicitat o mai mare securitate juridică și armonizarea normelor privind protecția datelor cu caracter personal. În conformitate cu opinia părților, complexitatea normelor privind transferurile internaționale de date cu caracter personal constituie un impediment considerabil pentru operațiunile desfășurate, deoarece acestea trebuie să transfere în mod regulat date cu caracter personal din UE către alte părți ale lumii.

În conformitate cu politica sa privind „o mai bună legiferare”, Comisia a realizat o evaluare a impactului privind politicile alternative. 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

---

21 Grupul de lucru a fost înființat în 1996 (prin articolul 29 din Directiva 95/46/CE), 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.

22 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 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 privind protecția datelor. Documentele pot fi consultate la adresa: http://ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm.

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

24 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)].

25 SEC (2012) 72.

26 CESE 999/2011.

elaborarea unui cadru cuprinzător și coerent care acoperă toate domeniile de competență ale Uniunii, inclusiv cooperarea polițienească și judiciară în materie penală. Au fost evaluate trei opțiuni de politică cu grade de intervenție diferite: prima opțiune consta în aducerea unor modificări legislative minime și în utilizarea unor comunicări interpretative și a unor măsuri de sprijin în materie de politici, cum ar fi programe de finanțare și instrumente tehnice; a doua opțiune cuprindea un set de dispoziții legislative care să abordeze toate aspectele identificate în studiu, iar a treia opțiune consta în centralizarea protecției datelor la nivelul UE prin intermediul unor norme precise și detaliate cu privire la toate sectoarele, precum și crearea unei agenții a UE pentru monitorizarea și punerea în aplicare a dispozițiilor.

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. În urma analizei impactului global al diferitelor opțiuni, a fost privilegiată o opțiune de politică care se bazează pe cea de-a doua opțiune menționată anterior, la care se adaugă anumite elemente din cadrul celorlalte opțiuni și care este încorporată în prezenta propunere. Conform studiului de impact, punerea în aplicare a acestei opțiuni va conduce, printre altele, la îmbunătățiri considerabile în ceea ce privește securitatea juridică pentru operatorii de date și cetățeni, la reducerea sarcinilor administrative, la o aplicare mai coerentă a legislației privind protecția datelor în Uniune, la posibilitatea efectivă a persoanelor de a-și exercita drepturile în materie de protecție a datelor, la protejarea datelor cu caracter personal în cadrul UE și la o îmbunătățire a eficienței în ceea ce privește supravegherea și controlul aplicării normelor în acest domeniu. De asemenea, se așteaptă ca punerea în aplicare a opțiunilor de politică preferate să contribuie la îndeplinirea obiectivului Comisiei privind simplificarea și reducerea sarcinii administrative și a obiectivelor Agendei digitale pentru Europa, Planului de acțiune de la Stockholm și Strategiei Europa 2020.

Comitetul de evaluare a impactului a emis, la 9 septembrie 2011, un aviz cu privire la proiectul de evaluare a impactului, pe baza căruia i-au fost aduse 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;

– a fost adăugată o secțiune privind proporționalitatea;

– au fost pe deplin revizuite toate calculele și estimările privind sarcina administrativă din scenariul de bază și din opțiunea preferată, iar relația dintre costurile notificărilor și costurile generale ale fragmentării a fost clarificată (inclusiv anexa 10);

– au fost mai bine precizate impacturile asupra microîntreprinderilor și asupra întreprinderilor mici și mijlocii, în special cele privind desemnarea unor responsabili cu protecția datelor și realizarea unor studii de impact privind protecția datelor.

Raportul privind studiul de impact și rezumatul acestuia sunt publicate împreună cu propunerile.

3. ELEMENTELE JURIDICE ALE PROPUNERII

3.1. Temei juridic

Prezenta propunere se bazează pe articolul 16 din TFUE, care este noul temei juridic pentru adoptarea normelor în materie de protecție a datelor introduse prin Tratatul de la Lisabona. Această dispoziție permite adoptarea unor norme privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către statele membre, atunci când desfășoară activități care intră în domeniul de aplicare a dreptului Uniunii. De asemenea, permite adoptarea de norme referitoare la libera circulație a datelor cu caracter personal, inclusiv datele prelucrate de statele membre sau entități private.

Se consideră că regulamentul este instrumentul juridic cel mai adecvat pentru definirea cadrului privind protecția datelor cu caracter personal în Uniune. Aplicabilitatea directă a unui regulament în conformitate cu articolul 288 din TFUE va reduce fragmentarea legislativă și va oferi o mai mare securitate juridică prin introducerea unui ansamblu armonizat de reguli de bază, contribuind la îmbunătățirea protecției drepturilor fundamentale ale persoanelor și la funcționarea pieței interne.

Trimiterea la articolul 114 alineatul (1) din TFUE este necesară doar pentru modificarea Directivei 2002/58/CE, în măsura în care directiva respectivă prevede, de asemenea, dispoziții referitoare la protecția intereselor legitime ale abonaților care sunt persoane juridice.

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, pe baza următoarelor motive:

– dreptul la protecția datelor cu caracter personal, prevăzut la articolul 8 din Carta drepturilor fundamentale a Uniunii Europene, necesită același nivel de protecție a datelor pe tot cuprinsul Uniunii. Absența unor norme comune ale UE ar crea riscul unor niveluri diferite de protecție în statele membre și al apariției unor restricții privind fluxurile transfrontaliere de date cu caracter personal între statele membre cu standarde diferite în materie de protecție a datelor;

– datele cu caracter personal sunt transferate din ce în ce mai rapid dincolo de granițele naționale, atât interne, cât și externe. 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. De asemenea, 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 vor 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.

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[27], dreptul la protecția datelor cu caracter personal nu este, totuși, un drept absolut, ci trebuie să fie luat în considerare în raport cu funcția sa în societate[28]. 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.

Este posibil să fie afectate și alte drepturi fundamentale consacrate în cartă: libertatea de exprimare (articolul 11 din cartă); libertatea de a desfășura o activitate comercială (articolul 16); dreptul la proprietate și, în special, protecția proprietății intelectuale [articolul 17 alineatul (2)]; 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 un nivel ridicat de protecție a sănătății umane (articolul 35); dreptul de acces la documente (articolul 42); dreptul la o cale de atac eficientă și la un proces echitabil (articolul 47).

3.4. Explicarea detaliată a propunerii

3.4.1. CAPITOLUL I - DISPOZIȚII GENERALE

Articolul 1 definește obiectul regulamentului, și, precum articolul 1 din Directiva 95/46/CE, stabilește cele două obiective prevăzute de regulament.

Articolul 2 stabilește domeniul material de aplicare al regulamentului.

---

27 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.

28 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.

Articolul 3 definește domeniul teritorial de aplicare a regulamentului.

Articolul 4 conține definițiile termenilor utilizați în regulament. Unele definiții sunt preluate din Directiva 95/46/CE, în timp ce altele sunt modificate, completate cu elemente suplimentare sau nou introduse („încălcarea datelor cu caracter personal”, pe baza articolului 2 litera (h) din Directiva 2002/58/CE asupra confidențialității și comunicațiilor electronice[29], astfel cum a fost modificată prin Directiva 2009/136/CE[30], „date genetice”, „date biometrice”, „date privind sănătatea”, „sediu principal”, „reprezentant”, „întreprindere”, „grup de întreprinderi”, „reguli corporatiste obligatorii”, „copil”, a cărui definiție se bazează pe Convenția Națiunilor Unite privind drepturile copilului[31], și „autoritate de supraveghere”).

În definiția noțiunii de „consimțământ”, se adaugă criteriul „explicit” pentru a se evita orice paralelism care poate crea confuzie cu noțiunea de „consimțământ neechivoc” și pentru a dispune de o definiție unică și coerentă a consimțământului, în vederea garantării faptului că persoana în cauză își dă consimțământul în deplină cunoștință de cauză.

3.4.2. CAPITOLUL II – PRINCIPII

Articolul 5 enunță principiile legate de prelucrarea datelor cu caracter personal, care corespund celor prevăzute la articolul 6 din Directiva 95/46/CE. Noile elemente adăugate sunt, în special, principiul transparenței, clarificarea principiului minimizării datelor și instituirea unei responsabilități globale a operatorului.

Articolul 6 prezintă, pe baza articolului 7 din Directiva 95/46/CE, criteriile privind legalitatea prelucrării, fiind descrise în detaliu diverse aspecte ale acestora, cum ar fi criteriul privind echilibrul intereselor, precum și respectarea obligațiilor juridice și a interesului public.

Articolul 7 clarifică condițiile în care consimțământul constituie un temei juridic valabil pentru legalitatea prelucrării.

Articolul 8 stabilește condiții suplimentare pentru legalitatea prelucrării datelor cu caracter personal ale copiilor în ceea ce privește serviciile societății informaționale care sunt oferite direct acestora.

Articolul 9 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.

---

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

[30] Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 de modificare a Directivei 2002/22/CE privind serviciul universal și drepturile utilizatorilor cu privire la rețelele și serviciile de comunicații electronice, a Directivei 2002/58/CE privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice și a Regulamentului (CE) nr. 2006/2004 privind cooperarea dintre autoritățile naționale însărcinate să asigure aplicarea legislației în materie de protecție a consumatorului (Text cu relevanță pentru SEE), JO L 337, 18.12.2009, p. 11.

[31] Adoptată și deschisă spre semnare, ratificare și aderare prin Rezoluția Adunării generale a Organizației Națiunilor Unite 44/25 din 20.11.1989.

Articolul 10 clarifică faptul că operatorul nu este obligat să obțină informații suplimentare în vederea identificării persoanei vizate cu unicul scop de a respecta una dintre dispozițiile prezentului regulament.

3.4.3. CAPITOLUL III - DREPTURILE PERSOANEI VIZATE

3.4.3.1. Secțiunea 1 – Transparență și modalități

Articolul 11 introduce obligația pe care o au operatorii de a furniza informații transparente, ușor accesibile și inteligibile, această dispoziție fiind inspirată, în special, din Rezoluția de la Madrid privind standardele internaționale în materie de protecție a datelor cu caracter personal și a vieții private[32].

Articolul 12 stabilește obligația operatorului de a prevedea proceduri și mecanisme pentru exercitarea drepturilor persoanei vizate, inclusiv mijloace pentru introducerea unor cereri pe cale electronică, stabilirea unui termen pentru oferirea unui răspuns la o cerere a persoanei vizate și motivarea refuzurilor.

Articolul 13 prevede, pe baza articolului 12 litera (c) din Directiva 95/46/CE, drepturile referitoare la destinatari care sunt extinse astfel încât să includă toți destinatarii, inclusiv operatorii asociați și persoanele împuternicite de către operator.

3.4.3.2. Secțiunea 2 – Informare și acces la date

Articolul 14 prevede, pe baza articolelor 10 și 11 din Directiva 95/46/CE, obligațiile în materie de informare ale operatorului față de persoana vizată și furnizează informații suplimentare, inclusiv privind perioada de stocare a datelor și dreptul de a înainta o plângere, în ceea ce privește transferurile internaționale și sursa de proveniență a datelor. De asemenea, articolul menține posibilele derogări cuprinse în Directiva 95/46/CE, de exemplu, lipsa obligației de informare în cazul în care înregistrarea sau comunicarea datelor sunt prevăzute în mod expres de legislație. Această situație s-ar putea aplica, de exemplu, în cadrul procedurilor desfășurate de autoritățile din domeniul concurenței, de administrațiile fiscale sau vamale sau de serviciile competente în materie de securitate socială.

Articolul 15 prevede dreptul de acces al persoanei vizate la datele sale cu caracter personal, pe baza articolului 12 litera (a) din Directiva 95/46/CE la care se adaugă elemente noi, cum ar fi informarea persoanelor vizate cu privire la perioada de stocare a datelor, la dreptul acestora privind rectificarea și ștergerea datelor, precum și la dreptul de a depune o plângere.

3.4.3.3. Secțiunea 3 – Rectificare și ștergere

Articolul 16 prevede, pe baza articolului 12 litera (b) din Directiva 95/46/CE, dreptul persoanei vizate la rectificarea datelor.

Articolul 17 conferă persoanei vizate „dreptul de a fi uitat” și dreptul la ștergerea datelor cu caracter personal. Articolul dezvoltă și descrie dreptul la ștergerea datelor prevăzut la articolul 12 litera (b) din Directiva 95/46/CE, stabilind condițiile care stau la baza dreptului de

---

[32] Adoptată în cadrul Conferinței internaționale a comisarilor pentru protecția datelor și a vieții private din 5 noiembrie 2009. De asemenea, conform articolului 13 alineatul (3) din propunerea de regulament privind Legislația europeană comună în materie de vânzare [COM (2011) 635 final].

a fi uitat, inclusiv obligația operatorului care a făcut publice datele cu caracter personal de a informa părțile terțe cu privire la cererea persoanei vizate privind ștergea orice linkuri către datele sale cu caracter personal, sau orice copie sau reproducere a acestora. De asemenea, articolul integrează dreptul de limitare a prelucrării datelor în anumite cazuri, evitând termenul echivoc de „blocare”.

Articolul 18 introduce dreptul persoanei vizate la portabilitatea datelor, adică de a transfera date de la un sistem electronic de procesare la altul, fără a fi împiedicată de către operator să facă acest lucru. Ca o condiție preliminară și pentru a îmbunătăți în continuare accesul persoanelor la datele lor cu caracter personal, articolul prevede dreptul de a obține datele respective din partea operatorului într-o formă structurată și într-un format electronic utilizat în mod curent.

3.4.3.4. Secțiunea 4 - Dreptul la opoziție și crearea de profiluri

Articolul 19 prevede dreptul la opoziție al persoanei vizate. Acesta are la bază articolul 14 din Directiva 95/46/CE, la care aduce unele modificări, inclusiv în ceea ce privește sarcina probei și aplicarea acesteia în cazul marketingului direct.

Articolul 20 se referă la dreptul persoanei vizate de a nu fi supus unei măsuri bazate pe crearea de profiluri. Acesta are la bază articolul 15 alineatul (1) din Directiva 95/46 privind deciziile individuale automatizate, cu unele modificări și garanții suplimentare, luând în considerare Recomandarea Consiliului Europei referitoare la crearea de profiluri[33].

3.4.3.5. Secțiunea 5 - Restricții

Articolul 21 precizează măsura în care Uniunea sau statele membre pot menține sau introduce restricții cu privire la principiile stabilite la articolul 5 și cu privire la drepturile persoanei vizate, prevăzute la articolele 11 - 20 și la articolul 32. Această dispoziție se bazează pe articolul 13 din Directiva 95/46/CE și pe cerințele care derivă din Carta drepturilor fundamentale a Uniunii Europene și din Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale, astfel cum au fost interpretate de către Curtea de Justiție a Uniunii Europene și Curtea Europeană a Drepturilor Omului.

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

3.4.4.1. Secțiunea 1 — Obligații generale

Articolul 22 ia în considerare dezbaterea privind un „principiu al responsabilității” și descrie în detaliu obligația operatorului de a respecta dispozițiile prezentului regulament și de a demonstra acest lucru, inclusiv prin intermediul adoptării de politici interne și de mecanisme care să garanteze această conformitate.

Articolul 23 stabilește obligațiile operatorului care decurg din principiile privind protecția datelor începând cu momentul conceperii și protecția implicită a datelor.

---

[33] CM/Rec (2010) 13.

Articolul 24 se referă la operatorii asociați și clarifică responsabilitățile acestora în ceea ce privește relațiilor lor interne și cele cu persoana vizată.

Articolul 25 prevede obligația ca, în anumite condiții, operatorii care își au sediul în afara Uniunii să își desemneze un reprezentant în cadrul Uniunii, în cazul în care regulamentul se aplică activităților de prelucrare a datelor desfășurate de aceștia.

Articolul 26 clarifică poziția și obligațiile persoanelor împuternicite de către operator, bazându-se, în parte, pe articolul 17 alineatul (2) din Directiva 95/46/CE, la care adaugă elemente noi, inclusiv faptul că o persoană împuternicită care prelucrează date într-un alt mod decât cel prevăzut de instrucțiunile date de operator trebuie considerată ca fiind un operator asociat.

Articolul 27 privind prelucrarea datelor sub autoritatea operatorului și a persoanei împuternicite de către operator se bazează pe articolul 16 din Directiva 95/46/CE.

Articolul 28 introduce obligația pentru operatori și persoanele împuternicite de către operator de a păstra o documentație a operațiunilor de prelucrare aflate în responsabilitatea lor, în locul unei notificări generale a autorității de supraveghere prevăzute la articolul 18 alineatul (1) și la articolul 19 din Directiva 95/46/CE.

Articolul 29 clarifică obligațiile operatorului și ale persoanei împuternicite de operator în ceea ce privește cooperarea cu autoritatea de supraveghere.

3.4.4.2. Secțiunea 2 – Securitatea datelor

Articolul 30 prevede, pe baza articolului 17 alineatul (1) din Directiva 95/46/CE, obligația ca operatorul și persoana împuternicită de către operator să pună în aplicare măsurile adecvate pentru securizarea prelucrării datelor, extinzând această obligație la persoanele împuternicite de către operator, indiferent de tipul de contract încheiat cu operatorul.

Articolele 31 și 32 introduc obligația de a notifica încălcarea securității datelor cu caracter personal, care se întemeiază pe încălcarea securității datelor cu caracter personal prevăzută la articolul 4 alineatul (3) din Directiva 2002/58/CE asupra confidențialității și comunicațiilor electronice.

3.4.4.3. Secțiunea 3 – Evaluare a impactului cu privire la protecția datelor și autorizație prealabilă

Articolul 33 introduce obligația operatorilor și a persoanelor împuternicite de către operator de a efectua o evaluare a impactului cu privire la protecția datelor înaintea desfășurării unor operațiuni riscante de prelucrare a datelor.

Articolul 34, care dezvoltă conceptul de verificare prealabilă prevăzut la articolul 20 din Directiva 95/46/CE, se referă la cazurile în care autorizarea de către autoritatea de supraveghere și consultarea acesteia sunt obligatorii înainte de prelucrarea datelor.

3.4.4.4. Secțiunea 4 – Responsabilul cu protecția datelor

Articolul 35 introduce obligativitatea desemnării unui responsabilul cu protecția datelor pentru sectorul public și, în sectorul privat, pentru întreprinderile mari sau în cazurile în care activitățile principale ale operatorului sau ale persoanei împuternicite de către operator

constau în operațiuni de prelucrare a datelor care necesită o monitorizare regulată și sistematică. Această dispoziție are la bază articolul 18 alineatul (2) din Directiva 95/46/CE, care prevedea posibilitatea ca statele membre să introducă o astfel de cerință în locul cerinței de notificare generală.

Articolul 36 definește funcția de responsabil cu protecția datelor.

Articolul 37 prevede sarcinile principale ale responsabilului cu protecția datelor.

3.4.4.5. Secțiunea 5 – Coduri de conduită și certificare

Articolul 38 se referă la codurile de conduită, bazându-se pe conceptul de la articolul 27 alineatul (1) din Directiva 95/46/CE și clarifică conținutul codurilor și al procedurilor, împuternicind Comisia să decidă asupra validității generale a codurilor de conduită.

Articolul 39 introduce posibilitatea stabilirii unor mecanisme de certificare, precum și a unor sigilii și mărci în domeniul protecției datelor.

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

Articolul 40 prevede, ca principiu general, că respectarea obligațiilor menționate la acest capitol este obligatorie pentru orice transferuri de date cu caracter personal către țări terțe sau organizații internaționale, inclusiv transferurile ulterioare.

Articolul 41 stabilește, pe baza articolului 25 din Directiva 95/46/CE, criteriile, condițiile și procedurile pentru adoptarea de către Comisie a unei decizii privind caracterul adecvat al nivelului de protecție. Criteriile care vor fi luate în considerare în evaluarea efectuată de Comisie cu privire la gradul de adecvare al nivelului de protecție includ, în mod explicit, respectarea statului de drept, accesul la justiție și controlul independent. În forma actuală, articolul confirmă în mod explicit posibilitatea Comisiei de a evalua nivelul de protecție asigurat de un teritoriu sau de un sector de prelucrare a datelor dintr-o țară terță.

Articolul 42 prevede ca transferurile către țările terțe, cu privire la care Comisia nu a adoptat o decizie privind caracterul adecvat al nivelului de protecție, să prezinte garanții corespunzătoare, în special clauze standard de protecție a datelor, reguli corporatiste obligatorii și clauze contractuale. Posibilitatea de a face uz de clauzele standard ale Comisiei de protecție a datelor se bazează pe articolul 26 alineatul (4) din Directiva 95/46/CE. Ca element de noutate, în prezent, astfel de clauze standard de protecție a datelor ar putea fi, de asemenea, adoptate de o autoritate de supraveghere și declarate ca fiind general valabile de către Comisie. În prezent, regulile corporatiste obligatorii sunt menționate în mod specific în textul legislativ. Opțiunea privind clauzele contractuale oferă o anumită flexibilitate operatorului sau persoanei împuternicite de operator, sub rezerva autorizării prealabile de către autoritățile de supraveghere.

Articolul 43 descrie mai detaliat condițiile aplicabile transferurilor în baza regulilor corporatiste obligatorii, în temeiul practicilor și cerințelor actuale ale autorităților de supraveghere.

Articolul 44 definește și clarifică, pe baza dispozițiilor existente la articolul 26 din Directiva 95/46/CE, derogările aplicabile în cazul realizării unui transfer de date. Această

dispoziție se aplică, în special, transferurilor de date solicitate și necesare din motive importante, de interes public, de exemplu în cazul transferurilor internaționale de date între autoritățile de concurență, administrațiile fiscale sau vamale sau între servicii competente în materie de securitate socială sau de gestionare a pescuitului. În plus, un transfer de date poate, în situații limitate, să fie justificat de un interes legitim al operatorului sau al persoanei împuternicite de către operator, dar numai după evaluarea și documentarea circumstanțelor operațiunii de transfer respective.

Articolul 45 prevede în mod explicit elaborarea unor mecanisme de cooperare internațională privind protecția datelor cu caracter personal între Comisie și autoritățile de supraveghere din țările terțe, în special cele considerate ca asigurând un nivel de protecție adecvat, luând în considerare recomandarea Organizației pentru Cooperare și Dezvoltare Economică (OCDE) privind cooperarea transfrontalieră în aplicarea legislației privind protejarea confidențialității din 12 iunie 2007.

3.4.6. CAPITOLUL VI - AUTORITĂȚI INDEPENDENTE DE SUPRAVEGHERE

3.4.6.1. Secțiunea 1 – Statut independent

Articolul 46 prevede, pe baza articolului 28 alineatul (1) din Directiva 95/46/CE, obligația ca statele membre să instituie autorități de supraveghere, extinzând sfera de aplicare a misiunilor acestora astfel încât să cuprindă cooperarea între ele și cooperarea cu Comisia.

Articolul 47 clarifică condițiile de garantare a independenței autorităților de supraveghere, prin aplicarea jurisprudenței Curții de Justiție a Uniunii Europene[34] și, de asemenea, inspirându-se din articolul 44 din Regulamentul (CE) nr. 45/2001[35].

Articolul 48 prevede condițiile generale aplicabile membrilor autorității de supraveghere, prin aplicarea jurisprudenței relevante[36] și, de asemenea, inspirându-se din articolul 42 alineatele (2) - (6) din Regulamentul (CE) nr. 45/2001.

Articolul 49 prezintă normele privind instituirea autorității de supraveghere, pe care statele membre trebuie să le prevadă pe cale legislativă.

Articolul 50 prevede dispozițiile privind secretul profesional aplicabile membrilor și personalului autorității de supraveghere, acestea fiind bazate pe articolul 28 alineatul (7) din Directiva 95/46/CE.

3.4.6.2. Secțiunea 2 – Atribuții și competențe

Articolul 51 definește competența autorităților de supraveghere. Regula generală, bazată pe articolul 28 alineatul (6) din Directiva 95/46/CE (competența pe teritoriul propriului stat membru), este completată de către o nouă competență, cea de autoritate principală, în cazul în care același operator sau aceeași persoană împuternicită de către operator este numită în mai multe state membre pentru a se asigura o aplicare uniformă („ghișeu unic”). Atunci când

---

34 Curtea de Justiție a UE, hotărârea din 9.3.2010, Comisia/Germania, cauza C-518/07, ECR 2010 p. I-1885.

35 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.

36 Op. cit, nota de subsol 34.

acționează în capacitatea lor judiciară, instanțele sunt scutite de obligativitatea controlului de către autoritatea de supraveghere, însă nu de aplicarea normelor de fond în materie de protecție a datelor.

Articolul 52 prevede atribuțiile autorității de supraveghere, inclusiv audierea și examinarea plângerilor, precum și sensibilizarea publicului cu privire la riscurile, normele, garanțiile și drepturile cu privire la prelucrarea datelor cu caracter personal.

Articolul 53 prevede funcțiile autorității de supraveghere, bazându-se parțial pe articolul 28 alineatul (3) din Directiva 95/46/CE și pe articolul 47 din Regulamentul (CE) nr. 45/2001, la care adaugă unele elemente noi, inclusiv funcția de a sancționa infracțiunile administrative.

Articolul 54 prevede, pe baza articolului 28 alineatul (5) din Directiva 95/46/CE, obligația ca autoritățile de supraveghere să elaboreze rapoarte anuale de activitate.

3.4.7. CAPITOLUL VII – COOPERARE ȘI COERENȚĂ

3.4.7.1. Secțiunea 1 – Cooperarea

Articolul 55 introduce, pe baza articolului 28 alineatul (6) al doilea paragraf din Directiva 95/46/CE, norme explicite privind asistența reciprocă obligatorie, inclusiv sancțiunile în cazul nerespectării unei solicitări din partea altei autorități de supraveghere.

Articolul 56 introduce, pe baza articolului 17 din Decizia 2008/615/JAI[37], norme privind operațiunile comune, inclusiv dreptul autorităților de supraveghere de a participa la astfel de operațiuni.

3.4.7.2. Secțiunea 2 – Coerența

Articolul 57 introduce un mecanism pentru asigurarea coerenței în scopul aplicării uniforme a operațiunilor de prelucrare a datelor referitoare la persoane vizate în mai multe state membre.

Articolul 58 stabilește procedurile și condițiile pentru solicitarea unui aviz al Comitetului european pentru protecția datelor.

Articolul 59 se referă la avizele Comisiei privind aspecte abordate în cadrul mecanismului pentru asigurarea coerenței, care pot fie să confirme avizul Comitetului european pentru protecția datelor, fie să fie contrare acestui aviz, și privind proiectul de măsuri transmis de autoritatea de supraveghere. În cazul în care chestiunea a fost ridicată de către Comitetul european pentru protecția datelor, în conformitate cu articolul 58 alineatul (3), Comisia este susceptibilă să-și exercite puterea de apreciere și să emită un aviz ori de câte ori este necesar.

Articolul 60 se referă la deciziile Comisiei prin care se solicită autorității competente să își suspende proiectul de măsuri în cazul în care acest lucru este necesar pentru a se asigura aplicarea corectă a prezentului regulament.

Articolul 61 prevede posibilitatea adoptării de măsuri provizorii pe baza unei proceduri de urgență.

---

[37] Decizia 2008/615/JAI a Consiliului din 23 iunie 2008 privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere, JO L 210, 6.8.2008, p. 1.

Articolul 62 definește cerințele privind adoptarea actelor de punere în aplicare ale Comisie în cadrul mecanismului pentru asigurarea coerenței.

Articolul 63 prevede obligativitatea aplicării măsurilor prevăzute de o autoritate de supraveghere în toate statele membre în cauză, precizând că aplicarea mecanismului pentru asigurarea coerenței este o condiție prealabilă pentru valabilitatea juridică și aplicarea măsurii respective.

3.4.7.3. Secțiunea 3 – Comitetul european pentru protecția datelor

Articolul 64 instituie Comitetul european pentru protecția datelor, compus din șefii autorităților de supraveghere din fiecare stat membru și cei ai Autorității Europene pentru Protecția Datelor. Comitetul european pentru protecția datelor înlocuiește Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, înființat în temeiul articolului 29 din Directiva 95/46/CE. Articolul clarifică faptul că, în ceea ce privește Comisia, aceasta nu este membră a Comitetului european pentru protecția datelor, însă are dreptul de a participa la activitățile acestuia și de a fi reprezentat în cadrul său.

Articolul 65 subliniază și clarifică independența Comitetului european pentru protecția datelor.

Articolul 66 descrie, pe baza articolului 30 alineatul (1) din Directiva 95/46/CE, sarcinile Comitetului european pentru protecția datelor și prevede elemente suplimentare care reflectă extinderea domeniului de activitate al Comitetului atât în interiorul, cât și în afara Uniunii. Articolul prevede faptul că, pentru a fi capabilă să reacționeze în situații de urgență, Comisia are posibilitatea de a solicita un aviz într-un anumit termen.

Articolul 67 prevede, pe baza articolului 30 alineatul (6) din Directiva 95/46/CE, obligația Comitetului european pentru protecția datelor de a prezenta un raport anual cu privire la activitățile sale.

Articolul 68 stabilește procedurile de luare a deciziilor aplicate de Comitetul european pentru protecția datelor, inclusiv obligația acestuia de a adopta un regulament de procedură care ar trebui să cuprindă și mecanismele sale de funcționare.

Articolul 69 cuprinde dispozițiile privind președintele și vicepreședinții Comitetului european pentru protecția datelor.

Articolul 70 stabilește sarcinile președintelui.

Articolul 71 prevede că secretariatul Comitetului european pentru protecția datelor trebuie să fie asigurat de Autoritatea Europeană pentru Protecția Datelor și precizează sarcinile secretariatului.

Articolul 72 prezintă normele privind confidențialitatea.

3.4.8. CAPITOLUL VIII – CĂI DE ATAC, RĂSPUNDERE ȘI SANCȚIUNI

Articolul 73 prevede, pe baza articolului 28 alineatul (4) din Directiva 95/46/CE, dreptul oricărei persoane vizate de a depune o plângere la o autoritate de supraveghere. De asemenea, acesta specifică organismele, organizațiile sau asociațiile care pot depune o plângere în

numele persoanelor vizate sau, în cazul unei încălcări a securității datelor cu caracter personal, independent de o plângere înaintată de o persoană vizată.

Articolul 74 se referă la dreptul de a exercita o cale de atac împotriva unei autorități de supraveghere. Acesta se bazează pe dispoziția cu caracter general prevăzută la articolul 28 alineatul (3) din Directiva 95/46/CE. Articolul 74 prevede, în special, o cale de atac care să oblige autoritatea de supraveghere să acționeze ca urmare a unei plângeri și clarifică competența instanțelor din statul membru în care este stabilită autoritatea de supraveghere. De asemenea, prevede posibilitatea autorității de supraveghere din statul membru în care persoana vizată își are reședința de a introduce acțiuni, în numele persoanelor vizate, în fața instanțelor unui alt stat membru în care este stabilită autoritatea de supraveghere.

Articolul 75 se referă la dreptul de a exercita o cale de atac împotriva unui operator sau unei persoane împuternicite de către operator, pe baza articolului 22 din Directiva 95/46/CE, și prevede opțiunea de a se adresa instanțelor din statul membru în care pârâtul își are reședința sau din statul membru în care își are reședința persoana vizată. În cazul în care o procedură privind aceeași chestiune este în curs de examinare în cadrul mecanismului pentru asigurarea coerenței, instanța își poate suspenda procedurile, cu excepția cazurilor de urgență.

Articolul 76 prevede norme comune aplicabile acțiunilor în instanță, inclusiv dreptul organismelor, organizațiilor sau asociațiilor de a reprezenta persoanele vizate în fața instanțelor, dreptul autorităților de supraveghere de a acționa în justiție și obligativitatea informării instanțelor cu privire la procedurile paralele în alt stat membru, precum și posibilitatea ca, în acest caz, instanțele să suspende procedura[38]. Este prevăzută obligația statelor membre de a asigura o soluționare rapidă a acțiunilor în justiție[39].

Articolul 77 descrie dreptul la despăgubiri și răspunderea. Acesta se bazează pe articolul 23 din Directiva 95/46/CE, extinzând acest drept pentru a cuprinde prejudiciile cauzate de operatori și clarifică responsabilitatea operatorilor asociați și a persoanelor împuternicite de către operator.

Articolul 78 prevede obligația ca statele membre să stabilească norme referitoare la sancțiunile aplicabile în cazul încălcării dispozițiilor regulamentului și să se asigure că acestea sunt puse în aplicare.

Articolul 79 prevede obligația tuturor autorităților de supraveghere de a sancționa infracțiunile administrative enumerate în cadrul articolului, prin impunerea de amenzi până la o anumită valoare maximă, ținând cont de circumstanțele fiecărui caz în parte.

---

[38] Pe baza articolului 5 alineatul (1) din Decizia-cadru 2009/948/JAI a Consiliului din 30 noiembrie 2009 privind prevenirea și soluționarea conflictelor referitoare la exercitarea competenței în cadrul procedurilor penale, JO L 328, 15/12/2009, p. 42 și a articolului 13 alineatul (1) din Regulamentul (CE) nr. 1/2003 al Consiliului din 16 decembrie 2002 privind punerea în aplicare a normelor de concurență prevăzute la articolele 81 și 82 din tratat, JO L 1, 4.1.2003, p. 1.

[39] Pe baza articolului 18 alineatul (1) din 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).

3.4.9. CAPITOLUL IX - DISPOZIȚII REFERITOARE LA SITUAȚII SPECIFICE DE PRELUCRARE A DATELOR

Articolul 80 prevede obligația statelor membre de a pune în practică excepții și derogări de la anumite dispoziții ale regulamentului în cazul în care acestea sunt necesare pentru a crea un echilibru între dreptul la protecția datelor cu caracter personal și dreptul la libertatea de exprimare. Acesta se bazează pe articolul 9 din Directiva 95/46/CE, astfel cum a fost interpretat de Curtea de Justiție a UE[40].

Articolul 81 prevede obligația statelor membre ca, pe lângă condițiile pentru categoriile speciale de date, să asigure măsuri de protecție specifice în cazul prelucrării datelor în scopuri medicale.

