

GL243 - ÎNTREBĂRI FRECVENTE

Obiectivul prezentei anexe este de a răspunde, într-un format ușor de citit și simplificat, la unele dintre întrebările principale pe care ar putea să le aibă organizațiile cu privire la noile cerințe prevăzute prin RGPD pentru numirea unui RPD.

Desemnarea RPD (articolul 37)

1 Ce organizații au obligația să numească un RPD? [articolul 37 alineatul (1)]

RGPD prevede desemnarea unui RPD în trei cazuri specifice:

- cazul în care prelucrarea este efectuată de către o autoritate sau un organism public (indiferent de datele care sunt prelucrate);
- cazul în care 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; și
- cazul în care activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în prelucrarea pe scară largă a unor categorii speciale de date sau a unor date cu caracter personal privind condamnări penale și infracțiuni.

Este de reținut faptul că dreptul Uniunii sau al statului membru ar putea impune numirea RPD și în alte situații. În final, în cazul în care RGPD nu prevede în mod expres numirea unui RPD, organizațiile ar putea uneori să considere utilă desemnarea unui RPD pe bază de voluntariat. Grupul de lucru pentru protecția datelor în temeiul articolului 29 („GL29”) încurajează aceste eforturi voluntare.

Pentru mai multe informații, a se vedea secțiunea 2.1 din orientări.

2 Ce semnificație are noțiunea de „activități principale”? [articolul 37 alineatul (1) literele (b) și (c)]

„Activitățile principale” pot fi considerate drept operațiunile-cheie desfășurate pentru realizarea obiectivelor operatorului sau ale persoanei împuternicite de către operator. Acestea includ, de asemenea, toate activitățile în care prelucrarea datelor constituie o parte indisolubilă a activității operatorului sau a persoanei împuternicite de către operator. De exemplu, prelucrarea datelor privind starea de sănătate, cum ar fi dosarele medicale ale pacienților, ar trebui să fie considerată drept una dintre activitățile principale ale oricărui spital și, prin urmare, spitalele trebuie să numească RPD.

Pe de altă parte, toate organizațiile desfășoară anumite activități de sprijin, de exemplu, își plătesc angajații sau desfășoară activități standard de asistență TI. Acestea sunt funcții de asistență necesare pentru activitatea principală sau obiectul principal de activitate al organizației. Chiar dacă aceste activități sunt necesare sau esențiale, acestea sunt considerate, de regulă, ca fiind funcții auxiliare, nu activitatea principală.

Pentru mai multe informații, a se vedea secțiunea 2.1.2 din orientări.

3 Ce semnificație are noțiunea „pe scară largă”? [articolul 37 alineatul (1) literele (b) și (c)]

RGPD nu definește ceea ce înseamnă pe scară largă. GL29 recomandă să se țină cont, în special, de următorii factori atunci când se stabilește dacă prelucrarea este efectuată pe scară largă:

- numărul persoanelor vizate respective - fie ca număr specific, fie ca proporție din populația relevantă
- volumul de date și/sau intervalul diferitelor elemente de date prelucrate
- durata sau caracterul permanent al activității de prelucrare a datelor
- întinderea geografică a activității de prelucrare

printre exemplele de prelucrare pe scară largă se numără:

- prelucrarea datelor despre pacienți în cadrul activității obișnuite desfășurate de către un spital
- prelucrarea datelor referitoare la călătorii ale persoanelor care utilizează sistemul de transport public al unui oraș (de exemplu, urmărire prin intermediul permiselor de călătorie)
- prelucrarea datelor de geolocalizare în timp real a clienților unui lanț de restaurante fast-food în scopuri statistice de către un operator specializat în aceste activități
- prelucrarea datelor despre clienți în cadrul activității obișnuite desfășurate de către o societate de asigurări sau o bancă
- prelucrarea datelor cu caracter personal în scopuri de publicitate comportamentală de către un motor de căutare
- prelucrarea datelor (conținut, trafic, localizare) de către furnizorii de servicii de telefonie sau de internet

Printre exemplele care nu constituie prelucrare pe scară largă se numără:

- prelucrarea datelor despre pacienți de către un medic la nivel individual
- prelucrarea datelor cu caracter personal referitoare la condamnări penale și infracțiuni de către un avocat la nivel individual

Pentru mai multe informații, a se vedea secțiunea 2.1.3 din orientări.

