S.C. S.D.D.P. CONFIDENT S.R.L.

- Furnizor de servicii de formare profesională a adulţilor -

Bucureşti, Sectorul 4, Şos. Olteniţei, Nr. 225A, Etaj 1, Camera 4

- Centrul Incubator de Afaceri - CIAf -

Tel/Fax: 021.332.05.04; Tf. Mob. 0722.399.302; 0751.399.302

www.cursurisecuritate.ro / office@cursurisecuritate.ro

Operator de date cu caracter personal Nr. 17163

J40/17529/2006; C.Î.F.: 19157090

BAZA LEGISLATIVĂ PENTRU R.P.D.C.P.
(Data protection officer)

1. SFATURI UTILE despre DPO: CE TREBUIE SĂ ȘTIȚI !

Obiectivul prezentelor sfaturi este de a oferi un răspuns, într-o formă simplă și ușor de citit, la întrebările cheie pe care organizațiile le pot avea în legătură cu noile cerințe potrivit Regulamentului General privind Protecția Datelor (RGPD) de a desemna un DPO.

I. Desemnarea DPO

1. Ce organizații trebuie să numească un DPO?

Numirea unui DPO este o obligație:
• dacă prelucrarea este efectuată de o autoritatea publică sau un organism public (indiferent de datele prelucrate);
• dacă activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în operațiuni de prelucrare care necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă;
• dacă activități principale ale operatorului sau persoanei împuternicite de operator constau în prelucrarea pe scară largă a unor categorii speciale de date personale privind condamnările penale și/sau infracțiuni.

Aveți în vedere faptul că dreptul Uniunii sau dreptul intern poate impune numirea unui DPO și în alte situații.

În cele din urmă, chiar și în cazul în care desemnarea unui DPO nu este obligatorie, organizațiile pot considera, uneori, ca fiind utilă desemnarea unui DPO în mod voluntar. Grupul de Lucru Articolul 29 în domeniul protecției datelor („WP29“) încurajează aceste eforturi voluntare. Atunci când o organizație desemnează un DPO în mod voluntar, sunt aplicabile aceleași cerințe privind numirea, poziția și sarcinile ca și cum desemnarea ar fi obligatorie.
Sursa: Art. 37(1) din RGPD

2. Ce înseamnă „activitate principală”?

„Activitățile principale” pot fi considerate ca operațiuni cheie necesare pentru îndeplinirea obiectivelor operatorului sau persoanei împuternicite de operator. Acestea includ, de asemenea, toate activitățile în care prelucrarea de date reprezintă o parte indisolubilă a activității operatorului sau persoanei împuternicite de operator. De exemplu, prelucrarea datelor privind starea de sănătate, cum ar fi dosarele medicale ale pacientului ar trebui să fie considerată a fi una dintre activitățile principale în orice spital și, prin urmare, spitalele trebuie să desemneze un DPO.
Pe de altă parte, toate organizațiile efectuează anumite activități, spre exemplu, plata angajaților lor sau deținerea de activități standard de suport IT. Acestea sunt exemple de funcții de sprijin necesare pentru activitatea de bază sau principală a organizației. Chiar dacă aceste activități sunt necesare sau esențiale, acestea sunt de obicei considerate mai degrabă funcții auxiliare decât activitate principală.
Sursa: Art. 37(1)b) și c) din RGPD

3. Ce înseamnă „pe scară largă”

RGPD nu definește ce constituie prelucarea pe scară largă. WP29 recomandă ca următorii factori să fie luați în considerare atunci când se stabilește dacă prelucarea este efectuată pe o scară largă:
• numărul persoanelor vizate - ori un număr exact ori un procent din populația relevantă;
• volumul datelor și/sau gama de elemente diferite de date în curs de prelucrare;
• durata sau permanența activității de prelucrare a datelor;
• suprafața geografică a activității de prelucrare.
Exemple de prelucrări pe scară largă includ:
• prelucrarea datelor pacienților în activitatea regulată a unui spital;

• prelucrarea datelor de călătorie a unei persoane fizice ce utilizează sistemul de transport public (spre exemplu urmărirea cu ajutorul cardurilor de călătorie);
• prelucrarea în timp real a datelor de geolocalizare a clienților unei rețele internaționale de fast food în scopuri statistice de către o persoană împuternicită de operator specializată în furnizarea serviciilor de acest tip;
• prelucrarea datelor clienților în activitatea regulată a unei companii de asigurări sau a unei bănci;
• prelucrarea datelor personale de către un motor de căutare în scop de publicitate comportamentală;
• prelucrarea datelor (conținut, trafic, localizare) de către furnizorii de telefonie sau servicii de Internet.
Exemple ce nu constituie prelucrări pe scară largă includ:
• prelucrarea datelor pacientului de către un medic individual;
• prelucrarea datelor personale referitoare la condamnările penale și/sau infracțiuni de către un avocat individual.
Sursa: Art. 37(1)b) și c) din RGPD

4. Ce înseamnă „monitorizare periodică și sistematică”?

Noțiunea de monitorizare periodică și sistematică nu este definită în RGPD, dar include în mod clar toate formele de urmărire și profilare pe Internet, inclusiv în scop de publicitate comportamentală. Cu toate acestea, noțiunea de monitorizare nu este restrictionată în mediul online.
Exemple de activități care pot constitui o monitorizare periodică și sistematică a persoanelor vizate: operarea unei rețele de telecomunicații; furnizarea de servicii de telecomunicații; e-mail de direcționare repetată; activități de marketing bazate pe date; profilare și scoring în scopul evaluării riscurilor (de exemplu, în scopul de credit scoring, stabilirea primelor de asigurare, de prevenire a fraudelor, detectarea spălării banilor); urmărirea locației, spre exemplu, prin aplicații mobile; programe de loialitate; publicitate comportamentală; monitorizarea wellness, fitness și a datelor de sănătate prin intermediul dispozitivelor portabile; televiziune cu circuit închis; dispozitive conectate spre exemplu, contoare inteligente, mașini inteligente, automatizare acasă etc.
WP29 interpretează „**periodic**” ca însemnând una sau mai multe din următoarele:
• în curs de desfășurare sau care apare la anumite intervale într-o anumită perioadă;
• recurente sau repetate la perioade fixe;
• constante sau care au loc periodic.
WP29 interpretează „**sistematic**” ca însemnând una sau mai multe din următoarele:
• apărut conform sistemului;
• prearanjat, organizat sau metodic;
• luând loc ca parte a unui plan general de colectare a datelor;
• efectuat ca parte a unei strategii.
Sursa: Art.37(1)b) din RGPD

5. Mai multe organizații pot numi un DPO comun? Daca da, în ce condiții?

Da. Un grup de întreprinderi poate numi DPO unic, cu condiția ca aceasta să fie „ușor accesibil din fiecare întreprindere”. Noțiunea de accesibilitate se referă la sarciinile DPO ca punct de contact în ceea ce privește persoanele vizate, autoritatea de supraveghere, dar și pe plan intern în cadrul organizației.
Pentru a se asigura că DPO, intern sau extern, este accesibil, este important să se asigure că datele de contact ale acestuia sunt disponibile.

DPO, cu ajutorul unei echipe, dacă este necesar, trebuie să fie în măsură să comunice eficient cu persoanele vizate și să coopereze cu autoritățile de supraveghere implicate. Acest lucru înseamnă că respectiva comunicare trebuie să aibă loc în limba sau limbile utilizate de autoritățile de supraveghere și persoanele vizate. Disponibilitatea unui DPO (fie fizică în

același sediu cu angajații, prin intermediul unei linii telefonice sau prin alte mijloace sigure de comunicare) este esențială pentru a garanta că persoanele vizate vor fi în măsură să contacteze DPO.

Se poate desemna un singur DPO pentru mai multe autorități sau organisme publice, luând în considerare structura organizatorică și dimeniunea acestora. Sunt aplicabile aceleași considerente cu privire la resurse și comunicare. Având în vedere că DPO este responsabil pentru o varietate de atribuții, operatorul sau persoana împuternicită de operator trebuie să se asigure că un DPO unic, cu ajutorul unei echipe, poate efectua aceste competențe în mod eficient în ciuda faptul că este desemnat pentru mai multe autorități și organisme publice.
Sursa: Art. 37(2) și (3) din RGPD

6. Unde poate fi localizat DPO?

Pentru a se asigura că DPO este accesibil, WP29 recomandă ca DPO să fie localizat pe teritoriul UE, chiar dacă operatorul sau persoana împuternicită de operator nu este stabilită pe teritoriul UE. Cu toate acestea, nu poate fi exclus faptul că, în anumite situații în care operatorul sau persoana împuternicită de operator nu are sediul în UE, un DPO își poate îndeplini sarcinile într-un mod mai eficient dacă este localizat în afara UE.

7. Există posibilitatea desemnării unui DPO extern?

Da. DPO poate fi membru al personalului operatorului sau persoanei împuternicite de operator (DPO intern) sau își poate îndeplini sarcinile în baza unui contract de prestări servicii. Acest lucru înseamnă că DPO poate fi extern și, în acest caz, funcția sa poate fi exercitată în baza unui contract de prestări servicii încheiat cu o persoană fizică sau o organizație.

În situația în care funcția DPO este exercitată de un furnizor de servicii extern, o echipă de persoane fizice angajate ale respectivei entități poate îndeplini eficient sarcinile DPO ca o echipă, sub responsabilitatea unei singure persoane desemnate ca persoană de contact principală și „persoană responsabilă” pentru client. În această situație, este esențial ca fiecare membru al organizației care exercită funcțiile unui DPO să îndeplinească toate cerințele aplicabile potrivit RGPD.

Din motive de claritate juridică și o bună organizare și pentru a preveni conflictele de interes pentru membrii echipei, Ghidul recomandă existența unei alocări clare a sarcinilor în cadrul echipei DPO și desemnarea unei singure persoane ca persoană de contact principală și persoană „responsabilă” pentru fiecare client.
Sursa: Art. 37(6) din RGPD

8. Care sunt calitățile profesionale pe care trebuie să le posede un DPO?

DPO trebuie desemnat pe baza calităților profesionale și, în special a cunoștințelor de specialitate în dreptul și practicile în domeniul protecției datelor, precum și pe baza capacității de a-și îndeplini sarcinile.

Nivelul de expertiză necesar ar trebui determinat pe baza operațiunilor de prelucrare efectuate și a protecției necesare pentru datele cu caracter personal prelucrate. De exemplu, în situația în care o operațiune de prelucrare a datelor este deosebit de complexă sau în cazul în care este implicat un volum mare de date speciale, DPO poate necesita un nivel mai ridicat de expertiză și suport.

Aptitudinile și expertiza relevante includ:
• experiență în legislația și practicile de protecție a datelor la nivel național și european, precum și o înțelegere complexă a RGPD;
• înțelegerea operațiunilor de prelucrare efectuate;
• înțelegerea tehnologiilor de informații și de securitate a datelor;
• cunoașterea sectorului de afaceri și a organizației;
• abilitatea de a promova protecția datelor în cadrul organizației.
Sursa: Art. 37(5) din RGPD

II. Poziția DPO

9. Care sunt resursele ce trebuie prevăzute de operator sau persoana împuternicită pentru DPO?

DPO trebuie să beneficieze de resursele necesare pentru îndeplinirea sarcinilor sale.

În funcție de natura operațiunilor de prelucrare și a activităților și dimensiunii organizației, trebuie asigurate următoarele resurse pentru DPO:
• spijin activ al funcției DPO din partea managementului superior;
• timp suficient pentru DPO în vederea îndeplinirii atribuțiilor sale;
• sprijin corespunzător în ceea ce privește resursele financiare, infrastructură (sediu, facilități, echipament) și personal, după caz;
• comunicare oficială către toți angajații cu privire la desemnarea DPO;
• accesul necesar la alte servicii precum resurse umane, juridic, IT, securitate etc. astfel încât DPO să beneficieze de un sprijin esențial, reacții și informații din partea altor servicii;
• pregătire continuă.
Sursa: Art. 38(2) din RGPD

10. Care sunt garanțiile ce-i permit DPO să-și îndeplinească sarcinile în mod independent? Ce înseamnă „conflict de interese”?

Există anumite garanții ce-i permit DPO să acționeze în mod independent:
• nu primește instrucțiuni de la operator sau persoana împuternicită de operator în ceea ce privește îndeplinirea sarcinilor sale;
• nu este demis sau sancționat de operator pentru îndeplinirea sarcinilor sale;
• nu există conflict de interese cu alte posibile sarcini sau atribuții.

Celelalte sarcini sau atribuții ale DPO nu trebuie să genereze un conflic de interese. Acest lucru presupune, în special, faptul că DPO nu poate deține o poziție în cadrul organizației care ar conduce la posibilitatea ca DPO să stabilească scopurile și mijloacele de prelucrare a datelor cu caracter personal. Acest lucru trebuie luat în considerare de la caz la caz, ținându-se cont de structura organizațională specifică fiecărei organizații.

Ca regulă generală, funcții din cadrul organizației cu care poate intra în conflict pot include funcții de conducere (cum ar fi director executiv, director operațional, director financiar, șeful serviciului medical, șeful departamentului de marketing, șef departamentului de resurse umane sau șeful departamentului IT), dar, în același timp, și alte funcții inferioare dacă acestea conduc la posibilitatea de a stabili scopurile și mijloacelor de prelucrare. În plus, un conflict de interese poate apărea, de asemenea, de exemplu, în situația în care un DPO extern este rugat să reprezinte operatorul sau persoana împuternicită de operator în instanță, în cazurile care implică probleme de protecție a datelor.
Sursa: Art. 38(3) și 38(6) din RGPD

III. Sarcini DPO

11. Ce înseamnă „monitorizarea conformității”?

Ca parte a acestor sarcini de monitorizare a conformității, DPO poate, în special:
• să colecteze informații pentru a indentifica operațiunile de prelucrare;
• să analizeze și să verifice conformitatea operațiunilor de prelucrare;
• să informeze, să consilieze și să emită recomandări operatorului sau persoanei împuternicite de operator.
Sursa: Articolul 39(1)b) din RGPD

12. DPO este personal responsabil pentru nerespectarea cerințelor de protecție a datelor?

Nu. DPO nu este personal responsabil în situația în care există un caz de nerespectare a cerințelor de protecție a datelor. Operatorul sau persoana împuternicită de operator are obligația de a pune în aplicare măsuri tehnice și orgnizatorice adecvate pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul

Regulament. Respectarea normelor de protecției a datelor este o responsabilitate a operatorului sau a persoanei împuternicite de operator.

13. Care este rolul DPO în legătură cu DPIA și păstrarea evidenței operațiunilor de prelucrare?

În ceea ce privește **evaluarea impactului operațiunilor de prelucrare (DPIA)**, operatorul sau persoana împuternicită de operator solicită avizul DPO în legătură cu următoarele aspecte, printre care:

• dacă să efectueze sau nu DPIA;
• ce metodologie să fie folosită la efectuarea DPIA;
• dacă să efectueze DPIA intern sau să externalizeze;
• ce garanții (inclusiv măsuri tehnice și organizaționale) să pună în aplicare pentru reducerea oricăror riscuri la adresa drepturilor și intereselor persoanelor vizate;
• dacă DPIA a fost sau nu efectuată corect și dacă respectivele concluzii (dacă să continue sau nu prelucrarea și ce garanții să pună în aplicare) respectă RGPD.

În ceea ce privește păstrarea unei **evidențe a operațiunilor de prelucrare**, operatorul sau persoana împuternicită de operator, și nu DPO, are obligația de a păstra o evidență a operațiunilor de prelucrare.

Cu toate acestea, nimic nu împiedică operatorul sau persoana împuternicită de operator să atribuie DPO sarcina de a păstra o evidență a operațiunilor de prelucrare în numele operatorului sau persoanei împuternicite de operator. O astfel de evidență trebuie să fie considerată ca fiind unul dintre instrumentele care permit DPO să-și îndeplinească sarcinile de monitorizare a conformității, informare și consiliere a operatorului sau persoanei împuternicite de operator.

Sursa: Art.39(1)c) și Art. 30 din RGPD

2. GHIDUL privind Responsabilul cu protecția datelor (DPO)
„ARTICOLUL 29" PENTRU PROTECȚIA DATELOR

1. Introducere

Regulamentul General privind Protecția Datelor (RGPD) ce urmează să devină aplicabil la data de 25 mai 2018 oferă un cadru legal modernizat, de conformitate bazat de responsabilitate pentru protecția datelor în Europa.

Responsabilul cu protecția datelor (DPO) va reprezenta centrul acestui nou cadru juridic pentru multe organizații, facilitând respectarea prevederilor RGPD.

Potrivit RGPD, este obligatoriu ca anumiți operatori și persoane împuternicite de operatori să desemneze un DPO. Aceasta va fi situația pentru toate autoritățile și organismele publice (indiferent de tipul datelor prelucrate) și pentru celelalte organizații care - ca și activitate principală - monitorizează în mod sistematic și pe scară largă persoanele fizice sau prelucrează categorii speciale de date cu caracter personal pe scară largă.

Chiar și în situația în care RGPD nu impune în mod expres numirea unui DPO, organizațiile pot găsi ca fiind utilă desemnarea unui DPO în mod voluntar. Grupul de Lucru Articolul 29 („WP29") încurajează aceste eforturi voluntare.

DPO acționează ca intermediar între părțile interesate relevante (de exemplu autoritățile de supraveghere, persoanele vizate și unitățile de afaceri din cadrul unei organizații).

DPO nu este personal responsabil în caz de nerespectare a RGPD. RGPD spune clar că resposabil este operatorul sau persoana împuternicită de operator care trebuie să se asigure și să fie în măsură să demonstreze că prelucrarea este efectuată în conformitate cu disponzițiile sale (art. 24(1)). Respectarea normelor de protecție a datelor reprezintă responsabilitatea operatorului sau a persoanei împuternicite de operator.

Operatorul sau persoana împuternicită de operator are de asemenea un rol crucial în a permite îndeplinirea eficientă a atrtibuțiilor DPO. Numirea unui DPO reprezintă un prim pas, dar trebuie să se asigure că DPO are autonomie și resurse suficiente pentru îndeplinirea sarcinilor într-un mod eficient.

RGPD recunoaște DPO ca un actor-cheie în noul sistem de guvernare al protecției datelor și stabilește condițiile pentru numirea sa, poziția și sarcinile sale.

Obiectivul acestui ghid este de a clarifica prevederile relevante din RGPD pentru a ajuta operatorii și persoanele împuternicite de operator în vederea respectării legii, dar și pentru a ajuta DPO în ceea ce privește rolul său. Ghidul oferă, de asemenea, recomandări de bune practici, bazându-se pe experiența acumulată în unele state membre UE.