Articolul 82 autorizează statele membre să adopte legi specifice privind prelucrarea datelor cu caracter personal în contextul ocupării unui loc de muncă.

Articolul 83 prevede condiții specifice pentru prelucrarea datelor cu caracter personal în scopuri de cercetare istorică, statistică și științifică.

Articolul 84 autorizează statele membre să adopte norme specifice privind accesul autorităților de supraveghere la datele cu caracter personal și în incintele unor entități, în cazul în care operatorii sunt supuși obligației de păstrare a confidențialității.

Articolul 85 autorizează bisericile, în temeiul articolului 17 din Tratatul privind funcționarea Uniunii Europene, să aplice în continuare normele cuprinzătoare existente în materie de protecție a datelor, dacă acestea sunt în conformitate cu prezentul regulament.

3.4.10. CAPITOLUL X – ACTE DELEGATE ȘI ACTE DE PUNERE ÎN APLICARE

Articolul 86 conține dispozițiile 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 cu domeniu de aplicare general, care completează sau modifică anumite elemente neesențiale ale unui act legislativ (acte „cvasilegislative”).

Articolul 87 cuprinde dispoziții privind procedura comitetului necesară pentru a acorda Comisiei competențe de executare, în cazurile în care, în conformitate cu articolul 291 din TFUE, sunt necesare condiții uniforme de punere în aplicare a actelor obligatorii din punct de vedere juridic ale Uniunii. În acest caz, este aplicabilă procedura de examinare.

3.4.11. CAPITOLUL XI - DISPOZIȚII FINALE

Articolul 88 abrogă Directiva 95/46/CEE.

Articolul 89 oferă clarificări cu privire la relația cu Directiva 2002/58/CE asupra confidențialității și comunicațiilor electronice, aducându-i o serie de modificări.

---

[40] În ceea ce privește interpretarea Curții de Justiție a UE, a se vedea, de exemplu, hotărârea din 16 decembrie 2008 în cauza Satakunnan Markkinapörssi și Satamedia (C-73/07, Culegere 2008, p. I-9831).

Articolul 90 prevede obligația Comisiei de a evalua regulamentul și de a prezenta rapoarte conexe.

Articolul 91 stabilește data intrării în vigoare a regulamentului și definește o etapă de tranziție în ceea ce privește data aplicării acestuia.

4. IMPLICAȚIILE BUGETARE

Implicațiile bugetare specifice ale propunerii se referă la sarcinile atribuite Autorității Europene pentru Protecția Datelor, astfel cum se specifică în fișa financiară legislativă care însoțește prezenta propunere. Aceste implicații necesită reprogramarea rubricii 5 din cadrul financiar multianual.

Propunerea nu are implicații asupra cheltuielilor operaționale.

Fișa financiară legislativă care însoțește prezenta propunere de regulament vizează implicațiile bugetare pentru regulamentul în sine și pentru Directiva privind protecția datelor în domeniul polițienesc și judiciar.

2012/0011 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ŞI AL CONSILIULUI

privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal și libera circulație a acestor date (Regulament general privind protecția datelor)

(Text cu relevanță pentru SEE)

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 16 alineatul (2) și articolul 114 alineatul (1),

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Comitetului Economic și Social European[41],

după consultarea Autorității Europene pentru Protecția Datelor[42],

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 tratat 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 și a unei uniuni economice, la progresul economic și social, la consolidarea și convergența economiilor în cadrul pieței interne și la bunăstarea persoanelor fizice.

---

41 JO C , , p. .
42 JO C , , p. .

(3) 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[43] vizează armonizarea nivelului de protecție a drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește activitățile de prelucrare și garantarea liberei circulații a datelor cu caracter personal între statele membre.

(4) Integrarea economică și socială care rezultă din funcționarea pieței interne a condus la o creștere substanțială a fluxurilor transfrontaliere. Schimbul de date între actorii economici și sociali, publici și privați s-a intensificat în întreaga Uniune. Conform dreptului Uniunii, autoritățile naționale sunt chemate să coopereze și să facă schimb de date cu caracter personal pentru a putea să își îndeplinească atribuțiile sau să execute sarcini în numele unei autorități într-un alt stat membru.

(5) Evoluțiile tehnologice rapide și globalizarea au generat noi provocări pentru protecția datelor cu caracter personal. Amploarea schimbului și a colectării de date a crescut spectaculos. Tehnologia permite atât societăților private, cât și autorităților publice să utilizeze date cu caracter personal la un nivel fără precedent în cadrul activităților lor. Din ce în ce mai multe persoane fizice fac publice la nivel mondial informații cu caracter personal. Tehnologia a transformat deopotrivă economia și viața socială și necesită facilitarea în continuare a liberei circulații a datelor în cadrul Uniunii și a transferului către țări terțe și organizații internaționale, asigurând, totodată, un nivel ridicat de protecție a datelor cu caracter personal.

(6) 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, luând în considerare importanța creării unui climat de încredere care va permite economiei digitale să se dezvolte pe piața internă. Persoanele fizice ar trebui să aibă control asupra propriilor date cu caracter personal, iar securitatea juridică și practică pentru persoane fizice, operatori economici și autorități publice ar trebui să fie consolidată.

(7) Obiectivele și principiile Directivei 95/46/CE rămân solide, dar aceasta nu a prevenit fragmentarea modului în care protecția datelor este pusă în aplicare în Uniune, incertitudinea juridică și percepția publică larg răspândită conform căreia există riscuri semnificative pentru protecția persoanelor fizice care au legătură, în special, cu activitatea online. Diferențele dintre nivelurile de protecție a drepturilor și libertăților persoanelor fizice, în special a dreptului la protecția datelor cu caracter personal, în ceea ce privește prelucrarea datelor cu caracter personal permisă în statele membre pot împiedica libera circulație a datelor cu caracter personal în întreaga Uniune. Aceste diferențe pot constitui, prin urmare, un obstacol în desfășurarea de activități economice la nivelul Uniunii, pot denatura concurența și pot împiedica autoritățile să îndeplinească responsabilitățile care le revin în temeiul dreptului Uniunii. Această diferență între nivelurile de protecție este cauzată de existența unor deosebiri în ceea ce privește transpunerea și aplicarea Directivei 95/46/CE.

(8) Pentru a se asigura un nivel consecvent și ridicat de protecție a persoanelor fizice și pentru a se îndepărta obstacolele din calea circulației datelor cu caracter personal, nivelul protecției drepturilor și libertăților persoanelor fizice în ceea ce privește

---

[43] JO L 281, 23.11.1995, p. 31.

prelucrarea unor astfel de date trebuie să fie echivalent în toate statele membre. Aplicarea consecventă și omogenă a normelor în materie de protecție a drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal ar trebui să fie asigurată în întreaga Uniune.

(9) Protecția efectivă a datelor cu caracter personal în întreaga Uniune necesită nu numai consolidarea și detalierea drepturilor persoanelor vizate și a obligațiilor celor care prelucrează și decid prelucrarea datelor cu caracter personal, ci și competențe echivalente pentru monitorizarea și asigurarea conformității cu normele de protecție a datelor cu caracter personal și sancțiuni echivalente pentru autorii infracțiunilor în statele membre.

(10) Articolul 16 alineatul (2) din tratat mandatează Parlamentul European și Consiliul să stabilească normele privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal, precum și normele privind libera circulație a acestor date.

(11) În vederea asigurării unui nivel uniform de protecție pentru persoanele fizice în întreaga Uniune și a preîntâmpinării discrepanțelor care împiedică libera circulație a datelor în cadrul pieței interne, este necesar un regulament în scopul de a furniza securitate juridică și transparență pentru operatorii economici, inclusiv microîntreprinderile și întreprinderile mici și mijlocii, precum și de a oferi persoanelor fizice în toate statele membre același nivel de drepturi garantate din punct de vedere juridic, de obligații și de responsabilități pentru operatori și persoanele împuternicite de aceștia, pentru a se asigura o monitorizare coerentă a prelucrării datelor cu caracter personal, sancțiuni echivalente în toate statele membre, precum și cooperarea efectivă a autorităților de supraveghere ale diferitelor state membre. Pentru a se lua în considerare situația specifică a microîntreprinderilor și a întreprinderilor mici și mijlocii, prezentul regulament include mai multe derogări. În plus, instituțiile și organismele Uniunii, statele membre și autoritățile lor de supraveghere sunt încurajate să ia în considerare necesitățile specifice ale microîntreprinderilor și ale întreprinderilor mici și mijlocii în aplicarea prezentului regulament. Noțiunea de microîntreprinderi și de întreprinderi mici și mijlocii ar trebui să se bazeze pe Recomandarea 2003/361/CE a Comisiei din 6 mai 2003 privind definirea microîntreprinderilor și a întreprinderilor mici și mijlocii.

(12) Protecția conferită de prezentul regulament vizează persoanele fizice, indiferent de cetățenia sau de locul de reședință al acestora, în ceea ce privește prelucrarea datelor cu caracter personal. Referitor la prelucrarea datelor care privesc persoane juridice și, în special, întreprinderi cu personalitate juridică, inclusiv numele și tipul de persoană juridică și detaliile de contact ale persoanei juridice, protecția conferită de prezentul regulament nu ar trebui să poată fi invocată de nicio persoană. Aceasta ar trebui să se aplice, de asemenea, în cazul în care numele persoanei juridice conține numele uneia sau mai multor persoane fizice.

(13) 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 prezentului regulament.

(14) Prezentul regulament nu se referă nici la chestiuni de protecție a drepturilor și libertăților fundamentale, nici la libera circulație a datelor referitoare la activități care nu intră în domeniul de aplicare a dreptului Uniunii, nici la prelucrarea datelor cu caracter personal de către instituțiile, organismele, oficiile și agențiile Uniunii, care fac obiectul Regulamentului (CE) nr. 45/2001[44], și nici la prelucrarea datelor cu caracter personal de către statele membre atunci când desfășoară activități legate de politica externă și de securitate comună a Uniunii.

(15) Prezentul regulament nu ar trebui să se aplice prelucrării datelor cu caracter personal de către o persoană fizică, care sunt exclusiv personale sau casnice, cum ar fi corespondența și repertoriul de adrese, fără niciun scop lucrativ și, prin urmare, fără nicio legătură cu o activitate profesională sau comercială. Exceptarea ar trebui, de asemenea, să nu aplice operatorilor sau persoanelor împuternicite de către operatori care furnizează mijloacele de prelucrare a datelor cu caracter personal pentru astfel de activități personale sau casnice.

(16) Protecția 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 și libera circulație a acestor date fac obiectul unui instrument juridic specific la nivelul Uniunii. Prin urmare, prezentul regulament nu ar trebui să se aplice activităților de prelucrare în aceste scopuri. Cu toate acestea, datele prelucrate de către autoritățile publice în temeiul prezentului regulament, în cazul în care sunt utilizate în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor ar trebui să fie reglementate de un instrument juridic mai specific la nivelul Uniunii (Directiva XX/YYY).

(17) Prezentul regulament nu ar trebui să aducă atingere aplicării Directivei 2000/31/CE, în special normelor privind răspunderea furnizorilor intermediari de servicii prevăzute la articolele 12 - 15 din directiva menționată.

(18) Prezentul regulament permite luarea în considerare a principiului accesului publicului la documente oficiale, în aplicarea dispozițiilor prevăzute de acesta.

(19) Orice prelucrare în Uniune a datelor cu caracter personal în cadrul activităților unui sediu al unui operator sau al unei persoane împuternicite de către operator ar trebui efectuată în conformitate cu prezentul regulament, indiferent dacă procesul de prelucrare în sine are loc sau nu în cadrul Uniunii. Stabilirea implică exercitarea efectivă și reală a unei activități în cadrul unor înțelegeri stabile. Forma juridică a unor astfel de înțelegeri, prin intermediul unei sucursale sau al unei filiale cu personalitate juridică, nu este factorul determinant în această privință.

(20) Pentru a se asigura că persoanele fizice nu sunt lipsite de protecția la care au dreptul în temeiul prezentului regulament, prelucrarea datelor cu caracter personal ale persoanelor vizate care își au reședința în Uniune de către un operator care nu este

---

44 JO L 8, 12.1.2001, p. 1.

stabilit în Uniune ar trebui să facă obiectul prezentului regulament în cazul în care activitățile de prelucrare au legătură cu oferirea de bunuri sau servicii unor astfel de persoane vizate sau cu monitorizarea comportamentului acestor persoane vizate.

(21) Pentru a se determina dacă o activitate de prelucrare poate fi considerată ca „monitorizare a comportamentului" persoanelor vizate, ar trebui să se analizeze dacă persoanele fizice sunt urmărite pe internet cu tehnici de prelucrare a datelor care constau în aplicarea unui „profil" unei persoane fizice, în special în scopul de a lua decizii cu privire la aceasta sau de a analiza sau de a face previziuni referitoare la preferințele personale, comportamentele și atitudinile acesteia.

(22) În cazul în care legislația națională a unui stat membru se aplică în temeiul dreptului internațional public, prezentul regulament ar trebui să se aplice, de asemenea, unui operator care nu este stabilit în Uniune, ci, de exemplu, într-o misiune diplomatică sau într-un oficiu consular al unui stat membru.

(23) Principiile protecției ar trebui să se aplice oricărei informații referitoare la o persoană identificată sau identificabilă. Pentru a se determina dacă o persoană 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.

(24) Atunci când utilizează servicii online, persoanele fizice pot fi asociate cu identificatorii online furnizați de dispozitivele, aplicațiile, instrumentele și protocoalele lor, cum ar fi adresele IP sau identificatorii cookie. Aceștia pot lăsa urme care, combinate cu identificatorii unici și alte informații primite de servere, pot fi utilizate pentru crearea de profiluri ale persoanelor fizice și pentru identificarea lor. Prin urmare, numerele de identificare, datele de localizare, identificatorii online sau alți factori specifici nu trebuie neapărat să fie considerați ca atare date cu caracter personal în toate circumstanțele.

(25) Consimțământul ar trebui acordat în mod explicit prin orice metodă corespunzătoare care permite manifestarea liberă, specifică și informată a voinței persoanei vizate, fie printr-o declarație sau printr-un act neechivoc al acesteia, asigurându-se că persoana fizică este conștientă de faptul că își dă consimțământul pentru prelucrarea datelor cu caracter personal, inclusiv prin bifarea unei căsuțe atunci când vizitează un site internet sau prin orice altă declarație sau acțiune care indică în mod clar în acest context acceptarea de către persoana vizată a prelucrării propuse a datelor sale cu caracter personal. Prin urmare, absența unui răspuns sau a unei acțiuni nu ar trebui să constituie un consimțământ. Consimțământul ar trebui să vizeze toate activitățile de prelucrare efectuate în același scop sau în aceleași scopuri. În cazul în care consimțământul persoanei vizate trebuie acordat în urma unei cereri electronice, aceasta trebuie să fie clară și concisă și să nu perturbe în mod inutil utilizarea serviciului pentru care se acordă consimțământul.

(26) 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 fizice 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.

(27) Sediul principal al unui operator în Uniune ar trebui să fie determinat conform unor criterii obiective și ar trebui să implice exercitarea efectivă și reală a unor activități de gestionare care să determine principalele decizii cu privire la scopurile, condițiile și mijloacele de prelucrare în cadrul unor înțelegeri stabile. Acest criteriu nu ar trebui să depindă de realizarea efectivă a prelucrării datelor cu caracter personal în locul respectiv; prezența și utilizarea mijloacelor tehnice și a tehnologiilor de prelucrare a datelor cu caracter personal sau activitățile de prelucrare nu constituie, în sine, un astfel de sediu principal și, prin urmare, nu sunt criteriul determinant în acest sens. Sediul principal al persoanei împuternicite de către operator ar trebui să fie locul în care se află administrația centrală a acestuia în Uniune.

(28) Un grup de întreprinderi ar trebui cuprindă o întreprindere care exercită controlul și întreprinderile controlate de aceasta, în cadrul căruia întreprinderea care exercită controlul ar trebui să fie întreprinderea care poate exercita o influență dominantă asupra celorlalte întreprinderi, de exemplu, în temeiul proprietății, al participării financiare sau al regulilor care o reglementează sau al competenței de a pune în aplicare normele în materie de protecție a datelor cu caracter personal.

(29) Copii au nevoie de o protecție specifică a datelor lor cu caracter personal, întrucât pot fi mai puțin conștienți de riscurile, consecințele, garanțiile și drepturile lor în ceea ce privește prelucrarea datelor cu caracter personal. Pentru a se determina condițiile în care o persoană fizică este minor, prezentul regulament ar trebui să preia definiția stabilită în Convenția Organizației Națiunilor Unite privind drepturile copilului.

(30) Orice prelucrare a datelor cu caracter personal ar trebui să fie legală, echitabilă și transparentă în raport cu persoanele fizice vizate. În special, scopurile specifice în care datele sunt prelucrate ar trebui să fie explicite și legitime și să fie determinate la momentul colectării datelor. Datele ar trebui să fie adecvate, relevante și limitate la minimum necesar scopurilor în care datele sunt prelucrate; aceasta necesită, în special, asigurarea faptului că datele colectate nu sunt excesive și că perioada pentru care datele sunt stocate este limitată strict la minimum. Datele cu caracter personal ar trebui prelucrate doar în cazul în care scopul prelucrării nu ar putea fi îndeplinit prin alte mijloace. Ar trebui să fie luate toate măsurile rezonabile pentru a se asigura că datele cu caracter personal care sunt inexacte sunt rectificate sau șterse. În vederea asigurării faptului că datele nu sunt păstrate mai mult timp decât este necesar, ar trebui să se stabilească de către operator termene pentru ștergere sau revizuire periodică.

(31) Pentru ca prelucrarea datelor cu caracter personal să fie legală, aceasta ar trebui efectuată pe baza consimțământului persoanei în cauză sau în temeiul unui alt motiv

legitim, prevăzut de lege, fie în prezentul regulament, fie în alt act legislativ al Uniunii sau al statului membru la care se face referire în prezentul regulament.

(32) În cazul în care prelucrarea se bazează pe consimțământul persoanei vizate, sarcina probei cu privire la faptul că persoana vizată și-a dat consimțământul pentru operațiunea de prelucrare îi revine operatorului. În special, în contextul unei declarații scrise cu privire la un alt aspect, garanțiile ar trebui să asigure că persoana vizată este conștientă de faptul că și-a dat consimțământul și în ce măsură a făcut acest lucru.

(33) Pentru a se asigura consimțământul liber, ar trebui să se precizeze că un consimțământ nu constituie un temei juridic valabil în cazul în care persoana fizică nu dispune cu adevărat de libertatea de a alegere și ulterior nu poate să refuze sau să își retragă consimțământul fără a fi prejudiciată.

(34) Consimțământul nu ar trebui să constituie un temei juridic valabil pentru prelucrarea datelor cu caracter personal în cazul în care există un dezechilibru evident între persoana vizată și operator. Acest lucru este valabil, în special, atunci când persoana vizată se află într-o situație de dependență în raport cu operatorul, printre altele, în cazul în care datele cu caracter personal ale angajaților sunt prelucrate de către angajator în contextul ocupării unui loc de muncă. În cazul în care operatorul este o autoritate publică, nu ar exista un dezechilibru decât în ceea ce privește operațiuni specifice de prelucrare a datelor în cadrul cărora autoritatea publică poate impune o obligație în temeiul competențelor sale publice relevante, iar consimțământul nu poate fi considerat ca fiind acordat în mod liber, ținându-se cont de interesul persoanei vizate.

(35) Prelucrarea ar trebui să fie legală în cazul în care este necesară în cadrul unui contract sau în vederea încheierii unui contract.

(36) În cazul în care prelucrarea este efectuată în conformitate cu o obligație legală a operatorului sau în cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini de interes public sau în exercitarea autorității publice, prelucrarea ar trebui să aibă un temei juridic în dreptul Uniunii sau în legislația unui stat membru care îndeplinește cerințele prevăzute de Carta drepturilor fundamentale a Uniunii Europene, pentru orice limitare a drepturilor și libertăților. De asemenea, este de competența dreptului Uniunii sau a legislației naționale să determine dacă operatorul care îndeplinește o sarcină de interes public sau în exercitarea autorității publice ar trebui să fie o administrație publică sau altă persoană fizică sau juridică de drept public sau privat, cum ar fi o asociație profesională.

(37) Prelucrarea datelor cu caracter personal ar trebui, de asemenea, să fie considerată legală în cazul în care este necesară în scopul asigurării protecției unui interes care este esențial pentru viața persoanei vizate.

(38) Interesele legitime ale unui operator pot constitui un temei juridic pentru prelucrare, cu condiția să nu prevaleze interesele sau drepturile și libertățile fundamentale ale persoanei vizate. Aceasta ar necesita o evaluare atentă, în special în cazul în care persoana vizată este un minor, întrucât minorii necesită o protecție specifică. Persoana vizată ar trebui să aibă dreptul gratuit la opoziție în ceea ce privește prelucrarea, din motive legate de situația sa particulară. Pentru a se asigura transparența, operatorul ar trebui să aibă obligația de a informa în mod explicit persoana vizată cu privire la

interesele legitime urmărite și dreptul la opoziție și, de asemenea, ar trebui să aibă obligația de a documenta aceste interese legitime. Întrucât legiuitorul trebuie să furnizeze temeiul juridic pentru prelucrarea datelor de către autoritățile publice, acest temei juridic nu ar trebui să se aplice prelucrării de către autoritățile publice în îndeplinirea sarcinilor care le revin.

(39) Prelucrarea datelor în măsura strict necesară în scopul asigurării securității rețelelor și a informațiilor, și anume capacitatea unei rețele sau a unui sistem de informații de a face față, la un anumit nivel de încredere, evenimentelor accidentale sau acțiunilor ilegale sau rău intenționate care compromit disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor stocate sau transmise, precum și securitatea serviciilor conexe oferite de aceste rețele și sisteme sau accesibile prin intermediul acestora, de către autoritățile publice, echipele de intervenție în caz de urgență informatică (CERT), echipele de intervenție în cazul producerii unor incidente care afectează securitatea informatică (CSIRT), furnizorii de rețele și servicii de comunicații electronice, precum și de către furnizorii de servicii și tehnologii de securitate, constituie un interes legitim al operatorului de date în cauză. Acesta ar putea include, de exemplu, prevenirea accesului neautorizat la rețelele de comunicații electronice și a difuzării de coduri dăunătoare și oprirea atacurilor de „blocare a serviciului”, precum și prevenirea daunelor aduse calculatoarelor și sistemelor de comunicații electronice.

(40) Prelucrarea datelor cu caracter personal în alte scopuri ar trebui să fie permisă doar atunci când prelucrarea este compatibilă cu scopurile în care datele au fost inițial colectate, în special în cazul în care prelucrarea este necesară în scopuri de cercetare istorică, statistică sau științifică. În cazul în care celălalt scop nu este compatibil cu scopul inițial în care datele sunt colectate, operatorul ar trebuie să obțină consimțământul persoanei vizate cu privire la acest alt scop sau ar trebui să întemeieze prelucrarea legală pe un alt motiv legitim, în special în cazul în care acest fapt este prevăzut de dreptul Uniunii sau de legislația statului membru care se aplică operatorului. În orice caz, aplicarea principiilor stabilite de prezentul regulament și, în special, informarea persoanei vizate cu privire la aceste alte scopuri ar trebui să fie garantată.

(41) Datele cu caracter personal care sunt, prin natura lor, deosebit de sensibile și de vulnerabile în ceea ce privește drepturile fundamentale sau viața privată, necesită o protecție specifică. Astfel de date nu ar trebui să fie prelucrate, cu excepția cazului în care persoana vizată își dă consimțământul explicit. Cu toate acestea, derogări de la interdicția respectivă ar trebui prevăzute în mod explicit în ceea ce privește nevoile specifice, în special atunci când prelucrarea este efectuată în cadrul activităților legitime de către anumite asociații sau fundații al căror scop este de a permite exercitarea libertăților fundamentale.

(42) Derogarea de la interdicția prelucrării categoriilor de date sensibile ar trebui să fie permisă, de asemenea, în cazul în care este prevăzută de lege, sub rezerva unor garanții corespunzătoare, pentru a se asigura protecția datelor cu caracter personal și a altor drepturi fundamentale, atunci când motive de interes public justifică acest lucru și, în special, în scopuri medicale, inclusiv sănătatea publică, protecția socială și gestionarea serviciilor de asistență medicală, în special în scopul garantării calității și eficienței din punct de vedere al costurilor în ceea ce privește procedurile utilizate pentru soluționarea cererilor de prestații și servicii în sistemul asigurărilor de sănătate sau în scopuri de cercetare istorică, statistică și științifică.

(43) În plus, prelucrarea datelor cu caracter personal de către autoritățile publice în vederea realizării obiectivelor prevăzute de dreptul constituțional sau de dreptul internațional public, ale asociațiilor religioase recunoscute oficial se efectuează din motive de interes public.

(44) În cazul în care, în cadrul activităților electorale, funcționarea sistemului democratic necesită, într-un stat membru, ca partidele politice să colecteze date privind opiniile politice ale persoanelor, prelucrarea unor astfel de date poate fi permisă din motive de interes public, cu condiția să se prevadă garanțiile corespunzătoare.

(45) Dacă datele prelucrate de către un operator nu îi permit acestuia să identifice o persoană fizică, operatorul de date nu ar trebui să aibă obligația de a obține informații suplimentare în vederea identificării persoanei vizate, cu unicul scop de a respecta una dintre dispozițiile prezentului regulament. În cazul unei cereri de acces, operatorul ar trebui să aibă dreptul de a solicita persoanei vizate mai multe informații pentru a putea să localizeze datele cu caracter personal pe care le caută persoana respectivă.

(46) Principiul transparenței prevede că orice informații care se adresează publicului sau persoanei vizate ar trebui să fie ușor accesibile și ușor de înțeles și că se utilizează un limbaj simplu și clar. Acesta este important în special în cazul în care, în situații cum ar fi publicitatea online, multitudinea actorilor și complexitatea, din punct de vedere tehnologic, a practicii, este dificil ca persoana vizată să știe și să se înțeleagă dacă datele cu caracter personal care o privesc sunt colectate, de către cine și în ce scop. Întrucât copiii necesită o protecție specifică, orice informații și orice comunicare, în cazul în care prelucrarea vizează în mod specific un minor, ar trebui să fie exprimate într-un limbaj simplu și clar, astfel încât acesta să îl poată înțelege cu ușurință.

(47) Ar trebui prevăzute modalități de facilitare a exercitării de către persoana vizată a drepturile sale stipulate de prezentul regulament, inclusiv mecanismele de a solicita, în mod gratuit, în special, accesul la date, rectificarea și ștergerea acestora, precum și exercitarea dreptului la opoziție. Operatorul ar trebui să fie aibă obligația de a răspunde cererilor persoanelor vizate într-un termen fix și, în cazul în care nu se conformează cererii persoanei vizate, să motiveze acest refuz.

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

(49) Informațiile în legătură cu prelucrarea datelor cu caracter personal referitoare la persoana vizată ar trebui furnizate acesteia la momentul colectării sau, în cazul în care datele nu sunt colectate de la persoana vizată, într-o perioadă rezonabilă, în funcție de circumstanțele cazului. În cazul în care datele pot fi divulgate în mod legitim unui alt destinatar, persoana vizată ar trebui informată atunci când datele sunt divulgate pentru prima dată destinatarului.

(50) Cu toate acestea, nu este necesară impunerea obligației respective în cazul în care persoana vizată dispune deja de aceste informații sau în cazul în care înregistrarea sau divulgarea datelor este prevăzută în mod expres de lege sau în cazul în care informarea

persoanei vizate se dovedește imposibilă sau implică eforturi disproporționate. Acesta din urmă ar putea fi cazul în special atunci când prelucrarea se efectuează în scopuri de cercetare istorică, statistică sau științifică; în această privință, pot fi luate în considerare numărul persoanelor vizate, vechimea datelor și măsurile compensatorii adoptate.

(51) Orice persoană ar trebui să aibă dreptul de acces la datele colectate care o privesc și de a exercita 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, identitatea destinatarilor datelor, care este logica de prelucrare a datelor și care ar putea fi, cel puțin în cazul în care se bazează pe crearea de profiluri, consecințele unei astfel de prelucrări. Acest drept nu ar trebui să aducă atingere drepturilor și libertăților altora, inclusiv secretului comercial sau proprietății intelectuale și, în special, drepturilor de autor care asigură protecția programelor software. Cu toate acestea, considerațiile de mai sus nu ar trebui aibă drept rezultat refuzul de a furniza toate informațiile persoanei vizate.

(52) Operatorul ar trebui să ia toate măsurile rezonabile pentru a verifica identitatea unei persoane vizate care solicită acces la date, în special în contextul serviciilor online și al identificatorilor online. Un operator nu ar trebui să rețină datele cu caracter personal în scopul exclusiv de a fi în măsură să reacționeze la cereri potențiale.

(53) Orice persoană ar trebui să aibă dreptul de rectificare a datelor cu caracter personal care o privesc și „dreptul de a fi uitată”, în cazul în care păstrarea acestor date nu este în conformitate cu prezentul regulament. În special, persoanele vizate ar trebui să aibă dreptul ca datele lor cu caracter personal să fie șterse și să nu mai fie prelucrate, în cazul în care datele nu mai sunt necesare pentru scopurile în care sunt colectate sau sunt prelucrate, în cazul în care persoanele vizate și-au retras consimțământul pentru prelucrare sau în cazul în care acestea se opun prelucrării datelor cu caracter personal care le privesc sau în cazul în care prelucrarea datelor cu caracter personal ale acestora nu este conformă cu prezentul regulament. Acest drept este relevant în special în cazul în care persoana vizată și-a dat consimțământul când era minor și nu cunoștea pe deplin riscurile pe care le implică prelucrarea, iar ulterior dorește să elimine astfel de date cu caracter personal, în special de pe internet. Cu toate acestea, păstrarea în continuare a datelor ar trebui să fie permisă în cazul în care este necesară în scopuri de cercetare istorică, statistică și științifică, din motive de interes public în domeniul sănătății publice, pentru exercitarea dreptului la libertatea de exprimare, atunci când acest lucru este prevăzut de lege sau în cazul în care există un motiv pentru a restricționa prelucrarea datelor, în loc ca acestea să fie șterse.

(54) Pentru a se consolida „dreptul de a fi uitat” în mediul on-line, dreptul de ștergere ar trebui, de asemenea, să fie extins astfel încât un operator care a făcut publice date cu caracter personal ar trebui să aibă obligația de a informa terții care prelucrează astfel de date că o persoană vizată le solicită să șteargă orice linkuri către datele cu caracter personal respective sau copii sau reproduceri ale acestora. În scopul asigurării acestor informații, operatorul ar trebui să ia toate măsurile rezonabile, inclusiv măsuri tehnice, în ceea ce privește datele de a căror publicare este responsabil. În legătură cu publicarea datelor cu caracter personal de către un terț, operatorul ar trebui să fie considerat responsabil de publicare, în cazul în care acesta a autorizat publicarea de către terț.

(55) Pentru a se consolida în continuare controlul asupra propriilor date și dreptul lor de acces, persoanele vizate ar trebui să aibă dreptul, în cazul în care datele cu caracter personal sunt prelucrate prin mijloace electronice într-un format structurat și utilizat în mod curent, de a obține, de asemenea, o copie a datelor care le privesc într-un format electronic utilizat în mod curent. Persoana vizată ar trebui, de asemenea, să fie autorizată să transmită datele respective, pe care le-a furnizat, dintr-o aplicație automată, cum ar fi o rețea socială, către alta. Aceasta ar trebui să se aplice în cazul în care persoana vizată a furnizat datele sistemului de prelucrare automată, pe baza consimțământului său sau în cadrul executării unui contract.

(56) În cazurile în care datele cu caracter personal ar putea fi prelucrate în mod legal în scopul asigurării protecției intereselor vitale ale persoanei vizate sau din motive de interes public, de exercitare a autorității publice sau de urmărire a intereselor legitime ale unui operator, orice persoană vizată ar trebui, cu toate acestea, să aibă dreptul de a se opune prelucrării oricăror date care o privesc. Sarcina probei ar trebui să revină operatorului pentru a demonstra că interesele sale legitime pot prevala asupra intereselor sau a drepturilor și libertăților fundamentale ale persoanei vizate.

(57) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de marketing direct, persoana vizată ar trebui să aibă gratuit dreptul la opoziție cu privire la o astfel de prelucrare, care să poată fi invocat cu ușurință și în mod efectiv.

(58) Orice persoană fizică ar trebui să aibă dreptul de a nu fi supusă unei măsuri care se bazează pe crearea de profiluri prin mijloace de prelucrare automată a datelor. Cu toate acestea, o astfel de măsură ar trebui să fie permisă în cazul în care este autorizată în mod expres de lege, este efectuată în cadrul încheierii sau al executării unui contract sau în cazul în care persoana vizată și-a dat consimțământul. În orice caz, o astfel de prelucrare ar trebui să facă obiectul unor garanții corespunzătoare, inclusiv o informare specifică a persoanei vizate și dreptul de a obține intervenție umană, iar o astfel de măsură nu ar trebui să se refere la un minor.

(59) Dreptul Uniunii sau legislația unui stat membru pot impune restricții ale principiilor specifice, ale drepturilor de informare, acces, rectificare și ștergere sau ale dreptului la portabilitatea datelor, ale dreptului la opoziție, ale măsurilor bazate pe crearea de profiluri, precum și ale comunicării unei încălcări a securității datelor cu caracter personal persoanei vizate și ale anumitor obligații conexe ale operatorilor, în măsura în care acest lucru este necesar și proporțional într-o societate democratică pentru a se garanta siguranța publică, inclusiv protecția vieții oamenilor, în special ca răspuns la dezastre naturale sau provocate de om, prevenirea, investigarea și urmărirea penală a infracțiunilor sau a încălcării eticii în cazul profesiunilor reglementate, alte interese publice ale Uniunii sau ale unui stat membru, în special un interes economic sau financiar important al Uniunii sau al unui stat membru, sau protecția persoanei vizate sau a drepturilor și libertăților unor terți. Aceste restricții ar trebui să fie conforme cu cerințele prevăzute de Carta drepturilor fundamentale a Uniunii Europene și de Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale.

