ARTICOLUL 29 GRUPUL DE LUCRU PENTRU PROTECȚIA DATELOR

16/RO
GL 243 rev. 01

Orientări privind responsabilii cu protecția datelor („RPD”)

Adoptate la 13 decembrie 2016

Astfel cum au fost recent revizuite și adoptate la 5 aprilie 2017

Acest grup de lucru a fost instituit în temeiul articolului 29 din Directiva 95/46/CE. Acesta este un organ european privind protecția datelor și a vieții private cu rol consultativ și statut independent. Atribuțiile 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 statul de drept) din cadrul Comisiei Europene, Direcția Generală Justiție și Consumatori, B-1049 Bruxelles, Belgia, Nr. birou MO59 05/35

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

GRUPUL DE LUCRU PRIVIND 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,

având în vedere Regulamentul său de procedură,

ADOPTĂ PREZENTELE ORIENTĂRI:

Cuprins

1 Introducere

Regulamentul general privind protecția datelor (denumit în continuare „RGPD”),[1] care urmează să intre în vigoare la 25 mai 2018, oferă un cadru modern de conformitate pentru protecția datelor în Europa, bazat pe răspundere. Responsabilii cu protecția datelor (denumiți în continuare „RPD”) se vor afla în centrul acestui nou cadru juridic pentru numeroase organizații, facilitând conformitatea cu dispozițiile din RGPD.

În conformitate cu RGPD, anumiți operatori și persoane împuternicite de operatori au obligația de a desemna un RPD[2]. Acest lucru va fi valabil pentru toate autoritățile și organismele publice (indiferent de datele pe care le prelucrează), precum și pentru alte organizații care, ca activitate de bază, monitorizează persoane în mod sistematic și la scară largă, sau care prelucrează categorii speciale de date cu caracter personal la scară largă.

Chiar și în cazul în care RGPD nu prevede în mod expres numirea unui RPD, organizațiile ar putea uneori să considere utilă numirea unui RPD pe bază de voluntariat. Grupul de lucru pentru protecția datelor în temeiul articolului 29 („GL29”) încurajează aceste eforturi voluntare.

Conceptul de RPD nu este nou. Deși Directiva 95/46/CE[3] nu impunea niciunei organizații să numească un RPD, practica de a numi un RPD a fost totuși dezvoltată în mai multe state membre de-a lungul anilor.

Înainte de adoptarea RGPD, GL29 a susținut că RPD este o piatră de temelie pentru responsabilitate și că numirea unui RPD poate facilita conformitatea și, mai mult decât atât, poate deveni un avantaj concurențial pentru întreprinderi[4]. Pe lângă facilitarea conformității prin punerea în aplicare a unor instrumente în materie de responsabilitate (cum ar fi facilitarea evaluărilor privind impactul asupra protecției datelor și desfășurarea sau facilitarea de audituri), RPD acționează ca intermediari între părțile interesate relevante (de exemplu, autoritățile de supraveghere, persoanele vizate și unitățile operaționale din cadrul unei organizații).

În caz de neconformitate cu RGPD, RPD nu răspund personal. 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

---

[1] Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor). RGPD este relevant pentru SEE și se aplică după încorporarea acestuia în Acordul privind SEE.

[2] Numirea unui RPC are caracter obligatoriu și pentru autoritățile competente în temeiul articolului 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 urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI (JO L 119, 4.5.2016, p. 89–131), precum și în temeiul legislației naționale de punere în aplicare. Chiar dacă aceste orientări vizează responsabilii cu protecția datelor în temeiul RGPD, ele sunt, de asemenea, relevante în ceea ce privește responsabilii cu protecția datelor în temeiul Directivei 2016/680, în legătură cu dispozițiile similare ale acestora.

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

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

fie în măsură să demonstreze că prelucrarea se efectuează în conformitate cu dispozițiile acestuia [articolul 24 alineatul (1)]. Conformitatea privind protecția datelor este responsabilitatea operatorului sau a persoanei împuternicite de operator.

Operatorul sau persoana împuternicită de către operator are, de asemenea, un rol esențial în a permite îndeplinirea efectivă a atribuțiilor de către RPD. Numirea unui RPD este un prim pas, însă trebuie, de asemenea, ca acești responsabili cu protecția să beneficieze de autonomie și resurse suficiente pentru a-și îndeplini sarcinile cu eficacitate.

RGPR recunoaște statutul RPD de actor-cheie în noul sistem de guvernanță a datelor și prevede condiții pentru numirea acestuia, poziția și sarcinile care îi revin. Obiectivul prezentelor orientări este de a clarifica dispozițiile relevante din RGPD cu scopul de a ajuta operatorii și persoanele împuternicite de către operatori să respecte legislația și totodată să ajute RPD în îndeplinirea rolului lor. Orientările oferă, de asemenea, recomandări privind cele mai bune practici, pe baza experienței dobândite în unele state membre ale UE. GL29 va monitoriza punerea în aplicare a acestor orientări și poate să le completeze cu detalii suplimentare, după caz.

2 Numirea unui responsabil cu protecția datelor (RPD)

2.1. Numirea obligatorie

Articolul 37 alineatul (1) din RGPD prevede numirea unui RPD în trei cazuri specifice[5]:

a) cazul în care prelucrarea este efectuată de o autoritate sau un organism public[6];
b) 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; sau
c) 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[7] sau[8] a unor date cu caracter personal privind condamnări penale și infracțiuni[9].

În următoarele subsecțiuni, GL29 prezintă orientări în ceea ce privește criteriile și terminologia utilizată la articolul 37 alineatul (1).

Cu excepția cazului în care este evident că o organizație nu este obligată să numească un RPD, GL29 recomandă ca operatorii și persoanele împuternicite de către operatori să documenteze analiza internă efectuată pentru a stabili dacă va fi numit un RPD, pentru a putea demonstra că au fost luați în

[5] Este de reținut faptul că, în temeiul articolului 37 alineatul (4), dreptul Uniunii sau al statelor membre poate să prevadă numirea RPD și în alte situații.

[6] Cu excepția instanțelor care acționează în exercițiul funcției lor jurisdicționale. A se vedea articolul 32 din Directiva (UE) 2016/680.

[7] În temeiul articolului 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 persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală a unei persoane fizice.

[8] Articolul 37 alineatul (1)(c) utilizează cuvântul „*și*”. A se vedea secțiunea 2.1.5 de mai jos pentru explicații privind utilizarea cuvântului „*sau*” în locul cuvântului „*și*”.

[9] Articolul 10.

considerare factorii relevanți în mod corespunzător.[10]. Această analiză face parte din documentație conform principiului responsabilității. Aceasta ar putea fi solicitată de către autoritatea de supraveghere și ar trebui să fie actualizată dacă este cazul, de exemplu în cazul în care operatorii sau persoanele împuternicite de către operatori întreprind activități noi sau furnizează servicii noi care ar putea fi încadrate în cazurile enumerate la articolul 37 alineatul (1).