2. Desemnarea DPO

2.1. Desemnarea obligatorie

Art. 37(1) din RGPD solicită **desemnarea DPO în trei situații specifice**:
(*potrivit art. 37(4), dreptul Uniunii sau dreptul intern poate impune numirea unui DPO și în alte situații*)
a) atunci când prelucarea este efectuată de o autoritate publică sau un organism public;
b) atunci când activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în operațiuni de prelucrare care necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă; sau
c) atunci când activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în prelucrarea pe scară largă a unor categorii speciale de date (*potrivit art. 9, acestea includ date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoanei fizice, de date privind starea de sănătate sau de date privind viața sexuală sau*

orientarea sexuală a unei persoane fizice) sau/şi a unor categorii de date cu caracter personal privind condamnări penale și infracțiuni (a*rt. 10*).

În următoarele subsecțiuni WP29 oferă orientări cu privire la criteriile și terminologia folosită în art. 37(1).

Cu excepția cazului în care este evident faptul că o organizație nu este obligată să desemneze un DPO, WP29 recomandă ca operatorii și persoanele împuternicite de operator să documenteze evaluările interne efectuate pentru a determina dacă va fi numit un DPO, pentru a fi în măsură să demonstreze că au fost luați în considerare în mod corespunzător factorii relevanți (*a se vedea art. 24(1)).* Această analiză reprezintă o parte a documentației potrivit principiului responsabilității. Aceasta poate fi solicitată de autoritatea de supraveghere și ar trebui actualizată atunci când este necesar, de exemplu, în situația în care operatorii sau persoanele împuternicite de operatori întreprind activități noi sau furnizează servicii noi care se pot încadra în cazurile enumerate la art. 37(1).

În situația în care o organizație numește un DPO în mod voluntar, condițiile de la art. 37-39 se aplică numirii, poziției și sarcinilor ca și cum desemnarea ar fi obligatorie.

Nimic nu împiedică o organizație, care nu are obligația legală de a desemna un DPO și nu dorește să desemneze un DPO în mod voluntar, să angajeze personal sau consultanți externi cu sarcini legate de protecția datelor cu caracter personal. În acest caz, este important să se asigure că nu există nicio confuzie în ceea ce privește titlul, statutul, poziția și sarcinile acestora. Prin urmare, trebuie clarificat, în orice comunicare din cadrul companiei, precum și cu autoritățile pentru protecția datelor, persoanele vizate și publicul larg, că titlul acestei persoane sau consultant nu este cel de responsabil cu protecția datelor - DPO (a*cest lucru este de asemenea relevant pentru responsabilii principali cu protecția datelor (CPO – chief privacy officers) sau alți profesioniști în domeniu din cadrul companiilor care nu respectă întotdeauna cerințele RGPD, spre exemplu, în legătură cu resursele disponibile sau garanțiile de idependență și, dacă nu sunt respectate, nu pot fi considerați sau numiți DPO*).

DPO, obligatoriu sau voluntar, este desemnat pentru toate operațiunile efectuate de operator sau persoana împuternicită de operator.

2.1.1. „Autoritate publică sau organism public”

RGPD nu definește ce înseamnă „autoritate publică sau organism public”. WP29 consideră că o asemenea noțiune trebuie stabilită în conformitate cu dreptul intern. În consecință, autoritățile și organismele publice includ autoritățile naționale, regionale și locale, dar conceptul, în conformitate cu legislația națională aplicabilă, include, de asemenea, o serie de alte organisme guvernate de legislația în domeniul public (a se vedea, de exemplu definiția pentru „*organism din sectorul public*” și „*organism de drept public*”). În astfel de cazuri, desemnarea unui DPO este obligatorie.

O sarcină publică poate fi efectuată, iar o autoritate publică poate fi exercitată (*art. 6(1)e)*) nu numai de către autorități sau organisme publice, ci și de alte persoane fizice sau juridice de drept public sau privat, în sectoare precum servicii de transport public, furnizare de apă și energie, infrastructura rutieră, serviciul public de radiodifuziune, locuințe publice sau organisme disciplinare pentru profesiile reglementate, în conformitate cu reglementarea națională a fiecărui stat membru.

În aceste cazuri, persoanele vizate pot fi într-o situație foarte asemănătoare ca atunci când datele lor sunt prelucrate de o autoritate publică sau un organism public. În special, datele pot fi prelucrate în scopuri similare, iar persoanele fizice au de multe ori la fel de puține posibilități sau chiar deloc posibilitatea de a alege dacă datele lor vor fi prelucrate și modul în care vor fi prelucrare și pot solicita astfel protecția suplimentară pe care o poate aduce desemnarea unui DPO.

Chiar dacă nu există nicio obligație în astfel de cazuri, WP29 recomandă, ca bună practică, ca organizațiile private care îndeplinesc atribuții publice sau exercită o autoritate publică să desemneze un DPO. O astfel de activitatea a DPO acoperă toate operațiunile de prelucrare

efectuate, inclusiv cele care nu sunt legate de îndeplinirea unei sarcini publice sau exercitarea îndatoririlor oficiale (de exemplu, gestionarea unei baze de date a angajaților).

2.1.2. „Activități principale”

Art. 37(1)b) și c) din RGPD se referă la „*activitățile principale ale operatorului sau ale persoanei împuternicite de operator”.* Considerentul 97 specifică faptul că activitățile principale ale operatorului se referă la „*activitățile de bază și nu la prelucrarea datelor cu caracter personal drept activități auxiliare”.* „Activitățile principale” pot fi considerate ca operațiuni cheie necesare pentru îndeplinirea obiectivelor operatorului sau persoanei împuternicite de operator.

Cu toate acestea, „activitățile principale” nu ar trebui interpretate ca excluzând activitățile în care prelucrarea datelor reprezintă o parte indisolubilă a activității operatorului sau persoanei împuternicite de operator. De exemplu, activitatea principală a unui spital este de a oferi asistență medicală. Cu toate acestea, un spital nu poate oferi asistență medicală în condiții de siguranță și în mod eficient fără prelucrarea datelor privind starea de sănătate, cum ar fi dosarele medicale ale pacienților. Prin urmare, prelucrarea acestor date ar trebui să fie considerată a fi una dintre activitățile principale în orice spital și, prin urmare, spitalele trebuie să desemneze un DPO.

Ca un alt exemplu, ***o companie de securitate privată efectuează supravegherea unui număr de centre comerciale private și spații publice. Supravegherea este activitatea de bază a companiei, care, la rândul său, este indisolubil legată de prelucrarea datelor cu caracter personal. Prin urmare, această societate trebuie să desemneze, de asemenea, un DPO***.

Pe de altă parte, toate organizațiile efectuează anumite activități, spre exemplu, plata angajaților lor sau deținerea de activități standard de suport IT. Acestea sunt exemple de funcții de sprijin necesare pentru activitatea de bază sau principală a organizației. Chiar dacă aceste activități sunt necesare sau esențiale, acestea sunt de obicei considerate mai degrabă funcții auxiliare decât activitate principală.

2.1.3. „Pe scară largă”

Art. 37(1)b) și c) impune ca prelucrarea datelor cu caracter personal să fie efectuată pe o scară largă pentru declanșarea activității de desemnare a unui DPO. RGPD nu definește ce anume constituie prelucarea pe scară largă, deși Considerentul 91 oferă unele orientări (potrivit considerentului, ar putea fi incluse, în special, „*operațiunile de prelucrare pe scară largă care au drept obiectiv prelucrarea unui volum considerabill de date cu caracter personal la nivel regional, național sau supranațional și care ar putea afecta un număr mare de persoane vizate și care sunt susceptibile de a genera un risc ridicat*”. Pe de altă parte, considerentul prevede în mod expres că „*prelucrarea datelor cu caracter personal nu ar trebui considerată a fi la scară largă în cazul în care prelucrarea se referă la date cu caracter personal de la pacienți sau clienți ai unui anumit medic sau un alt profesionist în domeniul sănătății sau un avocat*”. Este important să se ia în considerare faptul că, în timp ce considerentul oferă exemple aflate la extremele scalei (prelucrare efectuată de un medic în comparație cu prelucrarea datelor dintr-o țară întreagă sau din Europa), există o zonă mare gri între aceste extreme. În plus, trebuie amintit faptul că acest considerent se referă la evaluările impactului asupra protecției datelor. Acest lucru implică faptul că unele elemente pot fi specifice în acest context și nu se aplică neapărat la desemnarea DPO în același mod).

Într-adevăr, nu este posibil să se ofere un număr exact, fie în ceea ce privește volumul de date prelucrate, fie în ceea ce privește numărul de persoane vizate, care ar fi aplicabil în toate situațiile. Cu toate acestea, acest lucru nu exclude posibilitatea ca, în timp, o anumită practică standard să se poată dezvolta astfel încât să identifice în termeni mai specifici și/sau cantitativ ce anume constituie „*pe scară largă*“ în ceea ce privește anumite tipuri de activități comune de prelucrare. WP29 intenționează de asemenea să contribuie la această dezvoltare, prin intermediul schimbului de exemple de praguri relevante pentru desemnarea unui DPO și publicarea acestora.

În orice caz, WP29 recomandă ca următorii factori să fie luați în considerare atunci când se stabilește dacă prelucrarea este efectuată pe o scară largă:
• numărul persoanelor vizate - ori un număr exact ori un procent din populația relevantă;
• volumul datelor și/sau gama de elemente diferite de date în curs de prelucrare;
• durata sau permanența activității de prelucrare a datelor;
• suprafața geografică a activității de prelucrare.

Exemple de prelucrări pe scară largă includ:
• prelucrarea datelor pacienților în activitatea regulată a unui spital;
• prelucrarea datelor de călătorie a unei persoane fizice ce utilizează sistemul de transport public (spre exemplu urmărire cu ajutorul cardurilor de călătorie);
• prelucrarea în timp real a datelor de geolocalizare a clienților unei rețele internaționale de fast food în scopuri statistice de către o persoană împuternicită de operator specializată în furnizarea serviciilor de acest tip;
• prelucrarea datelor clienților în activitatea regulată a unei companii de asigurări sau a unei bănci;
• prelucrarea datelor personale de către un motor de căutare în scop de publicitate comportamentală;
• prelucrarea datelor (conținut, trafic, localizare) de către furnizorii de telefonie sau servicii de Internet.

Exemple ce nu constituie prelucrări pe scară largă includ:
• prelucrarea datelor pacientului de către un medic individual;
• prelucrarea datelor personale referitoare la condamnările penale și infracțiuni de către un avocat individual.

2.1.4. „Monitorizarea periodică şi sistematică”

Noțiunea de monitorizare periodică și sistematică a persoanelor vizate nu este definită în RGPD, dar conceptul de „*monitorizare a comportamentului persoanelor vizate”* este menționat în Considerentul 24 („p*entru a determina dacă o activitate de prelucrare poate fi considerată ca monitorizare a comportamentului persoanelor vizate, ar trebui să se stabilească dacă persoanele fizice sunt urmărite pe Internet, inclusiv posibila utilizare ulterioară a unor tehnici de prelucrare a datelor cu caracter personal care constau în crearea unui profil al persoanei fizice, în special în scopul de a lua decizii cu privire la aceasta sau de a analiza sau a face previziuni referitoare la preferințele personale, comportamenatel și atitudinile acesteia*”) și include în mod clar toate formele de urmărire și profilarea pe Internet, inclusiv în scop de publicitate comportamentală.

Cu toate acestea, noțiunea de monitorizare nu este restrictionată în mediul online, iar urmărirea online ar trebui să fie considerată doar ca un exemplu de monitorizare a comportamentului persoanelor vizate (prin conținutului său Considerentul 24 se concentrează asupra aplicării extra-teritoriale a RGPD. În plus, există o diferență între sintagma „*monitorizarea comportamentului lor*” (art. 3(2)b) și „*monitorizarea periodică și sistematică a persoanelor vizate*” (art. 37(1)b)) care, prin urmare, ar putea fi considerată ca reprezentând o noțiune diferită).

WP29 interpretează **„periodic”** ca însemnând una sau mai multe din următoarele:
• în curs de desfășurare sau care apare la anumite intervale într-o anumită perioadă;
• recurente sau repetate la perioade fixe;
• constante sau care au loc periodic.

WP29 interpretează **„sistematic”** ca însemnând una sau mai multe din următoarele:
• apărut conform sistemului;
• prearanjat, organizat sau metodic;
• luând loc ca parte a unui plan general de colectare a datelor;
• efectuat ca parte a unei strategii.
Exemple de activități care pot constitui o monitorizare periodică și sistematică a persoanelor vizate:

operarea unei rețele de telecomunicații; furnizarea de servicii de telecomunicații; e-mail de direcționare repetată; activități de marketing bazate pe date; profilare și scoring în scopul evaluării riscurilor (de exemplu, în scopul de credit scoring, stabilirea primelor de asigurare, de prevenire a fraudelor, detectarea spălării banilor); urmărirea locației, spre exemplu, prin aplicații mobile; programe de loialitate; publicitate comportamentală; monitorizarea wellness, fitness și a datelor de sănătate prin intermediul dispozitivelor portabile; televiziune cu circuit închis; dispozitive conectate spre exemplu, contoare inteligente, mașini inteligente, automatizare acasă etc.

2.1.5. Categorii speciale de date și date referitoare la condamnările penale și infracțiuni

Art. 37(1)c) se referă la prelucrarea unor categoriilor speciale de date în conformitate cu art. 9, precum și a datelor cu caracter personal referitoare la condamnările penale și infracțiunie prevăzute la art. 10. Cu toate că prevederea folosește cuvântul „și", nu există un motiv pentru ca cele două criterii să fie aplicate simultan. Prin urmare, textul ar trebui să fie citit astfel încât să spună „sau".

2.2. DPO al persoanei împuternicite de operator

Art. 37 se aplică atât operatorilor (*operatorul este definit în art. 4(7) ca fiind persoană fizică sau juridică care stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal*) cât și persoanelor împuternicite de operator (*persoana împuternicită de operator este definită în art. 4(8) ca fiind persoana fizică sau juridică care prelucrează datele cu caracter personal în numele operatorului*) în ceea ce privește numirea unui DPO. În funcție de cine îndeplinește criteriile de desemnare obligatorie, în unele cazuri numai operatorul sau numai persoana împuternicită de operator, iar în alte cazuri atât operatorul, cât și persoana împuternicită de operator sunt obligați să numească un DPO (care ar trebui mai apoi să colaboreze).

Este important să se sublinieze faptul că, chiar dacă operatorul îndeplinește criteriile de desemnare obligatorie, persoana împuternicită de respectivul operator nu trebuie neapărat să numească un DPO. Totuși, acest lucru poate reprezenta o bună practică.

Exemple:

• O mică afacere de familie activă în distribuția de aparate de uz casnic într-un singur oraș folosește serviciile unei persoanei împuternicite de operator a cărui activitate de bază este de a oferi servicii de asistență și analiză pe pagina web cu activități specifice de publicitate și marketing. Activitățile afacerii de familie și clienții săi nu generează prelucrarea datelor pe „scară largă", având în vedere numărul mic de clienți și activitățile relativ limitate. Cu toate acestea, activitățile persoanei împuternicite de operator, având mulți clienți precum această mică întreprindere, luate împreună, efectuează prelucrări de date pe scară largă. Prin urmare, persoana împuternicită de operator trebuie să desemneze un DPO în temeiul art. 37(1)b). În același timp, afacerea de familie în sine nu are obligația de a desemna un DPO.

• O companie de dimensiune medie ce produce țiglă subcontractează serviciile de sănătate ale unei persoane împuternicite care are un număr mare de clienți. Persoana împuternicită de operator va desemna un DPO potrivit art. 37(1)c), cu condiția ca prelucrarea să fie pe scară largă. Cu toate acestea, producătorul nu are obligația de a numi un DPO.

DPO desemnat de o persoană împuternicită supraveghează, de asemenea, activitățile desfășurate de persoana împuternicită atunci când aceasta acționează în calitate de operator (spre exemplu resurse umane, IT, logistică).

2.3. Desemnarea unui singur DPO pentru mai multe organizații

Art. 37(2) permite unui grup de întreprinderi să numească un DPO unic, cu condiția ca aceasta să fie „*ușor accesibil din fiecare întreprindere".* Noțiunea de accesibilitate se referă la sarcinile DPO ca punct de contact în ceea ce privește persoanele vizate (art. 38(4): „*persoanele vizate pot contacta responsabilul cu protecția datelor cu privire la toate chestiunile legate de prelucrarea datelor lor și la exercitarea drepturilor în temeniul*

prezentului regulament"), autoritatea de supraveghere (art. 39(1)e): „*își asumă rolul de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă menționată la art. 36, precum și, dacă este cazul, consultarea cu privire la orice altă chestiune*"), dar și pe plan intern în cadrul organizației, având în vedere că una dintre sarcinile DPO este „de informare și consiliere a operatorului și persoanei împuternicite de operator, precum și a angajaților care se ocupă de prelucrare cu privire la obligațiile care le revin în temeiul prezentului Regulament" (*art. 39(1)a)*).

Pentru a se asigura că DPO, intern sau extern, este accesibil, este important să se asigure că datele de contact ale acestuia sunt disponibile în conformitate cu cerințele RGPR (*a se vedea Secțiunea 2.6. de mai jos*).

Potrivit art. 37(3), DPO unic poate fi desemnat pentru mai multe autorități sau organisme publice, luând în considerare structura organizatorică și dimeniunea acestora. Sunt aplicabile aceleași considerente cu privire la resurse și comunicare. Având în vedere că DPO este responsabil pentru o varietate de atribuții, operatorul sau persoana împuternicită trebuie să se asigure că un DPO unic, cu ajutorul unei echipe, poate efectua aceste competențe în mod eficient în ciuda faptul că este desemnat pentru mai multe autorități și organisme publice.

2.4. Accesibilitatea și localizarea DPO

Potrivit Secțiunii 4 din RGPD, accesibilitatea DPO trebuie să fie efectivă.
Pentru a se asigura că DPO este accesibil, WP29 recomandă ca DPO să fie localizat pe teritoriul UE, chiar dacă operatorul sau persoana împuternicită de operator nu este stabilită pe teritoriul UE.

2.5. Expertiza și abilitățile DPO

Art. 37(5) prevede că **DPO „*este desemnat pe baza calităților profesionale și, în special, a cunoștințelor de specialitate în dreptul și practicile în domeniul protecției datelor, precum și pe baza capacității de a îndeplini sarcinile prevăzute la art. 39*"**. Considerentul 97 prevede că nivelul necesar al cunoștințelor de specialitate ar trebuie să fie stabilit în funcție de operațiunile de prelucrare a datelor efectuate și de nivelul de protecție impus pentru datele cu caracter personal prelucrate.

• Nivelul de expertiză

Nivelul de expertiză necesar nu este strict definit, dar trebuie să fie proporțional cu sensibilitatea, complexitatea și volumul de date prelucrate de organizație. De exemplu, în situația în care o operațiune de prelucrare a datelor este deosebit de complexă sau în cazul în care este implicat un volum mare de date speciale, DPO poate necesita un nivel mai ridicat de expertiză și suport. Există de asemenea diferențe în funcție de faptul dacă organizația transferă în mod sistematic date cu caracter personal în afara UE sau dacă aceste transferuri sunt ocazionale. Astfel, DPO ar trebui ales cu atenție, ținând seama de aspectele de protecție a datelor care apar în cadrul organizației.