(60) Ar trebui să se stabilească 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 și să aibă obligația de a demonstra conformitatea fiecărei operațiuni de prelucrare cu prezentul regulament.

(61) Protecția drepturilor și libertăților persoanelor vizate în ceea ce privește prelucrarea datelor cu caracter personal necesită adoptarea de măsuri tehnice și organizatorice corespunzătoare, atât în momentul conceperii prelucrării, cât și în cel al prelucrării în sine, pentru a se asigura îndeplinirea cerințelor prezentului regulament. În scopul asigurării și al demonstrării conformității cu prezentul regulament, operatorul ar trebui să adopte politici interne și să pună în aplicare măsuri corespunzătoare, care să respecte, în special, principiul luării în considerare a protecției datelor începând cu momentul conceperii și cel al protecției implicite a datelor.

(62) Protecția drepturilor și libertăților persoanelor vizate, precum și responsabilitatea și răspunderea operatorilor și a persoanei împuternicite de către operator, în ceea ce privește, de asemenea, monitorizarea de către autoritățile de supraveghere și măsurile adoptate de acestea, necesită o atribuire clară a responsabilităților în temeiul prezentului regulament, 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.

(63) Atunci când un operator care nu este stabilit în Uniune prelucrează date cu caracter personal ale unor persoane vizate care își au reședința în Uniune, iar activitățile de prelucrare ale operatorului au legătură cu oferirea de bunuri și servicii unor astfel de persoane vizate sau cu monitorizarea comportamentului acestora, operatorul ar trebui să desemneze un reprezentant, cu excepția cazului în care operatorul este stabilit într-o țară terță care asigură un nivel adecvat de protecție sau în care operatorul este o întreprindere mică sau mijlocie sau o autoritate publică sau un organism public sau în care operatorul oferă doar ocazional bunuri sau servicii unor astfel de persoane vizate. Reprezentantul ar trebui să acționeze în numele operatorului, putând fi contactat de orice autoritate de supraveghere.

(64) Pentru a se stabili dacă un operator oferă doar ocazional bunuri și servicii persoanelor vizate care își au reședința în Uniune, ar trebui să se analizeze dacă din ansamblul activităților desfășurate de către operator rezultă că oferirea de bunuri și servicii unor astfel de persoane vizate este auxiliară activităților principale respective.

(65) În vederea demonstrării conformității cu prezentul regulament, operatorul sau persoana împuternicită de către operator ar trebui să documenteze fiecare operațiune de prelucrare. 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 respectivă, pentru a putea fi utilizată în scopul monitorizării operațiunilor de prelucrare respective.

(66) În vederea menținerii securității și a prevenirii prelucrărilor care încalcă dispozițiile prezentului regulament, operatorul sau persoana împuternicită de către operator ar trebui să evalueze riscurile inerente prelucrării și să pună în aplicare măsuri pentru atenuarea acestor riscuri. Măsurile respective ar trebui să asigure un nivel corespunzător de securitate, luând în considerare stadiul actual al tehnologiei și costurile punerii lor în aplicare în raport cu riscurile și natura datelor cu caracter personal a căror protecție trebuie asigurată. Atunci când se stabilesc standarde tehnice și măsuri organizatorice menite să asigure securitatea prelucrării, Comisia ar trebui să promoveze neutralitatea tehnologică, interoperabilitatea și inovarea, și, dacă este cazul, cooperarea cu țările terțe.

(67) Dacă nu este soluționată la timp și într-un mod adecvat, o încălcare a securității datelor cu caracter personal poate cauza persoanei fizice în cauză pierderi economice substanțiale și daune sociale, inclusiv fraudarea identității. Prin urmare, de îndată ce a luat cunoștință de producerea unei astfel de încălcări, operatorul ar trebui să o notifice autorității de supraveghere, fără întârziere nejustificată și, dacă este posibil, în termen de 24 de ore. În cazul în care termenul de 24 de ore nu este respectat, o explicație a motivelor întârzierii ar trebui să însoțească notificarea. Persoanele fizice ale căror date cu caracter personal ar putea fi afectate negativ de încălcare ar trebui să fie notificate fără întârziere nejustificată 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. Notificarea ar trebui să descrie natura încălcării securității datelor cu caracter personal și să formuleze recomandări pentru persoana fizică în cauză în scopul atenuării eventualelor efecte negative. Notificările persoanelor vizate ar trebui efectuate în cel mai scurt timp posibil în mod rezonabil și în strânsă cooperare cu autoritatea de supraveghere, respectându-se orientările furnizate de aceasta sau de alte autorități competente (de exemplu, autoritățile de aplicare a legii). De exemplu, pentru ca persoanele vizate să poată atenua un risc imediat de prejudiciere, acestea ar trebui notificate cu promptitudine, în timp ce necesitatea de a pune în aplicare măsuri corespunzătoare împotriva încălcării în continuare a securității datelor sau împotriva unor încălcări similare ale securității datelor ar putea justifica un termen mai îndelungat.

(68) Pentru a se determina dacă o încălcare a securității datelor cu caracter personal este notificată fără întârziere nejustificată autorității de supraveghere și persoanei vizate, ar trebui să se analizeze dacă operatorul a implementat și a aplicat măsuri tehnologice de protecție și organizatorice corespunzătoare în scopul de a stabili imediat dacă s-a produs o încălcare a securității datelor cu caracter personal și de a informa cu promptitudine autoritatea de supraveghere și persoana vizată, înainte de prejudicierea intereselor sale personale și economice, luându-se în considerare, în special, natura și gravitatea încălcării securității datelor cu caracter personal, precum și consecințele și efectele negative ale acesteia asupra persoanei vizate.

(69) 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 fraudării identității sau a altor forme de utilizare abuzivă. În plus, astfel de norme și proceduri ar trebui să țină cont de interesele legitime ale autorităților de aplicare a legii în cazurile în care divulgarea timpurie ar putea îngreuna în mod inutil investigarea circumstanțelor în care a avut loc o încălcare.

(70) Directiva 95/46/CE prevede o obligație generală de a notifica prelucrarea datelor cu caracter personal autorităților de supraveghere. Cu toate că obligația respectivă generează sarcini administrative și financiare, aceasta nu contribuie întotdeauna la îmbunătățirea protecției datelor cu caracter personal. Prin urmare, o astfel de obligație de notificare generală nediferențiată ar trebui să fie abrogată și înlocuită cu proceduri și mecanisme eficace care să pună accentul, în schimb, pe operațiunile de prelucrare care pot prezenta riscuri specifice pentru drepturile și libertățile persoanelor vizate prin

însăși natura lor, prin domeniul lor de aplicare sau prin scopurile lor. În astfel de cazuri, operatorul sau persoana împuternicită de către operator ar trebui să efectueze, înainte de prelucrare, o evaluare a impactului asupra protecției datelor, care ar trebui să includă, în special, măsurile avute în vedere, garanții și mecanisme pentru asigurarea protecției datelor cu caracter personal și pentru demonstrarea conformității cu prezentul regulament.

(71) Aceasta ar trebui să se aplice, în special, sistemelor de evidență de mari dimensiuni recent instituite, care au drept obiectiv prelucrarea unui volum considerabil de date cu caracter personal la nivel regional, național sau supranațional și care ar putea afecta un număr mare de persoane vizate.

(72) În unele circumstanțe ar putea fi judicios și economic ca o evaluare a impactului asupra protecției datelor să aibă o perspectivă mai extinsă decât cea a unui singur proiect, de exemplu, în cazul în care autorități sau organisme publice intenționează să instituie o aplicație sau o platformă de prelucrare comună sau în cazul în care mai mulți operatori preconizează să introducă o aplicație comună sau un mediu de prelucrare comun în cadrul unui sector sau segment industrial sau pentru o activitate orizontală utilizată pe scară largă.

(73) Evaluările impactului asupra protecției datelor ar trebui efectuate de către o autoritate publică sau un organism public în cazul în care o astfel de evaluare nu a fost deja realizată în contextul adoptării legislației naționale pe care se bazează îndeplinirea sarcinilor autorității publice sau ale organismului public și care reglementează anumite operațiuni sau serii de operațiuni de prelucrare în cauză.

(74) În cazul în care o evaluare a impactului asupra protecției datelor arată că operațiunile de prelucrare implică un nivel ridicat al riscurilor specifice pentru drepturile și libertățile persoanelor vizate, cum ar fi privarea persoanelor fizice de un drept, sau prin utilizarea noilor tehnologii specifice, autoritatea de supraveghere ar trebui să fie consultată, înainte de începerea operațiunilor, cu privire la o prelucrare riscantă care ar putea să nu fie conformă cu prezentul regulament și pentru a face propuneri în vederea remedierii unei astfel de situații. Această consultare ar trebui, de asemenea, să aibă loc în timpul elaborării fie a unei măsuri a parlamentului național, fie a unei măsuri întemeiate pe o astfel de măsură legislativă, care definește natura prelucrării și stabilește garanțiile corespunzătoare.

(75) În cazul în care prelucrarea este efectuată în sectorul public sau în cazul în care, în sectorul privat, prelucrarea este efectuată de o întreprindere de mari dimensiuni sau în cazul în care activitățile de bază ale întreprinderii, indiferent de dimensiunea acesteia, implică operațiuni de prelucrare care necesită o monitorizare regulată și sistematică, o persoană ar trebui să acorde asistență operatorului sau persoanei împuternicite de către operator pentru monitorizarea conformității, la nivel intern, cu prezentul regulament. Acești responsabilii cu protecția datelor, fie că sunt sau nu sunt angajați ai operatorului, ar trebui să fie în măsură să își îndeplinească atribuțiile și sarcinile în mod independent.

(76) Asociațiile sau alte organisme care reprezintă categorii de operatori ar trebui încurajate să elaboreze coduri de conduită, în limitele prezentului regulament, astfel încât să se faciliteze aplicarea efectivă a prezentului regulament, luându-se în considerare caracteristicile specifice ale prelucrării efectuate în anumite sectoare.

(77) Pentru a se îmbunătăți transparența și conformitatea cu prezentul regulament, ar trebui să se încurajeze instituirea de mecanisme de certificare, precum și de sigilii și mărci în materie de protecție a datelor, care să permită persoanelor vizate să evalueze rapid nivelul de protecție a datelor aferent produselor și serviciilor relevante.

(78) Fluxurile transfrontaliere de date cu caracter personal sunt necesare pentru dezvoltarea comerțului internațional și a cooperării internaționale. Creșterea acestor fluxuri a generat noi provocări și preocupări cu privire la protecția datelor cu caracter personal. Cu toate acestea, în cazul în care se transferă date cu caracter personal din Uniune către țări terțe sau organizații internaționale, nivelul de protecție a persoanelor fizice garantat în Uniune prin prezentul regulament nu ar trebui să fie diminuat. În orice caz, transferurile către țările terțe nu pot fi efectuate decât în deplină conformitate cu prezentul regulament.

(79) Prezentul regulament nu aduce atingere acordurilor internaționale încheiate între Uniune și țări terțe în vederea reglementării transferului de date cu caracter personal, inclusiv garanții corespunzătoare pentru persoanele vizate.

(80) Comisia poate decide, cu efect în întreaga Uniune, că anumite țări terțe sau un teritoriu sau 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.

(81) În conformitate cu valorile fundamentale pe care se întemeiază Uniunea, în special protecția drepturilor omului, Comisia ar trebui, în evaluarea sa referitoare la țara terță, 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.

(82) Comisia poate, de asemenea, să recunoască faptul că o țară terță sau un teritoriu sau un sector de prelucrare dintr-o țară terță sau o organizație internațională nu oferă un nivel adecvat de protecție a datelor. În consecință, transferul de date cu caracter personal către țara terță respectivă ar trebui să fie interzis. În acest caz, ar trebui să se prevadă dispoziții pentru consultări între Comisie și astfel de țări terțe sau organizații internaționale.

(83) În absența unei decizii privind caracterul adecvat al protecției, operatorul sau persoana împuternicită de către operator ar trebui să adopte măsuri pentru a compensa lipsa protecției datelor într-o țară terță prin intermediul unor garanții corespunzătoare pentru persoana vizată. Astfel de garanții corespunzătoare pot consta în utilizarea regulilor corporatiste obligatorii, a clauzelor standard de protecție a datelor adoptate de către Comisie, a clauzelor standard în materie de protecție a datelor adoptate de către o autoritate de supraveghere sau a clauzelor contractuale autorizate de o autoritate de supraveghere sau a altor măsuri adecvate și proporționale care sunt justificate având în vedere toate circumstanțele aferente unei operațiuni de transfer de date sau unui set de operațiuni de transfer de date și în cazurile autorizate de o autoritate de supraveghere.

(84) Posibilitatea ca operatorul sau persoana împuternicită de către operator să utilizeze clauze standard în materie de protecție a datelor adoptate de către Comisie sau de către

o autoritate de supraveghere nu ar trebui să împiedice operatorii sau persoanele împuternicite de către aceştia să includă clauze standard în materie de protecţie a datelor într-un contract mai amplu şi nici să adauge alte clauze, atât timp acestea cât nu contravin, direct sau indirect, clauzelor contractuale standard adoptate de către Comisie sau de către o autoritate de supraveghere sau nu prejudiciază drepturile sau libertăţile fundamentale ale persoanelor vizate.

(85) Un grup corporatist ar trebui să poată utiliza regulile corporatiste obligatorii aprobate pentru transferurile sale internaţionale dinspre Uniune către organizaţii din cadrul aceluiaşi grup de întreprinderi, atâta timp cât astfel de reguli corporatiste includ principii esenţiale şi drepturi exercitabile în scopul asigurării unor garanţii corespunzătoare pentru transferurile sau categoriile de transferuri de date cu caracter personal.

(86) Ar trebui să se prevadă posibilitatea de a se efectua transferuri în anumite circumstanţe în care persoana vizată şi-a dat consimţământul, în care transferul este necesar în legătură cu un contract sau cu o acţiune în justiţie, în care motive importante de interes public stabilite de dreptul Uniunii sau de legislaţia unui stat membru impun acest lucru sau în care transferul se efectuează dintr-un registru instituit prin lege şi destinat să fie consultat de către public sau de către persoane care au un interes legitim. În acest ultim caz, un astfel de transfer nu ar trebui să implice totalitatea datelor sau ansamblul categoriilor de date conţinute în registru, iar atunci când registrul este destinat să fie consultat de către persoane care au un interes legitim, transferul ar trebui să fie efectuat doar la cererea persoanelor respective sau dacă acestea sunt destinatarii.

(87) Aceste derogări ar trebui să se aplice, în special, transferurilor de date solicitate şi necesare pentru protecţia unor motive importante de interes public, de exemplu în cazurile transferurilor internaţionale de date între autorităţile din domeniul concurenţei, între administraţiile fiscale sau vamale, între autorităţile de supraveghere financiară, între serviciile competente în materie de securitate socială sau către autorităţile competente în scopul prevenirii, identificării, investigării şi urmăririi penale a infracţiunilor.

(88) Transferurile care nu pot fi considerate ca fiind frecvente sau masive, ar putea, de asemenea, să fie efectuate în scopul realizării intereselor legitime urmărite de operator sau de persoana împuternicită de către operator, după ce aceştia au evaluat toate circumstanţele aferente transferului de date. Pentru prelucrarea datelor în scopuri de cercetare istorică, statistică şi ştiinţifică, ar trebui să se ia în considerare aşteptările legitime ale societăţii cu privire la creşterea nivelului de cunoştinţe.

(89) În orice caz, atunci când Comisia nu a luat o decizie cu privire la nivelul adecvat de protecţie a datelor într-o ţară terţă, operatorul sau persoana împuternicită de către operator ar trebui să utilizeze soluţii care să ofere persoanelor vizate garanţia că vor continua să beneficieze de drepturi fundamentale şi garanţii în ceea ce priveşte prelucrarea datelor lor în Uniune, odată ce aceste date au fost transferate.

(90) Unele ţări terţe au adoptat legi, regulamente şi alte instrumente legislative care au drept obiectiv să reglementeze în mod direct activităţile de prelucrare a datelor persoanelor fizice şi juridice aflate sub jurisdicţia statelor membre. Aplicarea extrateritorială a acestor legi, regulamente şi alte instrumente legislative poate încălca dreptul internaţional şi poate împiedica asigurarea protecţiei persoanelor fizice

garantată în Uniune prin prezentul regulament. Transferurile ar trebui să fie permise numai în cazul îndeplinirii condițiilor prevăzute de prezentul regulament pentru un transfer către țări terțe. Acesta ar putea fi cazul, *inter alia*, atunci când divulgarea este necesară dintr-un motiv important de interes public recunoscut în dreptul Uniunii sau în legislația unui stat membru care se aplică operatorului. Condițiile în care există un motiv important de interes public ar trebui precizate pe larg de către Comisie într-un act delegat.

(91) 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, în special pentru a-și asigura protecția împotriva utilizării sau a divulgării ilegale a acestor informații. 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 acestora de a conlucra în context transfrontalier pot fi, de asemenea, îngreunate de insuficiența competențelor de prevenire sau remediere, de caracterul eterogen al regimurilor juridice și de existența unor obstacole de ordin practic, cum ar fi constrângerile în materie de resurse. Prin urmare, este necesar să se promoveze o cooperare mai strânsă între autoritățile de supraveghere a protecției datelor pentru a putea face schimb de informații și a desfășura investigații împreună cu omologii lor internaționali.

(92) 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. Statele membre pot institui mai multe autorități de supraveghere, pentru a reflecta structura lor constituțională, organizatorică și administrativă.

(93) În cazul în care un stat membru instituie mai multe autorități de supraveghere, acesta ar trebui să stabilească prin lege mecanisme care să asigure participarea efectivă a autorităților de supraveghere respective la mecanismul pentru asigurarea coerenței. Statul membru respectiv ar trebui, în special, să desemneze autoritatea de supraveghere care îndeplinește funcția de punct unic de contact pentru participarea efectivă a acestor autorități la mecanism, în scopul asigurării unei cooperări rapide și armonioase cu alte autorități de supraveghere, cu Comitetul european pentru protecția datelor și cu Comisia.

(94) 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.

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

(96) Autoritățile de supraveghere ar trebui să monitorizeze aplicarea dispozițiilor prevăzute de prezentul regulament și să contribuie la aplicarea consecventă a acestuia în întreaga Uniune, în scopul asigurării protecției persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal și al facilitării liberei circulații a datelor cu

caracter personal în interiorul pieței interne. În acest sens, autoritățile de supraveghere ar trebui să coopereze reciproc și cu Comisia.

(97) În cazul în care, în Uniune, prelucrarea datelor cu caracter personal în cadrul activităților unui sediu al unui operator sau al unei persoane împuternicite de către operator se efectuează în mai multe state membre, o singură autoritate de supraveghere ar trebui să aibă competența de a monitoriza activitățile operatorului sau ale persoanei împuternicite de către operator în întreaga Uniune și de a adopta deciziile aferente, în scopul intensificării aplicării consecvente, al furnizării securității juridice și al reducerii sarcinii administrative pentru astfel de operatori și de persoane împuternicite de către operatori.

(98) Autoritatea competentă, care furnizează un astfel de ghișeu unic, ar trebui să fie autoritatea de supraveghere a statului membru în care operatorul sau persoana împuternicită de către operator își are sediul principal.

(99) Cu toate că prezentul regulament se aplică, de asemenea, activităților instanțelor naționale, prelucrarea datelor cu caracter personal nu ar trebui să fie de competența autorităților de supraveghere, în cazul în care instanțele își exercită atribuțiile judiciare, în scopul asigurării protecției independenței judecătorilor în îndeplinirea sarcinilor lor judiciare. Cu toate acestea, derogarea ar trebui să se limiteze strict 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.

(100) Pentru a se asigura consecvența monitorizării și a aplicării prezentului regulament în întreaga Uniune, autoritățile de supraveghere ar trebui să aibă în fiecare stat membru aceleași atribuții și competențe efective, inclusiv competențe de investigare, de intervenție cu forță juridică obligatorie, de decizie și sancționare, în special în cazul plângerilor depuse de persoane fizice, precum și de a acționa în justiție. Competențele de investigare ale autorităților de supraveghere în ceea ce privește accesul în localuri ar trebui exercitate în conformitate cu dreptul Uniunii și cu legislația națională. Aceasta se referă, în special, la cerința de a obține în prealabil o autorizare judiciară.

(101) 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, sub control judiciar, în măsura în care este necesar, în funcție de caz. 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.

(102) Activitățile de creștere a gradului de conștientizare organizate pentru public de autoritățile de supraveghere ar trebui să includă măsuri specifice care să vizeze operatorii și persoanele împuternicite de către operatori, inclusiv microîntreprinderile și întreprinderile mici și mijlocii, precum și persoanele vizate.

(103) Autoritățile de supraveghere ar trebui să își acorde reciproc asistență în îndeplinirea atribuțiilor care le revin, pentru a se asigura consecvența aplicării și a asigurării aplicării prezentului regulament în piața internă.

(104) Fiecare autoritate de supraveghere ar trebui să aibă dreptul de a participa la operațiuni comune între autoritățile de supraveghere. Autoritatea de supraveghere căreia i s-a adresat solicitarea ar trebui să aibă obligația de a răspunde cererii într-un anumit termen.

(105) Pentru a se asigura aplicarea consecventă a prezentului regulament în întreaga Uniune, ar trebui să se instituie un mecanism pentru asigurarea coerenței în cadrul căruia autoritățile de supraveghere și Comisia să coopereze. Acest mecanism ar trebui să se aplice, în special, în cazul în care o autoritate de supraveghere intenționează să ia o măsură în ceea ce privește operațiunile de prelucrare care au legătură cu oferirea de bunuri sau servicii persoanelor vizate în mai multe state membre sau cu monitorizarea comportamentului unor astfel de persoane vizate sau care ar putea afecta în mod substanțial libera circulație a datelor cu caracter personal. Mecanismul ar trebui să se aplice, de asemenea, în cazul în care o autoritate de supraveghere sau Comisia solicită ca aspectul respectiv să fie abordat în cadrul mecanismului pentru asigurarea coerenței. Acest mecanism nu ar trebui să aducă atingere măsurilor pe care Comisia le poate adopta în exercitarea competențelor care îi revin în temeiul tratatelor.

(106) În aplicarea mecanismului pentru asigurarea coerenței, Comitetul european pentru protecția datelor ar trebui, într-un anumit termen, să emită un aviz în cazul în care o majoritate simplă a membrilor săi decide astfel sau în cazul în care o autoritate de supraveghere sau Comisia solicită acest lucru.

(107) Pentru a se asigura conformitatea cu prezentul regulament, Comisia poate adopta un aviz privind aspectul respectiv sau o decizie, prin care să se solicite autorității de supraveghere suspendarea proiectului său de măsură.

(108) Este posibil să existe o necesitate urgentă de a se acționa pentru asigurarea protecției intereselor persoanelor vizate, în special în cazul în care există pericolul ca exercitarea unui drept al unei persoane vizate să fie împiedicată în mod considerabil. Prin urmare, atunci când aplică mecanismul pentru asigurarea coerenței, o autoritate de supraveghere ar trebui să poată adopta măsuri provizorii, cu o anumită perioadă de valabilitate.

(109) Aplicarea acestui mecanism ar trebui să fie o condiție pentru valabilitatea juridică și executarea deciziei respective de către o autoritate de supraveghere. În alte cazuri cu relevanță transfrontalieră, autoritățile de supraveghere în cauză ar putea să își acorde reciproc asistență și să efectueze investigații comune, pe bază bilaterală sau multilaterală, fără declanșarea mecanismului pentru asigurarea coerenței.

(110) La nivelul Uniunii, ar trebui să se înființeze Comitetul european pentru protecția datelor. Acesta ar trebui să înlocuiască Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, instituit prin Directiva 95/46/CE. Acesta ar trebui să fie format din șefii autorității de supraveghere a fiecărui stat membru și din șeful Autorității Europene pentru Protecția Datelor. Comisia ar trebui să participe la activitățile sale. Comitetul european pentru protecția datelor ar trebui să contribuie la aplicarea consecventă a prezentului regulament în întreaga Uniune, inclusiv prin oferirea de consultanță Comisiei și prin promovarea cooperării autorităților de supraveghere în întreaga Uniune. Comitetul european pentru protecția datelor ar trebui să acționeze în mod independent în exercitarea sarcinilor sale.

(111) 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 o cale de atac, în cazul în care consideră că drepturile pe care le are în temeiul prezentului regulament 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.

(112) Orice organism, organizație sau asociație care are drept obiectiv asigurarea protecției drepturilor și 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 de a depune o plângere la o autoritate de supraveghere sau să exercite dreptul la o cale de atac în numele persoanelor vizate 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.

(113) Orice persoană fizică sau juridică ar trebui să aibă dreptul la o cale de atac împotriva deciziilor unei autorități de supraveghere care o privesc. Acțiunile inițiate împotriva unei autorități de supraveghere ar trebui să fie aduse în fața instanțelor statului membru în care este stabilită autoritatea de supraveghere.

(114) Pentru a se consolida protecția judiciară a persoanelor vizate în situațiile în care autoritatea de supraveghere competentă este stabilită în alt stat membru decât cel în care persoana vizată își are reședința, persoana vizată poate solicita oricărui organism, oricărei organizații sau oricărei asociații care are drept obiectiv asigurarea protecției drepturilor și intereselor persoanelor vizate în ceea ce privește protecția datelor acestora să introducă o acțiune în numele său împotriva autorității de supraveghere respective în fața instanței competente din celălalt stat membru.

(115) În situațiile în care autoritatea de supraveghere competentă stabilită în alt stat membru nu acționează sau a adoptat măsuri insuficiente în legătură cu o plângere, persoana vizată poate solicita autorității de supraveghere din statul membru în care își are reședința obișnuită să introducă o acțiune împotriva autorității de supraveghere respective în fața instanței competente din celălalt stat membru. Autoritatea de supraveghere poate decide, sub control judiciar, dacă este sau nu este oportun să se dea curs cererii.

(116) În ceea ce privește acțiunile inițiate împotriva unui operator sau unei persoane împuternicite de către operator, reclamantul ar trebui să aibă posibilitatea de a introduce acțiunea în fața instanțelor din statele membre în care operatorul sau persoana împuternicită de către operator are un sediu sau în care persoana vizată își are reședința, cu excepția cazului în care operatorul este o autoritate publică care acționează în exercitarea competențelor sale publice.

(117) În cazul în care există indicii conform cărora acțiuni paralele sunt pendinte în fața instanțelor din state membre diferite, instanțele ar trebui să aibă obligația de a se contacta reciproc. Instanțele ar trebui să aibă posibilitatea de a suspenda o acțiune atunci când o cauză paralelă este pendinte în alt stat membru. 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 prezentului regulament.

(118) Orice daună pe care o persoană o poate suferi din cauza unei prelucrări ilegale ar trebui să fie compensată de operator sau de persoana împuternicită de către operator, care poate fi exonerat(ă) de răspundere dacă dovedește că nu este răspunzător (răspunzătoare) pentru prejudiciu, în special în cazul în care acesta (aceasta) stabilește vina persoanei vizate sau în caz de forță majoră.

(119) Ar trebui impuse sancțiuni oricărei persoane, de drept privat sau public, care nu respectă prezentul regulament. 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.

(120) Pentru consolidarea și armonizarea sancțiunilor administrative în cazul încălcării prezentului regulament, fiecare autoritate de supraveghere ar trebui să aibă competența de a sancționa infracțiunile administrative. Prezentul regulament ar trebui să indice aceste infracțiuni și limita maximă a amenzilor administrative aferente, care ar trebui să fie stabilite în fiecare caz, proporțional cu situația specifică, luându-se în considerare în mod corespunzător, în special, natura, gravitatea și durata încălcării. Mecanismul pentru asigurarea coerenței poate fi, de asemenea, utilizat în scopul remedierii divergențelor în aplicarea sancțiunilor administrative.

(121) Prelucrarea datelor cu caracter personal exclusiv în scopuri jurnalistice, artistice sau literare ar trebui să îndeplinească criteriile pentru aplicarea unor derogări de la cerințele anumitor dispoziții din prezentul regulament, în vederea stabilirii unui echilibru între dreptul la protecția datelor cu caracter personal și dreptul la libertatea de exprimare și, mai ales, dreptul de a primi și de a comunica informații, astfel cum este garantat în special prin articolul 11 din Carta drepturilor fundamentale a Uniunii Europene. Acest lucru ar trebui să se aplice în special prelucrării datelor cu caracter personal din domeniul audiovizualului, precum și din arhivele de știri și din bibliotecile de ziare. Prin urmare, statele membre ar trebui să adopte măsuri legislative care să prevadă excepțiile și derogările necesare în vederea asigurării echilibrului între aceste drepturi fundamentale. Astfel de excepții și derogări ar trebui să fie adoptate de statele membre în ceea ce privește principiile generale, drepturile persoanelor vizate, operatorul și persoana împuternicită de operator, transferul de date cu caracter personal către țări terțe sau organizații internaționale, autoritățile de supraveghere independente, precum și cooperarea și coerența. Acest lucru nu trebuie totuși să determine statele membre să stabilească derogări de la celelalte dispoziții ale prezentului regulament. Pentru a ține seama de importanța dreptului la libertatea de exprimare în fiecare societate democratică, este necesar ca noțiunile legate de această libertate, cum ar fi jurnalismul, să fie interpretate în sens larg. Prin urmare, în scopul excepțiilor și derogărilor care urmează să fie stabilite în prezentul regulament, statele membre ar trebui să clasifice drept „jurnalistice” activitățile al căror scop este de a comunica publicului informații, opinii și idei, indiferent de suportul utilizat pentru transmiterea acestora. Aceste activități nu ar trebui să se limiteze la cele desfășurate de societăți de media și pot include activități cu sau fără scop lucrativ.

(122) Prelucrarea datelor cu caracter personal privind sănătatea, care reprezintă o categorie specială de date necesitând un nivel mai ridicat de protecție, poate fi adesea justificată de o serie de motive legitime în beneficiul persoanelor și al societății în general, în special în contextul asigurării continuității asistenței medicale transfrontaliere. Prin urmare, prezentul regulament ar trebui să prevadă condiții armonizate pentru prelucrarea datelor cu caracter personal privind sănătatea, sub rezerva unor garanții

specifice și corespunzătoare menite să protejeze drepturile fundamentale și datele cu caracter personal al persoanelor fizice. Acest lucru include dreptul persoanelor de a avea acces la datele lor cu caracter personal privind sănătatea, de exemplu datele din registrele lor medicale conținând informații precum diagnostice, rezultate ale examinărilor, evaluări ale medicilor curanți și orice tratament sau intervenție efectuată.

(123) Prelucrarea datelor cu caracter personal privind sănătatea poate fi necesară din motive de interes public în domeniile sănătății publice, fără consimțământul persoanei vizate. În acest context, conceptul de „sănătate publică" ar trebui interpretat astfel cum este definit în Regulamentul (CE) nr. 1338/2008 al Parlamentului European și al Consiliului din 16 decembrie 2008 privind statisticile comunitare referitoare la sănătatea publică, precum și la sănătatea și siguranța la locul de muncă, adică toate elementele referitoare la sănătate și anume starea de sănătate, inclusiv morbiditatea sau handicapul, factorii determinanți care au efect asupra stării de sănătate, necesitățile în domeniul asistenței medicale, resursele alocate asistenței medicale, furnizarea asistenței medicale și asigurarea accesului universal la aceasta, precum și cheltuielile și sursele de finanțare în domeniul sănătății și cauzele mortalității. Această prelucrare a datelor cu caracter personal privind sănătatea din motive de interes public nu ar trebui să ducă la prelucrarea acestor date în alte scopuri de către părți terțe, cum ar fi angajatorii, societățile de asigurări și băncile.

(124) Principiile generale privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal ar trebui să fie aplicabile și în contextul ocupării forței de muncă. Prin urmare, pentru a reglementa activitățile de prelucrare a datelor cu caracter personal ale angajaților în contextul ocupării forței de muncă, statele membre ar trebui să aibă posibilitatea, în limitele stabilite de prezentul regulament, de a adopta pe cale legislativă norme specifice de prelucrare a datelor cu caracter personal în sectorul ocupării forței de muncă.

(125) Pentru a fi legală, prelucrarea datelor cu caracter personal în scopuri de cercetare istorică, statistică sau științifică ar trebui să respecte și alte dispoziții legislative relevante, cum ar fi cele privind studiile clinice.

(126) În sensul prezentului regulament, cercetarea științifică ar trebui să includă cercetarea fundamentală, cercetarea aplicată și cercetarea finanțată din surse private și ar trebui, în plus, să ia în considerare obiectivul Uniunii de creare a unui spațiu european de cercetare, astfel cum este menționat la articolul 179 alineatul (1) din Tratatul privind funcționarea Uniunii Europene.

(127) În ceea ce privește competențele autorităților de supraveghere de a obține, de la operator sau de la persoana împuternicită de operator, accesul la datele cu caracter personal și accesul în clădirile sale, statele membre pot adopta, pe cale legislativă și în limitele stabilite de prezentul regulament, norme specifice pentru garantarea secretului profesional sau a altor obligații echivalente, în măsura în care acest lucru este necesar pentru a asigura un echilibru între dreptul la protecția datelor cu caracter personal și o obligație de păstrare a secretului profesional.

(128) Conform articolului 17 din Tratatul privind funcționarea Uniunii Europene, prezentul regulament respectă și nu aduce atingere statutului de care beneficiază, în temeiul dreptului național, bisericile și asociațiile sau comunitățile religioase din statele membre. Prin urmare, atunci când o biserică dintr-un stat membru aplică, la data

intrării în vigoare a prezentului regulament, norme cuprinzătoare de protecție a persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, aceste norme existente ar trebui să se aplice în continuare, în măsura în care se asigură conformitatea lor cu prezentul regulament. Ar trebui să se solicite acestor biserici și asociații religioase să prevadă instituirea unei autorități de supraveghere complet independente.

