GHID

RESPONSABILUL CU PROTECTIA DATELOR (DPO)

avocatoo | powered by LegalUp

Ofițerul responsabil cu protecția datelor

Rezumat

- GDPR introduce obligația pentru de a desemna un ofițer responsabil cu protecția datelor (DPO) dacă: (a) sunteți o autoritate publică sau un organism public sau (b) dacă desfășurați anumite tipuri de activități de prelucrare.
- DPO vă ajută să monitorizați conformarea intern cu GDPR, vă informează și să sfătuiește cu privire la obligațiile privind protecția datelor personale, oferă sfaturi cu privire la Evaluările de Impact (DPIA) si acționează ca persoană de contact pentru persoanele vizate și autoritatea de supraveghere.
- DPO trebuie să fie independent, un expert în protecția datelor, să dispună de resurse adecvate și să raporteze la cel mai înalt nivel de conducere.
- Un DPO poate fi un angajat existent sau poate fi numit extern.
- Un DPO poate fi și o persoană juridică, caz în care trebuie desemnată o persoană din partea respectivei societăți.
- În unele cazuri, mai multe organizații pot numi un singur DPO între acestea (*în special când vorbim despre grupurile de firme*).
- DPO vă poate ajuta să demonstrați conformitatea cu GDPR.

1. Aspecte de bifat

1.1. Numirea unui DPO

☐ Suntem o autoritate sau un organism public și am desemnat un DPO (cu excepția cazului în care suntem o instanță care acționează în exercițiul funcției noastre jurisdicționale).

☐ Nu suntem o autoritate sau un organism public, dar știm dacă natura activităților noastre de prelucrare necesită sau nu numirea unui DPO.

☐ Am desemnat un DPO pe baza calităților profesionale și a cunoștințelor de specialitate privind legislația și jurisprudența privind protecția datelor pe care le deține.

☐ Noi nu avem obligația de a desemna un DPO în conformitate cu GDPR, dar am hotărât să o facem în mod voluntar. Înțelegem că se aplică aceleași sarcini și responsabilități dacă ar fi fost necesar să numim un DPO.

1.2. Poziția unui DPO

☐ DPO-ul nostru raportează direct la cel mai înalt nivel de conducere și are independența necesară pentru a-și îndeplini sarcinile.

☐ Implicăm DPO-ul, în timp util, în toate problemele legate de protecția datelor cu caracter personal.

☐ DPO-ul nostru dispune de resurse suficiente pentru a-și putea îndeplini sarcinile.

☐ Nu sancționăm DPO pentru îndeplinirea sarcinilor.

☐ Ne asigurăm că orice alte sarcini sau îndatoriri pe care le atribuim DPO nu conduc la un conflict de interese cu rolul de DPO.

1.3. Sarcinile unui DPO

☐ DPO-ul nostru are sarcina de a monitoriza conformitatea cu GDPR și alte legi privind protecția datelor, politicile noastre de protecție a datelor, de informare și de audit.

☐ Vom ține cont de sfatul DPO-ului nostru și de informațiile pe care le furnizează cu privire la obligațiile noastre privind protecția datelor.

☐ Atunci când realizăm o DPIA, solicităm consultanță din partea DPO care monitorizează și procesul.

☐ DPO-ul nostru acționează ca o persoană de contact în relația cu ANSPDCP. Acesta colaborează cu ANSPDCP inclusiv în consultările prealabile prevăzute de Articolul 36 din Regulament, precum și în orice altă consultare.

☐ Atunci când își îndeplinește sarcinile, DPO-ul nostru are în vedere riscurile asociate operațiunilor de prelucrare a datelor și ia în considerare natura, scopul, contextul și scopurile prelucrării.

1.4. Accesibilitatea DPO

☐ DPO-ul nostru poate fi ușor contactat de angajați, persoane vizate și ANSPDCP.

☐ Am publicat datele de contact ale DPO-ului și le-am comunicat către ANSPDCP.

