

Ghid privind Responsabilul cu protecția datelor (‘DPOs’)

Adoptat în data de 13 decembrie 2016

Revizuit și adoptat în data de 5 aprilie 2017

Acest grup de lucru a fost creat în temeiul articolului 29 din Directiva 95/46/CE și este un organ consultativ european independent care se ocupă cu protecția și confidențialitatea datelor. Sarcinile sale sunt descrise la articolul 30 din Directiva 95/46/CE și la articolul 15 din Directiva 2002/58/CE.

Secretariatul este asigurat de Direcția C (Drepturi fundamentale și cetățenia Uniunii) din cadrul Comisiei Europene, Direcția Generală Justiție și Consumatori, B- 1049 Bruxelles, Belgia, biroul MO-59 05/35.

Adresa web: http://ec.europa.eu/justice/data-protection/index_en.htm

**GRUPUL DE LUCRU PENTRU PROTECȚIA PERSOANELOR ÎN CEEA CE PRIVEȘTE
PRELUCRAREA DATELOR CU CARACTER PERSONAL**

instituit prin Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995,

având în vedere articolele 29 și 30 din directiva respectivă,

având în vedere regulamentul său de procedură,

ADOPTĂ PREZENTUL GHID:

Cuprins

1	Introducere	4
2	Desemnarea responsabilului cu protecția datelor	5
2.1.	Desemnare obligatorie	5
2.1.1	„Autoritate publică sau organism public”	6
2.1.2	„Activități principale”	6
2.1.3	„Pe scară largă”	7
2.1.4	„Monitorizarea periodică și sistematică”	8
2.1.5	Categoriile speciale de date cu caracter personal referitoare la condamnări penale și infracțiuni	9
2.2.	Responsabilul cu protecția datelor al persoanei împuternicite	9
2.3.	Desemnarea unui singur responsabil cu protecția datelor pentru mai multe organizații	10
2.4.	Accesibilitatea și localizarea responsabilului cu protecția datelor	10
2.5.	Expertiza și abilitățile responsabilului cu protecția datelor	11
2.6.	Publicarea și comunicarea datelor de contact ale responsabilului cu protecția datelor	12
3	Poziția responsabilului cu protecția datelor	13
3.1.	Implicarea responsabilului cu protecția datelor în toate aspectele referitoare la protecția datelor cu caracter personal	13
3.2.	Resursele necesare	13
3.3.	Instrucțiuni și „îndeplinirea atribuțiilor și sarcinilor în mod independent”	14
3.4.	Demiterea sau sancționarea DPO pentru îndeplinirea sarcinilor sale	15
3.5.	Conflict de interese	16
4	Sarcinile DPO	16
4.1.	Monitorizarea respectării RGPD	16
4.2.	Rolul DPO în evaluarea impactului operațiilor de prelucrare	17
4.3.	Cooperarea cu autoritatea de supraveghere și asumarea rolului de punct de contact	18
4.4.	Abordarea bazată pe risc	18
4.5.	Rolul DPO în păstrarea evidenței	18
5	Anexă – Ghid DPO: Ce trebuie să știți	20
	Desemnarea DPO	20
1	Ce organizații ce trebuie să numească un DPO?	20
2	Ce înseamnă „activitate principală”?	20
3	Ce înseamnă „pe scară largă”	21
4	Ce înseamnă „monitorizare periodică și sistematică”?	21
5	Mai multe organizații pot numi un DPO comun? Dacă da, în ce condiții?	22
6	Unde poate fi localizat DPO?	22
7	Există posibilitatea desemnării unui DPO extern?	23
8	Care sunt calitățile profesionale pe care trebuie să le posedă un DPO?	23
	Poziția DPO	24
9	Care sunt resursele ce trebuie prevăzute de operator sau persoana împuternicită pentru DPO?	24
10	Care sunt garanțiile ce-i permit DPO să-și îndeplinească sarcinile în mod independent? Ce înseamnă „conflict de interese”?	24
	Sacini DPO	25
11	Ce înseamnă „monitorizarea conformității”?	25
12	DPO este personal responsabil pentru nerespectarea cerințelor de protecție a datelor?	25
13	Care este rolul DPO în legătură cu DPIA și păstrarea evidenței operațiunilor de prelucrare?	25

1 Introducere

Regulamentul General privind Protecția Datelor (RGPD)¹ 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 DPO². 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.

Conceptul de DPO nu este nou. Cu toate că Directiva 95/46/CE³ nu impune niciunei organizații să numească un DPO, această practică de numire a unui DPO s-a dezvoltat, de-a lungul anilor, în mai multe state membre.