(129) Pentru a se realiza obiectivele prezentului regulament, 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 libera circulație a datelor cu caracter personal 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. În special, ar trebui adoptate acte delegate în ceea ce privește legalitatea prelucrării; specificarea criteriilor și a condițiilor de obținere a consimțământului unui minor; prelucrarea unor categorii speciale de date; specificarea criteriilor și a condițiilor aplicabile cererilor în mod vădit excesive și taxelor pentru exercitarea drepturilor persoanelor vizate; criteriile și cerințele aplicabile pentru informarea persoanei vizate și dreptul de acces; „dreptul de a fi uitat” și dreptul la ștergere; măsurile bazate pe crearea de profiluri; criteriile și cerințele privind responsabilitatea operatorului și protecția datelor începând cu momentul conceperii și protecția implicită a datelor; persoana împuternicită de operator; criteriile și cerințele privind documentația și securitatea prelucrării; criteriile și cerințele aplicabile pentru stabilirea unei încălcări a securității datelor cu caracter personal și pentru notificarea acesteia către autoritatea de supraveghere, precum și circumstanțele în care o încălcare a securității datelor cu caracter personal ar putea aduce atingere persoanei vizate; criteriile și condițiile pentru operațiunile de prelucrare care necesită o evaluare a impactului asupra protecției datelor; criteriile și cerințele pentru determinarea unui nivel ridicat al riscurilor specifice care necesită o consultare prealabilă; desemnarea și sarcinile responsabilului cu protecția datelor; codurile de conduită; criteriile și cerințele privind mecanismele de certificare; criteriile și cerințele pentru transferurile prin intermediul regulilor corporatiste obligatorii; derogările aplicabile transferului; sancțiunile administrative; prelucrarea în scopuri medicale; prelucrarea în contextul ocupării forței de muncă și prelucrarea în scopuri de cercetare istorică, statistică și științifică. 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.

(130) În vederea asigurării unor condiții uniforme de punere în aplicare a prezentului regulament, Comisia ar trebui investită cu competențe de executare pentru a stabili: formulare tip legate de prelucrarea datelor cu caracter personal ale minorilor; proceduri standard și formulare tip pentru exercitarea drepturilor persoanelor vizate; formulare tip pentru informarea persoanei vizate; formulare tip și proceduri standard referitoare la dreptul de acces; dreptul la portabilitatea datelor; formulare tip în ceea ce privește responsabilitatea operatorului de a asigura protecția datelor începând cu momentul conceperii și protecția implicită a datelor; cerințe specifice privind securitatea prelucrării; formatul și procedurile standard pentru notificarea unei încălcări a securității datelor cu caracter personal în atenția autorității de supraveghere și pentru comunicarea unei încălcări a securității datelor cu caracter personal către

persoana vizată; standarde și proceduri pentru o evaluare a impactului asupra protecției datelor; formele și procedurile de autorizare prealabilă și de consultare prealabilă; standarde tehnice și mecanisme de certificare; nivelul adecvat de protecție oferit de o țară terță, de un teritoriu sau de un sector de prelucrare din țara terță respectivă sau de o organizație internațională; divulgările de informații neautorizate de dreptul Uniunii; asistența reciprocă; operațiunile comune; deciziile în cadrul mecanismului pentru asigurarea coerenței. 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[45]. În acest context, Comisia ar trebui să ia în considerare măsuri specifice pentru microîntreprinderi și pentru întreprinderi mici și mijlocii.

(131) Procedura de examinare ar trebui să fie utilizată pentru a se stabili formulare tip legate de obținerea consimțământului unui minor; proceduri standard și formulare tip pentru exercitarea drepturilor persoanelor vizate; formulare tip pentru informarea persoanei vizate; formulare tip și proceduri standard referitoare la dreptul de acces; dreptul la portabilitatea datelor; formulare tip în ceea ce privește responsabilitatea operatorului de a asigura protecția datelor începând cu momentul conceperii și protecția implicită a datelor; cerințe specifice privind securitatea prelucrării; formatul și procedurile standard pentru notificarea unei încălcări a securității datelor cu caracter personal în atenția autorității de supraveghere și pentru comunicarea unei încălcări a securității datelor cu caracter personal către persoana vizată; standarde și proceduri pentru o evaluare a impactului asupra protecției datelor; formele și procedurile de autorizare prealabilă și de consultare prealabilă; standarde tehnice și mecanisme de certificare; nivelul adecvat de protecție oferit de o țară terță, de un teritoriu sau de un sector de prelucrare din țara terță respectivă sau de o organizație internațională; divulgările de informații neautorizate de dreptul Uniunii; asistența reciprocă; operațiunile comune; deciziile în cadrul mecanismului pentru asigurarea coerenței, dat fiind că aceste acte au un domeniu de aplicare general.

(132) 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 și referitoare la aspectele comunicate de către autoritățile de supraveghere în cadrul mecanismului pentru asigurarea coerenței.

(133) Dat fiind că obiectivele prezentului regulament, și anume asigurarea unui nivel echivalent de protecție a persoanelor și libera circulație a datelor în întreaga Uniune, nu pot fi realizate în mod satisfăcător de către statele membre și, prin urmare, având în vedere amploarea și efectele acțiunii, pot fi realizate mai bine la nivelul Uniunii, Uniunea poate să adopte măsuri în conformitate cu principiul subsidiarității, astfel cum este prevăzut la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, astfel cum este enunțat la articolul respectiv, prezentul regulament nu depășește ceea ce este necesar pentru atingerea acestui obiectiv.

---

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

(134) Directiva 95/46/CE ar trebui să fie abrogată prin prezentul regulament. Cu toate acestea, deciziile Comisiei care au fost adoptate și autorizațiile care au fost emise de autoritățile de supraveghere pe baza Directivei 95/46/CE ar trebui să rămână în vigoare.

(135) Prezentul regulament ar trebui să se aplice tuturor aspectelor referitoare la protecția drepturilor și a libertăților fundamentale legate de prelucrarea datelor cu caracter personal, care fac obiectul unor obligații specifice cu același obiectiv ca cel stabilit în Directiva 2002/58/CE, inclusiv obligațiile privind operatorul și drepturile persoanelor fizice. Pentru a se clarifica relația dintre prezentul regulament și Directiva 2002/58/CE, aceasta din urmă ar trebui să fie modificată în consecință.

(136) În ceea ce privește Islanda și Norvegia, prezentul regulament reprezintă o dezvoltare a dispozițiilor acquis-ului Schengen, în măsura în care se aplică prelucrării datelor cu caracter personal de către autoritățile implicate în punerea în aplicare a acquis-ului, astfel cum prevede Acordul încheiat de Consiliul Uniunii Europene și Republica Islanda și Regatul Norvegiei privind asocierea acestora din urmă la punerea în aplicare, respectarea și dezvoltarea acquis-ului Schengen[46].

(137) În ceea ce privește Elveția, prezentul regulament reprezintă o dezvoltare a dispozițiilor acquis-ului Schengen, în măsura în care se aplică prelucrării datelor cu caracter personal de către autoritățile implicate în punerea în aplicare a acquis-ului, astfel cum prevede Acordul între Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană cu privire la asocierea Confederației Elvețiene la punerea în aplicare, respectarea și dezvoltarea acquis-ului Schengen[47].

(138) În ceea ce privește Liechtenstein, prezentul regulament reprezintă o dezvoltare a dispozițiilor acquis-ului Schengen, în măsura în care se aplică prelucrării datelor cu caracter personal de către autoritățile implicate în punerea în aplicare a acquis-ului, astfel cum prevede Protocolul între Uniunea Europeană, Comunitatea Europeană, Confederația Elvețiană și Principatul Liechtenstein privind aderarea Principatului Liechtenstein la Acordul între Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană privind asocierea Confederației Elvețiene la punerea în aplicare, respectarea și dezvoltarea acquis-ului Schengen[48].

(139) Având în vedere faptul că, așa cum a subliniat Curtea de Justiție a Uniunii Europene, dreptul la protecția datelor cu caracter personal nu este un drept absolut, ci trebuie luat în considerare în raport cu funcția pe care o îndeplinește în societate și echilibrat cu alte drepturi fundamentale, în conformitate cu principiul proporționalității, prezentul regulament respectă drepturile fundamentale și principiile recunoscute în Carta drepturilor fundamentale a Uniunii Europene consacrată în tratate, în special dreptul la respectarea vieții private și de familie, a reședinței și a secretului comunicațiilor, dreptul la protecția datelor cu caracter personal, libertatea de gândire, de conștiință și de religie, libertatea de exprimare și de informare, libertatea de a desfășura o activitate comercială, dreptul la o cale de atac eficientă și la un proces echitabil, precum și diversitatea culturală, religioasă și lingvistică.

---

[46] JO L 176, 10.7.1999, p. 36.
[47] JO L 53, 27.2.2008, p. 52.
[48] JO L 160, 18.6.2011, p. 19.

ADOPTĂ PREZENTUL REGULAMENT:

CAPITOLUL I
DISPOZIȚII GENERALE

Articolul 1
Obiect și obiective

1. Prezentul regulament stabilește normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, precum și normele referitoare la libera circulație a datelor cu caracter personal.

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

3. Libera circulație a datelor cu caracter personal în cadrul Uniunii nu poate fi limitată sau interzisă din motive legate de protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.

Articolul 2
Domeniul material de aplicare

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

2. Prezentul regulament nu se aplică prelucrării datelor cu caracter personal:

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

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

   (c) de către statele membre atunci când desfășoară activități care intră sub incidența capitolului 2 din Tratatul privind Uniunea Europeană;

   (d) de către o persoană fizică, fără niciun interes lucrativ, în cadrul activităților sale exclusiv personale sau domestice;

   (e) de către autoritățile competente în scopul prevenirii, investigării, identificării sau urmăririi penale a infracțiunilor sau al executării sancțiunilor penale.

3. Prezentul regulament nu aduce atingere aplicării Directivei 2000/31/CE, în special a normelor privind răspunderea furnizorilor de servicii intermediari, prevăzute la articolele 12 - 15 din directiva menționată.

Articolul 3
Domeniul teritorial de aplicare

1. Prezentul regulament se aplică prelucrării datelor cu caracter personal în cadrul activităților unui sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii.

2. Prezentul regulament se aplică prelucrării datelor cu caracter personal ale persoanelor vizate care își au reședința în Uniune de către un operator care nu este stabilit în Uniune, atunci când activitățile de prelucrare sunt legate de:

   (a) oferirea de bunuri sau servicii unor astfel de persoane vizate în Uniune sau

   (b) urmărirea comportamentului acestora.

3. Prezentul regulament se aplică prelucrării datelor cu caracter personal de către un operator care nu este stabilit în Uniune, ci într-un loc în care legislația națională a unui stat membru se aplică în temeiul dreptului internațional public.

Articolul 4
Definiții

În sensul prezentului regulament:

(1) „persoana 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 un identificator 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, ștergerea sau distrugerea;

(4) „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;

(5) „operator” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau orice alt organism care, singur sau împreună cu altele, 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;

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

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

(8) „consimțământul persoanei vizate” înseamnă orice manifestare de voință, liberă, specifică, informată și explicită, prin care persoana vizată acceptă, printr-o declarație sau printr-o acțiune pozitivă fără echivoc, ca datele sale cu caracter personal să fie prelucrate;

(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) „sediu principal” înseamnă, în ceea ce privește operatorul, locul de stabilire al acestuia pe teritoriul Uniunii, în care sunt luate principalele decizii privind scopurile, condițiile și mijloacele de prelucrare a datelor cu caracter personal; în cazul în care nu se ia nicio decizie pe teritoriul Uniunii cu privire la scopurile, condițiile și mijloacele de prelucrare a datelor cu caracter personal, sediul principal este locul în care se desfășoară principalele activități de prelucrare în cadrul activităților unui sediu al unui operator din Uniune. În ceea ce privește persoana împuternicită de operator, „sediu principal” înseamnă locul administrației sale centrale din Uniune;

(14) „reprezentant” înseamnă orice persoană fizică sau juridică stabilită în Uniune, desemnată explicit de către operator, care acționează și poate fi contactată în locul operatorului de către orice autoritate de supraveghere și alte organisme din Uniune, în ceea ce privește obligațiile care îi revin operatorului în temeiul prezentului regulament;

(15) „întreprindere” înseamnă orice entitate care desfășoară o activitate economică, indiferent de forma juridică a acesteia, cuprinzând, în special, persoane fizice și juridice, parteneriate sau asociații care desfășoară în mod regulat o activitate economică;

(16) „grup de întreprinderi” înseamnă o întreprindere care exercită controlul și întreprinderile controlate de aceasta;

(17) „reguli corporatiste obligatorii” înseamnă politicile în materie de protecție a datelor cu caracter personal care trebuie respectate de către un operator sau o persoană împuternicită de operator stabilită pe teritoriul unui stat membru al Uniunii, în ceea ce privește transferurile sau seturile de transferuri de date cu caracter personal către un operator sau o persoană împuternicită în una sau mai multe țări terțe în cadrul unui grup de întreprinderi;

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

(19) „autoritate de supraveghere” înseamnă o autoritate publică instituită de un stat membru în conformitate cu articolul 46.

CAPITOLUL II
PRINCIPII

Articolul 5
Principii legate de prelucrarea datelor cu caracter personal

Datele cu caracter personal trebuie:

(a) să fie prelucrate în mod legal, echitabil și transparent față de persoana vizată;

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

(c) să fie adecvate, pertinente și limitate la strictul necesar în ceea ce privește scopurile pentru care sunt prelucrate; aceste date sunt prelucrate numai dacă și atât timp cât scopurile nu pot fi îndeplinite prin prelucrarea unor informații care nu implică date cu caracter personal;

(d) să fie exacte și 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, să fie 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; datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate numai în scopuri de cercetare istorică, statistică sau științifică, în conformitate cu normele și condițiile prevăzute la articolul 83, și numai dacă se efectuează o reexaminare periodică în vederea evaluării necesității de a continua stocarea;

(f) să fie prelucrate sub răspunderea operatorului, care asigură și demonstrează conformitatea fiecărei operațiuni de prelucrare cu dispozițiile prezentului regulament.

Articolul 6
Legalitatea prelucrării

1. Prelucrarea datelor cu caracter personal este legală numai dacă și în măsura în care se aplică cel puțin una dintre următoarele condiții:

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

   (b) prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru executarea unor măsuri precontractuale la cererea persoanei vizate;

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

   (d) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate;

   (e) prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul;

   (f) prelucrarea este necesară în scopul intereselor legitime urmărite de operator, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un minor. Acest lucru nu se aplică în cazul prelucrării efectuate de către autoritățile publice în îndeplinirea misiunii lor.

2. Prelucrarea datelor cu caracter personal necesară în scopuri de cercetare istorică, statistică sau științifică este legală sub rezerva condițiilor și a garanțiilor prevăzute la articolul 83.

3. Temeiul juridic pentru prelucrarea menționată la alineatul (1) literele (c) și (e) trebuie să fie prevăzut în:

   (a) dreptul Uniunii sau

   (b) legislația statului membru care se aplică operatorului.

   Legislația statului membru trebuie să urmărească un obiectiv de interes public sau să fie necesară în vederea protejării drepturilor și libertăților celorlalți, să respecte substanța dreptului de protecție a datelor cu caracter personal și să fie proporțională cu obiectivul legitim urmărit.

4. În cazul în care scopul prelucrării ulterioare nu este compatibil cu scopul pentru care au fost colectate datele cu caracter personal, prelucrarea trebuie să se bazeze pe un temei juridic care presupune cel puțin unul din considerentele menționate la alineatul (1) literele (a) - (e). Acest lucru se aplică în special oricărei schimbări a termenilor și condițiilor generale ale unui contract.

5. Comisia trebuie să fie abilitată să adopte acte delegate în conformitate cu articolul 86 în scopul detalierii condițiilor menționate la alineatul (1) litera (f) pentru diverse

sectoare și situații de prelucrare a datelor, inclusiv în ceea ce privește prelucrarea datelor cu caracter personal referitoare la un minor.

Articolul 7
Condiții privind consimțământul

1. Operatorul suportă sarcina probei în ceea ce privește acordarea de către persoana vizată a consimțământului pentru prelucrarea datelor sale cu caracter personal în scopurile specificate.

2. În cazul în care consimțământul persoanei vizate urmează să fie acordat în contextul unei declarații scrise care se referă și la un alt aspect, solicitarea de a acorda consimțământul trebuie să fie prezentată într-o formă care o diferențiază de celălalt aspect.

3. Persoana vizată are dreptul să își retragă în orice moment consimțământul. Retragerea consimțământului nu afectează legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia.

4. Consimțământul nu reprezintă un temei juridic pentru prelucrare atunci când există un dezechilibru semnificativ între poziția persoanei vizate și cea a operatorului.

Articolul 8
Prelucrarea datelor cu caracter personal ale minorilor

1. În sensul prezentului regulament, în ceea ce privește oferirea de servicii ale societății informaționale în mod direct unui minor, prelucrarea datelor cu caracter personal ale unui minor cu vârsta sub 13 ani este legală numai dacă și în măsura în care consimțământul este acordat sau autorizat de părintele sau de tutorele minorului. Operatorul depune toate eforturile rezonabile pentru a obține consimțământul verificabil, ținând seama de tehnologiile disponibile.

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

3. Comisia este abilitată să adopte acte delegate în conformitate cu articolul 86 în scopul detalierii criteriilor și cerințelor referitoare la metodele de a obține consimțământul verificabil menționate la alineatul (1). În acest sens, Comisia ia în considerare măsuri specifice pentru microîntreprinderi și pentru întreprinderi mici și mijlocii.

4. Comisia poate să stabilească formulare tip pentru metodele specifice de obținere a consimțământului verificabil menționat la alineatul (1). Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare prevăzută la articolul 87 alineatul (2).

Articolul 9

Prelucrarea categoriilor speciale de date cu caracter personal

1. Se interzice prelucrarea datelor cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, religia sau convingerile, apartenența sindicală, precum și prelucrarea datelor genetice sau a datelor privind sănătatea, viața sexuală, condamnările penale sau măsurile de securitate conexe.

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

   (a) persoana vizată și-a dat consimțământul pentru prelucrarea acestor date cu caracter personal, în condițiile prevăzute la articolele 7 și 8, cu excepția cazului în care dreptul Uniunii sau legislația unui stat membru prevede că interdicția menționată la alineatul (1) nu poată fi ridicată de persoana vizată sau

   (b) prelucrarea este necesară în scopul respectării obligațiilor și al exercitării unor drepturi specifice ale operatorului în domeniul dreptului muncii, în măsura în care acest lucru este autorizat de dreptul Uniunii sau de legislația unui stat membru care prevede garanții adecvate sau

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

   (d) prelucrarea este efectuată, în cadrul activităților lor legitime și cu garanții adecvate, de către o fundație, o asociație sau orice alt organism cu scop nelucrativ și cu specific politic, filozofic, religios sau sindical, cu condiția ca prelucrarea să se refere numai la membrii sau la foștii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente în legătură cu scopurile sale și ca datele să nu fie comunicate terților fără consimțământul persoanelor vizate sau

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

   (f) prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță sau

   (g) prelucrarea este necesară pentru îndeplinirea unei sarcini de interes public, executate în baza dreptului Uniunii sau a legislației unui stat membru, care prevede măsurile corespunzătoare pentru protejarea intereselor legitime ale persoanei vizate sau

   (h) prelucrarea datelor privind sănătatea este necesară în scopuri legate de sănătate și sub rezerva condițiilor și a garanțiilor prevăzute la articolul 81 sau

   (i) prelucrarea este necesară în scopuri de cercetare istorică, statistică sau științifică, sub rezerva condițiilor și a garanțiilor prevăzute la articolul 83 sau

   (j) prelucrarea datelor referitoare la condamnări penale sau la măsuri de securitate conexe se efectuează fie sub controlul autorității publice, fie atunci când prelucrarea este necesară pentru conformarea cu o obligație legală sau de

reglementare care îi revine operatorului, fie pentru îndeplinirea unei sarcini executate din considerente importante de interes public, în măsura în care prelucrarea este autorizată de dreptul Uniunii sau de legislația unui stat membru care prevede garanții adecvate. Un registru complet al condamnărilor penale este ținut numai sub controlul autorității publice.

3. Comisia este abilitată să adopte acte delegate în conformitate cu articolul 86 în scopul detalierii criteriilor, condițiilor și garanțiilor corespunzătoare pentru prelucrarea categoriilor speciale de date cu caracter personal menționate la alineatul (1), precum și derogările prevăzute la alineatul (2).

Articolul 10
Prelucrarea care nu permite identificarea

În cazul în care datele prelucrate de către un operator nu îi permit acestuia să identifice o persoană fizică, operatorul nu are obligația de a obține informații suplimentare pentru a identifica persoana vizată numai în scopul respectării unei dispoziții ale prezentului regulament.

CAPITOLUL III
DREPTURILE PERSOANEI VIZATE

SECȚIUNEA 1
TRANSPARENȚĂ ȘI MODALITĂȚI

Articolul 11
Transparența informațiilor și a comunicărilor

1. Operatorul aplică politici transparente și ușor de accesat în ceea ce privește prelucrarea datelor cu caracter personal și exercitarea drepturilor persoanelor vizate.

2. Operatorul transmite persoanei vizate orice informație și orice comunicare cu privire la prelucrarea datelor cu caracter personal într-o formă inteligibilă, utilizând un limbaj clar și simplu, adaptat în funcție de persoana vizată, în special pentru orice informație adresată în mod expres unui minor.

Articolul 12
Proceduri și mecanisme de exercitare a drepturilor persoanei vizate

1. Operatorul stabilește proceduri pentru furnizarea informațiilor prevăzute la articolul 14 și pentru exercitarea drepturilor persoanelor vizate menționate la articolul 13 și la articolele 15 - 19. Operatorul prevede în special mecanisme pentru facilitarea introducerii unei cereri privind acțiunile menționate la articolul 13 și la articolele 15 - 19. În cazul în care datele cu caracter personal fac obiectul unei prelucrări automatizate, operatorul prevede, de asemenea, modalitățile de introducere a cererilor pe cale electronică.

2. Operatorul informează persoana vizată fără întârziere și, cel târziu, în termen de o lună de la primirea cererii, dacă a fost luată vreo măsură în temeiul articolului 13 și al

articolelor 15 - 19 și furnizează informațiile solicitate. Acest termen poate fi prelungit cu încă o lună, în cazul în care mai multe persoanele vizate își exercită drepturile și cooperarea acestora este necesară într-o măsură rezonabilă pentru a evita eforturi inutile și disproporționate din partea operatorului. Informațiile sunt furnizate în scris. În cazul în care persoana vizată introduce o cerere în format electronic, informațiile sunt furnizate în format electronic, cu excepția cazului în care persoana vizată solicită un alt format.

3. În cazul în care operatorul refuză să ia măsuri la cererea persoanei vizate, acesta informează persoana vizată cu privire la motivele refuzului și la posibilitățile de a depune o plângere în fața autorității de supraveghere și de a introduce o cale de atac în justiție.

4. Informațiile și măsurile luate în contextul cererilor menționate la alineatul (1) sunt gratuite. În cazul în care cererile sunt în mod vădit excesive, în special din cauza caracterului lor repetitiv, operatorul poate percepe o taxă pentru furnizarea informațiilor sau pentru luarea măsurilor solicitate ori poate să nu ia măsurile solicitate. În acest caz, operatorul suportă sarcina probei în ceea ce privește caracterul vădit excesiv al cererii.

5. Comisia este abilitată să adopte acte delegate în conformitate cu articolul 86 în scopul detalierii criteriilor și condițiilor privind cererile vădit excesive și taxele menționate la alineatul (4).

6. Comisia poate stabili formulare tip și proceduri standard în ceea ce privește comunicarea menționată la alineatul (2), inclusiv în format electronic. În acest sens, Comisia ia în considerare măsuri corespunzătoare pentru microîntreprinderi și pentru întreprinderi mici și mijlocii. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare prevăzută la articolul 87 alineatul (2).

Articolul 13
Drepturi referitoare la destinatari

Operatorul comunică fiecărui destinatar căruia i-au fost dezvăluite datele orice rectificare sau ștergere efectuată în conformitate cu articolele 16 și 17, cu excepția cazului în care acest lucru se dovedește imposibil sau presupune un efort disproporționat.

SECȚIUNEA 2
INFORMARE ȘI ACCES LA DATE

Articolul 14
Informații pentru persoana vizată

1. Atunci când sunt colectate date cu caracter personal referitoare la o persoană vizată, operatorul furnizează persoanei vizate cel puțin următoarele informații:

   (a) identitatea și datele de contact ale operatorului și, după caz, ale reprezentantului operatorului și ale responsabilului cu protecția datelor;

(b) scopurile în care sunt prelucrate datele cu caracter personal, inclusiv condițiile contractului și condițiile generale în cazul în care prelucrarea se întemeiază pe articolul 6 alineatul (1) litera (b) și interesele legitime urmărite de operator în cazul în care prelucrarea se întemeiază pe articolul 6 alineatul (1) litera (f);

(c) perioada în care vor fi stocate datele cu caracter personal;

(d) existența dreptului de a solicita operatorului accesul la datele cu caracter personal referitoare la persoana vizată, precum și rectificarea sau ștergerea acestora, sau a dreptului de a se opune prelucrării acestor date cu caracter personal;

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

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

(g) dacă este cazul, intenția operatorului de a efectua un transfer către o țară terță sau o organizație internațională și nivelul de protecție oferit de țara terță sau de organizația internațională respectivă, prin trimitere la o decizie a Comisiei privind caracterul adecvat al nivelului de protecție;

(h) orice altă informație necesară pentru garantarea unei prelucrări corecte față de persoana vizată, având în vedere circumstanțele specifice în care sunt colectate 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. În cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, operatorul transmite persoanei vizate, în plus față de informațiile menționate la alineatul (1), informații privind sursele din care provin datele cu caracter personal.

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

(a) în momentul în care datele cu caracter personal sunt colectate de la persoana vizată sau

(b) în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, în momentul înregistrării acestora sau într-un termen rezonabil după colectare, ținând seama de circumstanțele specifice în care datele respective sunt colectate sau prelucrate în alt mod sau dacă se preconizează comunicarea acestora către un alt destinatar, și cel târziu în momentul în care datele sunt comunicate pentru prima dată.

5. Dispozițiile alineatelor (1) - (4) nu se aplică atunci când:

(a) persoana vizată deține deja informațiile menționate la alineatele (1), (2) și (3) sau

(b) datele nu sunt colectate de la persoana vizată, iar furnizarea acestor informații se dovedește imposibilă sau ar presupune un efort disproporționat sau

(c) datele nu sunt colectate de la persoana vizată, iar înregistrarea sau divulgarea datelor este prevăzută în mod expres de lege sau

(d) datele nu sunt colectate de la persoana vizată, iar furnizarea acestor informații aduce atingere drepturilor și libertăților altor persoane, astfel cum sunt definite în dreptul Uniunii sau în legislația unui stat membru, în conformitate cu articolul 21.

6. În cazul menționat la alineatul (5) litera (b), operatorul prevede măsuri corespunzătoare pentru protejarea intereselor legitime ale persoanei vizate.

7. Comisia este abilitată să adopte acte delegate în conformitate cu articolul 86 în scopul detalierii criteriilor privind categoriile de destinatari menționate la alineatul (1) litera (f), a cerințelor privind notificarea posibilității de acces menționate la alineatul (1) litera (g), a criteriilor privind informațiile suplimentare necesare menționate la alineatul (1) litera (h) pentru sectoare și situații specifice, precum și a condițiilor și a garanțiilor corespunzătoare pentru derogările prevăzute la alineatul (5) litera (b). În acest sens, Comisia ia în considerare măsuri corespunzătoare pentru microîntreprinderi și pentru întreprinderi mici și mijlocii.

8. Comisia poate stabili formulare tip pentru transmiterea informațiilor menționate la alineatele (1) - (3), ținând seama, dacă este cazul, de particularitățile și nevoile specifice ale diverselor sectoare și situații de prelucrare a datelor. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare prevăzută la articolul 87 alineatul (2).

Articolul 15
Dreptul de acces al persoanei vizate

1. Persoana vizată are dreptul de a obține din partea operatorului, în orice moment, la cerere, confirmarea faptului că datele sale cu caracter personal sunt sau nu prelucrate. 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 datele cu caracter personal urmează să le fie divulgate sau le-au fost divulgate, în special dacă destinatarii sunt din țări terțe;

(d) perioada în care vor fi stocate datele cu caracter personal;

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

(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 sunt în curs de prelucrare și a oricărei informații disponibile cu privire la originea datelor;

(h) importanța și consecințele preconizate ale prelucrării, cel puțin în cazul măsurilor menționate la articolul 20.

2. Persoana vizată are dreptul de a obține din partea operatorului comunicarea datelor cu caracter personal care sunt în curs de prelucrare. În cazul în care persoana vizată introduce o cerere în format electronic, informațiile sunt furnizate în format electronic, cu excepția cazului în care persoana vizată solicită un alt format.

3. Comisia este abilitată să adopte acte delegate în conformitate cu articolul 86 în scopul detalierii criteriilor și cerințelor privind comunicarea către persoana vizată a conținutului datelor cu caracter personal menționate la alineatul (1) litera (g).

4. Comisia poate specifica formele și procedurile standard pentru solicitarea și acordarea accesului la informațiile menționate la alineatul (1), inclusiv pentru verificarea identității persoanei vizate și comunicarea datelor cu caracter personal către persoana vizată, ținând seama de particularitățile și nevoile specifice pentru diferitele sectoare și situații de prelucrare a datelor. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare prevăzută la articolul 87 alineatul (2).

SECȚIUNEA 3
RECTIFICARE ȘI ȘTERGERE

Articolul 16
Dreptul la rectificare

Persoana vizată are dreptul de a obține de la operator rectificarea datelor sale cu caracter personal care sunt inexacte. Persoana vizată are dreptul de a obține completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declarații corective suplimentare.

Articolul 17
Dreptul de a fi uitat și de a fi șters

1. Persoana vizată are dreptul de a obține din partea operatorului ștergerea datelor cu caracter personal care o privesc și încetarea difuzării acestor date, în special în ceea ce privește datele cu caracter personal care sunt puse la dispoziție de către persoana vizată atunci când era minor, în cazul în care se aplică unul dintre următoarele motive:

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

(b) persoana vizată își retrage consimțământul pe baza căruia are loc prelucrarea în conformitate cu articolul 6 alineatul (1) litera (a) sau în cazul în care perioada de stocare a datelor a expirat și nu există niciun alt temei legal pentru prelucrarea datelor;

(c) persoana vizată se opune prelucrării datelor cu caracter personal în temeiul articolului 19;

(d) prelucrarea datelor nu este conformă cu prezentul regulament din alte motive.

2. În cazul în care operatorul menționat la alineatul (1) a făcut publice datele cu caracter personal, acesta ia toate măsurile rezonabile, inclusiv măsuri tehnice, în ceea ce privește datele de a căror publicare este responsabil, pentru a informa terții care prelucrează astfel de date că persoana vizată le solicită să șteargă toate linkurile către datele cu caracter personal și orice copie sau reproducere a acestora. În cazul în care operatorul a autorizat un terț să publice date cu caracter personal, se consideră că operatorul este responsabil de publicarea datelor respective.

3. Operatorul efectuează ștergerea fără întârziere, cu excepția cazului în care păstrarea datelor cu caracter personal este necesară:

(a) pentru exercitarea dreptului la liberă exprimare, în conformitate cu articolul 80;

(b) din motive de interes public în domeniul sănătății publice, în conformitate cu articolul 81;

(c) în scopuri istorice, statistice și științifice, în conformitate cu articolul 83;

(d) pentru respectarea obligației legale de a păstra datele cu caracter personal prevăzută în legislația Uniunii sau a statului membru aplicabilă operatorului; legislațiile statelor membre trebuie să răspundă unui obiectiv de interes public, să respecte esența dreptului la protecția datelor cu caracter personal și să fie proporționale cu obiectivul legitim urmărit;

(e) în cazurile prevăzute la alineatul (4).

4. În loc să le șteargă, operatorul limitează prelucrarea datelor 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) operatorul nu mai are nevoie de datele cu caracter personal pentru a-și îndeplini atribuțiile, dar acestea trebuie să fie păstrate ca dovadă;

(c) prelucrarea acestora este ilegală, iar persoana vizată se opune ștergerii datelor, solicitând, în schimb, restricționarea utilizării lor;

(d) persoana vizată solicită transferul datelor cu caracter personal în alt sistem de prelucrare automată a datelor, în conformitate cu articolul 18 alineatul (2).

5. Datele cu caracter personal menționate la alineatul (4) pot fi prelucrate, cu excepția stocării, doar în scop probatoriu, fie cu consimțământul persoanei vizate, fie pentru protejarea drepturilor altor persoane fizice ori juridice fie pentru un obiectiv de interes public.

6. În cazul în care prelucrarea datelor cu caracter personal este limitată în conformitate cu alineatul (4), operatorul informează în acest sens persoana vizată înainte de ridicarea restricțiilor de prelucrare.

7. Operatorul pune în aplicare mecanisme pentru a asigura respectarea termenelor stabilite pentru ștergerea datelor cu caracter personal și/sau pentru o revizuire periodică a necesității de stocare a datelor.

8. În cazul în care se efectuează ștergerea, operatorul nu prelucrează în niciun alt fel datele personale.

9. Comisia este mandatată să adopte acte delegate în conformitate cu articolul 86 în scopul de a detalia:

   (a) criteriile și cerințele privind aplicarea alineatului (1) în anumite sectoare și în anumite situații de prelucrare a datelor;

   (b) condițiile de ștergere a linkurilor către datele cu caracter personal, a copiilor sau a reproducerilor acestora de care dispun serviciile de comunicații accesibile publicului, astfel cum se menționează la alineatul (2);

   (c) criteriile și condițiile de restricționare a prelucrării datelor cu caracter personal prevăzute la alineatul (4).

Articolul 18
Dreptul la portabilitatea datelor

1. În cazul în care datele cu caracter personal sunt prelucrate electronic într-un format structurat care este utilizat în mod curent, persoana vizată are dreptul să obțină, din partea operatorului, o copie a datelor care fac obiectul prelucrării electronice într-un format electronic structurat care este utilizat în mod curent și care permite persoanei vizate să utilizeze ulterior aceste date.