• Calitățile profesionale

Cu toate că art. 37(5) nu precizează calitățile profesionale care ar trebui să fie luate în considerare la desemnarea unui DPO, un element relevant ar fi ca DPO să aibă experiență în legislația și practicile de protecție a datelor la nivel național și european, precum și o înțelegere complexă a RGPD. De asemenea, ar fi util dacă autoritățile de supraveghere ar promova o formă adecvată și regulată pentru DPO.

Este utilă cunoașterea sectorului de afaceri și a organizării operatorului. DPO ar trebui, de asemenea, să înțeleagă operațiunile de prelucrare efectuate, precum și sistemele de informații și necesitățile de securitate și protecție a datelor ale operatorului.

În cazul unei autorități publice sau a unui organism public, DPO trebuie să aibă, de asemenea, cunoștință de regulile și procedurile administrative ale organizației.

• **Capacitatea de a îndeplini sarcinile**
Capacitatea de a-și îndeplini sarcinile ce revin DPO trebuie interpretată ca referindu-se atât la calitățile lor personale și la cunoștințe, cât și la poziția lor în cadrul organizației. Calitățile personale trebuie să includă, spre exemplu, integritatea și etica profesională; principala preocupare a DPO trebuie să fie respectarea RGPD. DPO joacă un rol-cheie în promovarea unei culturi de protecție a datelor în cadrul organizației și ajută la implementarea elementelor esențiale al RGPD, cum ar fi principiile de prelucrare a datelor (*Capitolul II*), drepturile persoanelor vizate (*Capitolul III*), asigurarea protecției datelor începând cu momentul conceperii și în mod implicit (*art. 25*), înregistrarea activităților de prelucrare (*art. 30*), securitatea prelucrării (*art. 32*), precum și notificarea și comunicarea încălcărilor de securitate (*art. 33 și 34*).

• **DPO în baza unui contract de prestări servicii**
Funcția DPO poate fi, de asemenea, exercitată în baza unui contract de prestări servicii încheiat cu o persoană fizică sau o organizație din afara organizației operatorului/persoanei împuternicite de operator. În acest ultim caz, este esențial ca fiecare membru al organizației care exercită funcțiile unui DPO să îndeplinească toate cerințele aplicabile din Secțiunea 4 din RGPD (de exemplu, este esențial ca nicio persoană să se afle în conflict de interese). Este la fel de important ca fiecare membru să fie protejat prin prevederile RGPD (de exemplu, să nu existe o reziliere abuzivă a contractului de prestări servicii pentru activitățile DPO, dar, de asemenea, să nu existe o concediere abuzivă a oricărui membru al organizației care îndeplinește sarcinile DPO). În același timp, calitățile profesionale și punctele forte pot fi combinate astfel încât mai multe persoane care lucrează într-o echipă să poată servi mai eficient clienții lor.

Din motive de claritate juridică și o bună organizare și pentru a preveni conflictele de interes pentru membrii echipei, se recomandă existența unei alocări clare a sarcinilor în cadrul echipei DPO și desemnarea unei singure persoane ca persoană de contact principală și persoană „responsabilă” pentru fiecare client. În general, ar fi util să se specifice aceste puncte în contractul de prestări servicii.

2.6. Publicarea și comunicarea datelor de contact ale DPO

Art. 37(7) din RGPD impune operatorului sau persoanei împuternicite de operator:
• să publice datele de contact ale DPO;
• să comunice datele de contact ale DPO autorităților de supraveghere relevante.

Obiectivul acestor cerințe este acela de a garanta că persoanele vizate (atât în interiorul cât și în exteriorul organizației) și autoritățile de supraveghere pot contacta DPO cu ușurință și în mod direct, fără a fi nevoie să contacteze o altă parte din organizație.

Confidențialitatea este la fel de importantă: de exemplu, angajații pot fi reticenți în a se plânge la DPO în cazul în care confidențialitatea comunicațiilor lor nu este garantată.

DPO este obligat să păstreze secretul sau confidențialitatea în ceea ce privește îndeplinirea sarcinilor sale, în conformitate cu dreptul Uniunii sau cu dreptul intern (*art. 38(5)*).

Datele de contact ale DPO trebuie să includă informații ce permit persoanelor vizate și autoritățile de supraveghere să contacteze DPO printr-o modalitate ușoară (adresă poștală, număr de telefon alocat special și/sau o adresă de email alocată special). Atunci când este cazul, în scopul comunicării cu publicul ar putea fi, de asemenea, furnizate alte mijloace de comunicare, de exemplu o linie telefonică special alocată sau un formular de contact adresat DPO de pe pagina web a organizației.

Art. 37(7) nu impune ca datele de contact publicate să includă numele DPO. Deși acest lucru ar putea fi o bună practică, operatorul sau persoana împuternicită de operator decide dacă acest lucru este necesar sau util în anumite situații (*este de remarcat faptul că art. 33(3)b), care descrie informațiile care trebuie furnizate autorității de supraveghere și persoanelor vizate în cazul unei încălcări a securității datelor cu caracter personal, spre deosebire de art. 37(7), impune în mod expres și comunicarea numelui DPO (și nu numai datele de contact)*).

Cu toate acestea, comunicarea numelui DPO către autoritatea de supraveghere este esențială pentru că DPO reprezintă punctul de contact între organizație și autoritatea de supraveghere (*art. 39(1)e)*).

Ca o chestiune de bună practică, WP29 recomandă, de asemenea, ca o organizație să informeze angajații săi în legătură cu numele și datele de contact ale DPO. De exemplu, numele și datele de contact ale DPO ar putea fi publicate intern pe Intranet-ul organizației, în directorul de telefon intern, și în organigrame.

3. Poziția DPO

3.1. Implicarea DPO în toate aspectele referitoare la protecția datelor cu caracter personal

Art. 38 din RGPD prevede că operatorul și persoana împuternicită de operator se asigură că DPO este „*implicat în mod corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal".*

Este important ca DPO sau echipa sa, să fie implicat, cât mai devreme posibil, în toate aspectele legate de protecția datelor. În ceea ce privește evaluările impactului asupra protecției datelor, RGPD prevede în mod explicit implicarea timpurie a DPO și precizează că operatorul solicită avizul DPO atunci când se efectuează o astfel de evaluare a impactului (*art. 35(2)*). Asigurarea că DPO este informat și consultat de la bun început va facilita respectarea RGPD, va promova o abordare privacy by design și, prin urmare, ar trebui să fie o procedură standard în cadrul guvernării organizației. În plus, este important ca DPO să fie văzut ca un partener de discuție în cadrul organizației și ca acesta să facă parte din grupurile de lucru relevante care se ocupă cu activități de prelucrare a datelor din cadrul organizației.

În consecință, organizația ar trebui să se asigure, de exemplu, că:
• DPO este invitat să participe în mod regulat la ședințele conducerii la nivel înalt și la nivel mediu.
• Prezența DPO este recomandată în cazul în care se iau decizii cu implicații asupra protecției datelor. Toate informațiile relevante trebuie să fie transmise DPO în timp util pentru a permite ca acesta să ofere o consiliere corespunzătoare.
• Avizului DPO trebuie să i se acorde întotdeauna o importanță deosebită. În caz de dezacord, WP29 recomandă, ca bună practică, documentarea motivelor pentru care nu a fost urmat avizul DPO.
• DPO trebuie să fie consultat cu promptitudine imediat ce a avut loc o încălcare a securității datelor sau un alt incident.

Atunci când este cazul, operatorul sau persoana împuternicită de operator ar putea elabora ghiduri privind protecția datelor sau proceduri care stabilesc situații când DPO trebuie să fie consultat.

3.2. Resursele necesare

Art. 38(2) din RGPD impune ca organizația să sprijine DPO prin „*asigurarea resurselor necesare pentru exercitarea sarcinilor sale, precum și accesarea datelor cu caracter personal și a operațiunilor de prelucrare, și pentru menținerea cunoștințelor sale de specialitate".*
Trebuie avute în vedere, în special, următoarele aspecte:
• Spijin activ al funcției DPO din partea managementului superior (cum ar fi la nivelul consiliului de conducere).
• Timp suficient pentru DPO în vederea îndeplinirii atribuțiilor sale. Acest lucru este deosebit de important în cazul în care un DPO intern este numit part-time sau în cazul în care DPO extern realizează protecția datelor în plus față de alte atribuții. În caz contrar, conflictul de priorități poate rezulta în neglijarea sarcinilor DPO. Este extrem de important să existe suficient timp pentru a se dedica sarcinilor DPO. Stabilirea unui procent de timp pentru funcția DPO atunci când aceasta nu este realizată full-time reprezintă o bună practică. De asemenea, o bună practică poate fi și determinarea timpului necesar pentru îndeplinirea

funcției, nivelul corespunzător de prioritate pentru sarcinile DPO, cât și pentru DPO (sau organizație) să elaboreze un plan de lucru.
• Sprijin corespunzător în ceea ce privește resursele financiare, infrastructură (sediu, facilități, echipament) și personal, după caz.
• Comunicare oficială către toți angajații, cu privire la desemnarea DPO, astfel încât să se asigure că este cunoscută existența și funcționarea DPO.
• Accesul necesar la alte servicii precum resurse umane, juridic, IT, securitate etc. astfel încât DPO să beneficieze de un sprijin esențial, reacții și informații din partea altor servicii.
• Pregătire continuă. DPO trebuie să aibă posibilitatea de a rămâne la curent cu evoluțiile în domeniul protecției datelor. Obiectivul ar trebui să fie de a crește în mod constant ***nivelul de expertiză al DPO***, iar acesta ar trebui ***încurajat să participe la cursuri de formare în legătură cu protecția datelor și la alte forme de dezvoltare profesională,*** cum ar fi parciparea la foruri privind protecția vieții private, seminarii etc.
• Având în vedere mărimea și structura organizației, ar putea fi necesară crearea unei echipe DPO (un DPO și personalul său). În astfel de cazuri, structura internă a echipei, sarcinile și responsabilitățile fiecărui membru ar trebui să fie în mod clar elaborate. În mod similar, atunci când funcția de DPO este exercitată de un furnizor extern de servicii, o echipă de persoane fizice care lucrează pentru respectiva entitate poate îndeplini în mod eficient sarcinile unui DPO ca o echipă, sub responsabilitatea unui punct de contact principal desemnat pentru client.

În general, cu cât operațiunile de prelucrare sunt mai complexe sau/și mai sensibile, cu atât mai mult DPO trebuie să beneficieze de resurse. Funcția de protecție a datelor trebuie să fie finanțată în mod eficient și suficient în ceea ce privește prelucrarea datelor efectuată.

3.3. Instrucțiuni și „*îndeplinirea atribuțiilor și sarcinilor în mod independent*”

Art. 38(3) stabilește anumite garanții de bază pentru a se asigura că DPO este în măsură să-și îndeplinească sarcinile cu un grad suficient de autonomie în cadrul organizației. În special, operatorii/persoanele împuternicite de operator trebuie să se asigure că DPO „*nu primește niciun fel de instrucțiuni în ceea ce privește îndeplinirea sarcinilor sale”.* Considerentul 97 adaugă faptul că DPO „*indiferent dacă este sau nu angajat al operatorului, ar trebui să fie în măsură să își îndeplinească atribuțiile și sarcinile în mod independent”.*

Acest lucru înseamnă că, îndeplinirea sarcinilor ce revin în temeiul art. 39, DPO nu trebuie să fie instruit cum să se ocupe de o problemă, de exemplu, ce rezultat ar trebui atins, cum să fie investigată o plângere sau dacă să consulte autoritatea de supraveghere. Mai mult, acesta nu trebuie să fie instruit să adopte o anumită perspectivă a problemei legată de legislația privind protecția datelor, de exemplu, o anumită interpretare a legii.

Cu toate acestea, autonomia DPO nu înseamnă că acesta are competențe de luare a deciziilor care se extind dincolo de sarcinile sale, potrivit art. 39.

Operatorul sau persoana împuternicită de operator este responsabil pentru respectarea legislației privind protecția datelor și trebuie să poată demonstra conformitatea (*art. 5(2)*). Dacă operatorul sau persoana împuternicită de operator ia decizii care sunt incompatibile cu RGPD și cu opinia DPO, DPO ar trebui să aibă posibilitatea de a-și exprima clar opinia sa divergentă la cel mai înalt nivel de management și persoanelor implicate în luarea deciziilor. În acest sens, art. 38(3) prevede că DPO „*răspunde direct în fața celui mai înalt nivel al conducerii operatorului sau persoanei împuternicite de operator”.* O asemenea raportare directă asigură că managementul superior (consiliul de conducere) este conștient de consilierea și recomandările DPO ca parte a misiunii DPO de a informa și a consilia operatorul sau persoana împuternicită de operator. Un alt exemplu de raportare directă este elaborarea unui raport anual al activităților DPO oferit la cel mai înalt nivel de management.

3.4. Demiterea sau sancționarea DPO pentru îndeplinirea sarcinilor sale

Art. 38(3) impune ca DPO să nu „*fie demis sau sancționat de operator sau persoana împuternicită de operator pentru îndeplinirea sarcinilor sale”.*

Această cerință întărește autonomia DPO și ajută la asigurarea că acesta acționează în mod independent și se bucură de o protecție suficientă în îndeplinirea sarcinilor sale în ceea ce privește protecție a datelor.

Sancțiunile sunt interzise potrivit RGPR numai în cazul în care acestea sunt impuse ca urmare a îndeplinirii sarcinilor DPO în calitate de DPO. De exemplu, un DPO poate considera că o anumită prelucrare este de natură să conducă la un risc ridicat și să consilieze operatorul sau persoana împuternicită de operator să efectueze o evaluare a impactului asupra protecției datelor, dar operatorul sau persoana împuternicită de operator nu este de acord cu evaluarea DPO. Într-o astfel de situație, DPO nu poate fi demis pentru oferirea acestui sfat.

Sancțiunile pot lua o varietate de forme și pot fi directe sau indirecte. Acestea ar putea consta, de exemplu, în lipsa sau întârzierea promovării; prevenirea de la avansarea în carieră; negare de beneficii pe care alți angajați le primesc. Nu este necesar ca aceste sancțiuni să fie realizate efectiv, o simplă amenințare este suficientă atât timp cât acestea sunt folosite pentru a sancționa DPO pe motive legate de activitățile sale de DPO.
Ca o regulă normală de management și cum ar fi cazul pentru orice alt angajat sau contractant în conformitate cu, și sub rezerva, dreptului intern în domeniul muncii sau contractelor și cel penal aplicabil, un DPO ar putea fi totuși demis, în mod legal, din alte motive decât cele privind îndeplinirea sarcinilor sale în calitate de DPO (de exemplu, în caz de furt, hărțuire fizică, psihologică sau sexuală sau abatere gravă similară).

În acest context, trebuie remarcat faptul că RGPD nu specifică modul în care și când un DPO poate fi demis sau înlocuit de către o altă persoană. Cu toate acestea, cu cât contractul unui DPO este mai stabil și există mai multe garanții împotriva concedierii abuzive, cu atât mai probabil DPO va fi în măsură să acționeze în mod independent. Prin urmare, WP29 ar saluta eforturile organizațiilor în acest sens.

3.5. Conflict de interese

Art. 38(6) permite DPO „*să îndeplinească și alte sarcini și atribuții".* Cu toate acestea, este nevoie ca organizația să se asigure că „*niciuna dintre aceste sarcini și atribuții nu generează un conflict".*

Absența conflictului de interese este strâns legată de obligația de a acționa în mod independent. Cu toate că îi este permis să aibă și alte funcții, acestuia îi pot fi încredințate alte sarcini și atribuții cu condiția ca acestea să nu dea naștere unor conflicte de interese. Acest lucru presupune, în special, faptul că DPO nu poate deține o poziție în cadrul organizației care ar conduce la posibilitatea ca DPO să stabilească scopurile și mijloacele de prelucrare a datelor cu caracter personal. Acest lucru trebuie luat în considerare de la caz la caz, ținându-se cont de structura organizațională specifică fiecărei organizații.

Ca regulă generală, funcții din cadrul organizației cu care poate intra în conflict pot include funcții de conducere (cum ar fi director executiv, director operațional, director financiar, șeful serviciului medical, șeful departamentului de marketing, șef departamentului de resurse umane sau șeful departamentului IT), dar, în același timp, și alte funcții inferioare dacă acestea conduc la posibilitatea de a stabili scopurile și mijloacelor de prelucrare. În plus, un conflict de interese poate apărea, de asemenea, de exemplu, în situația în care un DPO extern este rugat să reprezinte oporatorul sau persoana împuternicită de operator în instanță, în cazurile care implică probleme de protecție a datelor.

În funcție de activitățile, dimensiunea și structura organizației, o bună practică pentru operatori și persoanele împuternicite de operatori ar putea fi:
• să identifice funcțiile ce ar fi incompatibile cu funcția de DPO;
• să elaboreze norme interne în acest sens pentru a evita conflictele de interese;
• să includă o explicație mai generală cu privire la conflictele de interese;
• să declare că DPO-ul lor nu are niciun conflict de interese în ceea ce privește funcția sa ca și DPO, ca și modalitate de creștere a gradului de conștientizare a acestei cerințe;

• să includă garanții în normele interne ale organizației și să se asigure că anunțul de post vacant pentru funcția de DPO sau contractul de prestări servicii este suficient de precis și detaliat pentru a evita conflictul de interese. În acest context, trebuie avut în vedere faptul că respectivele conflicte de interese pot lua diverse forme în funcție de faptul dacă DPO este recrutat intern sau extern.

4. Sarcinile DPO

4.1. Monitorizarea respectării RGPD

Art. 39(1)b) încredințează DPO, printre alte sarcini, obligația de a monitoriza respectarea RGPD. Considerentul 97 precizează în continuare că DPO „*ar trebui să acorde asistență operatorului sau persoanei împuternicite de operator pentru monitorizarea conformității cu prezentul Regulament*".

Ca parte a acestor sarcini de monitorizare a conformității, DPO poate, în special:
• să colecteze informații pentru a indentifica operațiunile de prelucrare;
• să analizeze și să verifice conformitatea operațiunilor de prelucrare;
• să informeze, să consilieze și să emită recomandări operatorului sau persoanei împuternicite de operator.

Monitorizarea conformității nu înseamnă că DPO este personal responsabil în situația în care există un caz de nerespectare. RGPD spune clar că operatorul, și nu DPO, are obligația de a „*pune în aplicare măsuri tehnice și orgnizatorice adecvate pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul Regulament"* (*art. 24(1)*). Respectarea normelor de protecție a datelor este o responsabilitate corporativă a operatorului și nu a DPO.