Atunci când o organizație numește un RPD în mod voluntar se vor aplica cerințele prevăzute la articolele 37 și 39 la numire, precum și la stabilirea funcției și a sarcinilor, ca și când numirea ar fi fost obligatorie.

Nimic nu împiedică o organizație, care nu are obligația legală de a numi un RPD și care nu dorește să numească un RPD în mod voluntar, să angajeze personal sau consultanți externi cu sarcini legate de protecția datelor cu caracter personal. În acest caz, este important ca aceasta să se asigure că nu există nicio confuzie în ceea ce privește titlul, statutul, funcția și sarcinile care le revin. Prin urmare, ar trebui clarificat, în orice comunicare din cadrul societății, precum și cu autoritățile pentru protecția datelor, persoanele vizate și publicul, faptul că titlul acestei persoane sau al acestui consultant nu este acela de responsabil cu protecția datelor (RPD). [11]

RPD, indiferent dacă este obligatoriu sau voluntar, este numit pentru toate operațiunile de prelucrare desfășurate de operator sau de persoana împuternicită de operator.

2.1.1 „AUTORITATE SAU ORGANISM PUBLIC"

RGPD nu definește ceea ce constituie un „*o autoritate sau un organism public"*. GL29 consideră că o astfel de noțiune va fi definită în conformitate cu dreptul intern. În consecință, autoritățile și organismele publice includ autoritățile naționale, regionale și locale, însă, în conformitate cu dreptul național aplicabil, conceptul include, de regulă, și o serie de alte organisme de drept public[12]. În astfel de cazuri, numirea unui RPD este obligatorie.

O sarcină publică poate fi realizată, iar autoritatea publică poate fi exercitată[13] nu doar de către autorități sau organisme publice, ci și de alte persoane fizice sau juridice de drept public sau privat, în conformitate cu legislația națională a fiecărui stat membru, în sectoare precum serviciile de transport public, alimentarea cu apă și furnizarea de energie, infrastructura rutieră, serviciul public de radiodifuziune și locuințele sociale, sau de către organisme disciplinare pentru profesiile reglementate.

În aceste cazuri, persoanele vizate ar putea fi într-o situație foarte similară celei în care datele acestora sunt prelucrate de o autoritate sau un organism public. În mod specific, datele pot fi prelucrate în scopuri similare, iar persoanele au adesea, în mod similar, puține opțiuni sau nicio opțiune de a decide cu privire la problema dacă datele lor vor fi prelucrate și la modul de prelucrare a acestora și, prin

[10] A se vedea articolul 24 alineatul (1).

[11] Acest lucru este relevant și în cazul inspectorilor-șefi pentru protecția confidențialității (IPC) sau al altor profesioniști în domeniul confidențialității care există deja, la ora actuală, în unele societăți, care este posibil să nu poată îndeplini întotdeauna criteriile RGPD, de exemplu, în ceea ce privește resursele disponibile sau garanțiile pentru independență, iar dacă nu reușesc acest lucru, aceștia nu pot fi considerați și numiți drept RPD.

[12] A se vedea, spre exemplu, definiția pentru „*organism din sectorul public*" și „*organism de drept public*" de la articolul 2 alineatele (1) și (2) din Directiva 2003/98/CE a Parlamentului European și a Consiliului din 17 noiembrie 2003 privind reutilizarea informațiilor din sectorul public (JO L 345, 31.12.2003, p. 90).

[13] Articolul 6 alineatul (1) litera (e).

urmare, acestea ar putea avea nevoie de protecția suplimentară pe care o poate asigura numirea unui RPD.

Deși nu există nicio obligație în astfel de cazuri, GL29 recomandă, ca exemplu de bună practică, organizațiilor private care îndeplinesc sarcini publice sau exercită autoritate publică să numească un RPD. O astfel de activitate a RPD cuprinde toate operațiunile de prelucrare desfășurate, inclusiv cele care nu sunt legate de îndeplinirea unei sarcini publice sau exercitarea atribuțiilor oficiale (de exemplu, gestionarea unei baze de date a salariaților).

2.1.2 „ACTIVITĂȚI PRINCIPALE”

Articolul 37 alineatul (1) literele (b) și (c) din RGPD vizează „*activitățile principale ale operatorului sau ale persoanei împuternicite de operator”*. Considerentul 97 prevede faptul că activitățile principale ale unui operator se referă la „*activitățile sale de bază, și nu la prelucrarea datelor cu caracter personal drept activități auxiliare*”. „Activitățile principale” pot fi considerate drept operațiunile-cheie necesare pentru îndeplinirea obiectivelor operatorului sau ale persoanei împuternicite de către operator.

Cu toate acestea, „activitățile principale” nu ar trebui să fie interpretate ca excluzând activitățile în cazul în care prelucrarea datelor constituie o parte indisolubilă a activității operatorului sau a persoanei împuternicite de către operator. De exemplu, activitatea principală a unui spital este de a furniza asistență medicală. Cu toate acestea, spitalul nu ar putea furniza 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 drept una dintre activitățile principale ale oricărui spital, iar spitalele trebuie, prin urmare, să numească RPD.

Într-un alt exemplu, o societate privată de securitate supraveghează o serie de centre comerciale private și spații publice. Supravegherea este activitatea principală a societății, care, la rândul său, este legată în mod indisolubil de prelucrarea datelor cu caracter personal. Prin urmare, această societate trebuie, de asemenea, să numească un RPD.

Pe de altă parte, toate organizațiile desfășoară anumite activități, de exemplu, își plătesc angajații sau desfășoară activități standard de asistență TI. Acestea sunt exemple de 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.

2.1.3 „PE SCARĂ LARGĂ”

Articolul 37 alineatul (1) literele (b) și (c) prevede prelucrarea datelor cu caracter personal pe scară largă pentru a se putea lansa acțiunea de numire a RPD. RGPD nu definește prelucrarea pe scară largă, deși considerentul 91 oferă unele îndrumări[14].