2. În cazul în care persoana vizată a furnizat datele cu caracter personal și prelucrarea se bazează pe consimțământul acesteia sau pe un contract, persoana vizată are dreptul de a transmite aceste date cu caracter personal, precum și orice altă informație furnizată de persoana vizată și păstrată de un sistem automatizat de prelucrare, într-un alt sistem, într-un format electronic care este utilizat în mod curent, fără ca operatorul de la care sunt retrase datele cu caracter personal să poată împiedica acest lucru.

3. Comisia poate specifica formatul electronic prevăzut la alineatul (1), precum și normele tehnice, modalitățile și procedurile de transmitere a datelor cu caracter personal în conformitate cu alineatul (2). Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare prevăzută la articolul 87 alineatul (2).

SECȚIUNEA 4
DREPTUL LA OPOZIȚIE ȘI CREAREA DE PROFILURI

Articolul 19
Dreptul la opoziție

1. În orice moment, persoana vizată are dreptul de a se opune, pe motive legate de situația specială în care se află, prelucrării datelor cu caracter personal pe care se bazează pe articolul 6 alineatul (1) literele (d), (e) și (f), cu excepția cazului în care operatorul demonstrează că motivele legitime și imperioase care justifică prelucrarea primează asupra intereselor sau a drepturilor și libertăților fundamentale ale persoanei vizate.

2. Atunci când prelucrarea datelor cu caracter personal are drept scop marketingul direct, persoana vizată are dreptul de a se opune gratuit prelucrării datelor sale cu caracter personal în acest scop. Acest drept este explicit oferit persoanei vizate, într-un mod inteligibil, care să se poată distinge în mod clar de alte informații.

3. În cazul în care există o opoziție în conformitate cu alineatele (1) și (2), operatorul nu mai utilizează sau nu mai prelucrează respectivele datele cu caracter personal.

Articolul 20
Măsuri bazate pe crearea de profiluri

1. Orice persoană fizică are dreptul de a nu fi supusă unei măsuri care produce efecte juridice privind această persoană fizică sau care o afectează în mod semnificativ și care se bazează exclusiv pe prelucrarea automată menită să evalueze anumite aspecte personale privind această persoană fizică sau să analizeze ori să prevadă, în special, performanțele persoanei fizice la locul de muncă, situația sa economică, locul în care se află, sănătatea, preferințele personale, încrederea de care se bucură sau comportamentul acestuia.

2. Sub rezerva celorlalte dispoziții din prezentul regulament, o persoană poate fi supusă unei măsuri de acest tip, astfel cum se prevede la alineatul (1), numai dacă prelucrarea datelor:

   (a) se efectuează în faza de încheiere sau de executare a unui contract, atunci când a fost acceptată cererea de încheiere sau de executare a contractului, depusă de persoana vizată sau atunci când au fost invocate măsuri corespunzătoare intereselor legitime ale persoanei vizate, cum ar fi dreptul de a obține intervenție umană; sau

   (b) este autorizat în mod expres de legislația Uniunii sau a unui stat membru, care prevede, de asemenea, măsuri corespunzătoare pentru protejarea intereselor legitime ale persoanei vizate; sau

   (c) se bazează pe consimțământul persoanei vizate, sub rezerva condițiilor prevăzute la articolul 7 și a unor garanții corespunzătoare.

3. Prelucrarea automată a datelor cu caracter personal menite să evalueze anumite aspecte personale referitoare la o persoană fizică nu se bazează exclusiv pe categoriile speciale de date cu caracter personal la care se face referire la articolul 9.

4. În cazurile menționate la alineatul (2), informațiile pe care operatorul trebuie să le furnizeze în temeiul articolului 14 includ informații despre existența prelucrării, pentru o măsură de tipul celei la care se face referire la alineatul (1), precum și despre efectele preconizate ale acestei prelucrări asupra persoanei vizate.

5. Comisia este mandatată să adopte acte delegate în conformitate cu articolul 86 în scopul detalierii criteriilor și a cerințelor aferente măsurilor corespunzătoare pentru protejarea intereselor legitime ale persoanei vizate menționate la alineatul (2).

SECȚIUNEA 5
RESTRICȚII

Articolul 21
Restricții

1. Legislația Uniunii sau a statului membru poate restrânge printr-o măsură legislativă domeniul de aplicare a obligațiilor și a drepturilor prevăzute la articolul 5 literele (a) - (e), la articolele 11 - 20 și la articolul 32, atunci când o astfel de restricție constituie o măsură necesară și proporțională într-o societate democratică pentru a:

   (a) garanta securitatea publică;

   (b) asigura prevenirea, cercetarea, depistarea și urmărirea în justiție a infracțiunilor;

   (c) proteja alte interese publice ale Uniunii Europene sau ale unui stat membru, în special un interes economic sau financiar important al Uniunii sau al unui stat membru, inclusiv în domeniile monetar, bugetar și fiscal, precum și stabilitatea și integritatea pieței;

   (d) asigura prevenirea, investigarea, detectarea și punerea sub urmărire a încălcării eticii în cazul profesiunilor reglementate;

   (e) asigura funcția de monitorizare, inspectare sau reglementare legată, chiar și ocazional, de exercitarea autorității publice în cazurile menționate la literele (a), (b),(c) și (d);

   (f) asigura protecția persoanei vizate sau a drepturilor și libertăților altora.

2. În special, orice măsură legislativă menționată la alineatul (1) conține dispoziții specifice, cel puțin în ceea ce privește obiectivele care trebuie avute în vedere în cadrul procesului de prelucrare și stabilirea operatorului.

CAPITOLUL IV
OPERATORUL ȘI PERSOANA ÎMPUTERNICITĂ DE CĂTRE OPERATOR

SECȚIUNEA 1
OBLIGAȚII GENERALE

Articolul 22
Responsabilitatea operatorului

1. Operatorul adoptă politici și pune în aplicare măsuri adecvate pentru a garanta și a putea demonstra că prelucrarea datelor cu caracter personal se efectuează în conformitate cu prezentul regulament.

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

   (a) păstrarea documentației, în conformitate cu articolul 28;

   (b) punerea în aplicare a cerințelor privind securitatea datelor prevăzute la articolul 30;

   (c) efectuarea unei evaluări a impactului privind protecția datelor, în conformitate cu articolul 33;

   (d) respectarea cerințelor privind autorizarea prealabilă sau consultarea prealabilă a autorității de supraveghere, în conformitate cu articolul 34 alineatele (1) și (2);

   (e) desemnarea unui responsabil cu protecția datelor, în conformitate cu articolul 35 alineatul (1).

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

4. Comisia este mandatată să adopte acte delegate în conformitate cu articolul 86 în scopul detalierii criteriilor și a cerințelor măsurilor corespunzătoare menționate la alineatul (1), altele decât cele menționate la alineatul (2), condițiile pentru verificare și mecanismele de audit menționate la alineatul (3) și criteriile de proporționalitate prevăzute la alineatul (3), și în scopul de a prevedea măsuri specifice pentru microîntreprinderi și pentru întreprinderile mici și mijlocii.

Articolul 23
Protecția datelor începând cu momentul conceperii și protecția implicită a datelor

1. Având în vedere stadiul actual al tehnicii și costurile de implementare, operatorul pune în aplicare, atât în momentul stabilirii mijloacelor de prelucrare, cât și pe parcursul prelucrării propriu-zise, măsuri și proceduri tehnice și organizatorice

corespunzătoare astfel încât prelucrarea să îndeplinească cerințele prezentului regulament și să asigure protecția drepturilor persoanei vizate.

2. Operatorul pune în aplicare mecanisme care garantează că, implicit, se prelucrează numai datele cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării și că aceste date colectate sau păstrate nu depășesc pragul minim necesar pentru îndeplinirea acestor scopuri, atât în ceea ce privește volumul datelor, cât și perioada de stocare a acestora. În special, aceste mecanisme asigură că, implicit, datele cu caracter personal nu sunt accesibile unui număr nelimitat de persoane.

3. Comisia este mandatată să adopte acte delegate în conformitate cu articolul 86 în scopul detalierii criteriilor și a cerințelor aferente măsurilor și mecanismelor de certificare menționate la alineatele (1) și (2), în special în ceea ce privește cerințele legate de protecția datelor începând cu momentul conceperii aplicabile în cazul tuturor sectoarelor, al produselor și al serviciilor.

4. Comisia poate stabili standarde tehnice pentru cerințele menționate la alineatele (1) și (2). Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare prevăzută la articolul 87 alineatul (2).

Articolul 24
Operatori asociați

Atunci când un operator stabilește, împreună cu alți operatori, scopul, condițiile și mijloacele de prelucrare a datelor cu caracter personal, operatorii asociați stabilesc, de comun acord, responsabilitățile fiecăruia în ceea ce privește îndeplinirea obligațiilor care le revin în temeiul prezentului regulament, în special în ceea ce privește procedurile și mecanismele de exercitare a drepturilor persoanelor vizate, prin intermediul unui acord între acestea.

Articolul 25
Reprezentanții operatorilor care nu își au sediul în Uniune

1. În situația menționată la articolul 3 alineatul (2), operatorul desemnează un reprezentant în Uniune.

2. Prezenta obligație nu se aplică:

   (a) unui operator cu sediul într-o țară terță, în cazul în care Comisia a decis că această țară terță asigură un nivel adecvat de protecție în conformitate cu articolul 41; sau

   (b) unei întreprinderi cu mai puțin de 250 de angajați; sau

   (c) unei autorități sau unui organism public; sau

   (d) unui operator care furnizează numai ocazional bunuri sau servicii persoanelor vizate care își au reședința pe teritoriul Uniunii.

3. Reprezentantul își are sediul în unul dintre statele membre în care își au reședința persoanele vizate ale căror date cu caracter personal sunt prelucrate în legătură cu furnizarea de bunuri și servicii sau a căror conduită este monitorizată.

4. Desemnarea unui reprezentant de către operator nu aduce atingere acțiunilor în justiție care ar putea fi introduse împotriva operatorului însuși.

Articolul 26
Persoana împuternicită de către operator

1. În cazul în care o operațiune de prelucrare se realizează în numele operatorului, operatorul alege o persoană împuternicită care oferă garanții suficiente pentru punerea în aplicare a măsurilor și a procedurilor tehnice și organizatorice adecvate, astfel încât prelucrarea să respecte cerințele prevăzute în prezentul regulament și să asigure protecția drepturilor persoanei vizate, în special în ceea ce privește măsurile de securitate tehnică și de organizare privind prelucrarea care urmează să fie efectuată, și veghează la respectarea acestor măsuri.

2. Modul în care o persoană împuternicită de către operator efectuează prelucrarea este reglementată printr-un contract sau printr-un alt act juridic care obligă persoana împuternicită de către operator în raport cu operatorul și care prevede, în special, că persoana împuternicită de către operator:

   (a) acționează numai la instrucțiunile operatorului, în special în cazul în care transferul de date cu caracter personal utilizate este interzis;

   (b) angajează numai personal care s-a angajat să respecte confidențialitatea sau care sunt obligați prin lege să respecte confidențialitatea;

   (c) adoptă toate măsurile necesare în conformitate cu articolul 30;

   (d) recrutează o altă persoană împuternicită de către operator numai cu autorizarea prealabilă a operatorului;

   (e) în măsura în care acest lucru este posibil, având în vedere caracterul prelucrării, creează, în acord cu operatorul, condițiile tehnice și organizatorice necesare pentru ca operatorul să își îndeplinească obligația de a răspunde cererilor privind exercitarea, de către persoana vizată, a drepturilor prevăzute în capitolul III;

   (f) ajută operatorul să asigure respectarea obligațiilor prevăzute la articolele 30 - 34;

   (g) transmite operatorului toate rezultatele după terminarea procesului de prelucrare și nu prelucrează în nici un alt mod datele cu caracter personal;

   (h) pune la dispoziția operatorului și a autorității de supraveghere toate informațiile necesare pentru a se controla respectarea obligațiilor prevăzute în prezentul articol.

3. Operatorul și persoana împuternicită de către operator păstrează o dovadă scrisă a instrucțiunilor prezentate de operator și a obligațiilor care îi revin persoanei împuternicite de către operator menționate la alineatul (2).

4. În cazul în care o persoană împuternicită de către operator prelucrează datele cu caracter personal într-un alt mod decât cel prevăzut în instrucțiunile date de operator, persoana împuternicită de către operator este considerată responsabilă de prelucrarea datelor în ceea ce privește prelucrarea respectivă și face obiectul dispozițiilor privind operatorii asociați prevăzute la articolul 24.

5. Comisia este mandatată să adopte acte delegate în conformitate cu articolul 86 în scopul detalierii criteriilor și a cerințelor aferente responsabilităților, drepturilor și sarcinilor unei persoane împuternicite de către operator în conformitate cu alineatul (1), precum și condițiilor care permit facilitarea procesului de prelucrare a datelor cu caracter personal în cadrul unui grup de întreprinderi, în special pentru verificare și raportare.

Articolul 27

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

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

Articolul 28

Documentația

1. Fiecare operator și persoană împuternicită de operator și, dacă este cazul, reprezentantul operatorului, păstrează documentația referitoare la toate operațiunile de prelucrare derulate sub responsabilitatea sa.

2. Această documentație cuprinde cel puțin următoarele informații:

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

   (b) numele și datele de contact ale responsabilului cu protecția datelor, dacă este cazul;

   (c) scopul prelucrării datelor, inclusiv interesele legitime urmărite de responsabilul cu prelucrarea, atunci când prelucrarea se bazează pe articolul 6 alineatul (1) litera (f);

   (d) o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal care le privesc;

(e) destinatarii sau categoriile de destinatari ai datelor cu caracter personal, inclusiv operatorii cărora le sunt comunicate datele cu caracter personal în interesul legitim pe care îl urmăresc;

(f) dacă este cazul, transferurile de date către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și, în cazul transferurilor prevăzute la articolul 44 alineatul (1) litera (h), documentația care dovedește existența unor garanții corespunzătoare;

(g) o indicație generală a termenelor-limită pentru ștergerea diferitelor categorii de date;

(h) descrierea mecanismelor prevăzute la articolul 22 alineatul (3).

3. Operatorul și persoana împuternicită de către operator și, dacă este cazul, reprezentantul operatorului, pune documentația la dispoziția autorității de supraveghere, la cererea acesteia.

4. Obligațiile menționate la alineatele (1) și (2) nu se aplică următoarelor categorii de operatori și persoane împuternicite de către operatori:

(a) persoanelor fizice care prelucrează date cu caracter personal fără vreun interes comercial; sau

(b) întreprinderilor sau organizațiilor cu mai puțin de 250 de angajați care prelucrează date cu caracter personal doar ca o activitate auxiliară activităților sale principale.

5. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 86 în scopul detalierii criteriilor și a cerințelor referitoare la documentația la care se face referire la alineatul (1), pentru a ține seama în special de responsabilitățile operatorului și ale persoanei împuternicite de către operator și, dacă este cazul, de responsabilitățile reprezentantului operatorului.

6. Comisia poate să conceapă formulare standard pentru documentele la care se face referire la alineatul (1). Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare prevăzută la articolul 87 alineatul (2).

Articolul 29

Cooperarea cu autoritatea de supraveghere

1. Operatorul și persoana împuternicită de către operator și, dacă este cazul, reprezentantul operatorului, cooperează, la cerere, cu autoritatea de supraveghere pentru a-și îndeplini sarcinile care le revin, în special prin furnizarea informațiilor menționate la articolul 53 alineatul (2) litera (a) și prin asigurarea accesului prevăzut la același alineat litera (b).

2. Ca urmare a exercitării, de către autoritatea de supraveghere, a competențelor prevăzute la articolul 53 alineatul (2), operatorul și persoana împuternicită de către operator răspund autorității de supraveghere într-un termen rezonabil stabilit de către

autoritatea de supraveghere. Răspunsul include o descriere a măsurilor adoptate și a rezultatelor obținute, ca răspuns la observațiile autorității de supraveghere.

SECȚIUNEA 2
SECURITATEA DATELOR

Articolul 30
Securitatea prelucrării

1. Operatorul și persoana împuternicită de către operator pun în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura un nivel de securitate, în concordanță cu riscurile pe care le presupune prelucrarea și cu caracterul datelor cu caracter personal care trebuie protejate, având în vedere stadiul actual al tehnologiei și costurile punerii lor în aplicare.

2. În urma unei evaluări a riscurilor, operatorul și persoana împuternicită de operator adoptă măsurile prevăzute la alineatul (1) pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale ori a pierderii accidentale, și pentru prevenirea oricărei forme de prelucrare ilegală, în special divulgarea, accesul sau diseminarea neautorizată ori modificarea datelor cu caracter personal.

3. Comisia este mandatată să adopte acte delegate în conformitate cu articolul 86 în scopul detalierii criteriilor și a cerințelor referitoare la măsurile tehnice și organizatorice prevăzute la alineatele (1) și (2), stabilind inclusiv care este stadiul actual al tehnologiei pentru anumite sectoare și în anumite situații de prelucrare a datelor, ținând seama în special de evoluția tehnologiei și a soluțiilor de proiectare pentru protecția datelor începând cu momentul conceperii și cel al protecției implicite a datelor, cu excepția cazului în care se aplică alineatul (4).

4. Comisia poate adopta, dacă este cazul, acte de punere în aplicare pentru specificarea cerințelor prevăzute la alineatele (1) și (2) în diverse situații, în special pentru a:

   (a) preveni accesul neautorizat la date cu caracter personal;

   (b) preveni orice act neautorizat de divulgare, citire, copiere, modificare, ștergere sau eliminare a datelor cu caracter personal;

   (c) asigura verificarea legalității operațiunilor de prelucrare.

   Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare prevăzută la articolul 87 alineatul (2).

Articolul 31
Notificarea autorității de supraveghere în cazul încălcării securității datelor cu caracter personal

1. În cazul în care are loc o încălcare a securității datelor cu caracter personal, operatorul notifică acest lucru autorității 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. Notificarea autorității de supraveghere trebuie să fie

însoțită de o explicație motivată în cazul în care aceasta nu are loc în termen de 24 de ore.

2. În conformitate cu articolul 26 alineatul (2) litera (f), persoana împuternicită de către operator îl previne și îl informează pe operator imediat după ce s-a constatat încălcarea 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 și categoriile și numărul de înregistrări de date în cauză;

   (b) să comunice identitatea și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;

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

   (d) să descrie consecințele 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. 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. Această documentație trebuie să permită autorității de supraveghere să verifice conformitatea cu prezentul articol. Documentația respectivă include numai informațiile necesare în acest scop.

5. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 86 în scopul de a indica mai detaliat criteriile și cerințele 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 un format standard al notificării adresate autorității de supraveghere, procedurile aplicabile în cazul obligației de notificare și forma și modalitățile de întocmire a documentației la care se face referire la alineatul (4), inclusiv termenele pentru ștergerea informațiilor conținute în această documentație. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare prevăzută la articolul 87 alineatul (2).

Articolul 32

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

1. Atunci când încălcarea securității datelor cu caracter personal pune în pericol protecția datelor cu caracter personal și a vieții private a persoanei vizate, operatorul, după notificarea prevăzută la articolul 31, 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 31 alineatul (3) literele (b) și (c).

3. Informarea persoanei vizate cu privire la încălcarea securității datelor cu caracter personal a persoanei vizate 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 trebuie să asigure că datele devin neinteligibile persoanelor care nu sunt autorizate să le acceseze.

4. Fără a aduce atingere obligației operatorului de a comunica persoanei vizate încălcarea securității datelor cu caracter personal, în cazul în care operatorul nu a comunicat încă persoanei vizate că securitatea datelor sale cu caracter personal a fost încălcată, autoritatea de supraveghere poate, după analizarea posibilelor efecte negative ale încălcării, să îi solicite să facă acest lucru.

5. Comisia este mandatată să adopte acte delegate în conformitate cu articolul 86 în scopul detalierii criteriilor și a cerințelor privind circumstanțele în care o încălcare a securității datelor cu caracter personal ar putea aduce atingere datelor cu caracter personal menționate la alineatul (1).

6. Comisia poate stabili forma în care persoana vizată este informată conform alineatului (1) și procedurile aplicabile respectivei informări. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare prevăzută la articolul 87 alineatul (2).

SECȚIUNEA 3
EVALUAREA IMPACTULUI PRIVIND PROTECȚIA DATELOR AUTORIZAȚIA PREALABILĂ

Articolul 33
Evaluarea impactului privind protecția datelor

1. Atunci când operațiunile de prelucrare prezintă riscuri specifice pentru drepturile și libertățile persoanelor vizate prin însăși natura, domeniul de aplicare sau scopurile lor, operatorul sau persoana împuternicită de către operator, care acționează în numele operatorului, trebuie să efectueze o evaluare a impactului operațiunilor de prelucrare prevăzute asupra protecției datelor cu caracter personal.

2. Următoarele operațiuni de prelucrare prezintă în special riscurile specifice la care se face referire la alineatul (1):

   (a) o evaluare sistematică și cuprinzătoare a aspectelor personale referitoare la o persoană fizică sau care vizează analizarea ori întocmirea de previziuni în special în ceea ce privește situația economică a persoanei fizice, locul în care se află, sănătatea, preferințele personale, încrederea de care se bucură sau comportamentul acesteia, care se bazează pe prelucrarea automată și pe care se

bazează măsurile care produc efecte juridice sau care afectează în mod semnificativ persoana respectivă;

(b) prelucrarea informațiilor privind viața sexuală, sănătatea, rasa și originea etnică sau informații necesare pentru furnizarea de asistență medicală, studii epidemiologice sau studii privind boli mentale sau infecțioase prelucrarea datelor pentru adoptarea de măsuri sau decizii care vizează anumite persoane pe scară largă;

(c) monitorizarea zonelor accesibile publicului, mai ales în cazul utilizării pe scară largă a dispozitivelor optoelectronice (supravegherea video);

(d) procesarea datelor cu caracter personal în sistemele de evidență a datelor de mari dimensiuni privind minorii sau procesarea datelor biometrice sau genetice;

(e) alte operațiuni de prelucrare de date pentru care este necesară consultarea autorității de supraveghere în conformitate cu articolul 34 alineatul (2) litera (b).

3. Evaluarea trebuie să cuprindă cel puțin o descriere generală a operațiunilor de prelucrare avute în vedere, o evaluare a riscurilor privind drepturile și libertățile persoanelor vizate, măsurile preconizate în vederea evitării riscurilor, garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze conformitatea cu dispozițiile prezentului regulament, luând în considerare drepturile și interesele legitime ale persoanelor vizate și ale celorlalte persoane interesate.

4. Operatorul solicită avizul persoanelor vizate sau al reprezentanților acestora privind prelucrarea prevăzută, fără a aduce atingere protecției intereselor comerciale sau publice ori securității operațiunilor de prelucrare.

5. Atunci când operatorul este o autoritate sau un organism public și prelucrarea rezultă dintr-o obligație juridică în temeiul articolului 6 alineatul (1) litera (c), care prevede normele și procedurile referitoare la operațiunile de prelucrare și reglementate de legislația Uniunii, alineatele (1) - (4) nu se aplică, cu excepția cazului în care statele membre consideră că este necesară efectuarea unei astfel de evaluări înaintea desfășurării activităților de prelucrare.

6. Comisia este mandatată să adopte acte delegate în conformitate cu articolul 86 în scopul detalierii criteriilor și a cerințelor privind operațiunile de prelucrare care pot prezenta riscurile specifice menționate la alineatele (1) și (2), precum și cerințelor pentru evaluare la care se face referire la alineatul (3), inclusiv condițiile de scalabilitate, de verificare și posibilitatea auditării. În acest sens, Comisia ia în considerare măsuri specifice pentru microîntreprinderi și pentru întreprinderi mici și mijlocii.

7. Comisia poate să prevadă standarde și proceduri de realizare, verificare și auditare a evaluării menționate la alineatul (3). Actele de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 87 alineatul (2).

Articolul 34

Autorizarea prealabilă și consultarea prealabilă

1. Operatorul sau persoana împuternicită de către operator, după caz, obține o autorizație din partea autorității de supraveghere înainte de prelucrarea datelor cu caracter personal, pentru a asigura conformitatea prelucrării prevăzute cu prezentul regulament și în special pentru a atenua riscurile la care sunt expuse persoanele vizate, în cazul în care un operator sau o persoană împuternicită de către operator adoptă clauzele contractuale prevăzute la articolul 42 alineatul (2) litera (d) sau nu oferă garanții corespunzătoare printr-un instrument obligatoriu din punct de vedere juridic, astfel cum se menționează la articolul 42 alineatul (5) în ceea ce privește transferul de date cu caracter personal către o țară terță sau o organizație internațională.

2. Operatorul sau persoana împuternicită de către operator, care acționează în numele operatorului, consultă autoritatea de supraveghere înainte de prelucrarea datelor cu caracter personal în scopul de a garanta conformitatea prelucrării prevăzute cu prezentul regulament și, în special, pentru a atenua riscurile la care sunt expuse persoanele vizate, atunci când:

   (a) o evaluare a impactului privind protecția datelor, astfel cum se prevede la articolul 33, indică faptul că operațiunile de prelucrare pot prezenta, prin însăși natura, domeniul de aplicare sau scopurile lor, un grad înalt de riscuri specifice; sau

   (b) autoritatea de supraveghere consideră că este necesar să se efectueze o consultare prealabilă cu privire la operațiunile de prelucrare care pot prezenta riscuri specifice pentru drepturile și libertățile persoanelor vizate prin însăși natura, domeniul de aplicare și/sau scopurile lor, în conformitate cu alineatul (4).

3. Atunci când consideră că prelucrarea prevăzută nu este conformă cu prezentul regulament, în special în cazul în care riscurile nu sunt suficient identificate sau atenuate, autoritatea de supraveghere interzice prelucrarea prevăzută și prezintă propuneri adecvate pentru remedierea acestor aspecte neconforme.

4. Autoritatea de supraveghere întocmește și publică o listă de operațiuni de prelucrare care sunt supuse consultării prealabile în conformitate cu alineatul (2) litera (b). Autoritatea de supraveghere comunică aceste liste Comitetului european pentru protecția datelor.

5. În cazul în care lista prevăzută la alineatul (4) cuprinde activități de prelucrare care presupun furnizarea de bunuri și prestarea de servicii către persoane vizate din mai multe state membre sau la monitorizarea comportamentului lor ori pot afecta în mod substanțial libera circulație a datelor cu caracter personal în cadrul Uniunii, autoritatea de supraveghere aplică mecanismul pentru asigurarea coerenței prevăzut la articolul 57 înainte de adoptarea listei.

6. Operatorul sau persoana împuternicită de către operator furnizează autorității de supraveghere evaluarea impactului privind protecția datelor prevăzută la articolul 33 și, la cerere, orice altă informație care permite autorității de supraveghere să facă o

evaluare a conformității prelucrării și în special a riscurilor în privința protecției datelor cu caracter personal ale persoanei vizate și a garanțiilor aferente.

7. Statele membre consultă autoritatea de supraveghere în cadrul procesului de pregătire a unei măsuri legislative care urmează să fie adoptate de parlamentul național sau a unei măsuri bazate pe o astfel de măsură legislativă, care să definească natura prelucrării, pentru a asigura conformitatea prelucrării prevăzute cu prezentul regulament și în special pentru a atenua riscurile la care sunt expuse persoanele vizate.

8. Comisia este mandatată să adopte acte delegate în conformitate cu articolul 86 în scopul detalierii criteriilor și a cerințelor privind stabilirea gradului înalt de risc specific prevăzut la alineatul 2 litera (a).

9. Comisia poate elabora formulare și proceduri standard pentru autorizațiile și consultările prealabile menționate la alineatele (1) și (2), precum și formulare și proceduri standard de informare a autorităților de supraveghere, în conformitate cu alineatul (6). Actele de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 87 alineatul (2).

SECȚIUNEA 4
RESPONSABILUL CU PROTECȚIA DATELOR

Articolul 35
Desemnarea responsabilului cu protecția datelor

1. Operatorul și persoana împuternicită de către operator desemnează un responsabil cu protecția datelor atunci când:

   (a) prelucrarea este efectuată de o autoritate sau de un organism public; sau

   (b) prelucrarea este efectuată de o întreprindere cu 250 de angajați sau mai mult; sau

   (c) activitățile principale ale operatorului sau ale persoanei împuternicite de către operator constau în operațiuni de prelucrare care, prin natura lor, domeniul de aplicare și/sau scopul lor, necesită monitorizarea periodică și sistematică a persoanelor vizate.

2. În cazul menționat la alineatul (1) litera (b), un grup de întreprinderi poate numi un responsabil unic cu protecția datelor.

3. În cazul în care operatorul sau persoana împuternicită de către operator este o autoritate sau un organism public, responsabilul cu protecția datelor poate fi desemnat pentru mai multe dintre entitățile sale, luând în considerare structura organizatorică a autorității sau a organismului public.

4. În alte cazuri decât cele menționate la alineatul (1), operatorul, persoana împuternicită de către operator, asociațiile și alte organisme care reprezintă categorii de operatori sau persoane împuternicite de către operatori pot desemna un responsabil cu protecția datelor.

5. Operatorul sau persoana împuternicită de către operator desemnează responsabilul cu protecția datelor în baza calităților profesionale și, în special, a cunoștințelor de specialitate în materie de legislație și practici privind protecția datelor și a capacității de a îndeplini sarcinile menționate la articolul 37. Nivelul necesar al cunoștințelor de specialitate se stabilește în special în special în funcție de prelucrarea efectuată asupra datelor și de gradul de protecție impus pentru datele cu caracter personal prelucrate de către operator sau de persoana împuternicită de către operator.

6. Operatorul sau persoana împuternicită de către operator se asigură că orice alte îndatoriri profesionale ale responsabilului cu protecția datelor sunt compatibile cu sarcinile și atribuțiile persoanei care are calitatea de responsabil cu protecția datelor și că nu generează un conflict de interese.

7. Operatorul sau persoana împuternicită de către operator desemnează un responsabil cu protecția datelor pentru o perioadă de cel puțin doi ani. Mandatul responsabilului cu protecția datelor poate fi reînnoit. Pe durata mandatului, responsabilul cu protecția datelor poate fi demis doar dacă responsabilul cu protecția datelor nu mai îndeplinește condițiile cerute pentru exercitarea atribuțiilor sale.

8. Responsabilul cu protecția datelor poate fi un angajat al operatorului sau al persoanei împuternicite de către operator ori poate să își îndeplinească atribuțiile în baza unui contract de servicii.

9. Operatorul sau persoana împuternicită de către operator comunică autorității de supraveghere și publicului numele și datele de contact ale responsabilului cu protecția datelor.

10. Persoanele vizate au dreptul de a contacta responsabilul cu protecția datelor cu privire la toate problemele legate de prelucrarea datelor persoanelor vizate și de a solicita exercitarea drepturilor în temeiul prezentului regulament.

11. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 86 cu scopul de a specifica în detaliu criteriile și cerințele pentru activitățile principale ale operatorului sau ale persoanei împuternicite de către operator prevăzute la alineatul (1) litera (c), precum și criteriile privind calitățile profesionale ale responsabilului cu protecția datelor prevăzute la alineatul (5).

Articolul 36
Funcția responsabilului cu protecția datelor

1. 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 persoană împuternicită de către operator se asigură că responsabilul cu protecția datelor își exercită îndatoririle și atribuțiile în mod independent și că nu primește instrucțiuni în privința exercitării funcției. Responsabilul cu protecția datelor răspunde direct în fața conducerii operatorului sau a persoanei împuternicite de către operator.

3. Operatorul sau persoana împuternicită de către operator sprijină pe responsabilul cu protecția datelor în îndeplinirea sarcinilor sale și pune la dispoziție personalul, incinta, echipamentele și orice alte resurse necesare pentru îndeplinirea funcțiilor și atribuțiilor prevăzute la articolul 37.

Articolul 37
Sarcinile responsabilului cu protecția datelor

1. 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 temeiul prezentului regulament, păstrarea unei evidențe a acestei activități și a răspunsurilor primite;

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

   (c) monitorizarea aplicării prezentului regulament, în special în ceea ce privește cerințele legate de protecția datelor de la momentul conceperii, de protecția implicită a datelor, de securitatea datelor, de informațiile persoanelor vizate și de cererile acestora în exercitarea drepturilor lor în temeiul prezentului regulament;

   (d) asigurarea menținerii unei documentații actualizate, prevăzute la articolul 28;

   (e) monitorizarea documentației, a notificării și a comunicării cazurilor de încălcare a prevederilor legate de datele cu caracter personal, în temeiul articolelor 31 și 32;

   (f) monitorizarea efectuării de către operator sau de persoana împuternicită de către operator a evaluării impactului și a introducerii cererilor de autorizare sau consultare prealabilă, dacă este cazul, în conformitate cu articolele 33 și 34;

   (g) monitorizarea răspunsului la cererile adresate de autoritatea de supraveghere, și, în limitele competenței responsabilului cu protecția datelor, cooperarea cu autoritatea de supraveghere, la cererea acesteia sau din propria inițiativă a responsabilului cu protecția datelor;

   (h) asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare și, dacă este cazul, consultarea autorității de supraveghere, din proprie inițiativă.

2. Comisia este mandatată să adopte acte delegate în conformitate cu articolul 86 în scopul detalierii criteriilor și cerințelor privind sarcinile, certificarea, statutul, competențele și resursele responsabilului cu protecția datelor la care se face referire la alineatul (1).

SECȚIUNEA 5
CODURI DE CONDUITĂ ȘI CERTIFICARE

Articolul 38
Coduri de conduită

1. Statele membre, autoritățile de supraveghere și Comisia încurajează elaborarea de coduri de conduită menite să contribuie la buna aplicare a prezentului regulament, ținând seama de caracteristicile specifice ale diverselor sectoare de prelucrare a datelor, în special cu privire la:

   (a) prelucrarea datelor în mod echitabil și transparent;

   (b) colectarea datelor;

   (c) informarea publicului și a persoanelor vizate;

   (d) cererile persoanelor vizate în exercitarea drepturilor acestora;

   (e) informarea și protejarea copiilor;

   (f) transferul datelor către țări terțe sau organizații internaționale;

   (g) mecanisme de monitorizare și de asigurare a conformității cu codul de către operatorii care aderă la cod;

   (h) proceduri extrajudiciare și alte proceduri de soluționare a litigiilor pentru soluționarea diferendelor între operatori și persoanele vizate în ceea ce privește prelucrarea datelor cu caracter personal, fără a aduce atingere drepturilor persoanelor vizate, conform articolelor 73 și 75.