4.2. Rolul DPO în evaluarea impactului operațiunilor de prelucrare

Potrivit art. 35(1), operatorul și nu DPO efectuează, atunci când este necesar, o evaluare a impactului operațiunilor de prelucrare („DPIA"). Cu toate acestea, DPO poate avea un rol foarte important și util în asistarea operatorului. Potrivit principiului protecția datelor începând cu momentul conceperii, art.35(2) prevede în mod expres ca operatorul „*să solicite avizul"* DPO la realizarea DPIA. La rândul său, art. 39(1)c) prevede ca și sarcină pentru DPO „*să ofere consiliere la cerere în ceea ce privește DPIA și să monitorizese funcționarea acesteia, în conformitate cu art. 35".*

WP29 recomandă ca operatorul să solicite avizul DPO în legătură cu următoarele aspecte, printre care (art 39(1) precizează sarcinile DPO și indică faptul că DPO trebuie să aibă „*cel puțin*" următoarele atribuții. Prin urmare, nimic nu împiedică operatorul să atribuie DPO alte sarcini decât cele menționate în mod expres în art. 39(1) sau să specifice respectivele atribuții într-un mod detaliat):
• dacă să efectueze sau nu DPIA;
• ce metodologie să fie folosită la efectuarea DPIA;
• dacă să efectueze DPIA intern sau să externalizeze;
• ce garanții (inclusiv măsuri tehnice și organizaționale) să pună în aplicare pentru reducerea oricăror riscuri la adresa drepturilor și intereselor persoanelor vizate;
• dacă DPIA a fost sau nu efectuată corect și dacă respectivele concluzii (dacă să continue sau nu prelucrarea și ce garanții să pună în aplicare) respectă RGPD.

În situația în care operatorul nu este de acord cu opinia DPO, documentația DPIA ar trebui să justifice în mod specific în scris motivul pentru care nu a fost urmat avizul (art. 24(1) prevede că „*ținând seama de natura, domeniul de aplicare, contextul și sopurile prelucrării, precum și de riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta și a* ***fi în măsură să demonstreze*** *că prelucrarea se efectuează în conformitate cu prezentul Regulament. Respectivele măsuri se revizuiesc și de actualizează dacă este necesar*").

WP29 recomandă în continuare ca operatorul să sublinieze în mod clar, de exemplu în contractul cu DPO, dar și în informațiile furnizate angajaților, conducerii (și celorlalți acționari, după caz), sarcinile concrete ale DPO și obiectivul acestora, în special în ceea ce privește efectuarea DPIA.

4.3. Cooperarea cu autoritatea de supraveghere și asumarea rolului de punct de contact

Potrivit art. 39(1)d) și c), DPO ar trebui „*să coopereze cu autoritatea de supraveghere"* și „*să-și asume rolul de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă menționalăla art. 36, precum și, dacă este cazul, consultarea cu privire la orice altă chestiune".*

Aceste sarcini se referă la rolul de „persoană care facilitează" al DPO menționat în cuprinsul intruducerii acestui Ghid. DPO acționează ca punct de contract pentru a facilita accesul autorității de supraveghere la documente și informații pentru îndeplinirea atribuțiilor menționate la art. 57, precum și pentru exercitarea competențelor de investigarea, corectare, autorizare și consultare menționate la art. 58. Așa cum a fost deja menționat, DPO are obligația de a respecta secretul sau confidențialitatea în ceea ce privește îndeplinirea sarcinilor sale, în conformitate cu dreptul Uniuniii sau cu dreptul intern (*art. 38(5)*). Cu toate acestea, obligația secretului/confidențialității nu înterzice DPO să contacteze și să solicite consiliere din partea autorității de supraveghere. Art. 39(1)e) prevede că DPO poate consulta autoritatea de supraveghere cu privire la orice altă chestiune, după caz.

4.4. Abordare bazată pe risc

Art. 39(2) impune ca DPO „*să țină seamă în mod corespunzător de riscul asociat operațiunilor de prelucrare, luând în considerare natura, domeniul de aplicare, contextul și scopurile prelucrării".*

Acest articol reamintește de un principiu general și de bun simț care poate fi relevant pentru mai multe aspecte din activitatea zilnică a DPO. În esență, este nevoie ca DPO să prioritizeze activitățile sale și să-și concentreze eforturile asupra problemelor care prezintă riscuri mai mari pentru protecția datelor. Acest lucru nu înseamnă că ar trebui să-și neglijeze monitorizarea conformității operațiunilor de prelucrare a datelor care au un nivel relativ mai scăzut de risc, ci indică faptul că ar trebui să se concentreze, în primul rând, pe zonele cu risc mai mare.

Această abordare selectivă și pragmatică ar trebui să ajute DPO în consilierea operatorului cu privire la metodologia folosită la efectuarea DPIA, ce zone ar trebui să facă obiectul unui audit intern sau extern privind protecția datelor, ce activități interne de pregătire să fie oferite personalului sau managementului responsabil cu activitățile de prelucrare și ce operațiuni de prelucrare necesită mai mult timp și resurse.

4.5. Rolul DPO în păstrarea evidenței

Potrivit art. 30(1) și (2) operatorul sau persoana împuternicită de operator, și nu DPO, are obligația de a „*păstra o evidență a operațiunilor de prelucrare desfășurate sub responsabilitatea sa"* sau de a „*păstra o evidență a tuturor categoriilor de operațiuni de prelucrare efectuate în numele operatorului".*

În practică, DPO crează adesea inventare și deține un registru al operațiunilor de prelucrare pe baza informațiilor furnizate de diferitele departamente din cadrul organizației responsabile cu prelucrarea datelor cu caracter personal. Această practică a fost stabilită în conformitate cu diverse legislații naționale curente și în conformitate cu normele de protecție a datelor aplicabile instituțiilor și organismelor UE (*art. 24(1)d), Regulamentul (CE) 45/2001*).

Art. 39(1) prevede o listă minimă a sarcinilor DPO. Prin urmare, nimic nu împiedică operatorul sau persoana împuternicită de operator să atribuie DPO sarcina de a păstra o evidență a operațiunilor de prelucrare în numele operatorului sau persoanei împuternicite de operator.

3. REGULAMENTUL Nr. 679 din 27 aprilie 2016
privind protecţia persoanelor fizice în
ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera
circulaţie a acestor date şi de abrogare a Directivei 95/46/CE
(Regulamentul general privind protecţia datelor - RGPD)
- EXTRAS -

Preliminarii necesare

(1) Protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal este un drept fundamental. Articolul 8 alineatul (1) din **Carta drepturilor fundamentale a Uniunii Europene** ("carta") şi articolul 16 alineatul (1) din **Tratatul privind funcţionarea Uniunii Europene** (TFUE) prevăd dreptul oricărei persoane la protecţia datelor cu caracter personal care o privesc.

(2) Principiile şi normele referitoare la protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor lor cu caracter personal ar trebui, indiferent de cetăţenia sau de locul de reşedinţă al persoanelor fizice, să respecte drepturile şi libertăţile fundamentale ale acestora, în special dreptul la protecţia datelor cu caracter personal. Prezentul regulament urmăreşte să contribuie la realizarea unui spaţiu de libertate, securitate şi justiţie şi a unei uniuni economice, la progresul economic şi social, la consolidarea şi convergenţa economiilor în cadrul pieţei interne şi la bunăstarea persoanelor fizice.

.....

(4) Prelucrarea datelor cu caracter personal ar trebui să fie în serviciul cetăţenilor. Dreptul la protecţia datelor cu caracter personal nu este un drept absolut; acesta trebuie luat în considerare în raport cu funcţia pe care o îndeplineşte în societate şi echilibrat cu alte drepturi fundamentale, în conformitate cu principiul proporţionalităţii. Prezentul regulament respectă toate drepturile fundamentale şi libertăţile şi principiile recunoscute în **cartă** astfel cum sunt consacrate în tratate, în special respectarea vieţii private şi de familie, a reşedinţei şi a comunicaţiilor, a protecţiei datelor cu caracter personal, a libertăţii de gândire, de conştiinţă şi de religie, a libertăţii de exprimare şi de informare, a libertăţii de a desfăşura o activitate comercială, dreptul la o cale de atac eficientă şi la un proces echitabil, precum şi diversitatea culturală, religioasă şi lingvistică.

……..

(6) Evoluţiile tehnologice rapide şi globalizarea au generat noi provocări pentru protecţia datelor cu caracter personal. Amploarea colectării şi a schimbului de date cu caracter personal a crescut în mod semnificativ. Tehnologia permite atât societăţilor private, cât şi autorităţilor publice să utilizeze date cu caracter personal la un nivel fără precedent în cadrul activităţilor lor. Din ce în ce mai mult, persoanele fizice fac publice la nivel mondial informaţii cu caracter personal. Tehnologia a transformat deopotrivă economia şi viaţa socială şi ar trebui să faciliteze în continuare libera circulaţie a datelor cu caracter personal în cadrul Uniunii şi transferul către ţări terţe şi organizaţii internaţionale, asigurând, totodată, un nivel ridicat de protecţie a datelor cu caracter personal.

(7) Aceste evoluţii impun un cadru solid şi mai coerent în materie de protecţie a datelor în Uniune, însoţit de o aplicare riguroasă a normelor, luând în considerare importanţa creării unui climat de încredere care va permite economiei digitale să se dezvolte pe piaţa internă. Persoanele fizice ar trebui să aibă control asupra propriilor date cu caracter personal, iar securitatea juridică şi practică pentru persoane fizice, operatori economici şi autorităţi publice ar trebui să fie consolidată.

(8) În cazul în care prezentul regulament prevede specificări sau restricţionări ale normelor sale de către dreptul intern, statele membre pot, în măsura în care acest lucru este necesar pentru coerenţă şi pentru a asigura înţelegerea dispoziţiilor naţionale de către persoanele cărora li se aplică acestea, să încorporeze elemente din prezentul regulament în dreptul lor intern.

(9) Obiectivele şi principiile Directivei **95/46/CE** rămân solide, dar aceasta nu a prevenit fragmentarea modului în care protecţia datelor este pusă în aplicare în Uniune, insecuritatea

juridică sau percepţia publică larg răspândită conform căreia există riscuri semnificative pentru protecţia persoanelor fizice, în special în legătură cu activitatea online. Diferenţele dintre nivelurile de protecţie a drepturilor şi libertăţilor persoanelor fizice, în special a dreptului la protecţia datelor cu caracter personal, în ceea ce priveşte prelucrarea datelor cu caracter personal din statele membre pot împiedica libera circulaţie a datelor cu caracter personal în întreaga Uniune. Aceste diferenţe pot constitui, prin urmare, un obstacol în desfăşurarea de activităţi economice la nivelul Uniunii, pot denatura concurenţa şi pot împiedica autorităţile să îndeplinească responsabilităţile care le revin în temeiul dreptului Uniunii. Această diferenţă între nivelurile de protecţie este cauzată de existenţa unor deosebiri în ceea ce priveşte transpunerea şi aplicarea Directivei **95/46/CE**.

(10) Pentru a se asigura un nivel consecvent şi ridicat de protecţie a persoanelor fizice şi pentru a se îndepărta obstacolele din calea circulaţiei datelor cu caracter personal în cadrul Uniunii, nivelul protecţiei drepturilor şi libertăţilor persoanelor fizice în ceea ce priveşte prelucrarea unor astfel de date ar trebui să fie echivalent în toate statele membre. Aplicarea consecventă şi omogenă a normelor în materie de protecţie a drepturilor şi libertăţilor fundamentale ale persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal ar trebui să fie asigurată în întreaga Uniune. În ceea ce priveşte prelucrarea datelor cu caracter personal în vederea respectării unei obligaţii legale, a îndeplinirii unei sarcini care serveşte unui interes public sau care rezultă din exercitarea autorităţii publice cu care este învestit operatorul, statelor membre ar trebui să li se permită să menţină sau să introducă dispoziţii de drept intern care să clarifice într-o mai mare măsură aplicarea normelor prezentului regulament. În coroborare cu legislaţia generală şi orizontală privind protecţia datelor, prin care este pusă în aplicare Directiva **95/46/CE**, statele membre au mai multe legi sectoriale specifice în domenii care necesită dispoziţii mai precise. Prezentul regulament oferă, de asemenea, statelor membre o marjă de manevră în specificarea normelor sale, inclusiv în ceea ce priveşte prelucrarea categoriilor speciale de date cu caracter personal ("date sensibile"). În acest sens, prezentul regulament nu exclude dreptul statelor membre care stabileşte circumstanţele aferente unor situaţii de prelucrare specifice, inclusiv stabilirea cu o mai mare precizie a condiţiilor în care prelucrarea datelor cu caracter personal este legală.

(11) Protecţia efectivă a datelor cu caracter personal în întreaga Uniune necesită nu numai consolidarea şi stabilirea în detaliu a drepturilor persoanelor vizate şi a obligaţiilor celor care prelucrează şi decid prelucrarea datelor cu caracter personal, ci şi competenţe echivalente pentru monitorizarea şi asigurarea conformităţii cu normele de protecţie a datelor cu caracter personal şi sancţiuni echivalente pentru infracţiuni în statele membre.

.....

(13) În vederea asigurării unui nivel uniform de protecţie pentru persoanele fizice în întreaga Uniune şi a preîntâmpinării discrepanţelor care împiedică libera circulaţie a datelor în cadrul pieţei interne, este necesar un regulament în scopul de a furniza securitate juridică şi transparenţă pentru operatorii economici, inclusiv microîntreprinderi şi întreprinderi mici şi mijlocii, precum şi de a oferi persoanelor fizice în toate statele membre acelaşi nivel de drepturi, obligaţii şi responsabilităţi opozabile din punct de vedere juridic pentru operatori şi persoanele împuternicite de aceştia, pentru a se asigura o monitorizare coerentă a prelucrării datelor cu caracter personal, sancţiuni echivalente în toate statele membre, precum şi cooperarea eficace a autorităţilor de supraveghere ale diferitelor state membre. Pentru buna funcţionare a pieţei interne este necesar ca libera circulaţie a datelor cu caracter personal în cadrul Uniunii să nu fie restricţionată sau interzisă din motive legate de protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal. Pentru a se lua în considerare situaţia specifică a microîntreprinderilor şi a întreprinderilor mici şi mijlocii, prezentul regulament include o derogare pentru organizaţiile cu mai puţin de 250 de angajaţi în ceea ce priveşte păstrarea evidenţelor. În plus, instituţiile şi organele Uniunii şi statele membre şi autorităţile lor de supraveghere sunt încurajate să ia în considerare necesităţile specifice ale microîntreprinderilor şi ale întreprinderilor mici şi mijlocii în aplicarea prezentului

regulament. Noţiunea de microîntreprinderi şi de întreprinderi mici şi mijlocii ar trebui să se bazeze pe articolul 2 din anexa la Recomandarea 2003/361/CE a Comisiei ([1]).

([1])Recomandarea 2003/361/CE a Comisiei din 6 mai 2003 privind definirea microîntreprinderilor şi a întreprinderilor mici şi mijlocii [C(2003) 1422] (JO L 124, 20.5.2003, p. 36). *„Categoria microîntreprinderilor şi a întreprinderilor mici şi mijlocii (IMM-uri) este alcătuită din întreprinderi care angajează mai puţin de 250 de persoane şi care au o cifră de afaceri anuală care nu depăşeşte 50 de milioane de euro şi/sau un bilanţ contabil anual care nu depăşeşte 43 de milioane de euro.”*

Fragment din articolul 2 din anexa la Recomandarea 2003/361/CE

(14) Protecţia conferită de prezentul regulament ar trebui să vizeze persoanele fizice, indiferent de cetăţenia sau de locul de reşedinţă al acestora, în ceea ce priveşte prelucrarea datelor cu caracter personal ale acestora. Prezentul regulament nu se aplică prelucrării datelor cu caracter personal care privesc persoane juridice şi, în special, întreprinderi cu personalitate juridică, inclusiv numele şi tipul de persoană juridică şi datele de contact ale persoanei juridice.

(15) Pentru a preveni apariţia unui risc major de eludare, protecţia persoanelor fizice ar trebui să fie neutră din punct de vedere tehnologic şi să nu depindă de tehnologiile utilizate. Protecţia persoanelor fizice ar trebui să se aplice prelucrării datelor cu caracter personal prin mijloace automatizate, precum şi prelucrării manuale, în cazul în care datele cu caracter personal sunt cuprinse sau destinate să fie cuprinse într-un sistem de evidenţă. Dosarele sau seturile de dosare, precum şi copertele acestora, care nu sunt structurate în conformitate cu criterii specifice nu ar trebui să intre în domeniul de aplicare al prezentului regulament.

(16) Prezentul regulament nu se aplică chestiunilor de protecţie a drepturilor şi libertăţilor fundamentale sau la libera circulaţie a datelor cu caracter personal referitoare la activităţi care nu intră în domeniul de aplicare al dreptului Uniunii, de exemplu activităţile privind securitatea naţională. Prezentul regulament nu se aplică prelucrării datelor cu caracter personal de către statele membre atunci când acestea desfăşoară activităţi legate de politica externă şi de securitatea comună a Uniunii.

.....

(18) Prezentul regulament nu se aplică prelucrării datelor cu caracter personal de către o persoană fizică în cadrul unei activităţi exclusiv personale sau domestice şi care, prin urmare, nu are legătură cu o activitate profesională sau comercială. Activităţile personale sau domestice ar putea include corespondenţa şi repertoriul de adrese sau activităţile din cadrul reţelelor sociale şi activităţile online desfăşurate în contextul respectivelor activităţi. Cu toate acestea, prezentul regulament se aplică operatorilor sau persoanelor împuternicite de operatori care furnizează mijloacele de prelucrare a datelor cu caracter personal pentru astfel de activităţi personale sau domestice.

.....

(22) Orice prelucrare a datelor cu caracter personal în cadrul activităţilor unui sediu al unui operator sau al unei persoane împuternicite de operator din Uniune ar trebui efectuată în conformitate cu prezentul regulament, indiferent dacă procesul de prelucrare în sine are loc sau nu în cadrul Uniunii. Sediul implică exercitarea efectivă şi reală a unei activităţi în cadrul unor înţelegeri stabile. .....

.....

(26) **Principiile protecţiei datelor** ar trebui să se aplice oricărei informaţii referitoare la o persoană fizică identificată sau identificabilă. Datele cu caracter personal care au fost supuse pseudonimizării, care ar putea fi atribuite unei persoane fizice prin utilizarea de informaţii suplimentare, ar trebui considerate informaţii referitoare la o persoană fizică identificabilă. Pentru a se determina dacă o persoană fizică este identificabilă, ar trebui să se ia în considerare toate mijloacele, cum ar fi individualizarea, pe care este probabil, în mod rezonabil, să le utilizeze fie operatorul, fie o altă persoană, în scopul identificării, în mod direct sau indirect, a persoanei fizice respective. Pentru a se determina dacă este probabil, în mod rezonabil, să fie utilizate mijloace pentru identificarea persoanei fizice, ar trebui luaţi în considerare toţi factorii obiectivi, precum costurile şi intervalul de timp necesare pentru

identificare, ţinându-se seama atât de tehnologia disponibilă la momentul prelucrării, cât şi de dezvoltarea tehnologică. Principiile protecţiei datelor ar trebui, prin urmare, să nu se aplice informaţiilor anonime, adică informaţiilor care nu sunt legate de o persoană fizică identificată sau identificabilă sau datelor cu caracter personal care sunt anonimizate astfel încât persoana vizată nu este sau nu mai este identificabilă. Prin urmare, prezentul regulament nu se aplică prelucrării unor astfel de informaţii anonime, inclusiv în cazul în care acestea sunt utilizate în scopuri statistice sau de cercetare.