Anterior adoptării RGPD, WP29 a susținut că DPO reprezintă un punct important al responsabilității și că numirea unui DPO poate facilita respectarea și, în plus, poate reprezenta un avantaj competitiv pentru companii⁴. Pe lângă facilitarea respectării prin punerea în aplicare a instrumentelor de responsabilitate (cum ar fi facilitarea evaluărilor impactului asupra protecției datelor și efectuarea sau facilitarea auditurilor), 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 responsabil 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 dispozițiile 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 atribuțiilor 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.

¹ Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul General privind Protecția Datelor) (MO L 119, 4.5.2016). RGPD este relevant și pentru ZEE și va fi aplicabil după inserarea acestuia în Acordul ZEE.

² Numirea unui DPO este obligatorie pentru autoritățile competente potrivit art. 32 din Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmării penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Decizie-Cadru 2008/977/JAI (MO L 119, 4.5.2016, p. 89–131) și legislația națională de implementare. În timp ce acest ghid se concentrează pe DPO potrivit RGPD, acesta este de asemenea relevant și în situația DPO potrivit Directivei 2016/680, în ceea ce privește dispozițiile similare.

³ Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (MO L 281, 23.11.1995, p. 31).

⁴ A se vedea http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf

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. WP29 va monitoriza punerea în aplicare a acestor orientări și le va completa cu detalii suplimentare, după caz.

2 Desemnarea DPO

2.1. Desemnarea obligatorie

Art. 37(1) din RGPD solicită desemnarea DPA în trei situații specifice⁵:

- a) atunci când prelucrarea este efectuată de o autoritate publică sau un organism public⁶;
- b) atunci când activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în operațiuni de prelucrarea 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 date⁷ sau⁸ a unor categorii de date cu caracter personal privind condamnări penale și infracțiuni⁹.

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 relevanți¹⁰. 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,

⁵ Rețineți faptul că potrivit art. 37(4), dreptul Uniunii sau dreptul intern poate impune numirea unui DPO și în alte situații.

⁶ Cu excepția instanțelor care acționează în exercițiul funcției. A se vedea art. 32 din Directiva (UE) 2016/680.

⁷ 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..

⁸ Art. 37(1)c) folosește cuvântul „și”. A se vedea Secțiunea 2.1.5 de mai jos pentru explicația privind folosirea cuvântului „sau” în locul „și”.

⁹ Art. 10.

¹⁰ A se vedea art. 24(1).

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)¹¹.

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 public¹². În astfel de cazuri, desemnarea unui DPO este obligatorie.

O sarcină publică poate fi efectuată, iar o autoritate publică poate fi exercitată¹³ 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 prelucrate 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

¹¹ Acest 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 independență și, dacă nu sunt respectate, nu pot fi considerați sau numiți DPO.

¹² A se vedea, de exemplu definiția pentru „organism din sectorul public” și „organism de drept public” în art. 2(1) și (2) din Directiva 2003/98/CE a Parlamentului European și a Consiliului din 17 noiembrie 2003 privind reutilizarea informațiilor din sectorul public (MO L 345, 31.12.2003, p. 90).

¹³ Art. 6(1)e).

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 organizații 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 prelucrarea pe scară largă, deși Considerentul 91 oferă unele orientări¹⁴.

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

¹⁴ Potrivit considerentului, ar putea fi incluse, în special, „operațiunile de prelucrare pe scară largă care au drept obiectiv prelucrarea unui volum considerabil de date cu caracter personal la nivel regional, național sau supranațional și care ar putea afecta un număr mare de persoane vizate 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.

- 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 de 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 și 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 24¹⁵ și include în mod clar toate formele de urmărirea și profilarea pe Internet, inclusiv în scop de publicitate comportamentală.

Cu toate acestea, noțiunea de monitorizare nu este restricționată în mediul online, iar urmărirea online ar trebui să fie considerată doar ca un exemplu de monitorizare a comportamentului persoanelor vizate¹⁶.

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

¹⁵ „Pentru 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, comportamentele și atitudinile acesteia”.

¹⁶ Rețineți că prin conținutul 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

- 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 Categoriile 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 infracțiuni 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 operatorilor¹⁷ cât și persoanelor împuternicite de operator¹⁸ 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 persoane împuternicite de operator a cărei 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.

¹⁷ 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.

¹⁸ 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.

- 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 vizate¹⁹, autoritatea de supraveghere²⁰, 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”²¹.

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.²²

El sau ea, cu ajutorul unei echipe, dacă este necesar, trebuie să fie în măsură să comunice eficient cu persoanele vizate²³ și să coopereze²⁴ cu autoritățile de supraveghere implicate. Acest lucru înseamnă, de asemenea, 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.

Potrivit art. 37(3), DPO unic poate fi desemnat pentru mai multe autorități sau organisme publice, luând în considerare structura organizatorică și dimensiunea 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 faptului 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.