2. Pe scurt

2.1. Trebuie să numim un DPO?

Conform GDPR, trebuie numit un DPO atunci când:

(a) sunteți o autoritate sau un organism public, cu excepția instanțelor care acționează în exercițiul funcției lor jurisdicționale;
(b) activitățile principale de prelucrare necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă (*de exemplu*, monitorizare constantă pe online); sau
(c) activitățile principale constau în prelucrarea la scară largă a unor categorii speciale de date sau date referitoare la condamnări penale și infracțiuni.

Acest lucru se aplică atât operatorilor, cât și persoanelor împuternicite. Puteți desemna un DPO dacă doriți, chiar dacă nu vi se cere. Dacă decideți să desemnați în mod voluntar un DPO, trebuie să știți că aceleași cerințe ale funcției și ale sarcinilor se aplică dacă numirea a fost obligatorie.

! ANSPDCP recomandă numirea unui DPO în toate cazurile de prelucrare a datelor, chiar și atunci când nu este obligatoriu conform Regulamentului.

Indiferent dacă GDPR vă obligă să desemnați un DPO, trebuie să vă asigurați că organizația dvs. dispune de personal și de resurse suficiente pentru a-și îndeplini obligațiile în temeiul GDPR. Cu toate acestea, un DPO vă poate ajuta să operați conform cadrului legal prin consilierea și sprijinirea monitorizării conformității. În acest fel, se poate considera că un DPO joacă un rol-cheie în structura organizației pentru protecția datelor și contribuie la îmbunătățirea responsabilității în acest domeniu.

Dacă decideți că nu este necesar să desemnați un RPD, fie în mod voluntar, fie pentru că nu îndepliniți criteriile de mai sus, este o idee bună să înregistrați această decizie pentru a demonstra respectarea principiului responsabilității.

2.2. Care sunt ”activitățile principale”?

Pe lângă condiția de a fi autoritate sau organism public, celelalte condiții în care este necesară numirea unui DPO sunt:

- activitățile principale constau în activități de prelucrare care, datorită naturii, scopului și scopurilor lor, necesită o monitorizare regulată și sistematică a persoanelor pe scară largă; sau
- activitățile principale constau în prelucrarea pe scară largă a datelor din categoriile speciale sau în datele privind condamnările penale și infracțiunile.

Activitățile de bază sunt principalele activități ale organizației. Deci, dacă aveți nevoie să prelucrați date personale pentru a vă atinge obiectivele cheie, aceasta este o activitate de bază. Acest lucru este diferit de prelucrarea datelor cu caracter personal în alte scopuri secundare, ceea ce poate fi ceva pe care îl faceți tot timpul (de exemplu, salarizare sau informații privind resursele umane), dar care nu face parte din realizarea obiectivelor dvs. principale.

> ☞ ***Exemplu:***
>
> Pentru majoritatea organizațiilor, prelucrarea datelor cu caracter personal în scopuri de resurse umane va constitui o funcție secundară pentru principalele lor activități de afaceri și astfel nu va face parte din activitățile lor principale.
>
> Cu toate acestea, un furnizor de servicii de resurse umane procesează în mod necesar datele personale, ca parte a activităților sale principale, pentru a oferi servicii de resurse umane pentru organizațiile clienților săi. În același timp, va procesa, de asemenea, informații privind resursele umane pentru angajații săi, care vor fi considerate ca o funcție secundară și nu fac parte din activitățile sale principale.

2.3. Ce înseamnă "monitorizarea regulată și sistematică a persoanelor vizate la scară largă"?

Citește mai în amănunt despre prelucrarea pe scară largă și numirea unui DPO aici.

Există două elemente cheie ale acestei condiții care necesită numirea unui DPO: (a) *monitorizarea regulată și sistematică* și (b) *scara largă a prelucrării*. Deși GDPR nu definește "monitorizarea regulată și sistematică" sau "pe scară largă", Grupul de Lucru pentru Articolul 29 a furnizat o serie de orientări cu privire la acești termeni în orientările sale privind DPO.

Monitorizarea periodică și sistematică a persoanelor vizate include toate formele de urmărire și profilare, atât online, cât și offline. Un exemplu în acest sens este în sensul publicității comportamentale (*ie.* behavioural advertising).