Într-adevăr, nu este posibil să se stabilească un număr exact nici în ceea ce privește cantitatea de date prelucrate, nici în ceea ce privește numărul de persoane implicate, ceea ce ar fi valabil în toate situațiile. Aceasta nu exclude însă posibilitatea ca, în timp, să se elaboreze o practică standard pentru

[14] Conform considerentului, ar fi incluse, în special operațiunile „*de prelucrare la scară largă, care au drept obiectiv prelucrarea unui volum considerabil de date cu caracter personal la nivel regional, național sau supranațional, 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 specific faptul 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 de către un anumit medic, un alt profesionist în domeniul sănătății sau un avocat”*. Este important să se țină cont de faptul că, deși în considerent se oferă exemple la limitele scării (prelucrarea de către un medic la nivel individual, comparativ cu prelucrarea datelor unei țări întregi sau a întregii Europe); există o zonă gri semnificativă între aceste extreme. În plus, ar trebui să se rețină faptul că acest considerent se referă la evaluările impactului asupra protecției datelor. Acest lucru înseamnă că unele elemente ar putea fi specifice contextului respectiv și nu sunt neapărat valabile la numirea RPD exact în același mod.

identificarea concretă și/sau cantitativă a ceea ce constituie „*la scară largă*” în ceea ce privește anumite tipuri de activități de prelucrare comune. GL29 intenționează, de asemenea, să contribuie la această acțiune de elaborare, prin comunicarea și publicarea de exemple de praguri relevante pentru numirea unui RPD.

În orice caz, 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 furnizarea de astfel de servicii
- 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

2.1.4 „MONITORIZARE PERIODICĂ ȘI SISTEMATICĂ”

Noțiunea de monitorizare periodică și sistematică a persoanelor vizate nu este definită în RGPD, însă conceptul de „*monitorizare a comportamentului persoanelor vizate*” este menționat în considerentul 24[15] și include, în mod clar, toate formele de urmărire și creare de profiluri pe internet, inclusiv în scopul publicității comportamentale.

[15] *„Pentru a se 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 unei persoane fizice, în special în scopul de a lua decizii cu privire la aceasta sau de a analiza sau de a face previziuni referitoare la preferințele personale, comportamentele și atitudinile acesteia”.*

Însă noțiunea de „monitorizare” nu este limitată la mediul online, iar urmărirea online ar trebui considerată a fi doar un exemplu de monitorizare a comportamentului persoanelor vizate[16].

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

Printre exemplele de activități care ar putea constitui monitorizare periodică și sistematică a persoanelor vizate se numără: exploatarea unei rețele de telecomunicații; furnizarea de servicii de telecomunicații; reorientarea către adrese de e-mail (e-mail retargeting); activități de comercializare bazate pe date; 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.

2.1.5 CATEGORII SPECIALE DE DATE ȘI A DATELOR REFERITOARE LA CONDAMNĂRI PENALE ȘI INFRACȚIUNI

Articolul 37 alineatul (1) litera (c) se referă la prelucrarea unor categorii speciale de date prevăzute la articolul 9 și la date cu caracter personal privind condamnări penale și infracțiuni prevăzute la articolul 10. Deși în dispoziție este utilizat termenul „și”, nu există niciun motiv de politică pentru care să se impună aplicarea simultană a celor două criterii. Prin urmare, textul ar trebui să fie interpretat ca însemnând „sau”.

2.2. RPD al persoanei împuternicite de către operator

Articolul 37 se aplică atât în cazul operatorilor[17], cât și al persoanelor împuternicite de către operatori[18] în ceea ce privește numirea unui RPD. În funcție de cine îndeplinește criteriile privind numirea obligatorie, în unele cazuri doar operatorul sau doar persoana împuternicită de către operator, în alte

[16] Este de precizat că textul considerentului 24 vizează aplicarea extrateritorială a RGPD. În plus, există, de asemenea, o diferență între sintagma *„monitorizarea comportamentului lor”* [articolul 3 alineatul (2) litera (b)] și *„o monitorizare periodică și sistematică a persoanelor vizate pe scară largă”* [articolul 37 alineatul (1) litera (b)], care ar putea fi așadar considerată a fi o noțiune diferită.

cazuri, atât operatorul, cât și persoana împuternicită de către operator au obligația de a numi un RPD (aceștia trebuind apoi să colaboreze).

Este important să se sublinieze faptul că, chiar și în cazul în care operatorul îndeplinește criteriile pentru numirea obligatorie, persoana împuternicită de către acest operator nu trebuie să numească neapărat un RPD. Însă acesta ar putea fi un exemplu de bună practică.

Exemple:

- O mică întreprindere familială cu activitate de distribuire de aparate de uz casnic într-un singur oraș, utilizează serviciile unei persoane împuternicite de către operator, a cărei activitate principală este de a furniza servicii de analiză pe internet și asistență pentru publicitate și comercializare vizată. Activitățile întreprinderii familiale și clienții acesteia nu generează prelucrarea datelor „pe scară largă", având în vedere numărul redus de clienți și activitățile relativ limitate. Însă activitățile persoanei împuternicite de către operator, care are mulți clienți precum această întreprindere mică, luate împreună, realizează o prelucrare pe scară largă. Prin urmare, persoana împuternicită de către operator trebuie să numească un RPD în conformitate cu articolul 37 alineatul (1) litera (b). În același timp, întreprinderea familială în sine nu are obligația de a numi un RPD.

- O întreprindere mijlocie producătoare de plăci ceramice își subcontractează serviciile de sănătate în muncă unei persoane împuternicite de către operator din exterior, care are un număr mare de clienți similari. Persoana împuternicită de către operator numește un RPD în temeiul articolului 37 alineatul (1) litera (c) cu condiția ca prelucrarea să fie realizată pe scară largă. Însă producătorul nu are neapărat obligația de a numi un RPD.

RPD numit de către o persoană împuternicită de către operator supraveghează, de asemenea, activitățile desfășurate de către organizația cu rol de persoană împuternicită de către operator atunci când acționează în calitate de operator de date de drept (de exemplu, resursele umane, TI, logistică).

2.3. Numirea unui singur RPD pentru mai multe organizații

Articolul 37 alineatul (2) permite unui grup de întreprinderi să numească un singur RPD cu condiția ca acesta să fie „*ușor accesibil din fiecare întreprindere*". Conceptul de „accesibilitate" se referă la sarcinile RPD ca punct de contact privind persoanele vizate[19], autoritatea de supraveghere[20], dar și la nivel intern, în cadrul organizației, având în vedere că una dintre sarcinile RPD este *„informarea și*

[17] Operatorul este definit la articolul 4 alineatul (7) ca fiind persoana sau organismul care stabilește scopurile și mijloacele de prelucrare a datelor.

[18] Persoana împuternicită de către operator este definită la articolul 4 alineatul (8) ca fiind persoana sau organismul care prelucrează date în numele operatorului.

[19] Articolul 38 alineatul (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*".

[20] Articolul 39 alineatul (1) litera (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*".

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"[21].

Pentru a asigura accesibilitatea RPD, la nivel intern sau extern, este important să se asigure disponibilitatea detaliilor de contact ale acestora în conformitate cu cerințele RGPD[22].

Acesta, cu ajutorul unei echipe, dacă este necesar, trebuie să fie în măsură să comunice în mod eficient cu persoanele vizate[23] și să coopereze[24] cu autoritățile de supraveghere interesate. Aceasta înseamnă, de asemenea, că această comunicare trebuie să aibă loc în limba sau în limbile utilizate de către autoritățile de supraveghere și persoanele vizate în cauză. Disponibilitatea 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.