4 Ce înseamnă noțiunea de „monitorizare periodică și sistematică”? [articolul 37 alineatul (1) litera (b)]

Noțiunea de monitorizare periodică și sistematică a persoanelor vizate nu este definită în RGPD, însă include, în mod clar, toate formele de urmărire și creare de profiluri pe internet, inclusiv în scopul publicității comportamentale. Însă noțiunea de „monitorizare” nu se limitează la mediul online.

Conform interpretării de către GL29, cuvântul „periodică” ar avea una sau mai multe dintre următoarele semnificații:

- în regim permanent sau la anumite intervale, pentru o anumită perioadă
- în mod recurent sau repetat, la ore fixe
- în mod constant sau periodic

Conform interpretării de către GL29, cuvântul „sistematică” ar avea una sau mai multe dintre următoarele semnificații:

- care se realizează conform unui sistem
- în mod predeterminat, organizat sau metodic
- care are loc în cadrul unui plan general de colectare a datelor
- care are loc în cadrul unei strategii

Exemple: exploatarea unei rețele de telecomunicații; furnizarea de servicii de telecomunicații; reorientarea către adrese de e-mail (e-mail retargeting); crearea de profiluri și acordarea de puncte în scopul evaluării riscurilor (de exemplu, în scopul evaluării bonității, al stabilirii primelor de asigurare, al prevenirii fraudelor, al depistării acțiunilor de spălare a banilor); urmărirea locației, de exemplu, prin aplicații mobile; introducerea de programe de fidelizare; publicitatea comportamentală; monitorizarea datelor despre starea de bine, aptitudini și starea de sănătate prin intermediul dispozitivelor portabile; introducerea de programe de televiziune în circuit închis; introducerea de dispozitive conectate, cum ar fi dispozitivele de măsurare inteligente, vehiculele inteligente, sistemele automate la domiciliu etc.

Pentru mai multe informații, a se vedea secțiunea 2.1.4 din orientări.

5 Organizațiile pot numi un RPD comun? În caz afirmativ, în ce condiții? [articolul 37 alineatele (2) și (3)]

RGPD prevede faptul că un grup de întreprinderi poate numi un singur RPD cu condiția ca acesta să fie „ușor accesibil de la sediul fiecăreia dintre întreprinderi”. Noțiunea de accesibilitate se referă la sarcinile RPD ca punct de contact pentru persoanele vizate, autoritatea de supraveghere și, de asemenea, la nivel intern în cadrul organizației. Pentru a asigura accesibilitatea RPD, la nivel intern sau extern, este important să se asigure disponibilitatea detaliilor de contact ale acestora în conformitate cu RGPD. RPD trebuie să fie în măsură să comunice în mod eficient cu persoanele vizate și să coopereze cu autoritățile de supraveghere vizate. Aceasta înseamnă că această comunicare trebuie să aibă loc în limba sau în limbile utilizate de către autoritățile de supraveghere și persoanele vizate în cauză. Disponibilitatea personală a unui RPD (fie prin prezența fizică în aceeași locație ca și angajații, pe o linie telefonică de urgență sau prin alte mijloace sigure de comunicare) este esențială pentru a asigura posibilitatea ca persoanele vizate să fie contactate de către RPD.

Pentru mai multe informații, a se vedea secțiunea 2.3 din orientări.

6 Este posibilă numirea unui RPD extern [articolul 37 alineatul (6)]?

Da. În conformitate cu articolul 37 alineatul (6), RPD poate fi un membru al personalului operatorului sau al persoanei împuternicite de către operator (RPD intern) sau poate să își îndeplinească sarcinile în baza unui contract de servicii. Aceasta înseamnă că RPD poate fi extern și, în acest caz, funcția sa poate fi exercitată în baza unui contract de servicii încheiat cu o persoană sau o organizație.