Atunci când se stabilește dacă procesarea se face la scară largă, liniile directoare afirmă că trebuie să țineți cont de următorii factori:

- numărul persoanelor vizate în cauză;
- volumul de date cu caracter personal prelucrate;
- gama elementelor diferite de prelucrat;
- extinderea geografică a activității; și
- durata sau permanența activității de prelucrare.

> ☞ ***Exemplu:***
>
> Un site web al unui retailer utilizează algoritmi pentru a monitoriza căutările și achizițiile utilizatorilor săi și, pe baza acestor informații, le oferă recomandări. Întrucât acest lucru are loc în mod continuu și în conformitate cu criterii predefinite, acesta poate fi considerat ca o monitorizare regulată și sistematică a persoanelor vizate la scară largă.

2.4. Ce înseamnă prelucrarea pe scară largă a unor categorii speciale de date sau a unor date cu caracter personal privind condamnări penale și infracțiuni?

Prelucrarea datelor din categoriile speciale sau a condamnărilor penale sau a infracțiunilor reprezintă un risc mai mare decât alte date cu caracter personal. Deci, atunci când procesați acest tip de date pe scară largă, sunteți obligat să desemnați un DPO, care poate oferi mai multă supraveghere. Din nou, factorii relevanți pentru prelucrarea pe scară largă pot include:

- numărul persoanelor vizate în cauză;
- volumul de date cu caracter personal prelucrate;
- gama elementelor diferite de prelucrat;
- extinderea geografică a activității; și
- durata sau permanența activității de prelucrare.

> ☞ ***Exemplu:***
>
> O companie de asigurări de sănătate prelucrează o gamă largă de date personale despre un număr mare de persoane, inclusiv afecțiuni medicale și alte informații de sănătate. Aceasta poate fi considerată ca o prelucrare a datelor speciale pe scară largă.

2.5. Ce calități profesionale ar trebui să aibă un DPO?

GDPR spune că ar trebui să desemnăm un DPO pe baza calităților profesionale și, în special, a experienței și cunoștințelor de specialitate în domeniul protecției datelor.

Nu specifică acreditările exacte pe care ar trebui ca acesta să le aibă, dar spune că acest lucru ar trebui să fie proporțional cu tipul de prelucrare efectuat, ținând cont și de nivelul de protecție pe care îl au datele personale.

Deci, în cazul în care prelucrarea datelor cu caracter personal este deosebit de complexă sau riscantă, cunoștințele și abilitățile unui DPO trebuie să fie suficient de avansate pentru a asigura o supraveghere eficientă.

Ar fi de preferat (și chiar un avantaj) ca DPO-ul să aibă, de asemenea, o bună cunoaștere a industriei sau sectorului din care face parte organizația, precum și nevoile organizației de protecție a datelor și activitățile de prelucrare incidente.

2.6. Ce sarcini are un DPO?

Sarcinile principale ale DPO-ului sunt regăsite în Articolul 39 din Regulament, și anume:

(a) **informarea și consilierea operatorului, sau a persoanei împuternicite de operator**, precum și a angajaților care se ocupă de prelucrare cu privire la obligațiile care le revin în temeiul prezentului regulament și al altor dispoziții de drept al Uniunii sau drept intern referitoare la protecția datelor;
(b) **monitorizarea respectării Regulamentului**, a altor dispoziții de drept al Uniunii sau de drept intern referitoare la protecția datelor și a politicilor operatorului sau ale persoanei împuternicite de operator în ceea ce privește protecția datelor cu caracter personal, inclusiv alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;
(c) **furnizarea de consiliere la cerere** în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia;
(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, precum și, dacă este cazul, consultarea cu privire la orice altă chestiune.

! Este important de reținut că sarcinile DPO acoperă toate activitățile de prelucrare a datelor cu caracter personal, nu doar cele care necesită numirea lor în temeiul articolului 37 alineatul (1) din Regulament.