În conformitate cu articolul 37 alineatul (3), un singur RPD poate fi numit pentru mai multe autorități sau organisme publice, ținând cont de structura organizatorică și dimensiunea acestora. Se aplică aceleași considerații cu privire la resurse și comunicare. Având în vedere că RPD este responsabil de o serie de sarcini, operatorul sau persoana împuternicită de către operator trebuie să se asigure că un singur RPD, cu ajutorul unei echipe, dacă este necesar, poate îndeplini aceste sarcini în mod eficient, în pofida numirii sale pentru mai multe autorități și organisme publice.

2.4. Accesibilitatea și localizarea RPD

În conformitate cu secțiunea 4 din RGPD, accesibilitatea RPD ar trebui să fie efectivă.

Pentru asigurarea accesibilității RPD, GL29 recomandă ca RPD să se afle pe teritoriul Uniunii Europene, indiferent dacă operatorul sau persoana împuternicită de către operator este stabilit în Uniunea Europeană.

Cu toate acestea, nu se poate exclude faptul că, în anumite situații în care operatorul sau persoana împuternicită de către operator nu are un sediu pe teritoriul Uniunii Europene[25], un RPD ar putea fi în măsură să își desfășoare activitatea într-un mod mai eficace dacă se află în afara UE.

2.5. Expertiza și competențele RPD

Articolul 37 alineatul (5) 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*

[21] Articolul 39 alineatul (1) litera (a).

[22] A se vedea, de asemenea, secțiunea 2.6 de mai jos.

[23] Articolul 12 alineatul (1): *„Operatorul ia măsuri adecvate pentru a furniza persoanei vizate orice informații menționate la articolele 13 și 14 și orice comunicări în temeiul articolelor 15-22 și 34 referitoare la prelucrare, într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu, în special pentru orice informații adresate în mod specific unui copil."*

[24] Articolul 39 alineatul (1) litera (d) *: „cooperarea cu autoritatea de supraveghere"*

[25] A se vedea articolul 3 din RGPD cu privire la domeniul de aplicare teritorial.

și pe baza capacității de a îndeplini sarcinile prevăzute la articolul 39". Considerentul 97 prevede faptul că 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.

- **Nivelul de expertiză**

Nivelul de expertiză necesar nu este definit în mod strict, însă trebuie să fie proporțional cu caracterul sensibil, complexitatea și cantitatea de date pe care o prelucrează o organizație. 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. De asemenea, există o diferență în funcție de problema dacă organizația transferă în mod sistematic date cu caracter personal în afara Uniunii Europene sau dacă astfel de transferuri sunt ocazionale. Astfel, RPD ar trebui să fie ales cu atenție, ținându-se seama în mod corespunzător de aspectele legate de protecția datelor care apar în cadrul organizației.

- **Calități profesionale**

Deși articolul 37 alineatul (5) nu menționează calitățile profesionale de care ar trebui să se țină seama la numirea RPD, este relevant faptul că RPD trebuie să aibă experiență în legislația și practicile din domeniul protecției datelor la nivel național și european și să dețină cunoștințe aprofundate despre RGPD. De asemenea, este utilă promovarea de către autoritățile de supraveghere a unor acțiuni de formare adecvată și periodică a RPD.

Cunoașterea domeniului de activitate și a organizației operatorului este utilă. De asemenea, RPD ar trebui să înțeleagă bine operațiunile de prelucrare desfășurate și sistemele informatice, precum și cerințele operatorului legate de securitatea și protecția datelor.

În cazul unei autorități sau al unui organism public, RPD ar trebui să aibă, de asemenea, cunoștințe bune despre regulile și procedurile administrative ale organizației.

- **Capacitatea de îndeplinire a sarcinilor**

Capacitatea de îndeplinire a sarcinilor care îi revin RPD ar trebui să fie interpretată ca făcând referire atât la calitățile personale, cât și la cunoștințe, și totodată la poziția lor în cadrul organizației. Printre calitățile personale ar trebui să se includă, spre exemplu, integritatea și un înalt nivel de etică profesională; preocuparea principală a RPD ar trebui să fie asigurarea conformității cu RGPD. RPD joacă un rol esențial în promovarea unei culturi de protecție a datelor în cadrul organizației și contribuie la implementarea elementelor esențiale din RGPD, cum ar fi principiile de prelucrare a datelor cu caracter personal[26], drepturile persoanelor vizate[27], protecția datelor începând cu momentul

[26] Capitolul II.
[27] Capitolul III.

conceperii și protecția implicită[28], evidența activităților de prelucrare[29], securitatea procesului de prelucrare[30], precum și notificarea și comunicarea cazurilor de încălcare a protecției datelor[31].

- **RPD în baza unui contract de servicii**

Funcția RPD poate fi îndeplinită, de asemenea, în baza unui contract de servicii încheiat cu o persoană fizică sau o organizație din afara organizației operatorului/persoanei împuternicite de către operator. În acest din urmă caz, este esențial ca fiecare membru al organizației care îndeplinește funcțiile unui RPD să respecte toate cerințele aplicabile din secțiunea 4 din RGPD (de exemplu, este esențial ca niciunul să nu se afle într-o situație de conflict de interese). Este la fel de important ca fiecare astfel de membru să fie protejat de dispozițiile RGPD (de exemplu, să nu existe o reziliere abuzivă a contractului de servicii pentru activități desfășurate în calitate de RPD, și nici concedierea abuzivă a vreunuia dintre membrii organizației care îndeplinește sarcinile unui RPD). În același timp, competențele și punctele forte individuale pot fi combinate pentru ca mai multe persoane care lucrează în echipă să își poată servi într-un mod mai eficient clienții.

Din motive de claritate juridică și pentru o bună organizare, precum și pentru a preveni conflictele de interese pentru membrii echipei, se recomandă o alocare clară a sarcinilor în cadrul echipei RPD și numirea unei singure persoane ca persoană de contact principală și persoană „responsabilă" pentru fiecare client. În general, ar fi util și să se menționeze aceste puncte în contractul de servicii.

2.6. Publicarea și comunicarea datelor de contact ale RPD

Articolul 37 alineatul (7) din RGPD prevede ca operatorul sau persoana împuternicită de către operator:

- să publice datele de contact ale RPD și
- să comunice detaliile de contact ale RPD autorităților de supraveghere relevante.

Obiectivul acestor cerințe este de a asigura contactarea cu ușurință și în mod direct a RPD de către persoanele vizate (atât din interiorul, cât și din exteriorul organizației) și autoritățile de supraveghere fără ca acestea să fie nevoite să contacteze o altă parte a organizației. Confidențialitatea este la fel de importantă: de exemplu, angajații ar putea fi reticenți în a adresa o plângere responsabilului cu protecția datelor în cazul în care nu este garantată confidențialitatea comunicărilor lor.
RPD are obligația de a respecta secretul sau confidențialitatea în ceea ce privește îndeplinirea sarcinilor sale, în conformitate cu dreptul Uniunii sau cu dreptul intern [articolul 38 alineatul (5)].