În cazul în care RPD este extern, pentru respectivul RPD se aplică toate cerințele prevăzute la articolele 37-39. Astfel cum este prevăzut în orientări, atunci când funcția RPD este exercitată de către un prestator de servicii extern, o echipă de persoane care lucrează pentru entitatea respectivă ar putea îndeplini în mod eficient sarcinile unui RPD ca echipă, sub responsabilitatea unei persoane de contact principale și a „unui responsabil” desemnat pentru client. În acest caz, este esențial ca fiecare membru al organizației externe care îndeplinește funcțiile unui RPD să respecte toate cerințele relevante din RGPD.

Din motive de claritate juridică și pentru o bună organizare, orientările recomandă să se prevadă în contractul de servicii alocarea clară a sarcinilor în cadrul echipei RPD externe și numirea unei singure persoane ca persoană de contact principală și persoană „responsabilă” pentru client.

Pentru mai multe informații, a se vedea secțiunile 2.3, 2.4 și 3.5 din orientări.

7 Care sunt calitățile profesionale pe care ar trebui să le aibă RPD [articolul 37 alineatul (5)]?

RGPD prevede faptul că RPD „*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*”.

Nivelul necesar al cunoștințelor de specialitate ar trebui să fie stabilit în funcție de operațiunile de prelucrare a datelor efectuate și de nivelul de protecție impus pentru datele cu caracter personal prelucrate. Spre exemplu, în cazul în care o activitate de prelucrare a datelor este deosebit de complexă, sau în cazul în care este vorba despre un volum mare de date sensibile, este posibil ca RPD să aibă nevoie de un nivel mai ridicat de specializare și de sprijin.

Printre competențele și expertiza necesare se află:

- expertiză în legislația și practicile naționale și europene în materie de protecție a datelor, inclusiv înțelegerea aprofundată a RGPD
- înțelegerea operațiunilor de prelucrare desfășurate
- înțelegerea tehnologiilor informației și a securității datelor
- cunoașterea domeniului de activitate și a organizației
- capacitatea de a promova o cultură a protecției datelor în cadrul organizației

Pentru mai multe informații, a se vedea secțiunea 2.4 din orientări.

Funcția RPD (articolul 38)

8 Care sunt resursele de care ar trebui să fie puse la dispoziția RPD pentru a-și desfășura sarcinile?

Articolul 38 alineatul (2) din RGPD impune organizației să susțină RPD *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*”.

În funcție de natura operațiunilor de prelucrare, precum și de activitățile și dimensiunea organizației, ar trebui puse la dispoziția RPD următoarele resurse:

- sprijin activ pentru funcția RPD din partea personalului de conducere de nivel superior
- timp suficient pentru îndeplinirea de către RPD a sarcinilor sale
- sprijin adecvat în ceea ce privește resursele financiare, infrastructura (spații, facilități, echipamente) și personal, după caz
- comunicarea oficială cu privire la desemnarea RPD către toți membrii personalului
- accesul la alte servicii din cadrul organizației pentru ca RPD să poată primi sprijin, date și informații esențiale din partea serviciilor respective.
- formarea continuă

Pentru mai multe informații, a se vedea secțiunea 3.2 din orientări.

9 Care sunt garanțiile care îi permit RPD să își îndeplinească sarcinile în mod independent [articolul 38 alineatul (3)]?

Există mai multe garanții pentru a-i permite RPD să acționeze în mod independent, astfel cum este prevăzut la considerentul 97:

- nu există instrucțiuni din partea operatorilor sau a persoanelor împuternicite de către operatori în ceea ce privește exercitarea de către RPD a sarcinilor
- nu se prevede concedierea sau sancționarea de către operator în legătură cu îndeplinirea de către RPD a sarcinilor sale
- nu există un conflict de interese cu posibile alte sarcini și atribuții

Pentru mai multe informații, a se vedea secțiunile 3.3-3.5 din orientări.