- În îndeplinirea sarcinilor lor, un DPO trebuie să ia în considerare riscul asociat prelucrării pe care o întreprinde organizația. Acesta trebuie să aibă în vedere natura, scopul, contextul prelucrării.
- DPO ar trebui să acorde prioritate și să se concentreze asupra activităților mai riscante, de exemplu în cazul în care sunt prelucrate date din categorii speciale sau unde impactul potențial asupra persoanelor ar putea fi dăunător. Prin urmare, un DPO ar trebui să furnizeze organizației sfaturi bazate pe riscurile identificate.
- Dacă decideți să nu urmați sfaturile date de DPO, ar trebui să documentați motivele pentru a vă demonstra responsabilitatea în cazul unui control.

2.7. Poate un DPO să îndeplinească și alte sarcini?

GDPR spune că putem atribui unui DPO și alte sarcini și îndatoriri, atâta timp cât acestea nu duc la un conflict de interese cu sarcinile principale ale acestuia.

> ☞ ***Exemplu:***
>
> Articolul 30 din Regulament prevede că organizațiile trebuie să țină, în anumite cazuri, evidența operațiunilor de prelucrare. Nu există nimic care să împiedice atribuirea acestei sarcini unui DPO.

Practic, acest lucru înseamnă că un DPO nu poate deține o poziție în cadrul organizației care să îi permită acestuia să determine scopurile și mijloacele de prelucrare a datelor cu caracter personal. În același timp, nu este de așteptat ca un DPO să gestioneze prelucrarea datelor personale din punct de vedere de business, care ar putea avea drept rezultat un rol secundar al activității de protecție a datelor în interesele întreprinderilor.

> ☞ ***Exemplu:***
>
> Directorul de marketing al unei companii planifică o campanie de publicitate, inclusiv ce clienți ai companiei decide să targeteze, ce metodă de comunicare și ce detalii personale să folosească pentru această campanie. Această persoană nu poate îndeplini și funcția de DPO al companiei pentru ca procesul de luare a deciziilor este foarte probabil să ducă la un conflict de interes între scopurile companiei din punct de vedere al marketingului și al rezultatelor ce trebuie obținute și obligațiile companiei privind protecția datelor personale.
>
> Pe altă parte, o autoritate publică ar putea numi drept DPO persoana care se ocupă acum cu primirea corespondenței. Nu există niciun conflict de interes aici întrucât rolurile sunt de a oferi acces la date și a înregistra o informație brută, decât de a lua decizii cu privire la scopul prelucrării.

2.8. DPO poate un angajat existent al organizației?

Da. Atâta timp cât îndatoririle profesionale ale angajatului sunt compatibile cu îndatoririle DPO și nu duc la un conflict de interese, puteți să numiți un angajat existent în calitate de responsabil cu protecția datelor decât să creați un post nou, caz în care veți face o decizie de numire în conformitate cu politica internă a organizației.

2.9. Putem contracta din exterior rolul de DPO?

Puteți contracta rolul de DPO extern, pe baza unui contract de prestări servicii cu o persoană fizică sau o societate, caz în care trebuie menționată expres persoana care va ocupa această funcție. Un DPO extern va avea aceleași sarcini ca un DPO intern.

2.10. Putem împărți un DPO cu mai multe organizații?

- Puteți desemna un singur DPO care să acționeze pentru un grup de companii sau autorități publice.
- În cazul DPO-ul acoperă mai multe organizații, acesta trebuie să își poată îndeplini sarcinile în mod eficient, ținând cont de structura și dimensiunea organizațiilor respective. Aceasta înseamnă că trebuie să vă gândiți dacă un DPO poate acoperi în mod realist mai multe organizații, în funcție de complexitatea acestora. Trebuie să vă asigurați că acest DPO are resursele necesare pentru a-și îndeplini rolul și să fie sprijinit de o echipă, dacă este cazul.
- DPO-ul trebuie să fie ușor de contactat, astfel încât detaliile de contact să fie ușor accesibile angajaților dumneavoastră, ANSPCDCP și persoanelor ale căror date personale le prelucrați.