Datele de contact ale RPD ar trebui să conțină informații care să permită persoanelor vizate și autorităților de supraveghere să stabilească ușor legătura cu RPD (o adresă poștală, un număr de telefon specific și/sau o adresă de e-mail specifică). După caz, în scopuri de comunicare cu publicul, ar putea fi puse la asigurate și alte mijloace de comunicare, spre exemplu, o linie telefonică de urgență specială sau un formular de contact special adresat RPD pe site-ul organizației.

[28] Articolul 25.
[29] Articolul 30.
[30] Articolul 32.
[31] Articolele 33 și 34.

Articolul 37 alineatul (7) nu impune ca detaliile de contact publicate să includă numele RPD. Chiar dacă aceasta ar putea fi o bună practică, operatorul sau persoana împuternicită de către operator şi RPD sunt cei care decid dacă acest lucru este necesar sau util în împrejurările specifice date[32].

Însă este esențial să se comunice autorității de supraveghere numele RPD pentru ca acesta să poată exercita rolul de punct de contact între organizație și autoritatea de supraveghere [articolul 39 alineatul (1) litera (e)].

Ca exemplu de bune practici, GL29 recomandă, de asemenea, unei organizații să își informeze angajații cu privire la numele și datele de contact ale RPD. Spre exemplu, numele și datele de contact ale RPD ar putea fi publicate la nivel intern, în rețeaua intranet a organizației, în agenda telefonică internă și în organigrame.

3 Funcția RPD

3.1. Implicarea RPD în toate aspectele legate de protecția datelor cu caracter personal

Articolul 38 din RGDP prevede că operatorul şi persoana împuternicită de către operator se asigură de faptul că RPD *„este implicat în mod corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal”*.

Este esențial ca RPD sau echipa acestuia să se implice într-un stadiu incipient, pe cât posibil, în toate aspectele legate de protecția datelor. În ceea ce privește evaluarea impactului asupra protecției datelor, RGPD prevede în mod explicit implicarea timpurie a RPD și faptul că operatorul trebuie să solicite avizul RPD atunci când efectuează astfel de evaluări ale impactului[33]. Asigurarea faptului că RPD este informat și consultat de la bun început va facilita conformitatea cu RGPD și va promova o abordare privind protejarea vieții private din faza de proiectare și, prin urmare, ar trebui să fie o procedură standard în guvernanța organizației. În plus, este important ca RPD să fie considerat drept un partener de discuții în cadrul organizației și ca acesta să facă parte din grupurile de lucru relevante care se ocupă cu activități de prelucrare a datelor în cadrul organizației.

În consecință, organizația ar trebui să asigure, spre exemplu, că:

- RPD este invitat să participe în mod regulat la reuniunile de la nivelul personalului de conducere de nivel superior şi mediu.
- Prezența acestuia este recomandată în cazul în care se iau decizii cu implicații asupra protecției datelor. Toate informațiile relevante trebuie să fie transmise RPD în timp util, pentru a-i permite acestuia să ofere îndrumări corespunzătoare.
- Trebuie să se acorde întotdeauna importanța cuvenită avizului RPD. În cazul unui dezacord, GL29 recomandă, ca un exemplu de bună practică, documentarea motivelor pentru care nu se respectă avizul RPD.

[32] Este de remarcat că articolul 33 alineatul (3) litera (b), care detaliază informațiile care trebuie puse la dispoziția autorității de supraveghere și a persoanelor vizate în cazul unei încălcări a securității datelor cu caracter personal, spre deosebire de articolul 37 alineatul (7) prevede în mod specific şi comunicarea numelui RPD, nu doar a datelor de contact.

[33] La articolul 35 alineatul (2).

- RPD trebuie să fie consultat imediat după producerea unei încălcări a securității datelor sau apariția unui alt incident.

După caz, operatorul sau persoana împuternicită de către operator ar putea elabora orientări sau programe privind protecția datelor care să prevadă cazurile în care trebuie să fie consultat RPD.

3.2. Resursele necesare

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".* Trebuie să fie luate în considerare următoarele elemente, în mod specific:

- Acordarea de sprijin activ funcției RPD din partea personalului de conducere de nivel superior (cum ar fi la nivelul consiliului de administrație).
- Alocarea unei perioade de timp suficiente pentru îndeplinirea sarcinilor. Acest lucru este deosebit de important în cazul în care este numit un RPD la nivel intern cu fracțiune de normă sau în cazul în care RPD de la nivel extern asigură protecția datelor în plus față de alte îndatoriri. În caz contrar, existența unor priorități contradictorii ar putea conduce la neglijarea de către RPD a sarcinilor sale. Este esențial să se aloce timp suficient pentru sarcinile RPD. Este o bună practică să se stabilească un procent de timp pentru funcția RPD în cazul în care aceasta nu este îndeplinită în regim de normă întreagă. De asemenea, este o bună practică să se stabilească timpul necesar pentru îndeplinirea funcției, nivelul adecvat de prioritate pentru sarcinile RPD și elaborarea de către RPD (sau de către organizație) a unui plan de lucru.
- Acordarea de sprijin corespunzător în ceea ce privește resursele financiare, infrastructura (spații, facilități, echipamente) și personal, după caz.
- Comunicarea oficială a numirii RPD către întregul personal pentru a asigura cunoașterea existenței și funcției acestora în cadrul organizației.
- Asigurarea accesului necesar la alte servicii, cum ar fi serviciul de resurse umane, serviciul juridic, serviciul TI, serviciul de pază etc., pentru ca RPD să poată primi sprijin, date și informații esențiale din partea serviciilor respective.
- Formarea continuă. Responsabililor cu protecția datelor trebuie să li se ofere posibilitatea de a rămâne la curent cu privire la evoluțiile din domeniul protecției datelor. Obiectivul ar trebui să fie acela de a crește în mod constant nivelul de expertiză al RPD, iar aceștia ar trebui să fie încurajați să participe la cursuri de formare privind protecția datelor și la alte forme de dezvoltare profesională, cum ar fi participarea în cadrul forumurilor privind viața privată, al atelierelor de lucru etc.
- Având în vedere dimensiunea și structura organizației, ar putea fi necesar să se constituie o echipă RPD (RPD și personalul acestuia). În astfel de cazuri, structura internă a echipei, precum și sarcinile și responsabilitățile fiecăruia dintre membrii acesteia, ar trebui să fie redactate în mod clar. În mod similar, 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 desemnate pentru client.