2. Asociațiile și alte organisme care reprezintă categorii de operatori sau persoane împuternicite de către operatori într-un stat membru care intenționează să elaboreze coduri de conduită sau să modifice și să extindă codurile de conduită existente le pot prezenta în vederea emiterii unui aviz din partea autorității de supraveghere din statul membru respectiv. Autoritatea de supraveghere poate emite un aviz cu privire la conformitatea cu prezentul regulament a proiectului de cod de conduită sau a modificărilor aduse acestuia. Autoritatea de supraveghere solicită opiniile persoanelor vizate sau ale reprezentanților lor cu privire la aceste proiecte.

3. Asociațiile și alte organisme care reprezintă categorii de operatori în mai multe state membre pot prezenta Comisiei proiecte de coduri de conduită, precum și modificări sau extinderi ale codurilor de conduită existente.

4. Comisia poate adopta acte de punere în aplicare pentru a decide asupra valabilității generale în Uniune a codurilor de conduită și a modificărilor sau extinderilor la codurile de conduită existente care i-au fost prezentate în conformitate cu alineatul (3). Actele de punere în aplicare se adoptă în conformitate cu procedura de examinare prevăzută la articolul 87 alineatul (2).

5. Comisia asigură publicitatea adecvată pentru codurile asupra cărora s-a decis că au valabilitate generală în conformitate cu alineatul (4).

Articolul 39
Certificare

1. Statele membre și Comisia încurajează, în special la nivel european, instituirea de mecanisme de certificare în domeniul protecției datelor și de sigilii și mărci în domeniul protecției datelor, care să permită persoanelor vizate să evalueze rapid nivelul de protecție a datelor pe care îl asigură operatorii și persoanele împuternicite de către operatori. Mecanismele de certificare din domeniul protecției datelor contribuie la buna aplicare a prezentului regulament, luând în considerare caracteristicile specifice ale diverselor sectoare și ale diferitelor operațiuni de prelucrare.

2. Comisia este mandatată să adopte acte delegate în conformitate cu articolul 86 cu scopul detalierii criteriilor și cerințelor aplicabile mecanismelor de certificare din domeniul protecției datelor, menționate la alineatul (1), inclusiv a condițiilor de acordare și retragere, precum și a cerințelor în materie de recunoaștere în Uniune și în țările terțe.

3. Comisia poate stabili standarde tehnice pentru mecanismele de certificare și pentru sigiliile și mărcile din domeniul protecției datelor, precum și mecanisme de promovare și recunoaștere a mecanismelor de certificare și a sigiliilor și mărcilor din domeniul protecției datelor. Actele de punere în aplicare se adoptă în conformitate cu procedura de examinare prevăzută la articolul 87 alineatul (2).

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

Articolul 40
Principiul general al transferurilor

Datele cu caracter personal care fac obiectul prelucrării sau care urmează a fi prelucrate după ce sunt transferate într-o țară terță sau unei organizații internaționale pot fi transferate doar dacă, sub rezerva celorlalte dispoziții ale prezentului regulament, condițiile prevăzute în prezentul capitol sunt respectate de către operator și de persoana împuternicită de către operator, inclusiv în ceea ce privește transferurile ulterioare de date cu caracter personal din țara terță sau de la organizația internațională către o altă țară terță sau către o altă organizație internațională.

Articolul 41
Transferuri în baza unei decizii privind caracterul adecvat al nivelului de protecție

1. Transferul se poate realiza atunci când Comisia a decis că țara terță, un teritoriu ori un sector de prelucrare din acea țară terță sau organizația internațională în cauză

asigură un nivel de protecție adecvat. Transferurile realizate în aceste condiții nu necesită alte autorizări suplimentare.

2. Atunci când evaluează caracterul adecvat al nivelului de protecție, Comisia ia în considerare următoarele elemente:

(a) statul de drept, legislația relevantă în vigoare, atât cea generală, cât și cea specifică, inclusiv cea referitoare la securitatea publică, apărare, securitatea națională și dreptul penal, normele profesionale și măsurile de securitate care sunt 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 au responsabilitatea de a asigura respectarea normelor de protecție a datelor, de a asista și de a consilia persoanele vizate în ceea ce privește exercitarea drepturilor acestora 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 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 se adoptă în conformitate cu procedura de examinare menționată la articolul 87 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 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) al prezentului articol, în special în cazurile în care legislația relevantă, atât cea generală, cât și cea specifică, 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 87 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 87 alineatul (3).

6. În cazul în care Comisia ia o decizie în temeiul alineatului (5), 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, fără a aduce atingere articolelor 42-44. 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. Deciziile adoptate de Comisie în temeiul articolului 25 alineatul (6) sau al articolului 26 alineatul (4) din Directiva 95/46/CE rămân în vigoare, până când sunt modificate, înlocuite sau abrogate de către Comisie.

Articolul 42
Transferurile în baza unor garanții adecvate

1. În cazul în care Comisia nu a luat o decizie în temeiul articolului 41, operatorul sau persoana împuternicită de către operator poate transfera date cu caracter personal într-o țară terță sau unei organizații internaționale numai dacă operatorul sau persoana împuternicită de către operator a oferit garanții adecvate în ceea ce privește protecția datelor cu caracter personal printr-un instrument cu forță juridică obligatorie.

2. Garanțiile corespunzătoare menționate la alineatul (1) sunt furnizate, în special, prin:

   (a) reguli corporatiste obligatorii în conformitate cu articolul 43; sau

   (b) clauze standard de protecție a datelor adoptate de Comisie. Actele de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 87 alineatul (2); sau

   (c) clauze standard de protecție a datelor adoptate de o autoritate de supraveghere în conformitate cu mecanismul pentru asigurarea coerenței menționat la articolul 57, în condițiile în care Comisia a declarat că sunt general valabile în conformitate cu articolul 62 alineatul (1) litera (b); sau

   (d) clauze contractuale între operator sau persoana împuternicită de către operator și destinatarul datelor, aprobate de către o autoritate de supraveghere în conformitate cu alineatul (4).

3. Transferul realizat în baza clauzelor standard de protecție a datelor sau a regulilor corporatiste obligatorii menționate la alineatul (2) literele (a), (b) sau (c) nu necesită o altă autorizare suplimentară.

4. Atunci când transferul se realizează în baza unor clauzele contractuale, astfel cum se menționează în prezentul articol la alineatul (2) litera (d), operatorul sau persoana împuternicită de către operator obține de la autoritatea de supraveghere autorizarea prealabilă pentru clauzele contractuale, în conformitate cu articolul 34 alineatul (1). Dacă transferul are legătură cu activitățile de prelucrare care se referă la persoane vizate din alt stat membru sau din alte state membre, sau dacă afectează în mod semnificativ libera circulație a datelor cu caracter personal în cadrul Uniunii,

autoritatea de supraveghere aplică mecanismul pentru asigurarea coerenței prevăzut la articolul 57.

5. În cazul în care nu se furnizează garanții corespunzătoare în ceea ce privește protecția datelor cu caracter personal printr-un instrument cu forță juridică obligatorie, operatorul sau persoana împuternicită de către operator obține autorizarea prealabilă pentru transfer sau seria de transferuri, sau pentru dispozițiile care vor fi incluse în acordurile administrative care constituie temeiul pentru un astfel de transfer. Autorizarea acordată de autoritatea de supraveghere este în conformitate cu articolul 34 alineatul (1). Dacă transferul are legătură cu activitățile de prelucrare care se referă la persoane vizate din alt stat membru sau din alte state membre, sau dacă afectează în mod semnificativ libera circulație a datelor cu caracter personal în cadrul Uniunii, autoritatea de supraveghere aplică mecanismul pentru asigurarea coerenței prevăzut la articolul 57. Autorizațiile acordate de către autoritatea de supraveghere în temeiul articolului 26 alineatul (2) din Directiva 95/46/CE sunt valabile, până la data la care sunt modificate, înlocuite sau abrogate de către respectiva autoritate de supraveghere.

Articolul 43

Transferurile în baza regulilor corporatiste obligatorii

1. În conformitate cu mecanismul pentru asigurarea coerenței prevăzut la articolul 58, autoritatea de supraveghere aprobă regulile corporatiste obligatorii, cu condiția ca acestea:

   (a) să aibă forță juridică obligatorie și să se aplice fiecărui membru al grupului de întreprinderi al operatorului sau al persoanei împuternicite de către operator și să includă și pe salariații acestora;

   (b) să confere, în mod expres, drepturi opozabile persoanelor vizate;

   (c) să îndeplinească cerințele prevăzute la alineatul (2).

2. Regulile corporatiste obligatorii trebuie să precizeze cel puțin:

   (a) structura și datele de contact ale grupului de întreprinderi și membrii din componența sa;

   (b) transferurile de date sau setul de transferuri, inclusiv categoriile de date cu caracter personal, tipul prelucrării și scopurile prelucrării, categoriile de persoane vizate și identificarea țării terțe sau a țărilor terțe în cauză;

   (c) caracterul obligatoriu, atât pe plan intern, cât și extern;

   (d) principiile generale în materie de protecție a datelor, în special limitarea scopului, calitatea datelor, temeiul juridic pentru prelucrarea datelor, prelucrarea datelor sensibile cu caracter personal; măsuri de asigurare a securității datelor, precum și cerințele pentru transferurile ulterioare către organizații care nu au obligații în temeiul politicilor;

(e) drepturile persoanelor vizate și mijloacele de exercitare a acestor drepturi, inclusiv dreptul de a nu face obiectul unei măsuri bazate pe crearea de profiluri în conformitate cu articolul 20, dreptul de a depune o plângere în fața autorității de supraveghere competente și în fața instanțelor competente ale statelor membre, în conformitate cu articolul 75, precum și dreptul de a obține despăgubiri și, după caz, compensații pentru încălcarea regulilor corporatiste obligatorii;

(f) acceptarea de către operator sau de persoana împuternicită de către operator, cu sediul pe teritoriul unui stat membru, a răspunderii pentru orice încălcare a regulilor corporatiste obligatorii de către orice membru al grupului de întreprinderi care nu are sediul în Uniune; operatorul sau persoana împuternicită de către operator pot fi exonerați de răspundere, integral sau parțial, numai în condițiile în care dovedesc că membrul respectiv nu răspunde de evenimentul care a cauzat daune;

(g) modul în care informațiile privind regulile corporatiste obligatorii, în special cu privire la dispozițiile menționate la literele (d), (e) și (f) de la prezentul alineat sunt furnizate persoanelor vizate, conform articolului 11;

(h) sarcinile responsabilului cu protecția datelor, desemnat în conformitate cu articolul 35, inclusiv monitorizarea în cadrul grupului de întreprinderi a respectării regulilor corporatiste obligatorii, precum și monitorizarea formării și a gestionării plângerilor;

(i) mecanismele din cadrul grupului de întreprinderi în vederea garantării conformității cu regulile corporatiste obligatorii;

(j) mecanismele de comunicare și înregistrare a modificărilor aduse politicilor și de comunicare a acestor modificări autorității de supraveghere;

(k) mecanismul de cooperare cu autoritatea de supraveghere menite să asigure respectarea regulilor de către oricare membru al grupului de întreprinderi, în special prin punerea la dispoziția autorității de supraveghere a rezultatelor verificărilor cu privire la măsurile menționate la punctul (i) de la prezentul alineat.

3. Comisia este mandatată să adopte acte delegate în conformitate cu articolul 86 cu scopul detalierii criteriilor și cerințelor pentru regulile corporatiste obligatorii în sensul prezentului articol, în special în ceea ce privește criteriile pentru aprobarea lor, aplicarea literelor (b), (d), (e) și (f) de la alineatul (2) la regulile corporatiste obligatorii la care au aderat persoanele împuternicite de către operator și la alte cerințe necesare pentru a garanta protecția datelor cu caracter personal ale persoanelor vizate în cauză.

4. Comisia poate preciza formatul și procedurile pentru schimbul de informații prin mijloace electronice între operatori, persoanele împuternicite de către operatori și autoritățile de supraveghere pentru regulile corporative cu forță juridică obligatorie în sensul prezentului articol. Actele de punere în aplicare se adoptă în conformitate cu procedura de examinare prevăzută la articolul 87 alineatul (2).

Articolul 44
Derogări

1. În absența unei decizii privind caracterul adecvat al nivelului de protecție în conformitate cu articolul 41, sau a unor garanții adecvate în conformitate cu articolul 42, un transfer sau o serie de transferuri de date cu caracter personal către o țară terță sau o organizație internațională poate avea loc numai în condițiile în care:

   (a) persoana vizată și-a exprimat acordul cu privire la transferul propus, după ce a fost informată cu privire la riscurile acestor transferuri în lipsa unei decizii privind caracterul adecvat al nivelului de protecție și a garanțiilor corespunzătoare; sau

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

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

   (d) transferul este necesar din motive importante, de interes public; sau

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

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

   (g) transferul se realizează dintr-un registru care, potrivit dreptului Uniunii sau al statului membru, are scopul de a furniza informații publicului și care poate fi consultat fie de public, în general, fie de orice persoană care poate face dovada interesului legitim, în măsura în care sunt îndeplinite condițiile cu privire la consultare prevăzute de dreptul Uniunii sau al statului membru în acel caz specific; sau

   (h) transferul este necesar în scopul intereselor legitime urmărite de operator sau de persoana împuternicită de către operator, nu poate fi considerat frecvent sau voluminos, iar operatorul sau persoana împuternicită de către operator a evaluat toate circumstanțele aferente operațiunii de transfer de date sau seriei de operațiuni de transfer de date și în baza acestei evaluări a oferit garanții corespunzătoare în ceea ce privește protecția datelor cu caracter personal, în cazul în care acest lucru este necesar.

2. Transferul în temeiul alineatului (1) litera (g) nu implică totalitatea datelor cu caracter personal sau ansamblul categoriilor de date cu caracter personal cuprinse în registru. Atunci când registrul urmează a fi consultat de către persoane care au un interes legitim, transferul se efectuează numai la cererea persoanelor respective sau, în cazul în care acestea vor fi destinatarii.

3. În cazul în care prelucrarea se realizează în baza alineatului (1) litera (h), operatorul sau persoana împuternicită de către operator trebuie să acorde atenție deosebită naturii datelor, scopului și duratei operațiunii sau operațiunilor propuse de prelucrare, situației din țara de origine, din țara terță și din țara de destinație finală și garanțiilor corespunzătoare oferite în ceea ce privește protecția datelor cu caracter personal, în cazul în care este necesar.

4. Literele (b), (c) și (h) de la alineatul (1) nu se aplică în cazul activităților desfășurate de către autoritățile publice în exercitarea competențelor lor publice.

5. Interesul public prevăzut la alineatul (1) litera (d) trebuie să fie recunoscut în dreptul Uniunii sau în dreptul statului membru sub incidența căruia intră operatorul.

6. Operatorul sau persoana împuternicită de către operator consemnează evaluarea și garanțiile corespunzătoare oferite prevăzute la alineatul (1) litera (h) de la prezentul articol, în documentele prevăzute la articolul 28 și informează autoritatea de supraveghere cu privire la transfer.

7. Comisia este mandatată să adopte acte delegate în conformitate cu articolul 86 cu scopul detalierii „motivelor importante, de interes public”, în sensul alineatului (1) litera (d), precum și a criteriilor și cerințelor aplicabile garanțiilor corespunzătoare prevăzute la alineatul (1) litera (h).

Articolul 45

Cooperarea internațională în domeniul protecției datelor cu caracter personal

1. În ceea ce privește țările terțe și organizațiile internaționale, Comisia și autoritățile de supraveghere 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, 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 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 41 alineatul (3).

CAPITOLUL VI
AUTORITĂȚI DE SUPRAVEGHERE INDEPENDENTE

SECȚIUNEA 1
STATUT INDEPENDENT

Articolul 46
Autoritatea de supraveghere

1. Dispozițiile din fiecare stat membru prevăd că una sau mai multe autorități publice sunt responsabile de monitorizarea aplicării prezentului regulament și de contribuția la aplicarea uniformă a regulamentului 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. 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 și instituie un mecanism de asigurare a respectării de către celelalte autorități a normelor privind mecanismul pentru asigurarea coerenței prevăzut la articolul 57.

3. Fiecare stat membru notifică Comisiei dispozițiile din dreptul său pe care le adoptă în temeiul prezentului capitol până cel târziu la data menționată la articolul 91 alineatul (2) și, fără întârziere, orice modificare ulterioară pe care o aduce la aceste dispoziții.

Articolul 47
Independență

1. Autoritatea de supraveghere beneficiază de independență deplină în exercitarea îndatoririlor și competențelor care îi sunt încredințate.

2. În îndeplinirea îndatoririlor, 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, iar, 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 necesară pentru

buna executare a sarcinilor și competențelor, inclusiv a celor care urmează să fie efectuate în contextul asistenței reciproce, al cooperării și participării la Comitetul european pentru protecția datelor.

6. Fiecare stat membru se asigură că autoritatea de supraveghere dispune de personal propriu, 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 48

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 competențelor cerute pentru îndeplinirea îndatoririlor lor în special în domeniul protecției datelor cu caracter personal.

3. Funcțiile unui membru încetează în cazul expirării mandatului, în cazul demisiei sau 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 exercite îndatoririle până la numirea unui nou membru.

Articolul 49

Norme privind instituirea autorității de supraveghere

În limitele prezentului regulament, fiecare stat membru prevede, pe cale legislativă, următoarele:

(a) instituirea și statutul autorității de supraveghere;

(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 prezentului

regulament, care poate fi pe o perioadă mai scurtă în cazul în care acest lucru este necesar pentru a proteja independența autorității de supraveghere printr-o procedură de numiri eșalonate;

(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 50
Secretul profesional

În cursul mandatului și după încetarea mandatului, membrii și personalul autorității de supraveghere au obligația 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 51
Competență

1. Fiecare autoritate de supraveghere exercită, pe teritoriul statului membru de care aparține, funcțiile cu care este investită în conformitate cu prezentul regulament.

2. Atunci când prelucrarea datelor cu caracter personal are loc în contextul activităților unei unități a unui operator sau a unei persoane împuternicite de către operator, din Uniune, iar operatorul sau persoană împuternicită de către operator are unități pe teritoriul mai multor state membre, autoritatea de supraveghere a principalei unități a operatorului sau a persoanei împuternicite de către operator are competența supravegherii activităților de prelucrare desfășurate de operator sau de persoana împuternicită de către operator în toate statele membre, fără a aduce atingere dispozițiilor capitolului VII din prezentul regulament.

3. Autoritatea de supraveghere nu are competența de a supraveghea operațiunile de prelucrare ale instanțelor care acționează în exercițiul funcției lor jurisdicționale.

Articolul 52
Atribuții

1. Autoritatea de supraveghere:

(a) monitorizează și asigură aplicarea prezentului regulament;

(b) primește reclamațiile depuse de orice persoană vizată sau de o asociație care reprezintă persoana vizată respectivă, în conformitate cu articolul 73, 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 amănunțite sau coordonarea cu o altă autoritate de supraveghere;

(c) partajează informațiile cu alte autorități de supraveghere, oferă asistență reciprocă și asigură consecvența aplicării și a asigurării aplicării prezentului regulament;

(d) 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 la această autoritate de supraveghere;

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

(f) 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;

(g) autorizează și este consultată cu privire la operațiunile de prelucrare prevăzute la articolul 34;

(h) emite un aviz cu privire la proiectele de coduri de conduită, în conformitate cu articolul 38 alineatul (2);

(i) aprobă regulile corporatiste obligatorii în conformitate cu articolul 43;

(j) 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 copiilor.

3. La cerere, autoritatea de supraveghere oferă consiliere oricărei persoane vizate în exercitarea drepturilor în conformitate cu prezentul regulament 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. Îndeplinirea funcțiilor autorității de supraveghere este gratuită pentru persoana vizată.

6. În cazul în care cererile sunt în mod evident excesive, în special din cauza caracterului repetitiv al acestora, autoritatea de supraveghere poate percepe o taxă

sau poate să nu efectueze acțiunea care face obiectul cererii persoanei vizate. Sarcina probei cu privire la caracterul evident excesiv al cererii revine autorității de supraveghere.

Articolul 53
Funcții

1. Fiecare autoritate de supraveghere este abilitată:

(a) să notifice operatorul sau persoana împuternicită de către operator cu privire la presupusa încălcare a dispozițiilor care reglementează prelucrarea datelor cu caracter personal și, după caz, să dispună remedierea încălcării de către operator sau persoana împuternicită de către operator, în mod specific, pentru îmbunătățirea protecției de care beneficiază persoana vizată;

(b) să solicite operatorului sau persoanei împuternicite de către operator să respecte cererile persoanei vizate de exercitare a drepturilor prevăzute de prezentul regulament;

(c) să solicite operatorului sau persoanei împuternicite de către operator și, după caz, reprezentantului să furnizeze orice informații relevante pentru îndeplinirea funcțiilor sale;

(d) să asigure respectarea autorizațiilor prealabile și a consultărilor prealabile prevăzute la articolul 34;

(e) să adreseze un avertisment sau o mustrare operatorului sau persoanei împuternicite de către operator;

(f) să dispună rectificarea, ștergerea sau distrugerea tuturor datelor atunci când acestea au fost prelucrate cu încălcarea dispozițiilor prezentului regulament, precum și notificarea acestor acțiuni terților cărora le-au fost dezvăluite aceste date;

(g) să impună interdicția temporară sau definitivă privind prelucrarea;

(h) să suspende fluxurile de date către un destinatar într-o țară terță sau către o organizație internațională;

(i) să emită avize cu privire la orice aspect legat de protecția datelor cu caracter personal;

(j) să informeze parlamentul național, guvernul sau alte instituții politice, precum și publicul cu privire la orice aspect legat de protecția datelor cu caracter personal.

2. Fiecare autoritate de supraveghere are competențe de investigare pentru a obține din partea operatorului sau a persoanei împuternicite de către operator:

(a) accesul la toate datele cu caracter personal și la toate informațiile necesare pentru executarea atribuțiilor sale;

(b) accesul la oricare din localurile sale, inclusiv la eventualele echipamente și mijloace de prelucrare a datelor, în cazul în care există motive întemeiate de a presupune că se efectuează o activitate care contravine prezentului regulament.

Puterile prevăzute la litera (b) se exercită în conformitate cu dreptul Uniunii și cu legislația statului membru.

3. Fiecare autoritate de supraveghere este abilitată să aducă în atenția autorităților judiciare cazurile de încălcare a prezentului regulament și să se implice în procedurile judiciare, în special în conformitate cu articolul 74 alineatul (4) și articolul 75 alineatul (2).

4. Fiecare autoritate de supraveghere poate sancționa contravențiile de natură administrativă, în special cele prevăzute la articolul 79 alineatele (4), (5) și (6).

Articolul 54
Raport de activitate

Fiecare autoritate de supraveghere trebuie să întocmească un raport anual cu privire la activitățile sale. Raportul trebuie să fie prezentat parlamentului național și se pune la dispoziția publicului, Comisiei și Comitetului european pentru protecția datelor.

CAPITOLUL VII
COOPERARE ȘI COERENȚĂ

SECȚIUNEA 1
COOPERARE

Articolul 55
Asistență reciprocă

1. Autoritățile de supraveghere își furnizează reciproc informații relevante și asistență reciprocă pentru a pune în aplicare prezentul regulament 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 de autorizare și consultare prealabile, inspecții și comunicarea rapidă a informațiilor privind deschiderea dosarelor și evoluția ulterioară a acestora atunci când persoanele vizate în mai multe state membre sunt susceptibile de a fi afectate de operațiuni de prelucrare.

2. Fiecare autoritate de supraveghere ia toate măsurile corespunzătoare necesare pentru a răspunde solicitării din partea altei autorități de supraveghere, fără întârziere și cel târziu în termen de o lună de la data primirii cererii. Aceste măsuri pot include, în special, transmiterea informațiilor relevante privind cursul unei anchete sau măsuri de aplicare a legii pentru a pune capăt sau a interzice operațiunile de prelucrare care încalcă dispozițiile prezentului regulament.

3. Solicitarea de asistență cuprinde toate informațiile necesare, inclusiv scopul solicitării și motivele care stau la baza acesteia. Informațiile schimbate sunt utilizate numai în scopul pentru care au fost solicitate.

4. O autoritate de supraveghere căreia i se adresează o solicitare de asistență nu poate refuza să îi dea curs, cu excepția cazului în care:

   (a) nu are competența de a răspunde solicitării; sau

   (b) a da curs solicitării ar contraveni dispozițiilor prezentului regulament.

5. 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.

6. Autoritățile de supraveghere furnizează informațiile solicitate de către alte autorități de supraveghere prin mijloace electronice și în cel mai scurt timp, utilizând un formular standard.

7. Pentru acțiunile întreprinse în urma unei solicitări de asistență reciprocă nu se percepe nicio taxă.

8. În cazul în care o autoritate de supraveghere nu acționează în termen de o lună de la solicitarea din partea altei autorități de supraveghere, aceasta din urmă are competența de a lua o măsură provizorie pe teritoriul propriului stat membru, în conformitate cu articolul 51 alineatul (1), și sesizează Comitetul european pentru protecția datelor în conformitate cu procedura menționată la articolul 57.

9. Autoritatea de supraveghere precizează perioada de valabilitate a acestei măsuri provizorii. Această perioadă nu depășește trei luni. Autoritatea de supraveghere comunică fără întârziere aceste măsuri, motivate în mod corespunzător, Comitetului european pentru protecția datelor și Comisiei.

10. Comisia poate specifica forma și procedurile pentru asistența reciprocă menționată în prezentul articol, precum și modalitățile de schimb de informații prin mijloace electronice între autoritățile de supraveghere și între autoritățile de supraveghere și Comitetul european pentru protecția datelor, în special formularul standard menționat la alineatul (6). Actele de punere în aplicare respective sunt adoptate în conformitate cu procedura de examinare menționată la articolul 87 alineatul (2).

Articolul 56
Operațiuni comune ale autorităților de supraveghere

1. Pentru a intensifica cooperarea și asistența reciprocă, autoritățile de supraveghere întreprind misiuni comune de anchetă, măsuri comune de aplicare a legii și alte operațiuni comune, în care sunt implicați membri desemnați sau personal din partea autorităților de supraveghere ale altor state membre.

2. În cazul în care persoanele vizate în mai multe state membre sunt susceptibile de a fi afectate de operațiuni de prelucrare, o autoritate de supraveghere din fiecare dintre statele membre respective are dreptul de a participa la misiunile comune de anchetă

sau la operațiunile comune, după caz. Autoritatea de supraveghere competentă invită autoritățile de supraveghere din fiecare dintre aceste state membre să ia parte la misiunile comune de anchetă sau operațiunile comune respective și răspunde fără întârziere la solicitarea unei autorități de supraveghere care dorește să participe la operațiuni.

3. În calitate de autoritate de supraveghere gazdă, în conformitate cu propria legislație națională și cu acordul autorității de supraveghere care și-a detașat personalul, fiecare autoritate de supraveghere poate acorda competențe de executare, inclusiv încredința misiuni de anchetă membrilor sau personalului autorității de supraveghere din statul membru de origine, implicați în operațiuni comune sau, în măsura în care legislația autorității de supraveghere din statul membru de primire permite acest lucru, poate permite membrilor sau personalului autorității de supraveghere din statul membru de origine să își exercite competențele de executare în conformitate cu legislația autorității de supraveghere din statul membru de origine. Astfel de competențe de executare pot fi exercitate doar sub coordonarea și, de regulă, în prezența membrilor sau personalului autorității de supraveghere din statul membru de primire. Membrii sau personalul autorității de supraveghere din statul membru de origine sunt supuși legislației naționale a autorității de supraveghere din statul membru de primire. Aceasta își asumă răspunderea pentru acțiunile personalului.

4. Autoritățile de supraveghere definesc aspectele practice ale acțiunilor specifice de cooperare.

5. În cazul în care o autoritate de supraveghere nu se conformează, în termen de o lună, obligației prevăzute la alineatul (2), celelalte autorități de supraveghere au competența de a adopta o măsură provizorie pe teritoriul statului membru respectiv, în conformitate cu articolul 51 alineatul (1).

6. Autoritatea de supraveghere precizează perioada de valabilitate a măsurii provizorii menționate la alineatul (5). Această perioadă nu depășește trei luni. Autoritatea de supraveghere comunică fără întârziere aceste măsuri, motivate în mod corespunzător, Comitetului european pentru protecția datelor și Comisiei și prezintă situația spre analiză în cadrul mecanismului menționat la articolul 57.

SECȚIUNEA 2
COERENȚĂ

Articolul 57
Mecanismul pentru asigurarea coerenței

Pentru scopurile stabilite la articolul 46 alineatul (1), autoritățile de supraveghere cooperează între ele și cu Comisia prin mecanismul pentru asigurarea coerenței, astfel cum se prevede în prezenta secțiune.

Articolul 58

Avizul Comitetului european pentru protecția datelor

1. Înainte de a adopta o măsură menționată la alineatul (2), o autoritate de supraveghere comunică proiectul de măsură Comitetului european pentru protecția datelor și Comisiei.

2. Obligația prevăzută la alineatul (1) se aplică unei măsuri menite să producă efecte juridice și care:

   (a) se referă la activități de prelucrare legate de furnizarea de bunuri sau servicii persoanelor vizate în mai multe state membre, sau de monitorizarea comportamentului acestora; sau

   (b) pot afecta în mod substanțial libera circulație a datelor cu caracter personal în cadrul Uniunii; sau

   (c) vizează adoptarea unei liste de operațiuni de prelucrare care fac obiectul unei consultări prealabile în temeiul articolului 34 alineatul (5); sau

   (d) vizează determinarea clauzelor standard în materie de protecție a datelor menționate la articolul 42 alineatul (2) litera (c); sau

   (e) vizează autorizarea clauzelor contractuale menționate la articolul 42 alineatul (2) litera (d); sau

   (f) vizează aprobarea regulilor corporatiste obligatorii în sensul articolului 43.

3. Orice autoritate de supraveghere sau Comitetul european pentru protecția datelor poate solicita ca orice chestiune să fie abordată în cadrul mecanismului pentru asigurarea coerenței, în special în cazul în care o autoritate de supraveghere nu prezintă un proiect de măsură menționat la alineatul (2) sau nu respectă obligațiile privind asistența reciprocă în conformitate cu articolul 55 sau privind operațiunile comune în conformitate cu articolul 56.

4. Pentru a asigura aplicarea corectă și coerentă a prezentului regulament, Comisia poate solicita ca orice chestiune să fie abordată în cadrul mecanismului pentru asigurarea coerenței.

5. Autoritățile de supraveghere și Comisia comunică electronic orice informație relevantă, inclusiv, după caz, o sinteză a faptelor, proiectul de măsură, precum și motivele care fac necesară adoptarea unei astfel de măsuri, utilizând un formular standard.

6. Președintele Comitetului european pentru protecția datelor informează fără întârziere pe cale electronică membrii Comitetului european pentru protecția datelor și Comisia cu privire la orice informație relevantă care i-a fost comunicată, utilizând un formular standard. Președintele Comitetului european pentru protecția datelor furnizează traduceri ale informațiilor relevante, dacă este necesar.

7. În cazul în care Comitetul european pentru protecția datelor decide acest lucru prin majoritate simplă a membrilor săi sau în cazul în care orice autoritate de

supraveghere sau Comisia solicită acest lucru, Comitetul european pentru protecția datelor emite un aviz cu privire la chestiune în termen de o săptămână de la data la care informațiile relevante au fost furnizate în conformitate cu alineatul (5). Avizul este adoptat în termen de o lună cu majoritate simplă a membrilor Comitetului european pentru protecția datelor. Președintele Comitetului european pentru protecția datelor informează, fără întârziere nejustificată, autoritatea de supraveghere menționată, după caz, la alineatele (1) și (3), Comisia și autoritatea de supraveghere competentă în conformitate cu articolul 51 cu privire la aviz și îl publică.

8. Autoritatea de supraveghere menționată la alineatul (1) și autoritatea de supraveghere competentă în conformitate cu articolul 51 țin seama de avizul Comitetului european pentru protecția datelor și comunică pe cale electronică președintelui Comitetului european pentru protecția datelor și Comisiei, în termen de două săptămâni din momentul în care a fost informată cu privire la avizul președintelui Comitetului european pentru protecția datelor, dacă își păstrează sau își modifică proiectul de măsură și, dacă este cazul, transmite proiectul de măsură modificat, utilizând un formular standard.

Articolul 59
Avizul Comisiei

1. În termen de zece săptămâni din momentul în care o chestiune a fost ridicată în conformitate cu articolul 58, sau cel târziu în termen de șase săptămâni în cazul articolului 61, Comisia poate adopta, pentru a asigura aplicarea corectă și coerentă a prezentului regulament, un aviz cu privire la chestiunile ridicate în temeiul articolelor 58 sau 61.

2. Atunci când Comisia a adoptat un aviz în conformitate cu alineatul (1), autoritatea de supraveghere în cauză acordă atenție maximă avizului Comisiei și informează Comisia și Comitetul european pentru protecția datelor dacă intenționează să își mențină sau să modifice proiectul de măsură.

3. În timpul perioadei menționate la alineatul (1), autoritatea de supraveghere nu adoptă proiectul de măsură.

4. În cazul în care autoritatea de supraveghere în cauză intenționează să nu se conformeze avizului Comisiei, acesta informează Comisia și Comitetul european pentru protecția datelor respectând termenul menționat la alineatul (1) și furnizează o motivare. În acest caz, proiectul de măsură nu este adoptat timp de o lună suplimentară.