2.11. Putem avea mai mult de un DPO?

- GDPR prevede în mod clar că o organizație trebuie să numească un singur DPO care să îndeplinească sarcinile prevăzute la articolul 39, dar acest lucru nu împiedică numirea altor specialiști în domeniul protecției datelor ca parte a unei echipe care să ajute la susținerea activității DPO.
- Trebuie să stabiliți cel mai bun mod de a configura funcția DPO în cadrul organizației și dacă aceasta necesită o echipă de protecție a datelor. Cu toate acestea, trebuie să existe o persoană desemnată ca DPO în sensul GDPR care îndeplinește cerințele prevăzute la articolele 37-39.
- Dacă aveți o echipă, trebuie să precizați în mod clar rolurile și responsabilitățile membrilor săi și modul în care acestea se referă la DPO.
- Dacă angajați specialiști în domeniul protecției datelor, cu excepția unui DPO, este important ca aceștia să nu fie denumiți DPO, ceea ce reprezintă un rol specific cu cerințele specifice din cadrul GDPR.

2.12. Ce trebuie să facem ca să ajutăm DPO-ul?

Trebuie să vă asigurați că:

- Un DPO este fie implicat în toate problemele de protecție a datelor;
- Un DPO raportează până la cel mai înalt nivel managerial al organizației;
- Un DPO operează independent și nu este sancționat pentru îndeplinirea acestor îndatoriri;

- Aveți resursele adecvate (timp, resurse financiare, infrastructură, și acolo unde e necesar, membri auxiliari) pentru ca DPO să îndeplinească obligațiile GDPR și pentru a menține nivelul lor de cunoștințe la un nivel de expert;
- Oferiți acces adecvat DPO-ului la date personale si activități de prelucrare;
- Oferiți DPO-ului acces adecvat la alte servicii în cadrul organizației dumneavoastră în așa fel încâ ei să primească sprijinul esențial și informațiile necesare;
- Luați în considerare sfatul oferit de DPO atunci când este necesară o DPIA și
- Înregistrați detaliile DPO-ului ca parte din înregistrările activităților de prelucrare.

Acest lucru demonstrează importanța DPO pentru organizație și că trebuie să oferiți un sprijin suficient, astfel încât să își poată îndeplini rolul în mod independent. O parte din acest sprijin este cerința ca DPO să raporteze la cel mai înalt nivel de management. Acest lucru nu înseamnă că DPO trebuie gestionat la acest nivel, dar trebuie să aibă acces direct pentru a oferi consiliere managerilor de rang înalt care iau decizii privind prelucrarea datelor cu caracter personal.

2.13. Ce detalii trebuie să publicăm despre DPO?

GDPR vă cere să:

- publicați detaliile de contact ale responsabilului cu protecția datelor; și
- să le furnizați ANSPDPC.

Aceasta este pentru a permite persoanelor fizice, angajaților dvs. și ANSDPCDP să contacteze DPO după cum este necesar. Nu aveți obligația de a include numele DPO atunci când publicați detaliile de contact, dar puteți alege să furnizați acest lucru dacă credeți că este necesar sau util.

De asemenea, vi se solicită să furnizați datele de contact ale DPO în următoarele situații:

- atunci când consultă ANSPDCP în temeiul articolului 36 cu privire la o DPIA; și
- atunci când furnizează informații privind confidențialitatea persoanelor în temeiul articolelor 13 și 14.

Cu toate acestea, rețineți că trebuie să furnizați numele DPO dacă raportați o încălcare a datelor cu caracter personal ANSPDCP și persoanelor afectate de aceasta.

2.14. Este DPO responsabil pentru conformarea cu GDPR?

DPO nu este răspunzător personal pentru conformitatea cu protecția datelor. În calitate de operator sau persoană împuternicită aveți obligația de a respecta GDPR. Cu toate acestea,

DPO joacă un rol esențial în a vă ajuta să îndepliniți obligațiile de protecție a datelor ale organizației.