În general, cu cât operațiunile de prelucrare a datelor sunt mai complexe și/sau sensibile, cu atât trebuie să i se acorde mai multe resurse RPD. Funcția de protecție a datelor trebuie să fie eficace și asigurată cu resurse suficiente în raport cu acțiunea de prelucrare a datelor desfășurată.

3.3. Instrucțiuni și „*îndeplinirea atribuțiilor și sarcinilor care le revin în mod independent*"

Articolul 38 alineatul (3) stabilește unele garanții de bază pentru a obține certitudinea că RPD au capacitatea de a-și îndeplini sarcinile cu un grad suficient de autonomie în cadrul organizației lor. În mod specific, operatorii/persoanele împuternicite de către operatori trebuie să se asigure că RPD „*nu primește niciun fel de instrucțiuni în ceea ce privește îndeplinirea acestor sarcini.*" Considerentul 97 adaugă faptul că RPD „*indiferent dacă sunt sau nu angajați ai operatorului, ar trebui să fie în măsură să își îndeplinească atribuțiile și sarcinile în mod independent*".

Acest lucru înseamnă că, în îndeplinirea sarcinilor sale în temeiul articolului 39, RPD nu trebuie să primească instrucțiuni privind modul de abordare a unei probleme, de exemplu, ce rezultat ar trebui obținut, cum se examinează o plângere sau dacă să fie consultată autoritatea de supraveghere. În plus, acesta nu trebuie să primească instrucțiuni pentru a adopta un anumit punct de vedere cu privire la un aspect legat de legislația privind protecția datelor, de exemplu, să ofere o anumită interpretare a legii.

Autonomia RPD nu înseamnă însă că aceștia au competențe decizionale care depășesc sarcinile care le revin în temeiul articolului 39.

Operatorul și persoana împuternicită de către operator au în continuare responsabilitatea de a asigura conformitatea cu legislația în domeniul protecției datelor și trebuie să aibă posibilitatea de a demonstra conformitatea respectivă[34]. În cazul în care operatorul sau persoana împuternicită de către operator ia decizii care sunt incompatibile cu RGPD și cu avizul RPD, RPD ar trebui să aibă posibilitatea de a-și exprima în mod clar punctul de vedere la cel mai înalt nivel de conducere și înaintea persoanelor cu putere de decizie. În acest sens, articolul 38 alineatul (3) prevede faptul că RPD „*răspunde direct în fața celui mai înalt nivel al conducerii operatorului sau persoanei împuternicite de operator*". O astfel de raportare directă asigură cunoașterea de către personalul de conducere de nivel superior (de exemplu, consiliul de administrație) a îndrumărilor și recomandărilor care fac parte din misiunea RPD de a informa și a îndruma operatorul sau persoana împuternicită de către operator. Un alt exemplu de raportare directă este redactarea unui raport anual cu activitățile RPD și prezentarea acestuia la cel mai înalt nivel de conducere.

3.4. Concedierea sau sancționarea pentru îndeplinirea sarcinilor RPD

Articolul 38 alineatul (3) prevede că RPD nu ar trebui să fie *„demis sau sancționat de către operator sau de persoana împuternicită de operator pentru îndeplinirea sarcinilor sale"*.

Această cerință consolidează autonomia RPD și asigură faptul că aceștia acționează în mod independent și beneficiază de o protecție suficientă în îndeplinirea sarcinilor lor legate de protecția datelor.

[34] La articolul 5 alineatul (2).

Sancțiunile sunt interzise în conformitate cu RGPD doar în cazul în care acestea sunt impuse ca urmare a îndeplinirii de către RPD a sarcinilor sale în această calitate. De exemplu, un RPD ar putea să considere că o anumită prelucrare este susceptibilă de a genera un risc ridicat și să îndrume operatorul sau persoana împuternicită de către operator să efectueze o evaluare a impactului asupra protecției datelor, însă operatorul sau persoana împuternicită de către operator nu este de acord cu evaluarea propusă de RPD. Într-o astfel de situație, RPD nu poate fi respins pentru faptul că emite acest aviz.

Sancțiunile ar putea fi aplicate în diverse forme, putând fi directe sau indirecte. Acestea ar putea consta, de exemplu, în lipsa sau întârzierea promovării; împiedicarea avansării în carieră; refuzarea avantajelor de care beneficiază alți angajați. Nu este necesar să se aplice efectiv aceste sancțiuni, o simplă amenințare fiind suficientă atâta timp cât acestea sunt utilizate pentru a sancționa RPD din motive legate de activitățile sale desfășurate în calitate de RPD.

Ca și regulă administrativă obișnuită și așa cum ar fi cazul oricărui angajat sau contractant în baza și sub rezerva contractului național aplicabil sau a legislației în domeniul muncii și a dreptului penal, un RPD ar putea fi totuși concediat în mod legitim din alte motive decât cele legate de îndeplinirea sarcinilor sale în calitate de RPD (spre exemplu, în cazul furtului, al hărțuirii fizice, psihologice sau sexuale, ori al abuzului în serviciu în formă gravă)**.**

În acest context, ar trebui remarcat faptul că RGPD nu prevede modalitatea și momentul în care un RPD poate fi demis sau înlocuit de o altă persoană. Cu toate acestea, cu cât un contract cu un RPD este mai stabil și cu cât există mai multe garanții împotriva concedierii abuzive, cu atât este mai probabil ca aceștia să fie în măsură să acționeze în mod independent. Prin urmare, GL29 consideră că ar fi binevenite eforturile depuse de organizații în acest sens.

3.5. Conflictul de interese

Articolul 38 alineatul (6) prevede faptul că RPD poate „*îndeplini și alte sarcini și atribuții"*. Acesta prevede însă ca organizația să se asigure că „*niciuna dintre aceste sarcini și atribuții nu generează un conflict de interese*".

Absența conflictului de interese este strâns legată de cerința de a acționa în mod independent. Cu toate că RPD au permisiunea de a îndeplini și alte funcții, acestora li se pot încredința alte atribuții și sarcini doar cu condiția ca acestea să nu dea naștere unor situații de conflicte de interese. Aceasta presupune, în mod specific, faptul că 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 din cadrul organizației 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. În plus, ar putea să apară un conflict de interese, spre exemplu, și dacă i se solicită unui RPD de la nivel extern să reprezinte operatorul sau persoana împuternicită de către operator în instanță în cauze care implică probleme legate de protecția datelor.