(27) ***Prezentul regulament nu se aplică datelor cu caracter personal referitoare la persoane decedate***. Statele membre pot să prevadă norme privind prelucrarea datelor cu caracter personal referitoare la persoane decedate.

.....

(32) **Consimţământul** ar trebui acordat printr-o acţiune neechivocă care să constituie o manifestare liber exprimată, specifică, în cunoştinţă de cauză şi clară a acordului persoanei vizate pentru prelucrarea datelor sale cu caracter personal, ca de exemplu o declaraţie făcută în scris, inclusiv în format electronic, sau verbal. Acesta ar putea include bifarea unei căsuţe atunci când persoana vizitează un site, alegerea parametrilor tehnici pentru serviciile societăţii informaţionale sau orice altă declaraţie sau acţiune care indică în mod clar în acest context acceptarea de către persoana vizată a prelucrării propuse a datelor sale cu caracter personal. Prin urmare, absenţa unui răspuns, căsuţele bifate în prealabil sau absenţa unei acţiuni nu ar trebui să constituie un consimţământ. Consimţământul ar trebui să vizeze toate activităţile de prelucrare efectuate în acelaşi scop sau în aceleaşi scopuri. Dacă prelucrarea datelor se face în mai multe scopuri, consimţământul ar trebui dat pentru toate scopurile prelucrării. În cazul în care consimţământul persoanei vizate trebuie acordat în urma unei cereri transmise pe cale electronică, cererea respectivă trebuie să fie clară şi concisă şi să nu perturbe în mod inutil utilizarea serviciului pentru care se acordă consimţământul.

.....

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

(40) Pentru ca prelucrarea datelor cu caracter personal să fie legală, aceasta ar trebui efectuată pe baza consimţământului persoanei vizate sau în temeiul unui alt motiv legitim, prevăzut de lege, fie în prezentul regulament, fie în alt act din dreptul Uniunii sau din dreptul intern, după cum se prevede în prezentul regulament, inclusiv necesitatea respectării obligaţiilor legale la care este supus operatorul sau necesitatea de a executa un contract la care persoana vizată este parte sau pentru a parcurge etapele premergătoare încheierii unui contract, la solicitarea persoanei vizate.
.....

(42) În cazul în care prelucrarea se bazează pe consimţământul persoanei vizate, operatorul ar trebui să fie în măsură să demonstreze faptul că persoana vizată şi-a dat consimţământul pentru operaţiunea de prelucrare. În special, în contextul unei declaraţii scrise cu privire la un alt aspect, garanţiile ar trebui să asigure că persoana vizată este conştientă de faptul că şi-a dat consimţământul şi în ce măsură a făcut acest lucru. În conformitate cu Directiva **93/13/CEE** a Consiliului ([1]), ar trebui furnizată o declaraţie de consimţământ formulată în prealabil de către operator, într-o formă inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu, iar această declaraţie nu ar trebui să conţină clauze abuzive. Pentru ca acordarea consimţământului să fie în cunoştinţă de cauză, persoana vizată ar trebui să fie la curent cel puţin cu identitatea operatorului şi cu scopurile prelucrării pentru care sunt destinate datele cu caracter personal. Consimţământul nu ar trebui considerat ca fiind acordat în mod liber dacă persoana vizată nu dispune cu adevărat de libertatea de alegere sau nu este în măsură să refuze sau să îşi retragă consimţământul fără a fi prejudiciată.
([1])Directiva **93/13/CEE** a Consiliului din 5 aprilie 1993 privind clauzele abuzive în contractele încheiate cu consumatorii (JO L 95, 21.4.1993, p. 29).
(43) Pentru a garanta faptul că a fost acordat în mod liber, consimţământul nu ar trebui să constituie un temei juridic valabil pentru prelucrarea datelor cu caracter personal în cazul particular în care există un dezechilibru evident între persoana vizată şi operator, în special în cazul în care operatorul este o autoritate publică, iar acest lucru face improbabilă acordarea consimţământului în mod liber în toate circumstanţele aferente respectivei situaţii particulare. ***Consimţământul este considerat a nu fi acordat în mod liber*** în cazul în care aceasta nu permite să se acorde consimţământul separat pentru diferitele operaţiuni de prelucrare a datelor cu caracter personal, deşi acest lucru este adecvat în cazul particular, sau ***dacă executarea unui contract, inclusiv furnizarea unui serviciu, este condiţionată de consimţământ, în ciuda faptului că consimţământul în cauză nu este necesar pentru executarea contractului***.
(44) ***Prelucrarea ar trebui să fie considerată legală în cazul în care este necesară în cadrul unui contract sau în vederea încheierii unui contract***.
(45) În cazul în care prelucrarea este efectuată în conformitate cu o obligaţie legală a operatorului sau în cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care serveşte unui interes public sau care face parte din exercitarea autorităţii publice, prelucrarea ar trebui să aibă un temei în dreptul Uniunii sau în dreptul intern. Prezentul regulament nu impune existenţa unei legi specifice pentru fiecare prelucrare în parte. Poate fi suficientă o singură lege drept temei pentru mai multe operaţiuni de prelucrare efectuate în conformitate cu o obligaţie legală a operatorului sau în cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care serveşte unui interes public sau care face parte din exercitarea autorităţii publice. De asemenea, ar trebui ca scopul prelucrării să fie stabilit în dreptul Uniunii sau în dreptul intern. Mai mult decât atât, dreptul respectiv ar putea să specifice condiţiile generale ale prezentului regulament care reglementează legalitatea prelucrării datelor cu caracter personal, să determine specificaţiile pentru stabilirea operatorului, a tipului de date cu caracter personal care fac obiectul prelucrării, a persoanelor vizate, a entităţilor cărora le pot fi divulgate datele cu caracter personal, a limitărilor în funcţie de scop, a perioadei de stocare şi a altor măsuri pentru a garanta o prelucrare legală şi echitabilă. De asemenea, ar trebui să se stabilească în dreptul Uniunii sau în dreptul intern dacă operatorul care îndeplineşte o sarcină care serveşte unui interes public sau care face

parte din exercitarea autorităţii publice ar trebui să fie o autoritate publică sau o altă persoană fizică sau juridică guvernată de dreptul public sau, atunci când motive de interes public justifică acest lucru, inclusiv în scopuri medicale, precum sănătatea publică şi protecţia socială, precum şi gestionarea serviciilor de asistenţă medicală, de dreptul privat, cum ar fi o asociaţie profesională.

(46) Prelucrarea datelor cu caracter personal ar trebui, de asemenea, să fie considerată legală în cazul în care este necesară în scopul asigurării protecţiei unui interes care este esenţial pentru viaţa persoanei vizate sau pentru viaţa unei alte persoane fizice. Prelucrarea datelor cu caracter personal care are drept temei interesele vitale ale unei alte persoane fizice ar trebui efectuată numai în cazul în care prelucrarea nu se poate baza în mod evident pe un alt temei juridic. .....

(47) Interesele legitime ale unui operator, inclusiv cele ale unui operator căruia îi pot fi divulgate datele cu caracter personal sau ale unei terţe părţi, pot constitui un temei juridic pentru prelucrare, cu condiţia să nu prevaleze interesele sau drepturile şi libertăţile fundamentale ale persoanei vizate, luând în considerare aşteptările rezonabile ale persoanelor vizate bazate pe relaţia acestora cu operatorul. Acest interes legitim ar putea exista, de exemplu, atunci când există o relaţie relevantă şi adecvată între persoana vizată şi operator, cum ar fi cazul în care persoana vizată este un client al operatorului sau se află în serviciul acestuia. În orice caz, existenţa unui interes legitim ar necesita o evaluare atentă, care să stabilească inclusiv dacă o persoană vizată poate preconiza în mod rezonabil, în momentul şi în contextul colectării datelor cu caracter personal, posibilitatea prelucrării în acest scop. Interesele şi drepturile fundamentale ale persoanei vizate ar putea prevala în special în raport cu interesul operatorului de date atunci când datele cu caracter personal sunt prelucrate în circumstanţe în care persoanele vizate nu preconizează în mod rezonabil o prelucrare ulterioară. Întrucât legiuitorul trebuie să furnizeze temeiul juridic pentru prelucrarea datelor cu caracter personal de către autorităţile publice, temeiul juridic respectiv nu ar trebui să se aplice prelucrării de către autorităţile publice în îndeplinirea sarcinilor care le revin. Prelucrarea de date cu caracter personal strict necesară în scopul prevenirii fraudelor constituie, de asemenea, un interes legitim al operatorului de date în cauză. Prelucrarea de date cu caracter personal care are drept scop marketingul direct poate fi considerată ca fiind desfăşurată pentru un interes legitim.

.....

(50) Prelucrarea datelor cu caracter personal în alte scopuri decât scopurile pentru care datele cu caracter personal au fost iniţial colectate ar trebui să fie permisă doar atunci când prelucrarea este compatibilă cu scopurile respective pentru care datele cu caracter personal au fost iniţial colectate. În acest caz nu este necesar un temei juridic separat de cel pe baza căruia a fost permisă colectarea datelor cu caracter personal. ..... Pentru a stabili dacă scopul prelucrării ulterioare este compatibil cu scopul pentru care au fost colectate iniţial datele cu caracter personal, operatorul, după ce a îndeplinit toate cerinţele privind legalitatea prelucrării iniţiale, ar trebui să ţină seama, printre altele, de orice legătură între respectivele scopuri şi scopurile prelucrării ulterioare preconizate, de contextul în care au fost colectate datele cu caracter personal, în special de aşteptările rezonabile ale persoanelor vizate, bazate pe relaţia lor cu operatorul, în ceea ce priveşte utilizarea ulterioară a datelor, de natura datelor cu caracter personal, de consecinţele prelucrării ulterioare preconizate asupra persoanelor vizate, precum şi de existenţa garanţiilor corespunzătoare atât în cadrul operaţiunilor de prelucrare iniţiale, cât şi în cadrul operaţiunilor de prelucrare ulterioare preconizate. În cazul în care persoana vizată şi-a dat consimţământul sau prelucrarea se bazează pe dreptul Uniunii sau pe dreptul intern, care constituie o măsură necesară şi proporţională într-o societate democratică pentru a proteja, în special, obiective importante de interes public general, operatorul ar trebui să aibă posibilitatea de a prelucra în continuare datele cu caracter personal, indiferent de compatibilitatea scopurilor. În orice caz, aplicarea principiilor stabilite de prezentul regulament şi, în special, informarea persoanei vizate cu privire la aceste alte scopuri şi la drepturile sale, inclusiv dreptul la opoziţie, ar trebui să fie garantate. Indicarea unor posibile infracţiuni sau ameninţări la adresa siguranţei publice de

către operator şi transmiterea către o autoritate competentă a datelor cu caracter personal relevante în cazuri individuale sau în mai multe cazuri legate de aceeaşi infracţiune sau de aceleaşi ameninţări la adresa siguranţei publice ar trebui considerată ca fiind în interesul legitim urmărit de operator. Cu toate acestea, o astfel de transmitere în interesul legitim al operatorului sau prelucrarea ulterioară a datelor cu caracter personal ar trebui interzisă în cazul în care prelucrarea nu este compatibilă cu o obligaţie legală, profesională sau cu o altă obligaţie de păstrare a confidenţialităţii.

(51) Datele cu caracter personal care sunt, prin natura lor, deosebit de sensibile în ceea ce priveşte drepturile şi libertăţile fundamentale necesită o protecţie specifică, deoarece contextul prelucrării acestora ar putea genera riscuri considerabile la adresa drepturilor şi libertăţilor fundamentale. Aceste date cu caracter personal ar trebui să includă datele cu caracter personal care dezvăluie originea rasială sau etnică .....

Prelucrarea fotografiilor nu ar trebui să fie considerată în mod sistematic ca fiind o prelucrare de categorii speciale de date cu caracter personal, întrucât fotografiile intră sub incidenţa definiţiei datelor biometrice doar în cazurile în care sunt prelucrate prin mijloace tehnice specifice care permit identificarea unică sau autentificarea unei persoane fizice.

.....

(58) **Principiul transparenţei** prevede că orice informaţii care se adresează publicului sau persoanei vizate să fie concise, uşor accesibile şi uşor de înţeles şi să se utilizeze un limbaj simplu şi clar, precum şi vizualizare acolo unde este cazul. Aceste informaţii ar putea fi furnizate în format electronic, de exemplu atunci când sunt adresate publicului, prin intermediul unui site. .....

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

(60) Conform **principiilor prelucrării echitabile şi transparente**, persoana vizată este informată cu privire la existenţa unei operaţiuni de prelucrare şi la scopurile acesteia. Operatorul ar trebui să furnizeze persoanei vizate orice informaţii suplimentare necesare pentru a asigura o prelucrare echitabilă şi transparentă, ţinând seama de circumstanţele specifice şi de contextul în care sunt prelucrate datele cu caracter personal. În plus, persoana vizată ar trebui informată cu privire la crearea de profiluri, precum şi la consecinţele acesteia. Atunci când datele cu caracter personal sunt colectate de la persoana vizată, aceasta ar trebui informată, de asemenea, dacă are obligaţia de a furniza datele cu caracter personal şi care sunt consecinţele în cazul unui refuz. Aceste informaţii pot fi furnizate în combinaţie cu pictograme standardizate pentru a oferi într-un mod uşor vizibil, inteligibil şi clar lizibil o imagine de ansamblu semnificativă asupra prelucrării avute în vedere. În cazul în care pictogramele sunt prezentate în format electronic, acestea ar trebui să poată fi citite automat.

(61) Informaţiile în legătură cu prelucrarea datelor cu caracter personal referitoare la persoana vizată ar trebui furnizate acesteia la momentul colectării de la persoana vizată sau, în cazul în care datele cu caracter personal sunt obţinute din altă sursă, într-o perioadă rezonabilă, în funcţie de circumstanţele cazului. În cazul în care datele cu caracter personal pot fi divulgate în mod legitim unui alt destinatar, persoana vizată ar trebui informată atunci când datele cu caracter personal sunt divulgate pentru prima dată destinatarului. În cazul în care operatorul intenţionează să prelucreze datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost colectate, operatorul ar trebui să furnizeze persoanei vizate, înainte de această prelucrare ulterioară, informaţii privind scopul secundar respectiv şi alte informaţii necesare. În cazul în care originea datelor cu caracter personal nu a putut fi

comunicată persoanei vizate din cauză că au fost utilizate surse diverse, informaţiile generale ar trebui furnizate.

(62) Cu toate acestea, nu este necesară impunerea obligaţiei de a furniza informaţii în cazul în care persoana vizată deţine deja informaţiile, în cazul în care înregistrarea sau divulgarea datelor cu caracter personal este prevăzută în mod expres de lege sau în cazul în care informarea persoanei vizate se dovedeşte imposibilă sau ar implica eforturi disproporţionate. Acesta din urmă ar putea fi cazul în special atunci când prelucrarea se efectuează în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice. În această privinţă, ar trebui luate în considerare numărul persoanelor vizate, vechimea datelor şi orice garanţii adecvate adoptate.

.....

(65) O persoană vizată ar trebui să aibă dreptul la rectificarea datelor cu caracter personal care o privesc şi "dreptul de a fi uitată", în cazul în care păstrarea acestor date încalcă prezentul regulament sau dreptul Uniunii sau dreptul intern sub incidenţa căruia intră operatorul. În special, persoanele vizate ar trebui să aibă dreptul ca datele lor cu caracter personal să fie şterse şi să nu mai fie prelucrate, în cazul în care datele cu caracter personal nu mai sunt necesare pentru scopurile în care sunt colectate sau sunt prelucrate, în cazul în care persoanele vizate şi-au retras consimţământul 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. .....

Cu toate acestea, păstrarea în continuare a datelor cu caracter personal ar trebui să fie legală în cazul în care este necesară pentru exercitarea dreptului la libertatea de exprimare şi de informare, pentru respectarea unei obligaţii legale, pentru îndeplinirea unei sarcini care serveşte unui interes public sau .....

.....

(69) În cazurile în care datele cu caracter personal ar putea fi prelucrate în mod legal deoarece prelucrarea este necesară pentru îndeplinirea unei sarcini care serveşte unui interes public sau care rezultă din exercitarea autorităţii publice cu care este învestit operatorul sau pe baza intereselor legitime ale unui operator sau ale unei părţi terţe, o persoană vizată ar trebui să aibă totuşi dreptul de a se opune prelucrării oricăror date cu caracter personal care se referă la situaţia sa particulară. Ar trebui să revină operatorului sarcina de a demonstra că interesele sale legitime şi imperioase prevalează asupra intereselor sau a drepturilor şi libertăţilor fundamentale ale persoanei vizate.

.....

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

.....

(78) **Protecţia drepturilor şi libertăţilor persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter** personal necesită adoptarea de măsuri tehnice şi organizatorice corespunzătoare pentru a se asigura îndeplinirea cerinţelor din prezentul regulament. Pentru a fi în măsură să demonstreze conformitatea cu prezentul regulament, operatorul ar trebui să adopte politici interne şi să pună în aplicare măsuri care să respecte în special **principiul protecţiei datelor începând cu momentul conceperii şi cel al protecţiei implicite** a datelor. Astfel de măsuri ar putea consta, printre altele, în reducerea la minimum a prelucrării datelor cu caracter personal, pseudonimizarea acestor date cât mai curând posibil, transparenţa în ceea ce priveşte funcţiile şi prelucrarea datelor cu caracter personal, abilitarea persoanei vizate să monitorizeze prelucrarea datelor, abilitarea operatorului să creeze elemente de siguranţă şi să le îmbunătăţească. Atunci când

elaborează, proiectează, selectează şi utilizează aplicaţii, servicii şi produse care se bazează pe prelucrarea datelor cu caracter personal sau care prelucrează date cu caracter personal pentru a-şi îndeplini rolul, producătorii acestor produse şi furnizorii acestor servicii şi aplicaţii ar trebui să fie încurajaţi să aibă în vedere dreptul la protecţia datelor la momentul elaborării şi proiectării unor astfel de produse, servicii şi aplicaţii şi, ţinând cont de stadiul actual al dezvoltării, să se asigure că operatorii şi persoanele împuternicite de operatori sunt în măsură să îşi îndeplinească obligaţiile referitoare la protecţia datelor. Principiul protecţiei datelor începând cu momentul conceperii şi cel al protecţiei implicite a datelor ar trebui să fie luate în considerare şi în contextul licitaţiilor publice.

.....