📖 **Dispoziții relevante din Regulamentul GDPR:**

Preambul 26: În cazul în care prelucrarea este efectuată de o autoritate publică, cu excepția instanțelor sau a autorităților judiciare independente atunci când acționează în calitatea lor judiciară, în cazul în care, în sectorul privat, prelucrarea este efectuată de un operator a cărui activitate principală constă în operațiuni de prelucrare care necesită o monitorizare regulată și sistematică a persoanelor vizate pe scară largă, sau în cazul în care activitatea principală a operatorului sau a persoanei împuternicite de operator constă în prelucrarea pe scară largă de categorii speciale de date cu caracter personal și de date privind condamnările penale și infracțiunile, o persoană care deține cunoștințe de specialitate în materie de legislație și practici privind protecția datelor ar trebui să acorde asistență operatorului sau persoanei împuternicite de operator pentru monitorizarea conformității, la nivel intern, cu prezentul regulament. În sectorul privat, activitățile principale ale unui operator se referă la activitățile sale de bază, și nu la prelucrarea datelor cu caracter personal drept activități auxiliare. Nivelul necesar al cunoștințelor de specialitate ar trebui să fie stabilit în special în funcție de operațiunile de prelucrare a datelor efectuate și de nivelul de protecție impus pentru datele cu caracter personal prelucrate de operator sau de persoana împuternicită de operator. Acești responsabili cu protecția datelor, indiferent dacă sunt sau nu angajați ai operatorului, ar trebui să fie în măsură să își îndeplinească atribuțiile și sarcinile în mod independent.

Articolele 35-36: Articolul 35: Evaluarea impactului asupra protecției datelor

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

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

(3) Evaluarea impactului asupra protecției datelor menționată la alineatul (1) se impune mai ales în cazul:

(a) unei evaluări sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, și care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;

(b) prelucrării pe scară largă a unor categorii speciale de date, menționată la articolul 9 alineatul (1), sau a unor date cu caracter personal privind condamnări penale și infracțiuni, menționată la articolul 10; sau

(c) unei monitorizări sistematice pe scară largă a unei zone accesibile publicului.

(4) Autoritatea de supraveghere întocmește și publică o listă a tipurilor de operațiuni de prelucrare care fac obiectul cerinței de efectuare a unei evaluări a impactului asupra protecției datelor, în conformitate cu alineatul (1). Autoritatea de supraveghere comunică aceste liste comitetului menționat la articolul 68.

(5) Autoritatea de supraveghere poate, de asemenea, să stabilească și să pună la dispoziția publicului o listă a tipurilor de operațiuni de prelucrare pentru care nu este necesară o evaluare a impactului asupra protecției datelor. Autoritatea de supraveghere comunică aceste liste comitetului.

(6) Înainte de adoptarea listelor menționate la alineatele (4) și (5), autoritatea de supraveghere competentă aplică mecanismul pentru asigurarea coerenței menționat la articolul 63 în cazul în care aceste liste implică activități de prelucrare care presupun furnizarea de bunuri sau prestarea de servicii către persoane vizate sau monitorizarea comportamentului acestora în mai multe state membre ori care pot afecta în mod substanțial libera circulație a datelor cu caracter personal în cadrul Uniunii.

(7) Evaluarea conține cel puțin:

(a) o descriere sistematică a operațiunilor de prelucrare preconizate și a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator;

(b) o evaluare a necesității și proporționalității operațiunilor de prelucrare în legătură cu aceste scopuri;

(c) o evaluare a riscurilor pentru drepturile și libertățile persoanelor vizate menționate la alineatul (1); și

(d) măsurile preconizate în vederea abordării riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze conformitatea cu dispozițiile prezentului regulament, luând în considerare drepturile și interesele legitime ale persoanelor vizate și ale altor persoane interesate.

(8) La evaluarea impactului operațiunilor de prelucrare efectuate de operatorii sau de persoanele împuternicite de operatori relevante, se are în vedere în mod corespunzător respectarea de către operatorii sau persoanele împuternicite respective a codurilor de conduită aprobate menționate la articolul 40, în special în vederea unei evaluări a impactului asupra protecției datelor.