Articolul 60
Suspendarea unui proiect de măsură

1. În termen de o lună de la comunicarea menționată la articolul 59 alineatul (4) și în cazul în care Comisia are îndoieli serioase că proiectul de măsură ar garanta aplicarea corectă a prezentului regulament sau, dimpotrivă, că ar avea ca rezultat aplicarea incoerentă a regulamentului, Comisia, ținând cont de avizul emis de Comitetul european pentru protecția datelor în temeiul articolului 58 alineatul (7) sau al articolului 61 alineatul (2), poate adopta o decizie motivată care să oblige autoritatea

de supraveghere să suspende adoptarea proiectului de măsură, în cazul în care se consideră că acest lucru este necesar pentru:

(a) a concilia pozițiile divergente ale autorității de supraveghere și Comitetului european pentru protecția datelor, în cazul în care acest lucru pare încă posibil; sau

(b) a adopta o măsură în temeiul articolului 62 alineatul (1) litera (a).

2. Comisia precizează durata suspendării, care nu depășește 12 luni.

3. În timpul perioadei menționate la alineatul (2), autoritatea de supraveghere nu poate adopta proiectul de măsură.

Articolul 61
Procedura de urgență

1. În circumstanțe excepționale, atunci când o autoritate de supraveghere consideră că există o necesitate urgentă de a acționa pentru a asigura protecția intereselor persoanelor vizate, în special când există pericolul ca exercitarea dreptului persoanei vizate ar putea fi considerabil împiedicată prin modificarea situației existente, pentru a evita inconveniente importante sau din alte motive, prin derogare de la procedura menționată la articolul 58, aceasta poate adopta de îndată măsuri provizorii cu o perioadă de valabilitate determinată. Autoritatea de supraveghere comunică fără întârziere aceste măsuri, motivate în mod corespunzător, Comitetului european pentru protecția datelor și Comisiei.

2. În cazul în care o autoritate de supraveghere a adoptat o măsură în temeiul alineatului (1) și consideră că trebuie adoptate de urgență măsuri definitive, aceasta poate solicita un aviz de urgență din partea Comitetului european pentru protecția datelor, indicând motivele pentru solicitarea unui astfel de aviz, inclusiv pentru caracterul urgent al măsurilor definitive.

3. Orice autoritate de supraveghere poate solicita un aviz de urgență în cazul în care autoritatea de supraveghere competentă nu a luat o măsură adecvată într-o situație în care există o necesitate urgentă de a acționa pentru a proteja interesele persoanelor vizate, indicând motivele pentru solicitarea unui astfel de aviz, inclusiv pentru necesitatea urgentă de a acționa.

4. Prin derogare de la articolul 58 alineatul (7), un aviz de urgență menționat la alineatele (2) și (3) din prezentul articol este adoptat în termen de două săptămâni cu majoritate simplă a membrilor Comitetului european pentru protecția datelor.

Articolul 62
Acte de punere în aplicare

1. Comisia poate adopta acte de punere în aplicare pentru:

(a) a decide privind aplicarea corectă a prezentului regulament, în conformitate cu obiectivele și cerințele acestuia în ceea ce privește aspectele comunicate de

către autoritățile de supraveghere în temeiul articolului 58 sau 61, privind o chestiune în legătură cu care a fost adoptată o decizie motivată în temeiul articolului 60 alineatul (1), sau privind o chestiune în legătură cu care o autoritate de supraveghere nu prezintă un proiect de măsură și respectiva autoritate de supraveghere a indicat că nu intenționează să urmeze avizul Comisiei adoptat în temeiul articolului 59;

(b) a decide, în termenul menționat la articolul 59 alineatul (1), referitor la aplicabilitatea generală a proiectului de clauze standard în materie de protecție a datelor menționate la articolul 58 alineatul (2) litera (d);

(c) a defini forma și procedurile pentru aplicarea mecanismului pentru asigurarea coerenței menționat în prezenta secțiune;

(d) a defini modalitățile de realizare a schimbului electronic de informații între autoritățile de supraveghere și între autoritățile de supraveghere și Comitetul european pentru protecția datelor, în special formularul standard menționat la articolul 58 alineatele (5), (6) și (8).

Actele de punere în aplicare respective sunt adoptate în conformitate cu procedura de examinare menționată la articolul 87 alineatul (2).

2. Din motive imperative de urgență pe deplin justificate legate de interesul persoanelor vizate în cazurile menționate la alineatul (1) litera (a), Comisia adoptă acte de punere în aplicare imediat aplicabile, în conformitate cu procedura menționată la articolul 87 alineatul (3). Aceste acte rămân în vigoare pentru o perioadă de cel mult 12 luni.

3. Absența sau adoptarea unei măsuri în temeiul prezentei secțiuni nu aduce atingere altor măsuri adoptate de Comisie în temeiul tratatelor.

Articolul 63
Executare

1. În sensul prezentului regulament, o măsură executorie a autorității de supraveghere ale unui stat membru este executată în toate statele membre implicate.

2. În cazul în care o autoritate de supraveghere nu prezintă un proiect de măsură pentru a fi examinat în cadrul mecanismului pentru asigurarea coerenței, încălcând articolul 58 alineatele (1)-(5), măsura autorității de supraveghere nu este valabilă din punct de vedere juridic și nici executorie.

SECȚIUNEA 3
COMITETUL EUROPEAN PENTRU PROTECȚIA DATELOR

Articolul 64
Comitetul european pentru protecția datelor

1. Se instituie un Comitet european pentru protecția datelor.

2. Comitetul european pentru protecția datelor este alcătuit din șeful unei autorități de supraveghere din fiecare stat membru și din Autoritatea Europeană pentru Protecția Datelor.

3. În cazul în care într-un stat membru mai multe autorități de supraveghere sunt responsabile de monitorizarea punerii în aplicare a dispozițiilor prevăzute de prezentul regulament, acestea desemnează șeful uneia dintre aceste autorități de supraveghere ca reprezentant comun.

4. Comisia are dreptul de a participa la activitățile și reuniunile Comitetului european pentru protecția datelor și desemnează un reprezentant. Președintele Comitetului european pentru protecția datelor informează fără întârziere Comisia cu privire la toate activitățile Comitetului european pentru protecția datelor.

Articolul 65
Independență

1. Comitetul european pentru protecția datelor acționează independent în exercitarea sarcinilor sale în conformitate cu articolele 66 și 67.

2. Fără a aduce atingere solicitărilor din partea Comisiei menționate la articolul 66 alineatul (1) litera (b) și la articolul 66 alineatul (2), în îndeplinirea sarcinilor sale, Comitetul european pentru protecția datelor nu solicită și nu acceptă instrucțiuni de la nicio parte externă.

Articolul 66
Sarcinile Comitetului european pentru protecția datelor

1. Comitetul european pentru protecția datelor asigură aplicarea uniformă a prezentului regulament. În acest sens, din proprie inițiativă sau la solicitarea Comisiei, Comitetul european pentru protecția datelor are, în special, următoarele sarcini:

   (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 prezentului regulament;

   (b) să examineze, din proprie inițiativă sau la solicitarea unuia dintre membrii săi sau la cererea Comisiei, orice chestiune referitoare la punerea în aplicare a prezentului regulament și să emită orientări, recomandări și bune practici adresate autorităților de supraveghere pentru a încuraja aplicarea uniformă a prezentului regulament;

   (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 emită avize privind proiectele de decizii ale autorităților de supraveghere în conformitate cu mecanismul pentru asigurarea coerenței menționat la articolul 57;

(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 privind legislația și practicile în materie de protecție a datelor cu autoritățile de supraveghere a protecției datelor la nivel mondial.

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 furnizeze 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 87 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.

Articolul 67
Rapoarte

1. Comitetul european pentru protecția datelor prezintă Comisiei periodic și în timp util rezultatele activităților sale. Acesta întocmește un raport anual privind situația referitoare la protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal în Uniune și în țările terțe.

Raportul include analiza aplicării practice a orientărilor, recomandărilor și bunelor practici menționate la articolul 66 alineatul (1) litera (c).

2. Raportul este publicat și transmis Parlamentului European, Consiliului și Comisiei.

Articolul 68
Procedură

1. Comitetul european pentru protecția datelor adoptă decizii prin majoritate simplă a membrilor săi.

2. Comitetul european pentru protecția datelor își adoptă propriul regulament de procedură și își organizează propriile mecanisme de funcționare. În special, prevede dispoziții privind continuarea exercitării funcțiilor atunci când mandatul unui membru se încheie sau un membru demisionează, privind crearea de subgrupuri pentru aspecte și sectoare specifice și privind procedurile sale în ceea ce privește mecanismul pentru asigurarea coerenței menționat la articolul 57.

Articolul 69
Președintele

1. Comitetul european pentru protecția datelor alege un președinte și doi vicepreședinți din rândul membrilor săi. Unul dintre vicepreședinți este Autoritatea Europeană pentru Protecția Datelor, cu excepția cazului în care aceasta a fost aleasă președinte.

2. Mandatul președintelui și al vicepreședinților este de cinci ani și poate fi prelungit.

Articolul 70
Sarcinile președintelui

1. Președintele are următoarele sarcini:

   (a) să convoace reuniunile Comitetului european pentru protecția datelor și să stabilească ordinea de zi;

   (b) să asigure îndeplinirea la timp a sarcinilor Comitetului european pentru protecția datelor, în special în ceea ce privește mecanismul pentru asigurarea coerenței menționat la articolul 57.

2. Comitetul european pentru protecția datelor definește în regulamentul său de procedură repartizarea sarcinilor care revin președintelui și vicepreședinților.

Articolul 71
Secretariat

1. Comitetul european pentru protecția datelor are un secretariat. Autoritatea Europeană pentru Protecția Datelor asigură secretariatul.

2. Secretariatul oferă, sub conducerea președintelui, sprijin analitic, administrativ și logistic Comitetului european pentru protecția datelor.

3. Secretariatul este responsabil în special de următoarele:

   (a) gestionarea cotidiană a Comitetului european pentru protecția datelor;

   (b) comunicarea dintre membrii Comitetului european pentru protecția datelor, președintele acestuia și Comisie și comunicarea cu alte instituții și cu cetățenii;

   (c) utilizarea mijloacelor electronice pentru comunicarea internă și externă;

   (d) traducerea informațiilor relevante;

   (e) pregătirea și monitorizarea acțiunilor ulterioare reuniunilor Comitetului european pentru protecția datelor;

   (f) pregătirea, redactarea și publicarea avizelor și a altor texte adoptate de Comitetul european pentru protecția datelor.

Articolul 72
Confidențialitate

1. Discuțiile din cadrul Comitetului european pentru protecția datelor sunt confidențiale.

2. Documentele prezentate membrilor Comitetului european pentru protecția datelor, experților și reprezentanților părților terțe sunt confidențiale, cu excepția cazului în care accesul la aceste documente este acordat în conformitate cu Regulamentul (CE) nr. 1049/2001 sau Comitetul european pentru protecția datelor le face publice într-un alt mod.

3. Membrii Comitetului european pentru protecția datelor, experții și reprezentanții părților terțe respectă obligațiile de confidențialitate prevăzute la prezentul articol. Președintele se asigură că experții și reprezentanții părților terțe au cunoștință de cerințele de confidențialitate care le sunt impuse.

CAPITOLUL VIII
CĂI DE ATAC, RĂSPUNDERE ȘI SANCȚIUNI

Articolul 73
Dreptul de a depune o plângere la o autoritate de supraveghere

1. Fără a aduce atingere oricăror alte căi de atac administrative sau judiciare, 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 prezentul regulament.

2. 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 prezentului regulament au fost încălcate ca urmare a prelucrării datelor cu caracter personal.

3. 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 74
Dreptul la o cale de atac judiciară împotriva unei autorități de supraveghere

1. Orice persoană fizică sau juridică are dreptul de a exercita o cale de atac judiciară împotriva deciziilor unei autorități de supraveghere referitoare la persoana respectivă.

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 52 alineatul (1) litera (b).

3. Acțiunile introduse împotriva unei autorități de supraveghere sunt aduse în fața instanțelor din statul membru în care este stabilită autoritatea de supraveghere.

4. O persoană vizată la care se referă o decizie a unei autorități de supraveghere dintr-un alt stat membru decât cel în care persoana vizată își are reședința obișnuită poate solicita autorității de supraveghere din statul membru în care își are reședința obișnuită să introducă o acțiune în numele său împotriva autorității de supraveghere competente din celalalt stat membru.

5. Statele membre execută hotărârile definitive ale instanțelor menționate în prezentul articol.

Articolul 75

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

1. Fără a aduce atingere vreunei căi de atac administrative disponibile, inclusiv dreptului de a depune o plângere la o autoritate de supraveghere menționat la articolul 73, orice persoană fizică are dreptul la exercitarea unei căi de atac judiciare, în cazul în care consideră că drepturile de care beneficiază în temeiul prezentului regulament au fost încălcate ca urmare a prelucrării datelor sale cu caracter personal efectuate încălcând prezentul regulament.

2. Acțiunile introduse împotriva unui operator sau unei persoane împuternicite de operator sunt prezentate în fața instanțelor din statul membru unde operatorul sau persoana împuternicită de operator are un sediu. Alternativ, o astfel de acțiune poate fi intentată în fața instanțelor din statul membru în care persoana vizată își are reședința obișnuită, cu excepția cazului în care operatorul este o autoritate publică care acționează în exercitarea competențelor sale publice.

3. În cazul în care o acțiune care se referă la aceeași măsură, decizie sau practică este în curs în cadrul mecanismului pentru asigurarea coerenței menționat la articolul 58, o instanță poate suspenda acțiunile care i-au fost înaintate, cu excepția cazurilor în care caracterul urgent al chestiunii privind protecția drepturilor persoanei vizate nu îi permite să aștepte rezultatul acțiunii în cadrul mecanismului pentru asigurarea coerenței.

4. Statele membre execută hotărârile definitive ale instanțelor menționate în prezentul articol.

Articolul 76

Norme comune aplicabile acțiunilor în instanță

1. Orice organism, organizație sau asociație menționată la articolul 73 alineatul (2) are dreptul de a exercita drepturile menționate la articolele 74 și 75 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 prezentului regulament sau de a asigura coerența protecției datelor cu caracter personal în cadrul Uniunii.

3. În cazul în care o instanță competentă a unui stat membru are motive întemeiate să creadă că în alt stat membru se desfășoară acțiuni paralele, aceasta contactează instanța competentă din celălalt stat membru pentru a-i confirma existența unor astfel de acțiuni paralele.

4. În cazul în care astfel de acțiuni paralele în alt stat membru se referă la aceeași măsură, decizie sau practică, instanța poate suspenda acțiunea.

5. 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 77

Dreptul la despăgubiri și răspundere

1. Orice persoană care a suferit prejudicii ca urmare a unei operațiuni ilegale de prelucrare sau a unei acțiuni incompatibile cu dispozițiile prezentului regulament 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 78

Sancțiuni

1. Statele membre definesc normele privind sancțiunile aplicabile în cazul încălcării dispozițiilor prezentului regulament și iau toate măsurile necesare pentru a se asigura că acestea sunt puse în aplicare, inclusiv în cazul în care operatorul nu a respectat obligația de a desemna un reprezentant. Sancțiunile prevăzute trebuie să fie eficace, proporționale și disuasive.

2. În cazul în care operatorul a desemnat un reprezentant, sancțiunile sunt aplicate reprezentantului, fără a aduce atingere sancțiunilor care ar putea fi inițiate împotriva operatorului.

3. Fiecare stat membru informează Comisia cu privire la dispozițiile din propria legislație pe care le adoptă în temeiul alineatului (1), până cel târziu la data menționată la articolul 91 alineatul (2) și, fără întârziere, orice modificare ulterioară care le afectează.

Articolul 79
Sancțiuni administrative

1. Fiecare autoritate de supraveghere este abilitată să impună sancțiuni administrative în conformitate cu prezentul articol.

2. În fiecare caz individual, sancțiunea administrativă trebuie să fie eficace, proporțională și disuasivă. Valoarea amenzii administrative este fixată în funcție de natura, gravitatea și durata încălcării, de faptul că încălcarea a fost comisă intenționat sau din neglijență, de gradul de responsabilitate a persoanei fizice sau juridice și de încălcările comise anterior de către această persoană, de măsurile și procedurile tehnice și organizatorice puse în aplicare în temeiul articolului 23 și de gradul de cooperare cu autoritatea de supraveghere în vederea remedierii încălcării.

3. În cazul primei încălcări neintenționate a dispozițiilor prezentului regulament, se poate transmite o avertizare în scris, fără impunerea vreunei sancțiuni, atunci când:

   (a) o persoană fizică prelucrează date cu caracter personal fără vreun interes comercial; sau

   (b) o întreprindere sau o organizație cu mai puțin de 250 de angajați prelucrează date cu caracter personal doar ca o activitate auxiliară activităților sale principale.

4. Autoritatea de supraveghere impune o amendă de până la 250 000 EUR sau, în cazul unei întreprinderi, de până la 0,5 % din cifra sa de afaceri anuală mondială, oricărei entități care, intenționat sau din neglijență:

   (a) nu prevede mecanisme care să permită persoanelor vizate să formuleze solicitări sau nu răspunde prompt sau nu în forma adecvată persoanelor vizate, în temeiul articolului 12 alineatele (1) și (2);

   (b) percepe o taxă pentru informații sau pentru răspunsurile la solicitările persoanelor vizate, încălcând articolul 12 alineatul (4).

5. Autoritatea de supraveghere impune o amendă de până la 500 000 EUR sau, în cazul unei întreprinderi, de până la 1 % din cifra sa de afaceri anuală mondială, oricărei entități care, intenționat sau din neglijență:

   (a) nu furnizează persoanei vizate informațiile sau furnizează informații incomplete sau nu furnizează informațiile într-un mod suficient de transparent, în conformitate cu articolul 11, articolul 12 alineatul (3) și articolul 14;

(b) nu oferă acces persoanei vizate sau nu rectifică datele cu caracter personal în temeiul articolelor 15 și 16 sau nu comunică unui destinatar informațiile relevante, în temeiul articolului 13;

(c) nu respectă „dreptul de a fi uitat” ori dreptul la ștergere sau nu instituie mecanisme pentru a asigura că termenele sunt respectate sau nu ia toate măsurile necesare pentru a informa părțile terțe că o persoană vizată solicită ștergerea tuturor linkurilor către datele sale cu caracter personal, sau a tuturor copiilor sau a reproducerilor acestora, în temeiul articolului 17;

(d) nu furnizează o copie a datelor cu caracter personal în format electronic sau împiedică persoana vizată să transmită datele cu caracter personal către o altă aplicație, încălcând articolul 18;

(e) nu definește sau nu definește suficient responsabilitățile respective cu operatorii asociați în temeiul articolului 24;

(f) nu păstrează sau nu păstrează suficient documentația în temeiul articolului 28, articolului 31 alineatul (4) și al articolului 44 alineatul (3);

(g) nu respectă, în cazurile în care nu sunt implicate categorii speciale de date, în temeiul articolelor 80, 82 și 83, normele privind libertatea de exprimare sau normele privind prelucrarea în contextul ocupării unui loc de muncă sau condițiile pentru prelucrarea datelor în scopuri de cercetare istorică, statistică și științifică.

6. Autoritatea de supraveghere impune o amendă de până la 1 000 000 EUR sau, în cazul unei întreprinderi, de până la 2 % din cifra sa de afaceri anuală mondială, oricărei entități care, intenționat sau din neglijență:

(a) prelucrează datele cu caracter personal fără niciun temei juridic sau fără un temei juridic suficient pentru prelucrare sau nu respectă condițiile privind consimțământul, în temeiul articolelor 6, 7 și 8;

(b) prelucrează categorii speciale de date, încălcând articolele 9 și 81;

(c) nu respectă o opoziție sau nu se conformează cerinței în temeiul articolului 19;

(d) nu respectă condițiile legate de măsurile bazate pe crearea de profiluri în temeiul articolului 20;

(e) nu adoptă norme interne sau nu pune în aplicare măsuri corespunzătoare pentru a asigura și a demonstra conformitatea în temeiul articolelor 22, 23 și 30;

(f) nu desemnează un reprezentant în temeiul articolului 25;

(g) prelucrează date cu caracter personal sau dă instrucțiuni de prelucrare a datelor cu caracter personal încălcând obligațiile privind prelucrarea în numele unui operator în temeiul articolelor 26 și 27;

(h) nu semnalează sau nu notifică o încălcare a securității datelor cu caracter personal sau nu notifică la timp ori complet autorității de supraveghere sau persoanei vizate încălcarea securității datelor, în temeiul articolelor 31 și 32;

(i) nu efectuează o evaluare a impactului privind protecția datelor sau prelucrează date cu caracter personal fără autorizare prealabilă sau consultarea prealabilă a autorității de supraveghere în temeiul articolelor 33 și 34;

(j) nu desemnează un responsabil cu protecția datelor sau nu asigură condițiile pentru îndeplinirea sarcinilor în temeiul articolelor 35, 36 și 37;

(k) utilizează abuziv sigiliile și mărcile din domeniul protecției datelor, în sensul articolului 39;

(l) efectuează sau dă instrucțiuni pentru transferarea de date către o țară terță sau o organizație internațională care nu este autorizată printr-o decizie privind caracterul adecvat sau prin garanții adecvate sau printr-o derogare în temeiul articolelor 40-44;

(m) nu respectă un ordin sau o interdicție temporară sau definitivă privind prelucrarea sau suspendarea fluxurilor de date emisă de autoritatea de supraveghere, în temeiul articolului 53 alineatul (1);

(n) nu respectă obligațiile de a oferi asistență sau de a răspunde sau de a furniza informațiile relevante autorității de supraveghere sau de a da acesteia acces la clădirile sale, în temeiul articolului 28 alineatul (3), al articolului 29, al articolului 34 alineatul (6) și al articolului 53 alineatul (2);

(o) nu respectă normele pentru garantarea secretului profesional, în temeiul articolului 84.

7. Comisia este mandatată să adopte acte delegate în conformitate cu articolul 86 în scopul actualizării valorilor amenzilor administrative menționate la alineatele (4), (5) și (6), ținând seama de criteriile menționate la alineatul (2).

CAPITOLUL IX
DISPOZIȚII REFERITOARE LA SITUAȚII SPECIFICE DE PRELUCRARE A DATELOR

Articolul 80

Prelucrarea datelor cu caracter personal și libertatea de exprimare

1. Statele membre prevăd exonerări și derogări de la dispozițiile privind principiile generale de la capitolul II, privind drepturile persoanei vizate de la capitolul III, privind operatorul și persoana împuternicită de către operator de la capitolul IV, privind transferul datelor cu caracter personal către țări terțe și organizații internaționale de la capitolul V, privind autoritățile de supraveghere independente de la capitolul VI și privind cooperarea și coerența de la capitolul VII, pentru prelucrarea datelor cu caracter personal efectuată numai în scopuri jurnalistice,

artistice sau literare, pentru a stabili un echilibru între dreptul la protecția datelor cu caracter personal și normele care reglementează libertatea de exprimare.

2. Fiecare stat membru informează Comisia cu privire la dispozițiile din propria legislație pe care le-a adoptat în temeiul alineatului (1) până la data menționată la articolul 91 alineatul (2) cel târziu, precum și, fără întârziere, cu privire la orice act legislativ de modificare sau orice modificare ulterioară care le afectează.

Articolul 81

Prelucrarea datelor cu caracter personal privind sănătatea

1. În limitele prevăzute de prezentul regulament și în conformitate cu articolul 9 alineatul (2), litera (h), prelucrarea datelor cu caracter personal privind sănătatea trebuie să se efectueze în baza legislației Uniunii sau a legislației statului membru care prevăd măsuri corespunzătoare și specifice pentru garantarea intereselor legitime ale persoanei vizate și care sunt necesare:

   (a) în scopuri legate de medicina preventivă sau a muncii, stabilirea diagnosticului, administrarea unor îngrijiri medicale sau a unui tratament sau de gestionarea serviciilor medicale, precum și în cazul în care datele respective sunt prelucrate de un cadru medical supus obligației de a respecta secretul profesional sau de o altă persoană supusă, de asemenea, unei obligații echivalente în ceea ce privește confidențialitatea în temeiul legislației statului membru ori al normelor stabilite de autoritățile naționale competente; sau

   (b) din motive de interes public în domeniul sănătății publice, cum ar fi protecția împotriva amenințărilor transfrontaliere grave la adresa sănătății sau asigurarea de standarde ridicate de calitate și siguranță, *inter alia* pentru medicamente sau aparatură medicală; sau

   (c) din alte motive de interes public în domenii precum protecția socială, în special în scopul asigurării calității și eficienței din punctul de vedere al costurilor a procedurilor utilizate pentru soluționarea cererilor de prestații și servicii în sistemul asigurărilor de sănătate.

2. Prelucrarea datelor cu caracter personal privind sănătatea, care este necesară în scopuri de cercetare istorică, statistică sau științifică, cum ar fi registrele de pacienți instituite pentru îmbunătățirea stabilirii diagnosticului și diferențierea între tipuri similare de boli, precum și pentru pregătirea de studii pentru terapii, face obiectul condițiilor și măsurilor de garantare prevăzute la articolul 83.

3. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 86 în scopul precizării în continuare a altor motive de interes public în domeniul sănătății publice, astfel cum se menționează la alineatul (1) litera (b), precum și a unor criterii și cerințe referitoare la garanții în ceea ce privește prelucrarea datelor cu caracter personal în scopurile menționate la alineatul (1).

Articolul 82

Prelucrarea în contextul ocupării unui loc de muncă

1. În limitele prezentului regulament, statele membre pot adopta pe cale legislativă norme specifice care reglementează prelucrarea datelor cu caracter personal ale angajaților în contextul ocupării unui loc de muncă, în special în scopul recrutării, îndeplinirii prevederilor contractului de muncă, inclusiv descărcarea de obligațiile stabilite prin lege sau prin acorduri colective, al gestionării, planificării și organizării muncii, al asigurării sănătății și securității la locul de muncă, precum și în scopul exercitării și beneficierii, în mod individual sau colectiv, de drepturile și beneficiile legate de ocuparea unui loc de muncă, precum și pentru încetarea raporturilor de muncă.

2. Fiecare stat membru informează Comisia cu privire la dispozițiile din propria legislație pe care le-a adoptat în temeiul alineatului (1) până la data menționată la articolul 91 alineatul (2) cel târziu, precum și, fără întârziere, cu privire la orice act legislativ de modificare sau orice modificare ulterioară care le afectează.

3. Comisia este mandatată să adopte acte delegate în conformitate cu articolul 86 în scopul detalierii criteriilor și cerințelor aplicabile în cazul garanțiilor în ceea ce privește prelucrarea datelor cu caracter personal în scopurile menționate la alineatul (1).

Articolul 83

Prelucrarea în scopuri de cercetare istorică, statistică și științifică

1. În limitele prezentului regulament, datele cu caracter personal pot fi prelucrate în scopuri de cercetare istorică, statistică sau științifică numai dacă:

   (a) aceste scopuri nu pot fi îndeplinite prin prelucrarea unor date care nu permit sau nu mai permit identificarea persoanelor vizate;

   (b) datele care permit atribuirea de informații unei persoane vizate identificate sau identificabile sunt păstrate separat de alte informații atât timp cât aceste scopuri pot fi îndeplinite în acest mod.

2. Organismele care desfășoară activități de cercetare istorică, statistică sau științifică pot publica sau face publice în alt mod date cu caracter personal numai dacă:

   (a) persoana vizată și-a dat consimțământul, sub rezerva condițiilor prevăzute la articolul 7;

   (b) publicarea datelor cu caracter personal este necesară pentru a prezenta rezultatele cercetării sau pentru a facilita cercetarea, în măsura în care interesele sau drepturile ori libertățile fundamentale ale persoanei vizate nu prevalează asupra acestor interese sau

   (c) persoana vizată a făcut publice datele respective.

3. Comisia este mandatată să adopte acte delegate în conformitate cu articolul 86 în scopul detalierii criteriilor și cerințelor aplicabile în cazul prelucrării datelor cu

caracter personal în scopurile menționate la alineatele (1) și (2), precum și a tuturor limitărilor necesare privind drepturile la informare și la acces ale persoanei vizate și care detaliază condițiile și garanțiile pentru drepturile persoanelor vizate în aceste circumstanțe.

Articolul 84
Obligații privind păstrarea confidențialității

1. În limitele prezentului regulament, statele membre pot adopta norme specifice pentru a stabili competențele de investigare ale autorităților de supraveghere, prevăzute la articolul 53 alineatul (2) în legătură cu operatori sau cu persoane împuternicite de operatori care trebuie să respecte, în temeiul dreptului intern sau al normelor stabilite de autoritățile naționale competente, obligația de a păstra secretul profesional sau alte obligații echivalente de confidențialitate, în cazul în care acest lucru este necesar și proporțional pentru a stabili un echilibru între dreptul la protecția datelor cu caracter personal și obligația păstrării confidențialității. Aceste norme se aplică doar în ceea ce privește datele cu caracter personal pe care operatorul sau persoana împuternicită de operator le-a primit sau le-a obținut în contextul unei activități care intră sub incidența acestei obligații de păstrare a confidențialității.

2. Fiecare stat membru notifică Comisiei normele adoptate în temeiul alineatului (1), până la data precizată la articolul 91 alineatul (2) cel târziu, precum și, fără întârziere, orice modificare ulterioară care le afectează.

Articolul 85
Normele existente în domeniul protecției datelor pentru biserici și asociații religioase

1. În cazul în care, într-un stat membru, bisericile și asociațiile sau comunitățile religioase aplică, la data intrării în vigoare a prezentului regulament, un set cuprinzător de norme de protecție a persoanelor fizice cu privire la prelucrarea datelor cu caracter personal, aceste norme pot continua să se aplice, cu condiția ca acestea să fie ajustate, pentru a fi conforme cu dispozițiile prezentului regulament.

2. Bisericile și asociațiile religioase care aplică un set cuprinzător de norme în conformitate cu alineatul (1) asigură instituirea unei autorități de supraveghere independente, în conformitate cu capitolul VI din prezentul regulament.

CAPITOLUL X
ACTE DELEGATE ȘI ACTE DE PUNERE ÎN APLICARE

Articolul 86
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 6 alineatul (5), articolul 8 alineatul (3), articolul 9 alineatul (3), articolul 12 alineatul (5), articolul 14 alineatul (7), articolul 15 alineatul (3) Articolul 17 alineatul (9), articolul 20

alineatul (6), articolul 22 alineatul (4), articolul 23 alineatul (3), articolul 26 alineatul (5), articolul 28 alineatul (5), articolul 30 alineatul (3), articolul 31 alineatul (5), articolul 32 alineatul (5), articolul 33 alineatul (6), articolul 34 alineatul (8), articolul 35 alineatul (11), articolul 37 alineatul (2), articolul 39 alineatul (2), articolul 43 alineatul (3), articolul 44 alineatul (7), articolul 79 alineatul (6), articolul 81 alineatul (3), articolul 82 alineatul (3) și articolul 83 alineatul (3), îi este conferită Comisiei pentru o perioadă de timp nedeterminată, de la data intrării în vigoare a prezentului regulament.

3. Delegarea de competențe menționată la articolul 6 alineatul (5), articolul 8 alineatul (3), articolul 9 alineatul (3), articolul 12 alineatul (5), articolul 14 alineatul (7), articolul 15 alineatul (3), articolul 17 alineatul (9), articolul 20 alineatul (6), articolul 22 alineatul (4), articolul 23 alineatul (3), articolul 26 alineatul (5), articolul 28 alineatul (5), articolul 30 alineatul (3), articolul 31 alineatul (5), articolul 32 alineatul (5), articolul 33 alineatul (6), articolul 34 alineatul (8), articolul 35 alineatul (11), articolul 37 alineatul (2), articolul 39 alineatul (2), articolul 43 alineatul (3), articolul 44 alineatul (7), articolul 79 alineatul (6), articolul 81 alineatul (3), articolul 82 alineatul (3) și articolul 83 alineatul (3) 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 6 alineatul (5), articolului 8 alineatul (3), articolului 9 alineatul (3), articolului 12 alineatul (5), articolului 14 alineatul (7), articolului 15 alineatul (3), articolului 17 alineatul (9), articolului 20 alineatul (6), articolului 22 alineatul (4), articolului 23 alineatul (3), articolului 26 alineatul (5), articolului 28 alineatul (5), articolului 30 alineatul (3), articolului 31 alineatul (5), articolului 32 alineatul (5), articolului 33 alineatul (6), articolului 34 alineatul (8), articolului 35 alineatul (11), articolului 37 alineatul (2), articolului 39 alineatul (2), articolului 43 alineatul (3), articolului 44 alineatul (7), articolului 79 alineatul (6), articolului 81 alineatul (3), articolului 82 alineatul (3) și articolului 83 alineatul (3), intră în vigoare numai în cazul în care nu a fost exprimată nici o obiecție din partea Parlamentului European sau a Consiliului, în termen de două 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 două luni, la inițiativa Parlamentului European sau a Consiliului.

Articolul 87
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 XI
DISPOZIȚII FINALE

Articolul 88
Abrogarea Directivei 95/46/CE

1. Directiva 95/46/CE se abrogă.

2. Trimiterile la directiva abrogată se interpretează ca trimiteri la prezentul regulament. Trimiterile la Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal instituit prin articolul 29 din Directiva 95/46/CE se interpretează ca trimiteri la Comitetul european pentru protecția datelor instituit prin prezentul regulament.

Articolul 89
Relația cu Directiva 2002/58/CE și modificarea acesteia

1. Prezentul regulament nu impune obligații suplimentare pentru persoanele fizice sau juridice în ceea ce privește prelucrarea datelor cu caracter personal în legătură cu furnizarea de servicii de comunicații electronice destinate publicului în rețelele de comunicații publice din Uniune cu privire la aspectele pentru care acestea fac obiectul unor obligații specifice cu același obiectiv precum cel prevăzut în Directiva 2002/58/CE.