(81) Pentru a asigura respectarea cerinţelor impuse de prezentul regulament în ceea ce priveşte prelucrarea care trebuie efectuată în numele operatorului de către **persoana împuternicită de operator**, atunci când atribuie activităţi de prelucrare unei persoane împuternicite de operator, acesta din urmă ar trebui să utilizeze numai persoane împuternicite care oferă garanţii suficiente, în special în ceea ce priveşte cunoştinţele de specialitate, fiabilitatea şi resursele, pentru a implementa măsuri tehnice şi organizatorice care îndeplinesc cerinţele impuse de prezentul regulament, inclusiv pentru securitatea prelucrării. Aderarea de către persoana împuternicită de operator la un cod de conduită aprobat sau la un mecanism de certificare aprobat poate fi utilizată drept element care să demonstreze respectarea obligaţiilor de către operator. Efectuarea prelucrării de către o persoană împuternicită de un operator ar trebui să fie reglementată printr-un contract sau un alt tip de act juridic, în temeiul dreptului Uniunii sau al dreptului intern, care creează obligaţii pentru persoana împuternicită de operator în raport cu operatorul şi care stabileşte obiectul şi durata prelucrării, natura şi scopurile prelucrării, tipul de date cu caracter personal şi categoriile de persoane vizate, şi ar trebui să ţină seama de sarcinile şi responsabilităţile specifice ale persoanei împuternicite de operator în contextul prelucrării care trebuie efectuată, precum şi de riscul pentru drepturile şi libertăţile persoanei vizate. Operatorul şi persoana împuternicită de operator pot alege să utilizeze un contract individual sau clauze contractuale standard care sunt adoptate fie direct de Comisie, fie de o autoritate de supraveghere în conformitate cu mecanismul de asigurare a coerenţei şi apoi adoptate de Comisie. După finalizarea prelucrării în numele operatorului, persoana împuternicită de operator ar trebui să returneze sau să şteargă, în funcţie de opţiunea operatorului, datele cu caracter personal, cu excepţia cazului în care există o cerinţă de stocare a datelor cu caracter personal în temeiul dreptului Uniunii sau al dreptului intern care instituie obligaţii pentru persoana împuternicită de operator.

(82) În vederea demonstrării conformităţii cu prezentul regulament, operatorul sau persoana împuternicită de operator ar trebui să păstreze evidenţe ale activităţilor de prelucrare aflate în responsabilitatea sa. Fiecare operator şi fiecare persoană împuternicită de operator ar trebui să aibă obligaţia de a coopera cu autoritatea de supraveghere şi de a pune la dispoziţia acesteia, la cerere, aceste evidenţe, pentru a putea fi utilizate în scopul monitorizării operaţiunilor de prelucrare respective.

(83) În vederea menţinerii securităţii şi a prevenirii prelucrărilor care încalcă prezentul regulament, operatorul sau persoana împuternicită de operator ar trebui să **evalueze riscurile** inerente prelucrării şi să implementeze măsuri pentru atenuarea acestor riscuri, cum ar fi **criptarea**. **Măsurile** respective ar trebui să asigure un nivel corespunzător de securitate, inclusiv confidenţialitatea, luând în considerare stadiul actual al dezvoltării şi costurile implementării în raport cu riscurile şi cu natura datelor cu caracter personal a căror protecţie trebuie asigurată. La evaluarea riscului pentru securitatea datelor cu caracter personal, ar trebui **să se acorde atenţie riscurilor pe care le prezintă prelucrarea datelor, cum ar fi distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod, în mod accidental sau ilegal, care pot duce în special la prejudicii fizice, materiale sau morale**.

(84) Pentru a favoriza respectarea dispoziţiilor prezentului regulament în cazurile în care operaţiunile de prelucrare sunt susceptibile să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, operatorul ar trebui să fie responsabil de efectuarea unei **evaluări a impactului asupra protecţiei datelor**, care să estimeze, în special, originea, natura, specificitatea şi gravitatea acestui risc. Rezultatul evaluării ar trebui luat în considerare la stabilirea măsurilor adecvate care trebuie luate pentru a demonstra că prelucrarea datelor cu caracter personal respectă prezentul regulament. În cazul în care o evaluare a impactului asupra protecţiei datelor arată că operaţiunile de prelucrare implică un risc ridicat, pe care operatorul nu îl poate atenua prin măsuri adecvate sub aspectul tehnologiei disponibile şi al costurilor implementării, ar trebui să aibă loc o consultare a autorităţii de supraveghere înainte de prelucrare.

(85) Dacă nu este soluţionată la timp şi într-un mod adecvat, o încălcare a securităţii datelor cu caracter personal poate conduce la prejudicii fizice, materiale sau morale aduse persoanelor fizice, cum ar fi pierderea controlului asupra datelor lor cu caracter personal sau limitarea drepturilor lor, discriminare, furt sau fraudă de identitate, pierdere financiară, inversarea neautorizată a pseudonimizării, compromiterea reputaţiei, pierderea confidenţialităţii datelor cu caracter personal protejate prin secret profesional sau orice alt dezavantaj semnificativ de natură economică sau socială adus persoanei fizice în cauză. Prin urmare, de îndată ce a luat cunoştinţă de producerea unei încălcări a securităţii datelor cu caracter personal, operatorul ar trebui să notifice această încălcare autorităţii de supraveghere, fără întârziere nejustificată şi, dacă este posibil, în cel mult 72 de ore după ce a luat la cunoştinţă de existenţa acesteia, cu excepţia cazului în care operatorul este în măsură să demonstreze, în conformitate cu principiul responsabilităţii, că încălcarea securităţii datelor cu caracter personal nu este susceptibilă să genereze un risc pentru drepturile şi libertăţile persoanelor fizice. Atunci când notificarea nu se poate realiza în termen de 72 de ore, aceasta ar trebui să cuprindă motivele întârzierii, iar informaţiile pot fi furnizate treptat, fără altă întârziere.

(86) Operatorul ar trebui să comunice persoanei vizate o încălcare a securităţii datelor cu caracter personal, fără întârzieri nejustificate, atunci când încălcarea este susceptibilă să genereze un risc ridicat pentru drepturile şi libertăţile persoanei fizice, pentru a-i permite să ia măsurile de precauţie necesare. Comunicarea ar trebui să descrie natura încălcării securităţii datelor cu caracter personal şi să cuprindă recomandări pentru persoana fizică în cauză în scopul atenuării eventualelor efecte negative. Comunicările către persoanele vizate ar trebui efectuate în cel mai scurt timp posibil în mod rezonabil şi în strânsă cooperare cu autoritatea de supraveghere, respectându-se orientările furnizate de aceasta sau de alte autorităţi competente, cum ar fi autorităţile de aplicare a legii. De exemplu, necesitatea de a atenua un risc imediat de producere a unui prejudiciu ar presupune comunicarea cu promptitudine către persoanele vizate, în timp ce necesitatea de a implementa măsuri corespunzătoare împotriva încălcării în continuare a securităţii datelor cu caracter personal sau împotriva unor încălcări similare ale securităţii datelor cu caracter personal ar putea justifica un termen mai îndelungat pentru comunicare.

(87) Ar trebui să se stabilească dacă au fost implementate toate măsurile tehnologice de protecţie şi organizatorice corespunzătoare în scopul de a se stabili imediat dacă s-a produs o încălcare a securităţii datelor cu caracter personal şi de a se informa cu promptitudine autoritatea de supraveghere şi persoana vizată. Faptul că notificarea a fost efectuată fără întârziere nejustificată ar trebui stabilit luându-se în considerare, în special, natura şi gravitatea încălcării securităţii datelor cu caracter personal, precum şi consecinţele şi efectele negative ale acesteia asupra persoanei vizate. Această notificare poate conduce la o intervenţie a autorităţii de supraveghere, în conformitate cu sarcinile şi competenţele specificate în prezentul regulament.

(88) La stabilirea de norme detaliate privind formatul şi procedurile aplicabile notificării referitoare la încălcările securităţii datelor cu caracter personal, ar trebui să se acorde atenţia cuvenită circumstanţelor în care a avut loc încălcarea, stabilindu-se inclusiv dacă protecţia datelor cu caracter personal a fost sau nu a fost asigurată prin măsuri tehnice de protecţie

corespunzătoare, care să limiteze efectiv probabilitatea fraudării identităţii sau a altor forme de utilizare abuzivă. În plus, astfel de norme şi proceduri ar trebui să ţină cont de interesele legitime ale autorităţilor de aplicare a legii în cazurile în care divulgarea timpurie ar putea îngreuna în mod inutil investigarea circumstanţelor în care a avut loc o încălcare a datelor cu caracter personal.

.....

(90) ..... operatorul ar trebui să efectueze, înainte de prelucrare, **o evaluare a impactului asupra protecţiei datelor**, în scopul evaluării gradului specific de probabilitate a materializării riscului ridicat şi gravitatea acestuia, având în vedere natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi sursele riscului. Respectiva evaluare a impactului ar trebui să includă, în special, măsurile, garanţiile şi mecanismele avute în vedere pentru atenuarea riscului respectiv, pentru asigurarea protecţiei datelor cu caracter personal şi pentru demonstrarea conformităţii cu prezentul regulament.

(91) Aceasta ar trebui să se aplice, în special, operaţiunilor de prelucrare la scară largă, care au drept obiectiv prelucrarea unui volum considerabil de date cu caracter personal la nivel regional, naţional sau supranaţional, ...

(109) Posibilitatea ca operatorul sau persoana împuternicită de operator să utilizeze clauze standard în materie de protecţie a datelor, adoptate de Comisie sau de o autoritate de supraveghere, nu ar trebui să împiedice operatorii sau persoanele împuternicite de aceştia să includă clauzele standard în materie de protecţie a datelor într-un contract mai amplu, precum un contract între persoana împuternicită de operator şi o altă persoană împuternicită de operator, şi nici să adauge alte clauze sau garanţii suplimentare, atât timp cât acestea nu contravin, direct sau indirect, clauzelor contractuale standard adoptate de Comisie sau de o autoritate de supraveghere sau nu prejudiciază drepturile sau libertăţile fundamentale ale persoanelor vizate. Operatorii şi persoanele împuternicite de operatori ar trebui să fie încurajaţi să ofere garanţii suplimentare prin intermediul unor angajamente contractuale care să completeze clauzele standard în materie de protecţie.

.....

(146) Operatorul sau persoana împuternicită de operator ar trebui să plătească despăgubiri pentru orice prejudiciu pe care o persoană îl poate suferi ca urmare a unei prelucrări care încalcă prezentul regulament. Operatorul sau persoana împuternicită de operator ar trebui să fie exoneraţi de răspundere dacă dovedesc că nu sunt în niciun fel răspunzători pentru prejudiciu. .....

CAPITOLUL I: Dispoziţii generale

Art. 1: Obiect şi obiective

(1) Prezentul regulament stabileşte normele referitoare la protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal, precum şi normele referitoare la libera circulaţie a datelor cu caracter personal.

(2) Prezentul regulament asigură protecţia drepturilor şi libertăţilor fundamentale ale persoanelor fizice şi în special a dreptului acestora la protecţia datelor cu caracter personal.

(3) Libera circulaţie a datelor cu caracter personal în interiorul Uniunii nu poate fi restricţionată sau interzisă din motive legate de protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal.

Art. 2: Domeniul de aplicare material

(1) Prezentul regulament se aplică prelucrării datelor cu caracter personal, efectuată total sau parţial prin mijloace automatizate, precum şi prelucrării prin alte mijloace decât cele automatizate a **datelor cu caracter personal care fac parte dintr-un sistem de evidenţă a datelor** sau care sunt destinate să facă parte dintr-un sistem de evidenţă a datelor.

.....

Art. 3: Domeniul de aplicare teritorial

(1) Prezentul regulament se aplică prelucrării datelor cu caracter personal în cadrul activităţilor unui sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, indiferent dacă prelucrarea are loc sau nu pe teritoriul Uniunii.

.....

Art. 4: Definiţii

În sensul prezentului regulament:

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

2. "**prelucrare**" înseamnă orice operaţiune sau set de operaţiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziţie în orice alt mod, alinierea sau combinarea, restricţionarea, ştergerea sau distrugerea;

3. "**restricţionarea prelucrării**" înseamnă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;

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

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

6. "**sistem de evidenţă a datelor**" înseamnă orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcţionale sau geografice;

7. "**operator**" înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care, singur sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile şi mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern;

8. "**persoană împuternicită de operator**" înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

9. "**destinatar**" înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terţă. Cu toate acestea, autorităţile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autorităţile publice respective respectă normele aplicabile în materie de protecţie a datelor, în conformitate cu scopurile prelucrării;

10. "**parte terţă**" înseamnă o persoană fizică sau juridică, autoritate publică, agenţie sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator şi persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;

11. "**consimţământ**" al persoanei vizate înseamnă orice manifestare de voinţă liberă, specifică, informată şi lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declaraţie sau printr-o acţiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;

12. "**încălcarea securităţii datelor cu caracter personal**" înseamnă o încălcare a securităţii care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea;
13. "**date genetice**" înseamnă datele cu caracter personal referitoare la caracteristicile genetice moştenite sau dobândite ale unei persoane fizice, care oferă informaţii unice privind fiziologia sau sănătatea persoanei respective şi care rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză;
14. "**date biometrice**" înseamnă acele date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice;
15. "**date privind sănătatea**" înseamnă date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistenţă medicală, care dezvăluie informaţii despre starea de sănătate a acesteia;
16. "**sediu principal**" înseamnă:
(a) în cazul unui operator cu sedii în cel puţin două state membre, locul în care se află administraţia centrală a acestuia în Uniune, cu excepţia cazului în care deciziile privind scopurile şi mijloacele de prelucrare a datelor cu caracter personal se iau într-un alt sediu al operatorului din Uniune, sediu care are competenţa de a dispune punerea în aplicare a acestor decizii, caz în care sediul care a luat deciziile respective este considerat a fi sediul principal;
(b) în cazul unei persoane împuternicite de operator cu sedii în cel puţin două state membre, locul în care se află administraţia centrală a acesteia în Uniune, sau, în cazul în care persoana împuternicită de operator nu are o administraţie centrală în Uniune, sediul din Uniune al persoanei împuternicite de operator în care au loc activităţile principale de prelucrare, în contextul activităţilor unui sediu al persoanei împuternicite de operator, în măsura în care aceasta este supusă unor obligaţii specifice în temeiul prezentului regulament;
17. "**reprezentant**" înseamnă o persoană fizică sau juridică stabilită în Uniune, desemnată în scris de către operator sau persoana împuternicită de operator în temeiul articolului 27, care reprezintă operatorul sau persoana împuternicită în ceea ce priveşte obligaţiile lor respective care le revin în temeiul prezentului regulament;
18. "**întreprindere**" înseamnă o persoană fizică sau juridică ce desfăşoară o activitate economică, indiferent de forma juridică a acesteia, inclusiv parteneriate sau asociaţii care desfăşoară în mod regulat o activitate economică;
.....
21. "**autoritate de supraveghere**" înseamnă o autoritate publică independentă instituită de un stat membru în temeiul articolului 51;
.....

CAPITOLUL II: Principii

Art. 5: Principii legate de prelucrarea datelor cu caracter personal

(1) Datele cu caracter personal sunt:
a) prelucrate în mod legal, echitabil şi transparent faţă de persoana vizată ("legalitate, echitate şi transparenţă");
b) colectate în scopuri determinate, explicite şi legitime şi nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile iniţiale, în conformitate cu articolul 89 alineatul (1) ("limitări legate de scop");
c) adecvate, relevante şi limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate ("reducerea la minimum a datelor");

d) exacte şi, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt şterse sau rectificate fără întârziere ("exactitate");
e) păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depăşeşte perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1), sub rezerva punerii în aplicare a măsurilor de ordin tehnic şi organizatoric adecvate prevăzute în prezentul regulament în vederea garantării drepturilor şi libertăţilor persoanei vizate ("limitări legate de stocare");
f) prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecţia împotriva prelucrării neautorizate sau ilegale şi împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare ("integritate şi confidenţialitate").
(2) Operatorul este responsabil de respectarea alineatului (1) şi poate demonstra această respectare ("responsabilitate").

Art. 6: Legalitatea prelucrării

(1) Prelucrarea este legală numai dacă şi în măsura în care se aplică cel puţin una dintre următoarele condiţii:
a) persoana vizată şi-a dat consimţământul 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 a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;
c) prelucrarea este necesară în vederea îndeplinirii unei obligaţii legale care îi revine operatorului;
d) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;
e) prelucrarea este necesară pentru îndeplinirea unei sarcini care serveşte unui interes public sau care rezultă din exercitarea autorităţii publice cu care este învestit operatorul;
f) prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terţă, cu excepţia cazului în care prevalează interesele sau drepturile şi libertăţile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.

.....

Art. 7: Condiţii privind consimţământul

(1) În cazul în care prelucrarea se bazează pe consimţământ, operatorul trebuie să fie în măsură să demonstreze că persoana vizată şi-a dat consimţământul pentru prelucrarea datelor sale cu caracter personal. **(2)** În cazul în care consimţământul persoanei vizate este dat în contextul unei declaraţii scrise care se referă şi la alte aspecte, cererea privind consimţământul trebuie să fie prezentată într-o formă care o diferenţiază în mod clar de celelalte aspecte, într-o formă inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu. Nicio parte a respectivei declaraţii care constituie o încălcare a prezentului regulament nu este obligatorie.
(3) Persoana vizată are dreptul să îşi retragă în orice moment consimţământul. Retragerea consimţământului nu afectează legalitatea prelucrării efectuate pe baza consimţământului înainte de retragerea acestuia. Înainte de acordarea consimţământului, persoana vizată este informată cu privire la acest lucru. Retragerea consimţământului se face la fel de simplu ca acordarea acestuia.
(4) Atunci când se evaluează dacă consimţământul este dat în mod liber, se ţine seama cât mai mult de faptul că, printre altele, executarea unui contract, inclusiv prestarea unui serviciu,

este condiţionată sau nu de consimţământul cu privire la prelucrarea datelor cu caracter personal care nu este necesară pentru executarea acestui contract.
.....
Art. 9: Prelucrarea de categorii speciale de date cu caracter personal
(1) Se interzice prelucrarea de date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenenţa la sindicate şi prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viaţa sexuală sau orientarea sexuală ale unei persoane fizice.
(2) Alineatul (1) nu se aplică în următoarele situaţii:
.....
c) prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice, atunci când persoana vizată se află în incapacitate fizică sau juridică de a-şi da consimţământul;
.....
e) prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod manifest de către persoana vizată;
f) prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanţă sau ori de câte ori instanţele acţionează în exerciţiul funcţiei lor judiciare;
.....
Art. 11: Prelucrarea care nu necesită identificare
(1) În cazul în care scopurile pentru care un operator prelucrează date cu caracter personal nu necesită sau nu mai necesită identificarea unei persoane vizate de către operator, operatorul nu are obligaţia de a păstra, obţine sau prelucra informaţii suplimentare pentru a identifica persoana vizată în scopul unic al respectării prezentului regulament.
.....