(9) Operatorul solicită, acolo unde este cazul, avizul persoanelor vizate sau al reprezentanților acestora privind prelucrarea prevăzută, fără a aduce atingere protecției intereselor comerciale sau publice ori securității operațiunilor de prelucrare.

(10) Atunci când prelucrarea în temeiul articolului 6 alineatul (1) litera (c) sau (e) are un temei juridic în dreptul Uniunii sau al unui stat membru sub incidența căruia intră operatorul, iar dreptul respectiv reglementează operațiunea de prelucrare specifică sau setul de operațiuni specifice în cauză și deja s-a efectuat o evaluare a impactului asupra protecției datelor ca parte a unei evaluări a impactului generale în contextul adoptării respectivului temei juridic, alineatele (1)-(7) nu se aplică, cu excepția cazului în care statele membre consideră că este necesară efectuarea unei astfel de evaluări înaintea desfășurării activităților de prelucrare.

(11) Acolo unde este necesar, operatorul efectuează o analiză pentru a evalua dacă prelucrarea are loc în conformitate cu evaluarea impactului asupra protecției datelor, cel puțin atunci când are loc o modificare a riscului reprezentat de operațiunile de prelucrare.

Articolul 36: Consultarea prealabilă

(1) Operatorul consultă autoritatea de supraveghere înainte de prelucrarea atunci când evaluarea impactului asupra protecției datelor prevăzută la articolul 35 indică faptul că prelucrarea ar genera un risc ridicat în absența unor măsuri luate de operator pentru atenuarea riscului.

(2) Atunci când consideră că prelucrarea prevăzută menționată la alineatul (1) ar încălca prezentul regulament, în special atunci când riscul nu a fost identificat sau atenuat într-o măsură suficientă de către operator, autoritatea de supraveghere oferă consiliere în scris operatorului și, după caz, persoanei împuternicite de operator, în cel mult opt săptămâni de la primirea cererii de consultare, și își poate utiliza oricare dintre competențele menționate la articolul 58. Această perioadă poate fi prelungită cu șase săptămâni, ținându-se seama de complexitatea prelucrării prevăzute. Autoritatea de supraveghere informează operatorul și, după caz, persoana împuternicită de operator, în termen de o lună de la primirea cererii, cu privire la orice astfel de prelungire, prezentând motivele întârzierii. Aceste perioade pot fi suspendate până când autoritatea de supraveghere a obținut informațiile pe care le-a solicitat în scopul consultării.

(3) Atunci când consultă autoritatea de supraveghere în conformitate cu alineatul (1), operatorul îi furnizează acesteia:

(a) dacă este cazul, responsabilitățile respective ale operatorului, ale operatorilor asociați și ale persoanelor împuternicite de operator implicate în activitățile de prelucrare, în special pentru prelucrarea în cadrul unui grup de întreprinderi;

(b) scopurile și mijloacele prelucrării preconizate;

(c) măsurile și garanțiile prevăzute pentru protecția drepturilor și libertăților persoanelor vizate, în conformitate cu prezentul regulament;

(d) dacă este cazul, datele de contact ale responsabilului cu protecția datelor;

(e) evaluarea impactului asupra protecției datelor prevăzută la articolul 35; și

(f) orice alte informații solicitate de autoritatea de supraveghere.

(4) Statele membre consultă autoritatea de supraveghere în cadrul procesului de pregătire a unei propuneri de măsură legislativă care urmează să fie adoptată de un parlament național sau a unei măsuri de reglementare întemeiate pe o astfel de măsură legislativă, care se referă la prelucrarea.

(5) În pofida alineatului (1), dreptul intern poate impune operatorilor să se consulte cu autoritatea de supraveghere și să obțină în prealabil autorizarea din partea acesteia în legătură cu prelucrarea de către un operator în vederea îndeplinirii unei sarcini exercitate de acesta în interes public, inclusiv prelucrarea în legătură cu protecția socială și sănătatea publică.