10 Care sunt „celelalte sarcini și atribuții” ale unui RPD, care ar putea genera un conflict de interese [articolul 38 alineatul (6)]?

RPD nu poate deține o funcție în cadrul organizației, prin care să stabilească scopurile și mijloacele de prelucrare a datelor cu caracter personal. Datorită organigramei specifice din cadrul fiecărei organizații, acest aspect trebuie să fie analizat de la caz la caz.

Ca regulă generală, printre funcțiile contradictorii se pot include funcțiile personalului de conducere de nivel superior (precum funcția de director general, de director general administrativ, de director financiar, de medic primar, de șef al departamentului de marketing, de șef al serviciului de resurse umane sau de șef al departamentelor TI), însă și alte roluri de rang inferior în organigramă dacă astfel de poziții sau roluri conduc la stabilirea scopurilor și a mijloacelor de prelucrare.

Pentru mai multe informații, a se vedea secțiunea 3.5 din orientări.

Sarcinile RPD (articolul 39)

11 Ce semnificație are noțiunea „monitorizarea respectării” RGPD [articolul 39 alineatul (1) litera (b)]?

În cadrul acestor sarcini de monitorizare a conformității, RPD ar putea, în mod specific:

- să colecteze informații pentru identificarea activităților de prelucrare
- să analizeze și să verifice conformitatea activităților de prelucrare și
- să informeze, să îndrume și să emită recomandări pentru operatorul sau persoana împuternicită de către operator

Pentru mai multe informații, a se vedea secțiunea 4.1 din orientări.

12 Este RPD responsabil personal de nerespectarea RGPD?

Nu, RPD nu este responsabil personal de nerespectarea RGPD. RGPD prevede în mod clar faptul că operatorul sau persoana împuternicită de către operator este cel sau cea care trebuie să se asigure și să fie în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul regulament [articolul 24 alineatul (1)]. Respectarea normelor de protecție a datelor este responsabilitatea operatorului sau a persoanei împuternicite de către operator.

13 Care este rolul RPD în ceea ce privește evaluarea impactului asupra protecției datelor [articolul 37 alineatul (1) litera (c)] și păstrarea evidenței activităților de prelucrare (articolul 30)?

În ceea ce privește evaluarea impactului asupra protecției datelor, operatorul sau persoana împuternicită de către operator ar trebui să solicite avizul RPD cu privire la următoarele aspecte, printre altele:

- dacă să efectueze o EIPD
- ce metodologie să urmeze atunci când efectuează o EIPD
- dacă să efectueze evaluarea EIPD la nivel intern sau să o externalizeze
- ce garanții (inclusiv măsuri tehnice și organizaționale) să aplice pentru a atenua eventualele riscuri asupra drepturilor și a intereselor persoanelor vizate
- dacă evaluarea impactului asupra protecției datelor a fost corect efectuată și dacă concluziile sale (privind începerea prelucrării și garanțiile care să fie aplicate) sunt în conformitate cu GDPR.

Pentru mai multe informații, a se vedea secțiunea 4.2 din orientări.

În ceea ce privește păstrarea evidenței activităților de prelucrare, operatorul sau persoana împuternicită de către operator, nu RPD, este cel sau cea care trebuie să păstreze evidența operațiunilor de prelucrare. Însă nimic nu împiedică operatorul sau persoana împuternicită de către operator să atribuie RPD sarcina de a păstra evidența operațiunilor de prelucrare aflate sub responsabilitatea operatorului. O astfel de evidență ar trebui să fie considerată drept unul dintre instrumentele care permit RPD să își îndeplinească sarcinile de monitorizare a conformității, de informare și avizare a operatorului sau a persoanei împuternicite de către operator.

Pentru mai multe informații, a se vedea secțiunea 4.4 din orientări.