CAPITOLUL III: Drepturile persoanei vizate

Secţiunea 1: Transparenţă şi modalităţi

Art. 12: Transparenţa informaţiilor, a comunicărilor şi a modalităţilor de exercitare a drepturilor persoanei vizate
(1) Operatorul ia măsuri adecvate pentru a furniza persoanei vizate orice informaţii menţionate la articolele 13 şi 14 şi orice comunicări în temeiul articolelor 15-22 şi 34 referitoare la prelucrare, într-o formă concisă, transparentă, inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu, în special pentru orice informaţii adresate în mod specific unui copil. Informaţiile se furnizează în scris sau prin alte mijloace, inclusiv, atunci când este oportun, în format electronic. La solicitarea persoanei vizate, informaţiile pot fi furnizate verbal, cu condiţia ca identitatea persoanei vizate să fie dovedită prin alte mijloace.
.....
(3) În cazul în care persoana vizată introduce o cerere în format electronic, informaţiile sunt furnizate în format electronic acolo unde este posibil, cu excepţia cazului în care persoana vizată solicită un alt format.
(4) Dacă nu ia măsuri cu privire la cererea persoanei vizate, operatorul informează persoana vizată, fără întârziere şi în termen de cel mult o lună de la primirea cererii, cu privire la motivele pentru care nu ia măsuri şi la posibilitatea de a depune o plângere în faţa unei autorităţi de supraveghere şi de a introduce o cale de atac judiciară.
.....

Secţiunea 2: Informare şi acces la date cu caracter personal

Art. 13: Informaţii care se furnizează în cazul în care datele cu caracter personal sunt colectate de la persoana vizată
(1) În cazul în care datele cu caracter personal referitoare la o persoană vizată sunt colectate de la aceasta, operatorul, în momentul obţinerii acestor date cu caracter personal, furnizează persoanei vizate toate informaţiile următoare:
a) identitatea şi datele de contact ale operatorului şi, după caz, ale reprezentantului acestuia;

b) datele de contact ale responsabilului cu protecţia datelor, după caz;
c) scopurile în care sunt prelucrate datele cu caracter personal, precum şi temeiul juridic al prelucrării;
d) în cazul în care prelucrarea se face în temeiul articolului 6 alineatul (1) litera (f), interesele legitime urmărite de operator sau de o parte terţă;
e) destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
.....
(2) În plus faţă de informaţiile menţionate la alineatul (1), în momentul în care datele cu caracter personal sunt obţinute, operatorul furnizează persoanei vizate următoarele informaţii suplimentare necesare pentru a asigura o prelucrare echitabilă şi transparentă:
.....
b) existenţa dreptului de a solicita operatorului, în ceea ce priveşte datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ştergerea acestora sau restricţionarea prelucrării sau a dreptului de a se opune prelucrării, precum şi a dreptului la portabilitatea datelor;
.....
d) dreptul de a depune o plângere în faţa unei autorităţi de supraveghere;
e) dacă furnizarea de date cu caracter personal reprezintă o obligaţie legală sau contractuală sau o obligaţie necesară pentru încheierea unui contract, precum şi dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal şi care sunt eventualele consecinţe ale nerespectării acestei obligaţii;
.....

Art. 14: Informaţii care se furnizează în cazul în care datele cu caracter personal nu au fost obţinute de la persoana vizată

(1) În cazul în care datele cu caracter personal nu au fost obţinute de la persoana vizată, operatorul furnizează persoanei vizate următoarele informaţii:
a) identitatea şi datele de contact ale operatorului şi, după caz, ale reprezentantului acestuia;
b) datele de contact ale responsabilului cu protecţia datelor, după caz;
c) scopurile în care sunt prelucrate datele cu caracter personal, precum şi temeiul juridic al prelucrării;
d) categoriile de date cu caracter personal vizate;
e) destinatarii sau categoriile de destinatari ai datelor cu caracter personal, după caz;
f) dacă este cazul, intenţia operatorului de a transfera date cu caracter personal către un destinatar dintr-o ţară terţă .....
(2) Pe lângă informaţiile menţionate la alineatul (1), operatorul furnizează persoanei vizate următoarele informaţii necesare pentru a asigura o prelucrare echitabilă şi transparentă în ceea ce priveşte persoana vizată:
.....
f) sursa din care provin datele cu caracter personal şi, dacă este cazul, dacă acestea provin din surse disponibile public;
.....

Art. 15: Dreptul de acces al persoanei vizate

(1) Persoana vizată are dreptul de a obţine din partea operatorului o confirmare că se prelucrează sau nu date cu caracter personal care o privesc şi, în caz afirmativ, acces la datele respective şi la următoarele informaţii:
a) scopurile prelucrării;
b) categoriile de date cu caracter personal vizate;
c) destinatarii sau categoriile de destinatari cărora datele cu caracter personal le-au fost sau urmează să le fie divulgate, în special destinatari din ţări terţe sau organizaţii internaţionale;
d) acolo unde este posibil, perioada pentru care se preconizează că vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;

e) existenţa dreptului de a solicita operatorului rectificarea sau ştergerea datelor cu caracter personal ori restricţionarea prelucrării datelor cu caracter personal referitoare la persoana vizată sau a dreptului de a se opune prelucrării;
f) dreptul de a depune o plângere în faţa unei autorităţi de supraveghere;
g) în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, orice informaţii disponibile privind sursa acestora;
.....
Secţiunea 3: Rectificare şi ştergere
Art. 16: Dreptul la rectificare
Persoana vizată are dreptul de a obţine de la operator, fără întârzieri nejustificate, rectificarea datelor cu caracter personal inexacte care o privesc. Ţinându-se seama de scopurile în care au fost prelucrate datele, persoana vizată are dreptul de a obţine completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declaraţii suplimentare.
Art. 17: Dreptul la ştergerea datelor ("dreptul de a fi uitat")
(1) Persoana vizată are dreptul de a obţine din partea operatorului ştergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, iar operatorul are obligaţia de a şterge datele cu caracter personal fără întârzieri nejustificate în cazul în care se aplică unul dintre următoarele motive:
a) datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;
b) persoana vizată îşi retrage consimţământul pe baza căruia are loc prelucrarea, ..., şi nu există niciun alt temei juridic pentru prelucrare;
c) persoana vizată se opune prelucrării în temeiul articolului 21 alineatul (1) şi nu există motive legitime care să prevaleze în ceea ce priveşte prelucrarea sau persoana vizată se opune prelucrării în temeiul articolului 21 alineatul (2);
.....
Secţiunea 4: Dreptul la opoziţie şi procesul decizional individual automatizat
Art. 21: Dreptul la opoziţie
(1) În orice moment, persoana vizată are dreptul de a se opune, din motive legate de situaţia particulară în care se află, prelucrării în temeiul articolului 6 alineatul (1) ..... a datelor cu caracter personal care o privesc, inclusiv creării de profiluri pe baza respectivelor dispoziţii. Operatorul nu mai prelucrează datele cu caracter personal, cu excepţia cazului în care operatorul demonstrează că are motive legitime şi imperioase care justifică prelucrarea şi care prevalează asupra intereselor, drepturilor şi libertăţilor persoanei vizate sau că scopul este constatarea, exercitarea sau apărarea unui drept în instanţă.
.....

CAPITOLUL IV: Operatorul şi persoana împuternicită de operator
Secţiunea 1: Obligaţii generale
Art. 24: Responsabilitatea operatorului
(1) Ţinând seama de natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi de riscurile cu grade diferite de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice, operatorul pune în aplicare măsuri tehnice şi organizatorice adecvate pentru a garanta şi a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul regulament. Respectivele măsuri se revizuiesc şi se actualizează dacă este necesar.
.....
Art. 25: Asigurarea protecţiei datelor începând cu momentul conceperii şi în mod implicit
(1) Având în vedere stadiul actual al tehnologiei, costurile implementării, şi natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi riscurile cu grade diferite de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice pe care le prezintă prelucrarea, operatorul, atât în momentul stabilirii mijloacelor de prelucrare, cât şi în cel al prelucrării în sine, pune în aplicare măsuri tehnice şi organizatorice adecvate, cum ar fi

pseudonimizarea, care sunt destinate să pună în aplicare în mod eficient principiile de protecţie a datelor, precum reducerea la minimum a datelor, şi să integreze garanţiile necesare în cadrul prelucrării, pentru a îndeplini cerinţele prezentului regulament şi a proteja drepturile persoanelor vizate.

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

.....

Art. 28: Persoana împuternicită de operator

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

.....

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

a) prelucrează datele cu caracter personal numai pe baza unor instrucţiuni documentate din partea operatorului, inclusiv în ceea ce priveşte transferurile de date cu caracter personal către o ţară terţă sau o organizaţie internaţională, cu excepţia cazului în care această obligaţie îi revine persoanei împuternicite în temeiul dreptului Uniunii sau al dreptului intern care i se aplică; în acest caz, notifică această obligaţie juridică operatorului înainte de prelucrare, cu excepţia cazului în care dreptul respectiv interzice o astfel de notificare din motive importante legate de interesul public;

b) se asigură că persoanele autorizate să prelucreze datele cu caracter personal s-au angajat să respecte confidenţialitatea sau au o obligaţie statutară adecvată de confidenţialitate;

.....

Art. 30: Evidenţele activităţilor de prelucrare

(1) Fiecare operator şi, după caz, reprezentantul acestuia păstrează o evidenţă a activităţilor de prelucrare desfăşurate sub responsabilitatea lor. Respectiva evidenţă cuprinde următoarele informaţii:

a) numele şi datele de contact ale operatorului şi, după caz, ale operatorului asociat, ale reprezentantului operatorului şi ale responsabilului cu protecţia datelor;

b) scopurile prelucrării;

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

d) categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din ţări terţe sau organizaţii internaţionale;

e) dacă este cazul, transferurile de date cu caracter personal către o ţară terţă sau o organizaţie internaţională, inclusiv identificarea ţării terţe sau a organizaţiei internaţionale .....;

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

g) acolo unde este posibil, o descriere generală a măsurilor tehnice şi organizatorice de securitate menţionate la articolul 32 alineatul (1).

(2) Fiecare operator şi, după caz, persoana împuternicită de operator păstrează o evidenţă a tuturor categoriilor de activităţi de prelucrare desfăşurate în numele operatorului, care cuprind:
a) numele şi datele de contact ale persoanei sau persoanelor împuternicite de operator şi ale fiecărui operator în numele căruia acţionează această persoană (aceste persoane), precum şi ale reprezentantului operatorului sau al persoanei împuternicite de operator, după caz;
b) categoriile de activităţi de prelucrare desfăşurate în numele fiecărui operator;
c) dacă este cazul, transferurile de date cu caracter personal către o ţară terţă sau o organizaţie internaţională, inclusiv identificarea ţării terţe sau a organizaţiei internaţionale .....;
d) acolo unde este posibil, o descriere generală a măsurilor tehnice şi organizatorice de securitate menţionate la articolul 32 alineatul (1).
(3) Evidenţele menţionate la alineatele (1) şi (2) se formulează în scris, inclusiv în format electronic.
(4) Operatorul sau persoana împuternicită de acesta, precum şi, după caz, reprezentantul operatorului sau al persoanei împuternicite de operator pun evidenţele la dispoziţia autorităţii de supraveghere, la cererea acesteia.
(5) ***Obligaţiile menţionate la alineatele 1 şi 2 nu se aplică unei întreprinderi sau organizaţii cu mai puţin de 250 de angajaţi***, cu excepţia cazului în care prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile şi libertăţile persoanelor vizate, prelucrarea nu este ocazională sau prelucrarea include categorii speciale de date, astfel cum se prevede la articolul 9 alineatul (1), sau date cu caracter personal referitoare la condamnări penale şi infracţiuni, astfel cum se menţionează la articolul 10.

Art. 31: Cooperarea cu autoritatea de supraveghere

Operatorul şi persoana împuternicită de operator şi, după caz, reprezentantul acestora cooperează, la cerere, cu autoritatea de supraveghere în îndeplinirea sarcinilor lor.

Secţiunea 2: Securitatea datelor cu caracter personal

Art. 32: Securitatea prelucrării

(1) Având în vedere stadiul actual al dezvoltării, costurile implementării şi natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi riscul cu diferite grade de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice, operatorul şi persoana împuternicită de acesta implementează măsuri tehnice şi organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând printre altele, după caz:
a) pseudonimizarea şi criptarea datelor cu caracter personal;
b) capacitatea de a asigura confidenţialitatea, integritatea, disponibilitatea şi rezistenţa continuă ale sistemelor şi serviciilor de prelucrare;
c) capacitatea de a restabili disponibilitatea datelor cu caracter personal şi accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;
d) un proces pentru testarea, evaluarea şi aprecierea periodică ale eficacităţii măsurilor tehnice şi organizatorice pentru a garanta securitatea prelucrării.
(2) La evaluarea nivelului adecvat de securitate, se ţine seama în special de riscurile prezentate de prelucrare, generate în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.
(3) Aderarea la un cod de conduită aprobat, menţionat la articolul 40, sau la un mecanism de certificare aprobat, menţionat la articolul 42, poate fi utilizată ca element prin care să se demonstreze îndeplinirea cerinţelor prevăzute la alineatul (1) din prezentul articol.
(4) Operatorul şi persoana împuternicită de acesta iau măsuri pentru a asigura faptul că orice persoană fizică care acţionează sub autoritatea operatorului sau a persoanei împuternicite de operator şi care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepţia cazului în care această obligaţie îi revine în temeiul dreptului Uniunii sau al dreptului intern.

Art. 33: Notificarea autorităţii de supraveghere în cazul încălcării securităţii datelor cu caracter personal

(1) În cazul în care are loc o încălcare a securităţii datelor cu caracter personal, operatorul notifică acest lucru autorităţii de supraveghere competente în temeiul articolului 55, fără întârzieri nejustificate şi, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoştinţă de aceasta, cu excepţia cazului în care este susceptibilă să genereze un risc pentru drepturile şi libertăţile persoanelor fizice.

(2) Persoana împuternicită de operator înştiinţează operatorul fără întârzieri nejustificate după ce ia cunoştinţă de o încălcare a securităţii datelor cu caracter personal.

(3) Notificarea menţionată la alineatul (1) cel puţin:

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

b) comunică numele şi datele de contact ale responsabilului cu protecţia datelor sau un alt punct de contact de unde se pot obţine mai multe informaţii;

c) descrie consecinţele probabile ale încălcării securităţii datelor cu caracter personal;

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

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

(5) Operatorul păstrează documente referitoare la toate cazurile de încălcare a securităţii datelor cu caracter personal, care cuprind o descriere a situaţiei de fapt în care a avut loc încălcarea securităţii datelor cu caracter personal, a efectelor acesteia şi a măsurilor de remediere întreprinse. Această documentaţie permite autorităţii de supraveghere să verifice conformitatea cu prezentul articol.

Art. 34: Informarea persoanei vizate cu privire la încălcarea securităţii datelor cu caracter personal

(1) În cazul în care încălcarea securităţii datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, operatorul informează persoana vizată fără întârzieri nejustificate cu privire la această încălcare.

(2) În informarea transmisă persoanei vizate prevăzută la alineatul (1) din prezentul articol se include o descriere într-un limbaj clar şi simplu a caracterului încălcării securităţii datelor cu caracter personal, precum şi cel puţin informaţiile şi măsurile menţionate la articolul 33 alineatul (3) literele (b), (c) şi (d).

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

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

b) operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat pentru drepturile şi libertăţile persoanelor vizate menţionat la alineatul (1) nu mai este susceptibil să se materializeze;

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

(4) În cazul în care operatorul nu a comunicat deja încălcarea securităţii datelor cu caracter personal către persoana vizată, autoritatea de supraveghere, după ce a luat în considerare probabilitatea ca încălcarea securităţii datelor cu caracter personal să genereze un risc ridicat, poate să îi solicite acestuia să facă acest lucru sau poate decide că oricare dintre condiţiile menţionate la alineatul (3) sunt îndeplinite.

Art. 35: Evaluarea impactului asupra protecţiei datelor

(1) Având în vedere natura, domeniul de aplicare, contextul şi scopurile prelucrării, în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operaţiunilor de prelucrare prevăzute asupra protecţiei datelor cu caracter personal. O evaluare unică poate aborda un set de operaţiuni de prelucrare similare care prezintă riscuri ridicate similare.

(2) La realizarea unei evaluări a impactului asupra protecţiei datelor, operatorul solicită avizul responsabilului cu protecţia datelor, dacă acesta a fost desemnat.

.....

Secţiunea 4: Responsabilul cu protecţia datelor

Art. 37: Desemnarea responsabilului cu protecţia datelor

(1) Operatorul şi persoana împuternicită de operator desemnează un responsabil cu protecţia datelor ori de câte ori:

a) prelucrarea este efectuată de o autoritate sau un organism public, cu excepţia instanţelor care acţionează în exerciţiul funcţiei lor jurisdicţionale;

b) activităţile principale ale operatorului sau ale persoanei împuternicite de operator constau în operaţiuni de prelucrare care, prin natura, domeniul de aplicare şi/sau scopurile lor, necesită o monitorizare periodică şi sistematică a persoanelor vizate pe scară largă; sau

c) activităţile principale ale operatorului sau ale persoanei împuternicite de operator constau în prelucrarea pe scară largă a unor categorii speciale de date, menţionate la articolul 9, sau a unor date cu caracter personal privind condamnări penale şi infracţiuni, menţionată la articolul 10.

(2) Un grup de întreprinderi poate numi un responsabil cu protecţia datelor unic, cu condiţia ca responsabilul cu protecţia datelor să fie uşor accesibil din fiecare întreprindere.

(3) În cazul în care operatorul sau persoana împuternicită de operator este o autoritate publică sau un organism public, poate fi desemnat un responsabil cu protecţia datelor unic pentru mai multe dintre aceste autorităţi sau organisme, luând în considerare structura organizatorică şi dimensiunea acestora.

(4) În alte cazuri decât cele menţionate la alineatul (1), operatorul sau persoana împuternicită de operator ori asociaţiile şi alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori pot desemna sau, acolo unde dreptul Uniunii sau dreptul intern solicită acest lucru, desemnează un responsabil cu protecţia datelor. Responsabilul cu protecţia datelor poate să acţioneze în favoarea unor astfel de asociaţii şi alte organisme care reprezintă operatori sau persoane împuternicite de operatori.

(5) Responsabilul cu protecţia datelor este desemnat pe baza calităţilor profesionale şi, în special, a cunoştinţelor de specialitate în dreptul şi practicile din domeniul protecţiei datelor, precum şi pe baza capacităţii de a îndeplini sarcinile prevăzute la articolul 39.

(6) Responsabilul cu protecţia datelor poate fi un membru al personalului operatorului sau persoanei împuternicite de operator sau poate să îşi îndeplinească sarcinile în baza unui contract de servicii.

(7) Operatorul sau persoana împuternicită de operator publică datele de contact ale responsabilului cu protecţia datelor şi le comunică autorităţii de supraveghere.

Art. 38: Funcţia responsabilului cu protecţia datelor

(1) Operatorul şi persoana împuternicită de operator se asigură că responsabilul cu protecţia datelor este implicat în mod corespunzător şi în timp util în toate aspectele legate de protecţia datelor cu caracter personal.

(2) Operatorul şi persoana împuternicită de operator sprijină responsabilul cu protecţia datelor în îndeplinirea sarcinilor menţionate la articolul 39, asigurându-i resursele necesare pentru executarea acestor sarcini, precum şi accesarea datelor cu caracter personal şi a operaţiunilor de prelucrare, şi pentru menţinerea cunoştinţelor sale de specialitate.