¹⁹ 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”.

²⁰ 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”.

²¹ Art. 39(1)a).

²² A se vedea Secțiunea 2.6 de mai jos.

²³ Art. 12(1): „Operatorul adoptă măsuri adecvate pentru a furniza persoanei vizate orice informații menționate la art. 13 și 14 și orice comunicări potrivit art. 15-22 și 34 referitoare la prelucrare, într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, folosind un limbaj clar și simplu, în special pentru orice informații adresate în mod specific unui copil”.

²⁴ Art. 39(1)d): „cooperarea cu autoritatea de supraveghere”

Cu toate acestea, nu poate fi exclus faptul că, în anumite situații în care operatorul sau persoana împuternicită de operator nu are sediul în UE²⁵, un DPO își poate îndeplini sarcinile într-un mod mai eficient dacă este localizat în afara 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 datelor²⁶, drepturile persoanelor vizate²⁷, asigurarea protecției datelor începând cu

²⁵ A se vedea art. 3 din RGPD privind domeniul de aplicare teritorial.

²⁶ Capitolul II.

²⁷ Capitolul III.

momentul conceperii și în mod implicit²⁸, înregistrarea activităților de prelucrare²⁹, securitatea prelucrării³⁰, precum și notificarea și comunicarea încălcărilor de securitate.³¹

- **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 poate 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.³²

²⁸ Art. 25.

²⁹ Art. 30.

³⁰ Art. 32.

³¹ Art. 33 și 34.

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.³³ 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

³² 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).

³³ Art. 35(2).

operațiunilor de prelucrare, și pentru menținerea cunoștințelor sale de specialitate". Trebuie avute în vedere, în special, următoarele aspecte:

- Sprijin 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 (sediul, 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 participarea 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 și 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.³⁴ 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 protecția a datelor.

Sancțiunile sunt interzise potrivit RGPR numai în cazul în care acestea sunt impuse ca urmare a îndeplinirea 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, dreptul 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).

³⁴ Art. 5(2).

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 a 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 personale. 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.

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 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 identifica operațiunilor de prelucrare
- să analizeze și să verifice conformitatea operațiunilor 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 organizatorice 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 protecției 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 monitorizeze funcționarea acesteia, în conformitate cu art. 35”.

WP29 recomandă ca operatorul să solicite avizul DPO în legătură cu următoarele aspecte, printre care³⁵:

- 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 avizul³⁶.

³⁵ 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.

³⁶ Art. 24(1) prevede că „ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul Regulament. Respectivul 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, inclusive consultarea prealabilă menționată la art. 36, precum și, dacă este cazul, consultarea cu privire la orice altă chestiune”.

Aceste sarcini se referă rolul de „persoană care facilitează” al DPO menționat în cuprinsul intruducerii acestui Ghid. DPO acționează ca punct de contact 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 Uniunii sau cu dreptul intern (art. 38(5)). Cu toate acestea, obligația secretului/confidențialității nu interzice 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 fac 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 „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.³⁷

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. 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.

În orice caz, evidența păstrată potrivit art. 30 trebuie văzută și ca un instrument care permite operatorului și autorității de supraveghere, la cerere, să aibă o imagine de ansamblu asupra tuturor operațiunilor de prelucrare a datelor cu caracter personal efectuate de o organizație. Astfel, este o condiție prealabilă pentru conformitate și, ca atare, o măsură eficientă de responsabilizare.

³⁷ Art. 24(1)d), Regulamentul (CE) 45/2001.

5 ANEXĂ – GHID DPO: CE TREBUIE SĂ ȘTIȚI

Obiectivul prezentei anexe 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.

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 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 organizații 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 prelucrarea pe scară largă. 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 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 de 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

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 profilarea pe Internet, inclusiv în scop de publicitate comportamentală. Cu toate acestea, noțiunea de monitorizare nu este restricționată 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? Dacă 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 sarcinile 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 dimensiunea 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 faptului 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

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:

- sprijin 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 (sediul, 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 conflict 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 personale. 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

11 Ce înseamnă „monitorizarea conformității”?

Ca parte a acestor sarcini de monitorizare a conformității, DPO poate, în special:

- să colecteze informații pentru a identifica operațiunilor de prelucrare
- să analizeze și să verifice conformitatea operațiunilor 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 organizatorice 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

Adoptat la Bruxelles, la 13 decembrie 2016

Pentru Grupul de Lucru,

Președintele

Isabelle FARQUE-PIERROTIN

Revizuit și adoptat la 5 aprilie 2017

Pentru Grupul de Lucru,

Președintele

Isabelle FARQUE-PIERROTIN