Articolele 37-39:

Articolul 37: Desemnarea responsabilului cu protecția datelor

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

(a) prelucrarea este efectuată de o autoritate sau un organism public, cu excepția instanțelor care acționează în exercițiul funcției lor jurisdicționale;

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

(c) activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în prelucrarea pe scară largă a unor categorii speciale de date, menționată la articolul 9, sau a unor date cu caracter personal privind condamnări penale și infracțiuni, menționată la articolul 10.

(2) Un grup de întreprinderi poate numi un responsabil cu protecția datelor unic, cu condiția ca responsabilul cu protecția datelor să fie ușor 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 protecția datelor unic pentru mai multe dintre aceste autorități sau organisme, luând în considerare structura organizatorică și dimensiunea acestora.

(4) În alte cazuri decât cele menționate la alineatul (1), operatorul sau persoana împuternicită de operator ori asociațiile și 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 protecția datelor. Responsabilul cu protecția datelor poate să acționeze în favoarea unor astfel de asociații și alte organisme care reprezintă operatori sau persoane împuternicite de operatori.

(5) Responsabilul cu protecția datelor este desemnat pe baza calităților profesionale și, în special, a cunoștințelor de specialitate în dreptul și practicile din domeniul protecției datelor, precum și pe baza capacității de a îndeplini sarcinile prevăzute la articolul 39.

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

(7) Operatorul sau persoana împuternicită de operator publică datele de contact ale responsabilului cu protecția datelor și le comunică autorității de supraveghere.

Articolul 38: Funcția responsabilului cu protecția datelor

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

(2) Operatorul și persoana împuternicită de operator sprijină responsabilul cu protecția datelor în îndeplinirea sarcinilor menționate la articolul 39, asigurându-i resursele necesare pentru executarea acestor sarcini, precum și accesarea datelor cu caracter personal și a operațiunilor de prelucrare, și pentru menținerea cunoștințelor sale de specialitate.

(3) Operatorul și persoana împuternicită de operator se asigură că responsabilul cu protecția datelor nu primește niciun fel de instrucțiuni în ceea ce privește îndeplinirea acestor sarcini. Acesta nu este demis sau sancționat de către operator sau de persoana împuternicită de operator pentru îndeplinirea sarcinilor sale.

Responsabilul cu protecția datelor răspunde direct în fața celui mai înalt nivel al conducerii operatorului sau persoanei împuternicite de operator.

(4) Persoanele vizate pot contacta responsabilul cu protecția datelor cu privire la toate chestiunile legate de prelucrarea datelor lor și la exercitarea drepturilor lor în temeiul prezentului regulament.

(5) Responsabilul cu protecția datelor are obligația de a respecta secretul sau confidențialitatea în ceea ce privește îndeplinirea sarcinilor sale, în conformitate cu dreptul Uniunii sau cu dreptul intern.

(6) Responsabilul cu protecția datelor poate îndeplini și alte sarcini și atribuții. Operatorul sau persoana împuternicită de operator se asigură că niciuna dintre aceste sarcini și atribuții nu generează un conflict de interese.

Articolul 39: Sarcinile responsabilului cu protecția datelor

(1) Responsabilul cu protecția datelor are cel puțin următoarele sarcini:

(a) informarea și consilierea operatorului, sau a persoanei împuternicite de operator, precum și a angajaților care se ocupă de prelucrare cu privire la obligațiile care le revin în temeiul prezentului regulament și al altor dispoziții de drept al Uniunii sau drept intern referitoare la protecția datelor;

(b) monitorizarea respectării prezentului regulament, a altor dispoziții de drept al Uniunii sau de drept intern referitoare la protecția datelor și a politicilor operatorului sau ale persoanei împuternicite de operator în ceea ce privește protecția datelor cu caracter personal, inclusiv alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;

(c) furnizarea de consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării 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 menționată la articolul 36, precum și, dacă este cazul, consultarea cu privire la orice altă chestiune.

(2) În îndeplinirea sarcinilor sale, responsabilul cu protecția datelor ține seama în mod corespunzător de riscul asociat operațiunilor de prelucrare, luând în considerare natura, domeniul de aplicare, contextul și scopurile prelucrării.

gdpr@avocatoo.ro
legalup.avocatoo.ro

avocatoo | powered by LegalUp