

Biblia Responsabilului cu Protecția Datelor – 77 Q&A

1. Care este rolul DPO cu ocazia unui control din partea Autorității de supraveghere?

Din punct de vedere legal, la nivel general, responsabilul cu protecția datelor trebuie să fie implicat în mod corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal. Când vorbim despre rolul DPO am putea face o confuzie cu atribuțiile acestuia, noțiuni care, deși aparent sunt similare, în realitate sunt diferite. Rolul DPO se raportează la atribuțiile prevăzute la art. 39 din GDPR, dar nu se va limita la acestea.

Funcția DPO trebuie să asigure îmbunătățirea permanentă și continuă a protecției datelor cu caracter personal. Așadar, pe lângă atribuțiile pe care le are potrivit GDPR (atribuții în evaluarea impactului operațiunilor de prelucrare, menținerea unei legături cu autoritatea de supraveghere etc.), DPO trebuie să își îndeplinească rolul raportat la rațiunile pentru care acesta a fost desemnat, și anume calitățile profesionale și cunoștințele de specialitate în dreptul și practicile din domeniul protecției datelor, precum și capacitatea de a îndeplini sarcinile prevăzute la articolul 39 antementionat.

Așadar, rolul DPO este foarte important în activitatea unui operator deoarece, prin cunoștințele acestuia, nivelul protecției datelor cu caracter personal al operatorului crește concomitent și direct proporțional cu calitățile profesionale și cunoștințele de specialitate deținute de DPO.

Ghidul responsabilului cu protecția datelor emis de Grupul de lucru instituit pe art. 29 din vechea directivă prevede că nivelul de expertiză necesar ar trebui determinat pe baza operațiunilor de prelucrare efectuate și a protecției necesare pentru datele cu caracter personal prelucrate. De exemplu, în situația în care o operațiune de prelucrare a datelor este deosebit de complexă sau în cazul în care este implicat un volum mare

Biblia Responsabilului cu Protecția Datelor – 77 Q&A

de date speciale, DPO poate necesita un nivel mai ridicat de expertiză și suport. Aptitudinile și expertiza relevante includ:

- experiență în legislația și practicile de protecție a datelor la nivel național și european, precum și o înțelegere complexă a RGPD;
- înțelegerea operațiunilor de prelucrare efectuate;
- înțelegerea tehnologiilor de informații și de securitate a datelor;
- cunoașterea sectorului de afaceri și a organizației;
- abilitatea de a promova protecția datelor în cadrul organizației.

Concluzionând, rolul DPO nu se rezumă doar la atribuții. Rolul DPO trebuie să se raporteze la progres și finalitate, respectiv asigurarea unui nivel cât mai ridicat al protecției datelor cu caracter personal.

2. Când este obligatorie DPIA pentru operator?

Evaluarea impactului asupra protecției datelor (DPIA) este obligatorie atunci când un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice. În acest caz, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operațiunilor de prelucrare prevăzute asupra protecției datelor cu caracter personal.

Prin Decizia nr. 174/2018 privind lista operațiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecției datelor cu caracter personal, ANSPDCP (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal) a statuat cazurile în care este necesară DPIA respectiv atunci când:

a) prelucrarea datelor cu caracter personal în vederea realizării unei evaluări sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, și care stă la baza

Biblia Responsabilului cu Protecția Datelor – 77 Q&A

unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;

b) prelucrarea pe scară largă a datelor cu caracter personal privind originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate, a datelor genetice, a datelor biometrice pentru identificarea unică a unei persoane fizice, a datelor privind sănătatea, viața sexuală sau orientarea sexuală ale unei persoane fizice sau a datelor cu caracter personal referitoare la condamnări penale și infracțiuni;

c) prelucrarea datelor cu caracter personal având ca scop monitorizarea sistematică pe scară largă a unei zone accesibile publicului, cum ar fi supravegherea video în centre comerciale, stadioane, piețe, parcuri sau alte asemenea spații;

d) prelucrarea pe scară largă a datelor cu caracter personal ale persoanelor vulnerabile, în special ale minorilor și ale angajaților, prin mijloace automate de monitorizare și/sau înregistrare sistematică a comportamentului, inclusiv în vederea desfășurării activităților de reclamă, marketing și publicitate;

e) prelucrarea pe scară largă a datelor cu caracter personal prin utilizarea inovatoare sau implementarea unor tehnologii noi, în special în cazul în care operațiunile respective limitează capacitatea persoanelor vizate de a-și exercita drepturile, cum ar fi utilizarea tehnicilor de recunoaștere facială în vederea facilitării accesului în diferite spații;

f) prelucrarea pe scară largă a datelor generate de dispozitive cu senzori care transmit date prin internet sau prin alte mijloace (aplicații „Internetul lucrurilor”, cum ar fi smart TV, vehicule conectate, contoare inteligente, jucării inteligente, orașe inteligente sau alte asemenea aplicații);

Biblia Responsabilului cu Protecția Datelor – 77 Q&A

g) prelucrarea pe scară largă și/sau sistematică a datelor de trafic și/sau de localizare a persoanelor fizice (cum ar fi monitorizarea prin Wi-Fi, prelucrarea datelor de localizare geografică a pasagerilor în transportul public sau alte asemenea situații) atunci când prelucrarea nu este necesară pentru prestarea unui serviciu solicitat de persoana vizată.

Trebuie să avem în vedere și faptul că nu este obligatorie DPIA atunci când prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului sau când prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul.

Totuși, trebuie precizat că, deși în afară de cazurile prevăzute mai sus nu este obligatorie DPIA, este recomandat ca aceasta să fie realizată în cazul în care există incertitudini cu privire la realizarea operațiunilor de prelucrare. Astfel, se pot identifica riscuri, se poate asigura un nivel mai ridicat al protecției datelor și, nu în ultimul rând, se poate beneficia de capacitatea și expertiza DPO.

3. Care este rolul DPO în legătură cu întocmirea DPIA?

Rolul DPO în legătură cu întocmirea DPIA este de a supune filtrului și expertizei acestuia evaluarea impactului asupra protecției datelor. Pentru aceasta este necesar avizul responsabilului cu protecția datelor, dacă acesta a fost desemnat. Potrivit dispozițiilor Ghidului privind responsabilul cu protecția datelor emis de Grupul de lucru instituit pe art. 29 din vechea directivă, în ceea ce privește evaluarea impactului operațiunilor de prelucrare (DPIA), operatorul sau persoana împuternicită de operator solicită avizul DPO în legătură cu următoarele aspecte, printre care

- dacă să efectueze sau nu DPIA;
- ce metodologie să fie folosită la efectuarea DPIA;
- dacă să efectueze DPIA intern sau să externalizeze;