(3) Operatorul şi persoana împuternicită de operator se asigură că responsabilul cu protecţia datelor nu primeşte niciun fel de instrucţiuni în ceea ce priveşte îndeplinirea acestor sarcini. Acesta nu este demis sau sancţionat de către operator sau de persoana împuternicită de

operator pentru îndeplinirea sarcinilor sale. Responsabilul cu protecţia datelor răspunde direct în faţa celui mai înalt nivel al conducerii operatorului sau persoanei împuternicite de operator.
(4) Persoanele vizate pot contacta responsabilul cu protecţia datelor cu privire la toate chestiunile legate de prelucrarea datelor lor şi la exercitarea drepturilor lor în temeiul prezentului regulament.
(5) Responsabilul cu protecţia datelor are obligaţia de a respecta secretul sau confidenţialitatea în ceea ce priveşte îndeplinirea sarcinilor sale, în conformitate cu dreptul Uniunii sau cu dreptul intern.
(6) Responsabilul cu protecţia datelor poate îndeplini şi alte sarcini şi atribuţii. Operatorul sau persoana împuternicită de operator se asigură că niciuna dintre aceste sarcini şi atribuţii nu generează un conflict de interese.

Art. 39: Sarcinile responsabilului cu protecţia datelor

(1) Responsabilul cu protecţia datelor are cel puţin următoarele sarcini:
a) informarea şi consilierea operatorului, sau a persoanei împuternicite de operator, precum şi a angajaţilor care se ocupă de prelucrare cu privire la obligaţiile care le revin în temeiul prezentului regulament şi al altor dispoziţii de drept al Uniunii sau drept intern referitoare la protecţia datelor;
b) monitorizarea respectării prezentului regulament, a altor dispoziţii de drept al Uniunii sau de drept intern referitoare la protecţia datelor şi a politicilor operatorului sau ale persoanei împuternicite de operator în ceea ce priveşte protecţia datelor cu caracter personal, inclusiv alocarea responsabilităţilor şi acţiunile de sensibilizare şi de formare a personalului implicat în operaţiunile de prelucrare, precum şi auditurile aferente;
c) furnizarea de consiliere la cerere în ceea ce priveşte evaluarea impactului asupra protecţiei datelor şi monitorizarea funcţionării acesteia, în conformitate cu articolul 35;
d) cooperarea cu autoritatea de supraveghere;
e) asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă menţionată la articolul 36, precum şi, dacă este cazul, consultarea cu privire la orice altă chestiune.
(2) În îndeplinirea sarcinilor sale, responsabilul cu protecţia datelor ţine seama în mod corespunzător de riscul asociat operaţiunilor de prelucrare, luând în considerare natura, domeniul de aplicare, contextul şi scopurile prelucrării.

Secţiunea 5: Coduri de conduită şi certificare

Art. 40: Coduri de conduită

(1) Statele membre, autorităţile de supraveghere, comitetul şi Comisia încurajează elaborarea de coduri de conduită menite să contribuie la buna aplicare a prezentului regulament, ţinând seama de caracteristicile specifice ale diverselor sectoare de prelucrare şi de nevoile specifice ale microîntreprinderilor şi ale întreprinderilor mici şi mijlocii.
(2) Asociaţiile şi alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori pot pregăti coduri de conduită sau le pot modifica sau extinde pe cele existente, în scopul de a specifica modul de aplicare a prezentului regulament, cum ar fi în ceea ce priveşte:
a) prelucrarea în mod echitabil şi transparent;
b) interesele legitime urmărite de operatori în contexte specifice;
c) colectarea datelor cu caracter personal;
d) pseudonimizarea datelor cu caracter personal;
e) informarea publicului şi a persoanelor vizate;
f) exercitarea drepturilor persoanelor vizate;
g) informarea şi protejarea copiilor şi modalitatea în care trebuie obţinut consimţământul titularilor răspunderii părinteşti asupra copiilor;
h) măsurile şi procedurile menţionate la articolele 24 şi 25 şi măsurile de asigurare a securităţii prelucrării, menţionate la articolul 32;
i) notificarea autorităţilor de supraveghere cu privire la încălcările securităţii datelor cu caracter personal şi informarea persoanelor vizate cu privire la aceste încălcări;

j) transferul de date cu caracter personal către ţări terţe sau organizaţii internaţionale; sau
k) proceduri extrajudiciare şi alte proceduri de soluţionare a litigiilor pentru soluţionarea litigiilor între operatori şi persoanele vizate în ceea ce priveşte prelucrarea, fără a aduce atingere drepturilor persoanelor vizate, în temeiul articolelor 77 şi 79.
.....
Art. 42: Certificare
(1) Statele membre, autorităţile de supraveghere, comitetul şi Comisia încurajează, în special la nivelul Uniunii, instituirea de mecanisme de certificare în domeniul protecţiei datelor, precum şi de sigilii şi mărci în acest domeniu, care să permită demonstrarea faptului că operaţiunile de prelucrare efectuate de operatori şi de persoanele împuternicite de operatori respectă prezentul regulament. Sunt luate în considerare necesităţile specifice ale microîntreprinderilor şi ale întreprinderilor mici şi mijlocii.
(2) Mecanismele de certificare din domeniul protecţiei datelor, sigiliile sau mărcile aprobate în temeiul alineatului (5) din prezentul articol sunt instituite nu numai pentru a fi respectate de operatorii sau de persoanele împuternicite de operatori care fac obiectul prezentului regulament, ci şi pentru a demonstra existenţa unor garanţii adecvate oferite de operatorii sau de persoanele împuternicite de operatori care nu fac obiectul prezentului regulament, în temeiul articolului 3, în cadrul transferurilor de date cu caracter personal către ţări terţe sau organizaţii internaţionale în condiţiile menţionate la articolul 46 alineatul (2) litera (f). Aceşti operatori sau persoane împuternicite de operatori îşi asumă angajamente cu caracter obligatoriu şi executoriu, prin intermediul unor instrumente contractuale sau al altor instrumente obligatorii din punct de vedere juridic, în scopul aplicării garanţiilor adecvate respective, inclusiv cu privire la drepturile persoanelor vizate.
(3) Certificarea este voluntară şi disponibilă prin intermediul unui proces transparent.
(4) Certificarea în conformitate cu prezentul articol nu reduce responsabilitatea operatorului sau a persoanei împuternicite de operator de a respecta prezentul regulament şi nu aduce atingere sarcinilor şi competenţelor autorităţilor de supraveghere care sunt competente în temeiul articolului 55 sau 56.
(5) Organismele de certificare menţionate la articolul 43 sau autoritatea de supraveghere competentă emit o certificare în temeiul prezentului articol, pe baza criteriilor aprobate de către autoritatea de supraveghere competentă respectivă în temeiul articolului 58 alineatul (3), sau de către comitet în temeiul articolului 63. În cazul în care criteriile sunt aprobate de comitet, aceasta poate duce la o certificare comună, şi anume sigiliul european privind protecţia datelor.
(6) Operatorul sau persoana împuternicită de operator care supune activităţile sale de prelucrare mecanismului de certificare oferă organismului de certificare menţionat la articolul 43 sau, după caz, autorităţii de supraveghere competente, toate informaţiile necesare pentru desfăşurarea procedurii de certificare, precum şi accesul la activităţile de prelucrare respective.
(7) Certificarea este eliberată unui operator sau unei persoane împuternicite de operator pentru o perioadă maximă de trei ani şi poate fi reînnoită în aceleaşi condiţii, cu condiţia ca cerinţele relevante să fie îndeplinite în continuare. Certificarea este retrasă, după caz, de către organismele de certificare menţionate la articolul 43 sau de către autoritatea de supraveghere competentă în cazul în care nu mai sunt îndeplinite cerinţele pentru certificare.
(8) Comitetul regrupează toate mecanismele de certificare şi sigiliile şi mărcile de protecţie a datelor într-un registru şi le pune la dispoziţia publicului prin orice mijloc corespunzător.
.....

CAPITOLUL VIII: Căi de atac, răspundere şi sancţiuni
Art. 77: 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 special în statul membru în care îşi are reşedinţa obişnuită, în care se află locul său de

muncă sau în care a avut loc presupusa încălcare, în cazul în care consideră că prelucrarea datelor cu caracter personal care o vizează încalcă prezentul regulament.
(2) Autoritatea de supraveghere la care s-a depus plângerea informează reclamantul cu privire la evoluţia şi rezultatul plângerii, inclusiv posibilitatea de a exercita o cale de atac judiciară în temeiul articolului 78.
.....
Art. 82: Dreptul la despăgubiri şi răspunderea
(1) Orice persoană care a suferit un prejudiciu materiale sau moral ca urmare a unei încălcări a prezentului regulament are dreptul să obţină despăgubiri de la operator sau de la persoana împuternicită de operator pentru prejudiciul suferit.
(2) Orice operator implicat în operaţiunile de prelucrare este răspunzător pentru prejudiciul cauzat de operaţiunile sale de prelucrare care încalcă prezentul regulament. Persoana împuternicită de operator este răspunzătoare pentru prejudiciul cauzat de prelucrare numai în cazul în care nu a respectat obligaţiile din prezentul regulament care revin în mod specific persoanelor împuternicite de operator sau a acţionat în afara sau în contradicţie cu instrucţiunile legale ale operatorului.
(3) Operatorul sau persoana împuternicită de operator este exonerat(ă) de răspundere în temeiul alineatului (2) dacă dovedeşte că nu este răspunzător (răspunzătoare) în niciun fel pentru evenimentul care a cauzat prejudiciul.
.....
Art. 83: Condiţii generale pentru impunerea amenzilor administrative
(1) Fiecare autoritate de supraveghere asigură faptul că impunerea unor amenzi administrative în conformitate cu prezentul articol pentru încălcările prezentului regulament menţionate la alineatele (4), (5) şi, (6) este, în fiecare caz, eficace, proporţională şi disuasivă.
(2) În funcţie de circumstanţele fiecărui caz în parte, amenzile administrative sunt impuse în completarea sau în locul măsurilor menţionate la articolul 58 alineatul (2) literele (a)-(h) şi (j). Atunci când se ia decizia dacă să se impună o amendă administrativă şi decizia cu privire la valoarea amenzii administrative în fiecare caz în parte, se acordă atenţia cuvenită următoarelor aspecte:
a) natura, gravitatea şi durata încălcării, ţinându-se seama de natura, domeniul de aplicare sau scopul prelucrării în cauză, precum şi de numărul persoanelor vizate afectate şi de nivelul prejudiciilor suferite de acestea;
b) dacă încălcarea a fost comisă intenţionat sau din neglijenţă;
c) orice acţiuni întreprinse de operator sau de persoana împuternicită de operator pentru a reduce prejudiciul suferit de persoana vizată;
d) gradul de responsabilitate al operatorului sau al persoanei împuternicite de operator ţinându-se seama de măsurile tehnice şi organizatorice implementate de aceştia în temeiul articolelor 25 şi 32;
e) eventualele încălcări anterioare relevante comise de operator sau de persoana împuternicită de operator;
f) gradul de cooperare cu autoritatea de supraveghere pentru a remedia încălcarea şi a atenua posibilele efecte negative ale încălcării;
g) categoriile de date cu caracter personal afectate de încălcare;
h) modul în care încălcarea a fost adusă la cunoştinţa autorităţii de supraveghere, în special dacă şi în ce măsură operatorul sau persoana împuternicită de operator a notificat încălcarea;
i) în cazul în care măsurile menţionate la articolul 58 alineatul (2) au fost dispuse anterior împotriva operatorului sau persoanei împuternicite de operator în cauză cu privire la acelaşi obiect, respectarea respectivelor măsuri;
j) aderarea la coduri de conduită aprobate, în conformitate cu articolul 40, sau la mecanisme de certificare aprobate, în conformitate cu articolul 42; şi
k) orice alt factor agravant sau atenuant aplicabil circumstanţelor cazului, cum ar fi beneficiile financiare dobândite sau pierderile evitate în mod direct sau indirect de pe urma încălcării.

(3) În cazul în care un operator sau o persoană împuternicită de operator încalcă în mod intenţionat sau din neglijenţă, pentru aceeaşi operaţiune de prelucrare sau pentru operaţiuni de prelucrare conexe, mai multe dispoziţii din prezentul regulament, cuantumul total al amenzii administrative nu poate depăşi suma prevăzută pentru cea mai gravă încălcare.
(4) Pentru încălcările dispoziţiilor următoare, în conformitate cu alineatul (2), se aplică amenzi administrative de până la 10.000.000 EUR sau, în cazul unei întreprinderi, de până la 2 % din cifra de afaceri mondială totală anuală corespunzătoare exerciţiului financiar anterior, luându-se în calcul cea mai mare valoare:
a) obligaţiile operatorului şi ale persoanei împuternicite de operator în conformitate cu articolele 8, 11, 25-39, 42 şi 43;
b) obligaţiile organismului de certificare în conformitate cu articolele 42 şi 43;
c) obligaţiile organismului de monitorizare în conformitate cu articolul 41 alineatul (4).
(5) Pentru încălcările dispoziţiilor următoare, în conformitate cu alineatul (2), se aplică amenzi administrative de până la 20.000.000 EUR sau, în cazul unei întreprinderi, de până la 4 % din cifra de afaceri mondială totală anuală corespunzătoare exerciţiului financiar anterior, luându-se în calcul cea mai mare valoare:
a) principiile de bază pentru prelucrare, inclusiv condiţiile privind consimţământul, în conformitate cu articolele 5, 6, 7 şi 9;
b) drepturile persoanelor vizate în conformitate cu articolele 12-22;
c) transferurile de date cu caracter personal către un destinatar dintr-o ţară terţă sau o organizaţie internaţională, în conformitate cu articolele 44-49;
d) orice obligaţii în temeiul legislaţiei naţionale adoptate în temeiul capitolului IX;
e) nerespectarea unui ordin sau a unei limitări temporare sau definitive asupra prelucrării, sau a suspendării fluxurilor de date, emisă de către autoritatea de supraveghere în temeiul articolului 58 alineatul (2), sau neacordarea accesului, încălcând articolul 58 alineatul (1).
(6) Pentru încălcarea unui ordin emis de autoritatea de supraveghere în conformitate cu articolul 58 alineatul (2) se aplică, în conformitate cu alineatul (2) din prezentul articol, amenzi administrative de până la 20.000.000 EUR sau, în cazul unei întreprinderi, de până la 4 % din cifra de afaceri mondială totală anuală corespunzătoare exerciţiului financiar anterior, luându-se în calcul cea mai mare valoare.
(7) Fără a aduce atingere competenţelor corective ale autorităţilor de supraveghere menţionate la articolul 58 alineatul (2), fiecare stat membru poate prevedea norme prin care să se stabilească dacă şi în ce măsură pot fi impuse amenzi administrative autorităţilor publice şi organismelor publice stabilite în statul membru respectiv.
.....

Art. 84: Sancţiuni

(1) Statele membre stabilesc normele privind alte sancţiuni aplicabile în caz de încălcare a prezentului regulament, în special pentru încălcări care nu fac obiectul unor amenzi administrative în temeiul articolului 83, şi iau toate măsurile necesare pentru a garanta faptul că acestea sunt puse în aplicare. Sancţiunile respective sunt eficace, proporţionale şi disuasive.
(2) Fiecare stat membru informează Comisia cu privire la dispoziţiile de drept intern pe care le adoptă în temeiul alineatului (1) până la 25 mai 2018, precum şi, fără întârziere, cu privire la orice modificare ulterioară a acestora.

Art. 86: Prelucrarea şi accesul public la documente oficiale

Datele cu caracter personal din documentele oficiale deţinute de o autoritate publică sau de un organism public sau privat pentru îndeplinirea unei sarcini care serveşte interesului public pot fi divulgate de autoritatea sau organismul respectiv în conformitate cu dreptul Uniunii sau cu dreptul intern sub incidenţa căruia intră autoritatea sau organismul, pentru a stabili un echilibru între accesul public la documente oficiale şi dreptul la protecţia datelor cu caracter personal în temeiul prezentului regulament.
.....

Art. 88: Prelucrarea în contextul ocupării unui loc de muncă

(1) Prin lege sau prin acorduri colective, statele membre pot prevedea norme mai detaliate pentru a asigura protecţia drepturilor şi a libertăţilor cu privire la prelucrarea datelor cu caracter personal ale angajaţilor în contextul ocupării unui loc de muncă, în special în scopul recrutării, al îndeplinirii clauzelor contractului de muncă, inclusiv descărcarea de obligaţiile stabilite prin lege sau prin acorduri colective, al gestionării, planificării şi organizării muncii, al egalităţii şi diversităţii la locul de muncă, al asigurării sănătăţii şi securităţii la locul de muncă, al protejării proprietăţii angajatorului sau a clientului, precum şi în scopul exercitării şi beneficierii, în mod individual sau colectiv, de drepturile şi beneficiile legate de ocuparea unui loc de muncă, precum şi pentru încetarea raporturilor de muncă.

(2) Aceste norme includ măsuri corespunzătoare şi specifice pentru garantarea demnităţii umane, a intereselor legitime şi a drepturilor fundamentale ale persoanelor vizate, în special în ceea ce priveşte transparenţa prelucrării, transferul de date cu caracter personal în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună şi sistemele de monitorizare la locul de muncă.

.....

Art. 90: Obligaţii privind păstrarea confidenţialităţii

(1) Statele membre pot adopta norme specifice pentru a stabili competenţele autorităţilor de supraveghere, prevăzute la articolul 58 alineatul (1) literele (e) şi (f), în legătură cu operatori sau cu persoane împuternicite de operatori care, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul normelor stabilite de organismele naţionale competente, au obligaţia de a păstra secretul profesional sau alte obligaţii echivalente de confidenţialitate, în cazul în care acest lucru este necesar şi proporţional pentru a stabili un echilibru între dreptul la protecţia datelor cu caracter personal şi obligaţia păstrării confidenţialităţii. Respectivele norme se aplică doar în ceea ce priveşte datele cu caracter personal pe care operatorul sau persoana împuternicită de operator le-a primit în urma sau în contextul unei activităţi care intră sub incidenţa acestei obligaţii de păstrare a confidenţialităţii.

.....

CAPITOLUL XI: Dispoziţii finale

Art. 94: Abrogarea Directivei 95/46/CE

(1) Decizia **95/46/CE** se abrogă cu efect de la 25 mai 2018.

.....

Art. 99: Intrare în vigoare şi aplicare

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

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

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

-****-

Adoptat la Bruxelles, 27 aprilie 2016.

Pentru Parlamentul European

Preşedintele

M. SCHULZ

Pentru Consiliu

Preşedintele

J.A. HENNIS-PLASSCHAERT

Publicat în Jurnalul Oficial cu numărul 119L din data de 4 mai 2016

---------- // ----------

Pentru conformitate, cu prevederile legale,

Directorul Şcolii CONFIDENT

Col. (r) Vasile CIREŞ