În funcție de activitățile, dimensiunea și structura organizației, următoarele pot fi considerate bune practici pentru operatori sau persoanele împuternicite de către operatori:

- identificarea de funcții care să fie incompatibile cu funcția RPD
- elaborarea de norme interne în acest sens pentru a se evita conflictele de interese
- includerea unei explicații mai generale cu privire la conflictele de interese
- declararea faptului că RPD din cadrul organizației lor nu are niciun conflict de interese în ceea ce privește funcția sa de RPD, ca mijloc de sensibilizare cu privire la această cerință
- includerea de garanții în normele interne ale organizației și asigurarea faptului că anunțul de post vacant pentru postul de RPD sau contractul de prestări servicii este suficient de precis și de detaliat pentru a evita un conflict de interese. În acest context, ar trebui să se rețină, de asemenea, faptul că ar putea exista diferite forme ale conflictelor de interese în funcție de faptul dacă RPD este recrutat pe plan intern sau extern

4 Sarcinile RPD

4.1. Monitorizarea conformității cu RGPD

Articolul 39 alineatul (1) litera (b) încredințează RPD, printre altele, sarcina de a monitoriza conformitatea cu RGPD. Considerentul 97 prevede în continuare faptul că RPD „*ar trebui să acorde asistență operatorului sau persoanei împuternicite de operator pentru monitorizarea conformității, la nivel intern, cu prezentul regulament*".

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
- să informeze, să îndrume și să emită recomandări pentru operatorul sau persoana împuternicită de către operator

Monitorizarea conformității nu înseamnă că RPD este cel care răspunde personal atunci când există un caz de neconformitate. RGPD prevede în mod clar faptul că operatorul, nu RPD, este cel care 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*" [articolul 24 alineatul (1)]. Conformitatea privind protecția datelor este responsabilitatea corporativă a operatorului, nu a RPD.

4.2. Rolul RPD în evaluarea impactului asupra protecției datelor

În conformitate cu articolul 35 alineatul (1), este sarcina operatorului, nu a RPD, de a efectua, după caz, o evaluare a impactului asupra protecției datelor (denumită în continuare „EIPD"). Cu toate acestea, RPD poate juca un rol foarte important și util în acordarea de asistență operatorului. Conform principiului privind protecția datelor începând cu momentul conceperii, articolul 35 alineatul (2) prevede în mod specific faptul că operatorul „*solicită avizul"* RPD atunci când efectuează EIPD. În schimb, articolul 39 alineatul (1) litera (c) sarcina atribuită RPD constă în „*furnizarea de consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia, în conformitate cu articolul 35*".

GL29 recomandă operatorului să solicite avizul RPD cu privire la următoarele aspecte, printre altele [35]:

- 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 RGPD

Dacă operatorul nu este de acord cu avizul dat de RPD, în documentația EIPD ar trebui să se justifice în mod concret în scris de ce nu s-a ținut cont de aviz[36].

În continuare, GL29 recomandă ca operatorul să prezinte în mod clar, de exemplu în contractul RPD, și în informările adresate angajaților, conducerii (și altor părți interesate, după caz), sarcinile concrete ale RPD și domeniul lor de aplicare, în special în ceea ce privește efectuarea EIPD.

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

În conformitate cu articolul 39 alineatul (1) literele (d) și (e), RPD ar trebui să asigure „*cooperarea cu autoritatea de supraveghere*" și „*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"*.

Aceste sarcini se referă la rolul de „facilitator" al RPD, care este menționat în introducerea la prezentele orientări. RPD acționează ca punct de contact pentru a facilita accesul autorității de supraveghere la documentele și informațiile necesare pentru îndeplinirea sarcinilor menționate la articolul 57, precum și pentru exercitarea competențelor sale de investigare, de remediere, de autorizare și de avizare menționate la articolul 58. Astfel cum s-a menționat deja, RPD are obligația de a respecta secretul sau confidențialitatea în ceea ce privește îndeplinirea sarcinilor sale, în conformitate cu dreptul Uniunii sau al statului membru [articolul 38 alineatul (5)]. Cu toate acestea, obligația de a respecta secretul/confidențialitatea nu interzice RPD să contacteze și să solicite avizul autorității de supraveghere. Articolul 39 alineatul (1) litera (e) prevede că RPD poate consulta autoritatea de supraveghere cu privire la orice altă chestiune, după caz.

[35] La articolul 39 alineatul (1) sunt menționate sarcinile RPD, precizându-se faptul că acesta are „*cel puțin"* următoarele sarcini. Prin urmare, nimic nu împiedică operatorul să îi atribuie RPD alte sarcini decât cele menționate în mod explicit la articolul 39 alineatul (1) sau să prevadă sarcinile respective în mai multe detalii.

[36] Articolul 24 alineatul (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. Respectivele măsuri se revizuiesc și se actualizează dacă este necesar*".

4.4. Abordarea bazată pe risc

Articolul 39 alineatul (2) prevede că RPD „*ține seama în mod corespunzător de riscul asociat operațiunilor de prelucrare, luând în considerare natura, domeniul de aplicare, contextul și scopurile prelucrării*".

Acest articol reamintește un principiu general și de bun simț, care ar putea fi relevant pentru multe aspecte ale activității cotidiene a unui RPD. În esență, acesta impune RPD să stabilească prioritatea activităților lor și să își concentreze eforturile asupra aspectelor care prezintă riscuri mai mari pentru protecția datelor. Aceasta nu înseamnă că RPD ar trebui să neglijeze monitorizarea conformității operațiunilor de prelucrare a datelor care prezintă un nivel al riscurilor comparativ mai scăzut, însă articolul indică faptul că aceștia ar trebui să se concentreze, în primul rând, pe domeniile cu grad sporit de risc.

Această abordare pragmatică și selectivă ar trebui să ajute RPD să îndrume operatorul cu privire la metodologia de utilizat la efectuarea unei EIPD, la domeniile care ar trebui să facă obiectul unui audit intern sau extern în ceea ce privește protecția datelor, la activitățile de formare internă care să fie asigurate pentru personal sau personalul de conducere responsabil cu activități de prelucrare a datelor și la operațiunile de prelucrare cărora să le consacre mai mult timp și resurse.

4.5. Rolul RPD în sistemul de păstrare a evidenței

Articolul 30 alineatele (1) și (2) prevede faptul că operatorul sau persoana împuternicită de către operator, nu RPD, este cel sau cea care „*păstrează o evidență a activităților de prelucrare desfășurate sub responsabilitatea lor*" sau care „*păstrează o evidență a tuturor categoriilor de activități de prelucrare desfășurate în numele operatorului*".

În practică, RPD creează deseori inventare și țin un registru al operațiunilor de prelucrare pe baza informațiilor puse la dispoziția lor de către diferitele departamente din cadrul organizației lor, care sunt responsabile cu prelucrarea datelor cu caracter personal. Această practică a fost consacrată în cadrul multor acte legislative actuale din dreptul intern și în conformitate cu normele privind protecția datelor aplicabile instituțiilor și organismelor UE[37].

Articolul 39 alineatul (1) prevede o listă de sarcini pe care RPD trebuie să le dețină ca cerințe minime. Prin urmare, 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 sau a persoanei împuternicite de către operator. 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.