2 Articolul 1 alineatul (2) din Directiva 2002/58/CE se elimină.

Articolul 90
Evaluarea

Comisia transmite Parlamentului European și Consiliului, la intervale regulate, rapoarte privind evaluarea și revizuirea prezentului regulament. Primul raport se transmite în termen de cel mult patru ani de la data intrării în vigoare a prezentului regulament. Ulterior, următoarele rapoarte se transmit o dată la patru ani. Comisia transmite, dacă este necesar, propuneri corespunzătoare în vederea modificării prezentului regulament, precum și alinierea altor instrumente juridice, în special ținând seama de realizările din domeniul tehnologiei informațiilor și având în vedere progresele societății informaționale. Rapoartele se publică.

Articolul 91

Intrarea în vigoare și aplicarea

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

2. Se aplică începând cu [*doi ani de la data menționată la alineatul (1*)].

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

Adoptată la Bruxelles, 25.1.2012.

Pentru Parlamentul European	*Pentru Consiliu*
Președintele	*Președintele*

FIȘĂ FINANCIARĂ LEGISLATIVĂ

1. CADRUL PROPUNERII/INIȚIATIVEI

1.1. Denumirea propunerii/inițiativei

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

1.3. Tipul propunerii/inițiativei

1.4. Obiective

1.5. Motivul (motivele) propunerii/inițiativei

1.6. Durata acțiunii și impactul financiar al acesteia

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

2. MĂSURI DE GESTIONARE

2.1. Dispoziții în materie de monitorizare și raportare

2.2. Sistemul de gestiune și control

2.3. Măsuri de prevenire a fraudelor și a neregulilor

3. IMPACTUL FINANCIAR ESTIMAT AL PROPUNERII/INIȚIATIVEI

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

3.2. Impactul estimat asupra cheltuielilor

3.2.1. Sinteza impactului estimat asupra cheltuielilor

3.2.2. Impactul estimat asupra creditelor operaționale

3.2.3. Impactul estimat asupra creditelor cu caracter administrativ

3.2.4. Compatibilitatea cu cadrul financiar multianual actual

3.2.5. Participarea terților la finanțare

3.3. Impactul estimat asupra veniturilor

FIȘĂ FINANCIARĂ LEGISLATIVĂ

1. CADRUL PROPUNERII/INIȚIATIVEI

Prezenta fișă financiară detaliază cerințele în materie de cheltuieli administrative pentru punerea în practică a reformelor privind protecția datelor, astfel cum se precizează în evaluarea impactului corespunzătoare. Reforma include două propuneri legislative, un regulament general privind protecția datelor și o directivă privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, investigării, identificării sau urmăririi penale a infracțiunilor sau al executării pedepselor. Prezenta fișă financiară acoperă impactul bugetar al ambelor instrumente.

În funcție de repartizarea sarcinilor, resursele sunt necesare Comisiei și Autorității Europene pentru Protecția Datelor (AEPD).

În ceea ce privește Comisia, resursele necesare sunt deja incluse în propunerea de perspectivă financiară 2014-2020. Protecția datelor reprezintă unul dintre obiectivele programului „Drepturi și cetățenie", care va sprijini, de asemenea, măsuri pentru punerea în practică a acestui cadru juridic. Creditele administrative care includ necesarul de personal sunt prevăzute în bugetul administrativ al DG JUST.

În ceea ce privește AEPD, resursele necesare vor trebui să fie luate în considerare la elaborarea bugetelor anuale respective pentru AEPD. Resursele sunt prezentate în detaliu în anexa la prezenta fișă financiară. Pentru a asigura resursele necesare pentru noile sarcini ale Comitetului european pentru protecția datelor, al cărui secretariat va fi asigurat de către AEPD, va fi necesară reprogramarea rubricii 5 din perspectiva financiară 2014-2020.

1.1. Denumirea propunerii/inițiativei

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). 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, investigării, identificării sau urmăririi penale a infracțiunilor sau al executării pedepselor și libera circulație a acestor date.

1.2. Domeniul (domeniile) de politică în cauză în structura ABM/ABB[49]

Justiție – protecția datelor cu caracter personal

Impactul bugetar privește Comisia și AEPD. Impactul asupra bugetului Comisiei este prezentat în detaliu în tabelele din prezenta fișă financiară. Cheltuielile operaționale constituie o parte a programului „Drepturi și cetățenie” și au fost luate deja în considerare în fișa financiară a programului respectiv, întrucât cheltuielile administrative fac parte din pachetul financiar al DG Justiție. Elementele privind AEPD sunt prezentate în anexă.

1.3. Tipul propunerii/inițiativei

☐ Propunere/inițiativă care se referă la **o acțiune nouă**

☐ Propunere/inițiativă care se referă la **o acțiune nouă ca urmare a unui proiect-pilot/a unei acțiuni pregătitoare**[50]

☑ Propunere/inițiativă care se referă la **prelungirea unei acțiuni existente**

☐ Propunere/inițiativă care se referă la **o acțiune reorientată către o acțiune nouă**

1.4. Obiective

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

Reforma urmărește să completeze îndeplinirea obiectivelor inițiale, ținând seama de noile evoluții și provocări, și anume:

- creșterea eficacității dreptului fundamental la protecția datelor și oferirea posibilității pentru persoane de a deține controlul asupra datelor lor, în special în contextul evoluțiilor tehnologice și al unei globalizări tot mai accentuate;

- consolidarea dimensiunii de piață internă a protecției datelor prin reducerea fragmentării, consolidarea coerenței și simplificarea cadrului de reglementare, ceea ce duce la eliminarea unor costuri inutile și la reducerea sarcinii administrative.

În plus, intrarea în vigoare a Tratatului de la Lisabona - și în special introducerea unui nou temei juridic (articolul 16 din TFUE) - oferă oportunitatea îndeplinirii unui nou obiectiv, și anume

- stabilirea unui cadru cuprinzător privind protecția datelor care să acopere toate domeniile.

[49] ABM (Activity Based Management): gestionarea pe activități – ABB (Activity Based Budgeting): stabilirea bugetului pe activități.

[50] Astfel cum sunt menționate la articolul 49 alineatul (6) litera (a) sau (b) din Regulamentul financiar.

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

Obiectivul specific nr. 1

Asigurarea unei aplicări coerente a normelor în materie de protecție a datelor

Obiectivul specific nr. 2

Simplificarea sistemului actual de guvernanță pentru a contribui la asigurarea unei aplicări mai coerente

Activitatea (activitățile) ABM/ABB în cauză

[…]

1.4.3. Rezultatul (rezultatele) și impactul preconizate

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

În ceea ce privește operatorii de date, atât entitățile publice, cât și cele private beneficiază de mai multă securitate juridică prin norme și proceduri UE de protecție a datelor armonizate și clare, asigurându-se condiții de concurență echitabile și aplicarea coerentă a normelor în materie de protecție a datelor, precum și o reducere semnificativă a sarcinii administrative.

Persoanele fizice vor beneficia un control mai bun al datelor lor cu caracter personal, vor avea încredere în mediul digital și vor rămâne protejați, inclusiv în cazul în care datele lor cu caracter personal sunt prelucrate în străinătate. De asemenea, vor constata o creștere a responsabilității celor care prelucrează date cu caracter personal.

Un sistem cuprinzător pentru protecția datelor va acoperi, de asemenea, domenii precum poliția și justiția, reglementând fostul pilon al treilea și aspecte care nu sunt acoperite de acesta.

1.4.4. Indicatori de rezultat și de impact

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

(a se vedea evaluarea impactului, secțiunea 8)

Indicatorii sunt evaluați periodic și includ următoarele elemente:

- timpul și mijloacele financiare alocate de operatorii de date pentru a respecta legislația în „alte state membre”;
- resursele alocate DPA-urilor;
- organismele pentru protecția datelor instituite în cadrul organizațiilor publice și private;
- utilizarea analizelor de impact privind protecția datelor;
- numărul de plângeri ale persoanelor vizate și compensațiile primite de acestea;
- numărul de cazuri care au avut drept rezultat urmărirea penală a operatorilor de date;

- amenzile aplicate operatorilor de date care nu au respectat protecția datelor.

1.5. Motivul (motivele) propunerii/inițiativei

1.5.1. Cerințe de îndeplinit pe termen scurt sau lung

Discrepanțele actuale în punerea în aplicare, interpretarea și executarea dispozițiilor directivei de către statele membre ***reprezintă un obstacol pentru funcționarea pieței interne și pentru cooperarea între autoritățile publice în ceea ce privește politicile UE***. Acest lucru contravine obiectivului fundamental al directivei, acela de a facilita libera circulație a datelor cu caracter personal pe piața internă. Dezvoltarea rapidă a noilor tehnologii și globalizarea agravează și mai mult această problemă.

Persoanele fizice beneficiază de drepturi de protecție a datelor diferite, din cauza fragmentării și a unei puneri în practică și aplicări inconsecvente în diferitele state membre. Mai mult, ***persoanele fizice nu cunosc, de multe ori, și nici nu dețin controlul asupra a ceea ce se întâmplă cu datele lor cu caracter personal*** și, prin urmare, nu ajung să își exercite drepturile în mod efectiv.

1.5.2. Valoarea adăugată a implicării UE

Statele membre, în mod individual, nu pot reduce problemele în situația actuală. Acesta este în special cazul acelor probleme care provin din fragmentarea legislației naționale de punere în aplicare a cadrului de reglementare al UE privind protecția datelor. Prin urmare, există un temei solid pentru crearea unui cadru juridic privind protecția datelor la nivelul UE. Este necesar, în special, să se instituie un cadru armonizat și coerent care să permită un transfer facil al datelor cu caracter personal dintr-un stat membru în altul, în cadrul UE, asigurându-se în același timp o protecție efectivă pentru toate persoanele fizice, pe întreg teritoriul UE.

1.5.3. Învățăminte desprinse din experiențele anterioare similare

Propunerile prezente se bazează pe experiența acumulată în contextul Directivei 95/46/CE și pe problemele întâmpinate din cauza fragmentării transpunerii și punerii în aplicare a directivei respective, care au blocat realizarea celor două obiective ale sale, și anume, un înalt nivel de protecție a datelor și o piață unică pentru protecția datelor.

1.5.4. Coerența și posibila sinergie cu alte instrumente relevante

Prezentul pachet de reformă privind protecția datelor are drept obiectiv crearea unui cadru solid, coerent și modern privind protecția datelor la nivelul UE – neutru din punct de vedere tehnologic și care să facă față în viitor provocărilor deceniilor următoare. Acesta va aduce beneficii persoanelor fizice – prin consolidarea drepturilor acestora privind protecția datelor, în special în mediul digital – și va simplifica mediul juridic pentru întreprinderi și sectorul public, stimulând astfel dezvoltarea economiei digitale pe piața internă a UE și în afara acesteia, în conformitate cu obiectivele strategiei Europa 2020.

Elementele principale ale pachetului de reformă privind protecția datelor constau în:

– un regulament care înlocuiește Directiva 95/46/CE;

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

Aceste propuneri legislative sunt însoțite de un raport privind punerea în aplicare de către statele membre a ceea ce constituie în prezent principalul instrument al UE pentru protecția datelor în domeniul cooperării polițienești și judiciare în materie penală, Decizia-cadru 2008/977/JAI.

1.6. Durata acțiunii și impactul financiar al acesteia

☐ Propunere/inițiativă pe **durată determinată**

1. ☐ Propunere/inițiativă în vigoare din [ZZ/LL]AAAA până la [ZZ/LL]AAAA

2. ☐ Impact financiar din AAAA până în AAAA

☑ Propunere/inițiativă pe **durată nedeterminată**

1. punere în aplicare cu o perioadă de creștere în intensitate din 2014 până în 2016,

2. urmată de o perioadă de funcționare în regim de croazieră.

1.7. Modul (modurile) de gestionare preconizat(e) [51]

☑ **Gestiune centralizată directă** de către Comisie

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

3. ☐ agențiilor executive

4. ☐ organismelor instituite de Comunități[52]

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

5. ☐ organismelor publice naționale/organismelor cu misiune de serviciu public

3. ☐ persoanelor cărora li se încredințează executarea unor acțiuni specifice în temeiul titlului V din Tratatul privind Uniunea Europeană, identificate în actul de bază relevant în sensul articolului 49 din Regulamentul financiar

☐ **Gestiune partajată** cu state membre

☐ **Gestiune descentralizată** împreună cu țări terțe

☐ **Gestiune în comun** cu organizații internaționale **(a se preciza)**

Dacă se indică mai multe moduri de gestionare, se furnizează detalii suplimentare în secțiunea „Observații".

Observații

//

[52] Astfel cum sunt menționate la articolul 185 din Regulamentul financiar.

2. MĂSURI DE GESTIONARE

2.1. Dispoziții în materie de monitorizare și raportare

A se preciza frecvența și condițiile aferente acestor dispoziții.

Prima evaluare va avea loc la 4 ani după intrarea în vigoare a instrumentelor juridice. În instrumentele juridice este inclusă o clauză explicită de revizuire prin care Comisia va evalua punerea în aplicare. Comisia va raporta ulterior Parlamentului European și Consiliului cu privire la evaluarea sa. O dată la patru ani va trebui să se efectueze câte o evaluare. Se va aplica metodologia Comisiei privind evaluarea. Aceste evaluări vor fi efectuate cu ajutorul unor studii specifice privind punerea în aplicare a instrumentelor juridice, al unor chestionare adresate autorităților naționale pentru protecția datelor, al unor discuții cu experți, al unor ateliere, al unor sondaje Eurobarometru ș.a.m.d.

2.2. Sistemul de gestiune și control

2.2.1. Riscul (riscurile) identificat(e)

A fost realizată o evaluare a impactului pentru reformarea cadrului privind protecția datelor în UE, pentru a însoți propunerile de regulamente și de directivă.

Noul instrument juridic va introduce un mecanism care să asigure coerența, și faptul că autoritățile independente de supraveghere din statele membre aplică cadrul în mod consecvent și coerent. Mecanismul va funcționa prin intermediul Comitetului european pentru protecția datelor alcătuit din conducătorii autorităților naționale de supraveghere și ai Autorității Europene pentru Protecția Datelor (AEPD), care va înlocui actualul Grup de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal. AEPD va asigura activitățile de secretariat pentru acest organism.

În cazul unor eventuale decizii divergente ale autorităților statelor membre, Comitetul european pentru protecția datelor va fi consultat pentru a emite un aviz cu privire la chestiunea respectivă. În cazul în care această procedură nu dă rezultate sau în cazul în care o autoritate de supraveghere refuză să se conformeze avizului, Comisia ar putea, pentru a asigura aplicarea corectă și coerentă a prezentului regulament, să emită un aviz sau, în cazul în care este necesar, să adopte o decizie, atunci când are îndoieli serioase cu privire la faptul că proiectul de măsură ar garanta aplicarea corectă a prezentului regulament sau când crede că ar avea drept rezultat o aplicare incoerentă a acestuia.

Mecanismul pentru asigurarea coerenței necesită resurse suplimentare pentru AEPD (12 ENI și credite administrative și operaționale adecvate, de exemplu, pentru sisteme și operațiuni informatice) pentru asigurarea activităților de secretariat și pentru Comisie (5 ENI și credite administrative și operaționale aferente) pentru tratarea cazurilor legate de coerență.

2.2.2. **Metoda (metodele) de control preconizată (preconizate)**

Metodele de control existente aplicate de către AEPD și de către Comisie vor acoperi creditele suplimentare.

2.3. Măsuri de prevenire a fraudelor și a neregulilor

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

Măsurile de prevenire existente aplicate de către AEPD și de către Comisie vor acoperi creditele suplimentare.

3. IMPACTUL FINANCIAR ESTIMAT AL PROPUNERII/INIȚIATIVEI

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

1. Linii bugetare de cheltuieli existente

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

Rubrica din cadrul financiar multianual	Linia bugetară	Tipul cheltuielilor	Contribuție			
	Număr [Descriere……...…….]	Dif./ Nedif. (53)	Țări AELS[54]	Țări candidate[55]	Țări terțe	În sensul articolului 18 alineatul (1) litera (aa) din Regulamentul financiar

53 = credite diferențiate / CND = credite nediferențiate.

54 AELS: Asociația Europeană a Liberului Schimb.

55 Țările candidate și, după caz, țările potențial candidate din Balcanii de Vest.

3.2. Impactul estimat asupra cheltuielilor

3.2.1. Sinteza impactului estimat asupra cheltuielilor

milioane EUR (cu 3 zecimale)

Rubrica din cadrul financiar multianual:	Numărul	

			Anul **N**[56]**= 2014**	Anul **N+1**	Anul **N+2**	Anul **N+3**	A se menționa numărul de ani necesar pentru a reflecta durata impactului (cf. punctul 1.6)			**TOTAL**
• Credite operaționale										
Numărul liniei bugetare	Angajamente	(1)								
	Plăți	(2)								
Numărul liniei bugetare	Angajamente	(1a)								
	Plăți	(2a)								
Credite cu caracter administrativ finanțate din bugetul anumitor programe[57]										
Numărul liniei bugetare		(3)								
TOTAL credite pentru DG	Angajamente	=1+1a +3								
	Plăți	=2+2a +3								

• TOTAL credite operaționale	Angajamente	(4)								
	Plăți	(5)								
• TOTAL credite cu caracter administrativ finanțate din bugetul anumitor programe		(6)								
TOTAL credite încadrate în RUBRICA 3 din cadrul financiar multianual	Angajamente	=4+ 6								
	Plăți	=5+ 6								

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

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

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

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

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

milioane EUR (cu 3 zecimale)

		Anul **N= 2014**	Anul **2015**	Anul **2016**	Anul **2017**	Anul **2018**	Anul **2019**	Anul **2020**	**TOTAL**
DG: JUST									
• Resurse umane		2,922	2,922	2,922	2,922	2,922	2,922	2,922	**20,454**
• Alte cheltuieli administrative		0,555	0,555	0,555	0,555	0,555	0,555	0,555	**3,885**
TOTAL DG JUST		**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**24,339**

TOTAL credite în cadrul RUBRICII 5 din cadrul financiar multianual	(Total angajamente = Total plăți)	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**24,339**

milioane EUR (cu 3 zecimale)

		Anul **N**[58]	Anul **N+1**	Anul **N+2**	Anul **N+3**	A se menționa numărul de ani necesar pentru a reflecta durata impactului (cf. punctul 1.6)			**TOTAL**
TOTAL credite în cadrul RUBRICILOR 1 - 5 din cadrul financiar multianual	Angajamente	3,477	3,477	3,477	3,477	3,477	3,477	3,477	24,339
	Plăți	3,477	3,477	3,477	3,477	3,477	3,477	3,477	24,339

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

3.2.2. Impactul estimat asupra creditelor operaționale

6. ☑ Propunerea/inițiativa nu implică utilizarea de credite operaționale

Un nivel ridicat de protecție a datelor cu caracter personal constituie, de asemenea, unul din obiectivele programului „Drepturi și cetățenie”

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

Credite de angajament în milioane EUR (cu 3 zecimale)

Obiective și realizări			Anul **N=2014**		Anul **N+1**		Anul **N+2**		Anul **N+3**		A se menționa numărul de ani necesar pentru a reflecta durata impactului (cf punctul 1 6)						**TOTAL**	
	REALIZĂRI																	
⇩	Tipul realizării [59]	Costul mediu al realizării	Numărul de realizări	Costuri	Numărul de realizări	Costuri	Numărul de realizări	Costuri	Numărul de realizări	Costuri	Numărul de realizări	Costuri	Numărul de realizări	Costuri	Numărul de realizări	Costuri	Număr total de realizări	Total costuri
OBIECTIVUL SPECIFIC Nr 1																		
- Realizare	Dosare[60]																	
Subtotal obiectivul specific nr 1																		
OBIECTIVUL SPECIFIC Nr 2																		
- Realizare	Cazuri[61]																	
Subtotal obiectivul specific nr 2																		
COSTURI TOTALE																		

[59] Realizările se referă la produse și servicii care urmează a fi furnizate (de ex.: numărul de schimburi de studenți finanțate, numărul de km de străzi construite etc.).

[60] Avize, decizii, întruniri privind procedurile ale Comitetului.

[61] Cazurile tratate în cadrul mecanismului pentru asigurarea coerenței.

3.2.3. Impactul estimat asupra creditelor cu caracter administrativ

3.2.3.1. Sinteză

8. ☐ Propunerea/inițiativa nu implică utilizarea de credite administrative

9. ☑ Propunerea/inițiativa implică utilizarea de credite administrative, conform explicațiilor de mai jos:

milioane EUR (cu 3 zecimale)

	Anul N [62] 2014	Anul **2015**	Anul **2016**	Anul **2017**	Anul **2018**	Anul **2019**	Anul **2020**	**TOTAL**
RUBRICA 5 din cadrul financiar multianual								
Resurse umane	2,922	2,922	2,922	2,922	2,922	2,922	2,922	**20,454**
Alte cheltuieli administrative	0,555	0,555	0,555	0,555	0,555	0,555	0,555	**3,885**
Subtotal RUBRICA 5 din cadrul financiar multianual	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**24,339**

În afara RUBRICII 5[63] din cadrul financiar multianual								
Resurse umane								
Alte cheltuieli cu caracter administrativ								
Subtotal în afara RUBRICII 5 din cadrul financiar multianual								

TOTAL	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**24,339**

62 Anul N este anul în care începe punerea în aplicare a propunerii/inițiativei.

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

3.2.3.2. Necesarul de resurse umane estimat

10. ☐ Propunerea/inițiativa nu implică utilizarea de resurse umane

11. ☑ Propunerea/inițiativa implică utilizarea de resurse umane, conform explicațiilor de mai jos:

Estimarea trebuie exprimată în echivalent normă întreagă (sau cel mult cu o zecimală)

		Anul **2014**	Anul **2015**	Anul **2016**	Anul **2017**	Anul **2018**	Anul **2019**	Anul **2020**
• Posturi din schema de personal (posturi de funcționari și de agenți temporari)								
XX 01 01 01 (la sediu și în birourile de reprezentare ale Comisiei)		22	22	22	22	22	22	22
XX 01 01 02 (în delegații)								
• Personal extern (în echivalent normă întreagă: ENI)[64]								
XX 01 02 01 (AC, INT, END din „pachetul global”)		2	2	2	2	2	2	2
XX 01 02 02 (AC, INT, JED, AL și END în delegații)								
XX 01 04 yy[65]	- la sediu[66]							
	- în delegații							
XX 01 05 02 (AC, INT, END – în cadrul cercetării indirecte)								
10 01 05 02 (AC, INT, END - în cadrul cercetării directe)								
Alte linii bugetare (a se preciza)								
TOTAL		**24**	**24**	**24**	**24**	**24**	**24**	**24**

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

Odată cu reforma, Comisia va trebui să îndeplinească sarcini noi în domeniul protecției persoanelor fizice privind prelucrarea datelor cu caracter personal, în plus față de cele realizate în mod curent. Sarcinile suplimentare se referă în principal la punerea în aplicare a noului mecanism pentru asigurarea coerenței care va garanta aplicarea coerentă a legislației armonizate în materie de protecție a datelor, evaluarea conformității țărilor terțe pentru care Comisia va fi unicul responsabil, precum și pregătirea măsurilor de punere în aplicare și a actelor delegate. Comisia va continua și celelalte sarcini pe care le efectuează în prezent (de exemplu, elaborarea de politici, transpunerea rezultatelor monitorizării, creșterea nivelului de sensibilizare, soluționarea plângerilor etc.).

64 AC= agent contractual; INT = personal pus la dispoziție de agenți de muncă temporară („Intérimaire”); JED = „Jeune Expert en Délégation” (experți secundari în delegații); AL= agent local; END= expert național detașat.

65 Sub plafonul pentru personal extern din credite operaționale (fostele linii „BA”).

66 În special pentru fonduri structurale, Fondul european agricol pentru dezvoltare rurală (FEADR) și Fondul european pentru pescuit (FEP).

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

Descrierea sarcinilor care trebuie efectuate:

Funcționari și agenți temporari	Responsabili de caz, care utilizează mecanismul pentru asigurarea coerenței pentru a garanta o aplicare unitară a normelor UE în materie de protecție a datelor. Sarcinile includ investigarea și cercetarea unor cazuri înaintate de autoritățile statelor membre în vederea adoptării unei decizii, negocierea cu statele membre și pregătirea deciziilor Comisiei. Având în vedere experiența recentă, s-ar putea să existe 5-10 cazuri pe an care să necesite utilizarea mecanismului pentru asigurarea coerenței. Soluționarea cererilor privind conformitatea necesită interacțiunea directă cu țara solicitantă, eventual gestionarea unor studii ale experților privind condițiile în țara respectivă, evaluarea condițiilor, pregătirea deciziilor relevante ale Comisiei și ale procesului, inclusiv ale comitetului care asistă Comisia și orice organisme specializate, după caz. Având în vedere experiența curentă se pot aștepta până la 4 cereri privind conformitatea anual. Procesul de adoptare de măsuri de punere în aplicare include acțiuni pregătitoare precum documente tematice, cercetare și consultări publice, precum și elaborarea instrumentelor și gestionarea procesului de negociere în cadrul comitetelor relevante sau al altor grupuri, precum și contactele cu părțile interesate în general. În domeniile care necesită o îndrumare mai specifică s-ar putea să se intervină în până la trei măsuri de punere în aplicare anual, în timp ce procesul ar putea dura până la 24 de luni, în funcție de intensitatea consultărilor.
Personal extern	Asistență tehnică și activități de secretariat

3.2.4. Compatibilitatea cu cadrul financiar multianual actual

12. ☐ Propunerea/inițiativa este compatibilă cu cadrul financiar multianual *următor*.

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

Tabelul de mai jos indică sumele reprezentând resursele financiare necesare anual pentru AEPD pentru noile sale atribuții de asigurare a activităților de secretariat ale Comitetului european pentru protecția datelor și pentru procedurile și instrumentele aferente pe durata următoarei perspective financiare, în plus față de cele incluse deja în planificare.

Anul	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**Total**
Personal etc.	1,555	1,555	1,543	1,543	1,543	1,543	1,543	10,823
Funcționare	0,850	1,500	1,900	1,900	1,500	1,200	1,400	10,250
Total	**2,405**	**3,055**	**3,443**	**3,443**	**3,043**	**2,743**	**2,943**	**21,073**

14. ☐ Propunerea/inițiativa necesită recurgerea la instrumentul de flexibilitate sau la revizuirea cadrului financiar multianual[67]

3.2.5. Participarea terților la finanțare

15. ☑Propunerea/inițiativa nu prevede cofinanțare din partea terților

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

Credite de angajament în milioane EUR (cu 3 zecimale)

	Anul **N**	Anul **N+1**	Anul **N+2**	Anul **N+3**	A se menționa numărul de ani necesar pentru a reflecta durata impactului (cf punctul 1 6)			Total
A se preciza organismul care asigură *co*finanțarea								
TOTAL credite cofinanțate								

3.3. *Impactul estimat asupra veniturilor*

17. ☑ Propunerea/inițiativa nu are impact financiar asupra veniturilor

18. ☐ Propunerea/inițiativa are următorul impact financiar:

- ☐ asupra resurselor proprii
- ☐ asupra diverselor venituri

milioane EUR (cu 3 zecimale)

Linia bugetară pentru venituri:	Credite disponibile pentru exercițiul bugetar în curs	Impactul propunerii/inițiativei[68]						
		Anul **N**	Anul **N+1**	Anul **N+2**	Anul **N+3**	A se introduce numărul de coloane necesar pentru a reflecta durata impactului (cf punctul 1 6)		

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

A se preciza metoda de calcul a impactului asupra veniturilor

[67] A se vedea punctele 19 și 24 din Acordul interinstituțional.

[68] În ceea ce privește resursele proprii tradiționale (taxe vamale, cotizațiile pentru zahăr), sumele indicate trebuie să fie sume nete, și anume sume brute după deducerea a 25 % pentru costuri de colectare.

Anexa la fișa financiară legislativă pentru propunerea de Regulament al Parlamentului European și al Consiliului privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal.

Metodologia aplicată și principalele ipoteze de bază

Costurile legate de noile sarcini care urmează să fie realizate de Autoritatea Europeană pentru Protecția Datelor (AEPD) care rezultă din cele două propuneri au fost estimate pentru cheltuielile de personal pe baza costurilor suportate de către Comisie pentru sarcini similare.

AEPD va găzdui secretariatul Comitetului european pentru protecția datelor care înlocuiește Grupul de lucru înființat în temeiul articolului 29. Având în vedere volumul de muncă curent pentru această sarcină, rezultă că sunt necesare 3 ENI suplimentare plus cheltuielile administrative și operaționale corespunzătoare. Acest volum de muncă va începe odată cu intrarea în vigoare a regulamentului.

Mai mult, AEPD va avea un rol în cadrul mecanismului pentru asigurarea coerenței despre care se preconizează că va necesita 5 ENI, precum și în dezvoltarea și operarea unui instrument informatic comun pentru APD-urile naționale, care va necesita doi membri suplimentari ai personalului.

Metoda de calcul a majorării în bugetul necesar destinat personalului pentru primii șapte ani este prezentată în detaliu în tabelul de mai jos. Un al doilea tabel prezintă bugetul operațional necesar,. Acesta va fi reflectat în bugetul UE la secțiunea IX AEPD.

Natura cheltuielilor	Calcul	Suma (în mii)							
		2014	2015	2016	2017	2018	2019	2020	Total
Salariile și indemnizațiile									
- președintelui Comitetului european pentru protecția datelor		0,300	0,300	0,300	0,300	0,300	0,300	0,300	2,100
- din care pentru funcționari și agenți temporari	=7*0 127	0,889	0,889	0,889	0,889	0,889	0,889	0,889	6,223
- din care pentru END	=1*0 073	0,073	0,073	0,073	0,073	0,073	0,073	0,073	0,511
- din care pentru agenți contractuali	=2*0 064	0,128	0,128	0,128	0,128	0,128	0,128	0,128	0,896
Cheltuieli legate de recrutare	=10*0 005	0,025	0,025	0,013	0,013	0,013	0,013	0,013	0,113
Cheltuieli de delegație		0,090	0,090	0,090	0,090	0,090	0,090	0,090	0,630
Alte cheltuieli pentru formare	=10*0 005	0,050	0,050	0,050	0,050	0,050	0,050	0,050	0,350
Totalul cheltuielilor administrative		**1,555**	**1,555**	**1,543**	**1,543**	**1,543**	**1,543**	**1,543**	**10,823**

Descrierea sarcinilor care trebuie efectuate:

Funcționari și agenți temporari	Funcționari responsabili cu activitățile de secretariat ale Comitetului pentru protecția datelor. Pe lângă suportul logistic, inclusiv aspecte bugetare și contractuale, acest lucru include pregătirea agendelor reuniunilor și invitațiilor experților, analizarea subiectelor de pe agenda grupului, gestionarea documentelor legate de lucrările grupului inclusiv protecția datelor relevante, confidențialitatea și cerințele pentru accesul publicului. Având în vedere toate subgrupurile și grupurile de experți, s-ar putea să fie necesară organizarea a până la 50 de reuniuni și de proceduri decizionale anual. Responsabili de caz care utilizează mecanismul pentru asigurarea coerenței pentru a garanta o aplicare unitară a normelor în materie de protecție a datelor. Sarcinile includ investigarea și cercetarea unor cazuri înaintate de autoritățile statelor membre în vederea adoptării unei decizii, negocierea cu statele membre și pregătirea deciziilor Comisiei. Având în vedere experiența recentă s-ar putea să existe 5-10 cazuri pe an care să necesite utilizarea mecanismului pentru asigurarea coerenței. Instrumentul IT va simplifica interacțiunea operațională dintre APD-urile naționale și operatorii obligați să facă schimb de informații cu autoritățile publice. Membri personalului responsabili vor asigura controlul calității, gestionarea proiectelor și monitorizarea bugetară a proceselor IT privind cerințele, proiectarea, aplicarea și operarea sistemelor.
Personal extern	Asistență tehnică și activități de secretariat.

Cheltuieli pentru AEPD legate de sarcini specifice

Obiective și realizări			Anul **N=2014**		Anul **N+1**		Anul **N+2**		Anul **N+3**		A se menționa numărul de ani necesar pentru a reflecta durata impactului (cf punctul 1 6)						**TOTAL**	
	REALIZĂRI																	
⇩	Tipul realizării[69]	Costul mediu al realizării	Numărul de realizări	Costuri	Numărul de realizări	Costuri	Numărul de realizări	Costuri	Numărul de realizări	Costuri	Numărul de realizări	Costuri	Numărul de realizări	Costuri	Numărul de realizări	Costuri	Număr total de realizări	Costuri totale
OBIECTIVUL SPECIFIC Nr 1[70]			Secretariatul Comitetului pentru protecția datelor															
- Realizare	Cazuri[71]	0,010	30	0,300	40	0,400	50	0,500	50	0,500	50	0,500	50	0,500	50	0,500	320	3,200
Subtotal obiectivul specific nr 1			30	0,300	40	0,400	50	0,500	50	0,500	50	0,500	50	0,500	50	0,500	320	3,200
OBIECTIVUL SPECIFIC Nr 2			Mecanismul pentru asigurarea coerenței															
- Realizare	Dosare[72]	0,050	5	0,250	10	0,500	10	0,500	10	0,500	8	0,400	8	0,400	8	0,400	59	2,950
Subtotal obiectivul specific nr 2			5	0,250	10	0,500	10	0,500	10	0,500	8	0,400	8	0,400	8	0,400	59	2,950
OBIECTIVUL SPECIFIC Nr 3			Instrumente IT comune pentru APD-uri (AEPD)															
- Realizare	Cazuri[73]	0,100	3	0,300	6	0,600	9	0,900	9	0,900	6	0,600	3	0,300	5	0,500	41	4,100
Subtotal pentru obiectivul specific nr 3			3	0,300	6	0,600	9	0,900	9	0,900	6	0,600	3	0,300	5	0,500	41	4,100
COSTURI TOTALE			38	0,850	56	1,500	69	1,900	69	1,900	64	1,500	61	1,200	63	1,400	420	10,250

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

70 Conform descrierii din secțiunea 1.4.2. „Obiectiv(e) specific(e)…”

71 Cazurile tratate în cadrul mecanismului pentru asigurarea coerenței.

72 Avize, decizii, întruniri privind procedurile, ale Comitetului.

73 Totaluri pentru fiecare estimare anuală a eforturilor pentru dezvoltarea și operarea instrumentelor IT