În orice caz, evidența prevăzută la articolul 30 ar trebui considerată, de asemenea, drept un instrument care permite operatorului și autorității de supraveghere, la cerere, să aibă o imagine de ansamblu a tuturor activităților de prelucrare a datelor cu caracter personal pe care le desfășoară o organizație. Astfel, aceasta este o condiție prealabilă pentru conformitatea și, ca atare, o măsură eficace de asumare a responsabilității.

[37] Articolul 24 alineatul (1) litera (d) din Regulamentul (CE) nr. 45/2001.

5 ANEXĂ — ORIENTĂRI PRIVIND RPD: CE TREBUIE SĂ ȘTIȚI

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 de Regulamentul general privind protecția datelor (RGPD) pentru numirea unui RPD.

Desemnarea RPD

1 Ce organizații trebuie să numească un RPD?

Desemnarea unui RPD este obligatorie:

- în cazul în care prelucrarea este efectuată de către o autoritate sau un organism public (indiferent de datele care sunt prelucrate)
- în cazul în care activitățile principale ale operatorului sau ale persoanei împuternicite de către operator constau în operațiuni de prelucrare care necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă
- în 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 cele din urmă, chiar dacă numirea unui RPD nu este obligatorie, organizațiile ar putea să considere uneori utilă numirea unui RPD în mod voluntar. Grupul de lucru pentru protecția datelor în temeiul articolului 29 („GL29”) încurajează aceste eforturi voluntare. Atunci când o organizație numește un RPD în mod voluntar, se vor aplica aceleași cerințe la numire, precum și la stabilirea funcției și a sarcinilor, ca și atunci când numirea ar fi fost obligatorie.

Sursa: Articolul 37 alineatul (1) din RGPD

2 Ce înseamnă „activități principale”?

„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 exemple de 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.

Sursa: Articolul 37 alineatul (1) literele (b) și (c) din RGPD

3 Ce înseamnă „pe scară largă”?

RGPD nu definește noțiunea de prelucrare 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

Sursa: Articolul 37 alineatul (1) literele (b) și (c) din RGPD

4 Ce înseamnă „monitorizare regulată și sistematică”?

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.

Printre exemplele de activități care ar putea constitui monitorizare periodică şi sistematică a persoanelor vizate se numără: exploatarea unei rețele de telecomunicații; furnizarea de servicii de telecomunicații; reorientarea către adrese de e-mail (e-mail retargeting); activități de comercializare bazate pe date; 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.

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

Sursa: Articolul 37 alineatul (1) litera (b) din RGPD

5 Organizațiile pot numi un RPD comun? În caz afirmativ, în ce condiții?

Da. 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. RPD, cu ajutorul unei echipe, dacă este necesar, trebuie să fie în măsură să comunice în mod eficient cu persoanele vizate și să coopereze cu autoritățile de supraveghere interesate. Aceasta înseamnă, de asemenea, că această comunicare trebuie să aibă loc în limba sau în limbile utilizate de către autoritățile de supraveghere și persoanele vizate în cauză. Disponibilitatea 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.

Un singur RPD poate fi numit pentru mai multe autorități sau organisme publice, ținând cont de structura organizatorică și dimensiunea acestora. Se aplică aceleași considerații cu privire la resurse și comunicare. Având în vedere că RPD este responsabil de o serie de sarcini, operatorul sau persoana împuternicită de către operator trebuie să se asigure că un singur RPD, cu ajutorul unei echipe, dacă este necesar, poate îndeplini aceste sarcini în mod eficient, în pofida numirii sale pentru mai multe autorități și organisme publice.

Sursa: Articolul 37 alineatele (2) și (3) din RGPD

6 Unde ar trebui să aibă sediul RPD?

Pentru asigurarea accesibilității RPD, GL29 recomandă ca RPD să se afle pe teritoriul Uniunii Europene, indiferent dacă operatorul sau persoana împuternicită de către operator este stabilit în Uniunea Europeană. Cu toate acestea, nu se poate exclude faptul că, în anumite situații în care operatorul sau persoana împuternicită de către operator nu are un sediu pe teritoriul Uniunii Europene, un RPD ar putea fi în măsură să își desfășoare activitatea într-un mod mai eficace dacă se află în afara UE.

7 Este posibilă numirea unui RPD extern?

Da. 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.

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 aplicabile din RGPD.

Din motive de claritate juridică și pentru o bună organizare, precum și pentru a preveni conflictele de interese în cazul membrilor echipei, 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.

Sursa: Articolul 37 alineatul (6) din RGPD

8 Care sunt calitățile profesionale pe care ar trebui să le aibă RPD?

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-și îndeplini sarcinile.

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 relevante 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

Sursa: Articolul 37 alineatul (5) din RGPD

9 Ce resurse ar trebui să fie puse la dispoziția RPD de către operator sau persoana împuternicită de către operator?

RPD trebuie să dispună de resursele necesare pentru a-și putea îndeplini sarcinile.

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.
- formare continuă

Sursa: Articolul 38 alineatul (2) din RGPD

10 Care sunt garanțiile care îi permit RPD să își îndeplinească sarcinile în mod independent? Ce înseamnă „conflict de interese”?

Există mai multe garanții pentru a-i permite RPD să acționeze în mod independent:

- 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 conflicte de interese cu posibile alte sarcini și atribuții

Celelalte sarcini și atribuții ale unui RPD nu trebuie să genereze un conflict de interese. Aceasta înseamnă, în primul rând, faptul că 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 din cadrul organizației 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. În plus, ar putea să apară un conflict de interese, spre exemplu, și dacă i se solicită unui RPD de la nivel extern să reprezinte operatorul sau persoana împuternicită de către operator în instanță în cauze care implică probleme legate de protecția datelor.

Sursa: Articolul 38 alineatele (3) și (6) din RGPD

Sarcinile RPD

11 Ce înseamnă „monitorizarea conformității”?

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
- să informeze, să îndrume și să emită recomandări pentru operatorul sau persoana împuternicită de către operator

Sursa: Articolul 39 alineatul (1) litera (b) din RGPD

12 Este RPD responsabil personal de neconformitatea cu cerințele privind protecția datelor?

Nu. RPD nu este responsabil personal de neconformitatea cu cerințele privind protecția datelor. 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 acest regulament. Conformitatea privind protecția 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 și păstrarea evidenței activităților de prelucrare?

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 cerințele privind protecția datelor.

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

sau a persoanei împuternicite de către operator. Astfel de evidențe ar trebui să fie considerate 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.

Sursa: Articolul 39 alineatul (1) litera (c) și articolul 30 din RGPD

Adoptate la Bruxelles, 13 decembrie 2016

Pentru grupul de lucru,
Președinte

Isabelle FALQUE-PIERROTIN

Astfel cum au fost revizuite și adoptate ultima dată la 5 aprilie 2017

Pentru grupul de lucru
Președinte

Isabelle FALQUE-PIERROTIN