Noutăți ale Regulamentului General privind Protecția Datelor

București

15 februarie 2018

Regulamentul General privind Protecţia Datelor

Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date (“**GDPR**”) a intrat în vigoare la data de 25 mai 2016 – **aplicabil din 25 mai 2018**

GDPR înlocuiește Directiva 95/46/EC – NU este necesară transpunerea în legislația națională

Noutăți ale Regulamentului General privind Protecția Datelor

- **Extinderea sferei de aplicabilitate teritorială a GDPR** asupra prelucrărilor efectuate de un operator sau împuternicit care nu e stabilit în UE, *dacă se oferă bunuri sau servicii către persoane aflate în UE sau se monitorizează comportamentul persoanelor din UE*

- **Modificarea sferei de aplicabilitate materială – Directiva 2016/680**

Noutăți ale Regulamentului General privind Protecția Datelor

- **Responsabilul cu protecția datelor (DPO)**
- **Cartografierea - păstrarea evidenței prelucrărilor**
- **Evaluarea de impact**
- **Noi drepturi:** dreptul de a fi uitat, restricționarea prelucrării, portabilitatea datelor
- **Notificarea încălcărilor de securitate**

Responsabilul cu protecţia datelor

OBLIGATORIU :

- **autoritățile publice și organismele publice**, cu excepția instanțelor judecătorești în exercitarea funcției lor jurisdicționale

- toți operatorii care realizează **monitorizări pe scară largă a persoanelor fizice sau prelucrări pe scară largă a unor categorii speciale de date**, prevăzute de art. 9 și 10 GDPR

ex. origine etnică, orientare politică, religioasă, date genetice, date biometrice, privind sănătatea sau referitoare la infracțiuni

Responsabilul cu protecţia datelor

- numit din cadrul personalului operatorului sau persoanei împuternicite de operator pe baza pe contract de prestări servicii (în domeniul public, poate fi desemnat pentru mai multe autorități sau instituții publice, luând în considerare structura organizatorică și dimensiunea acestora)

Condiții de numire (art. 37 GDPR):

- calități profesionale,
- cunoștințe de specialitate în dreptul și practicile din domeniul protecției datelor
- capacitate de îndeplinire a sarcinilor

Responsabilul cu protecţia datelor

- este **independent** – nu primește niciun fel de instrucțiuni în ceea ce privește îndeplinirea sarcinilor

- răspunde direct în fața celui mai înalt nivel al conducerii

- beneficiază de protecție specială - nu poate fi demis sau sancționat pentru îndeplinirea sarcinilor sale

- are obligația de a respecta confidențialitatea în îndeplinirea sarcinilor sale

SARCINI:

- **informare și consiliere** a operatorului/persoanei împuternicite, a angajaţilor acestora care se ocupă de prelucrări de date

- **monitorizarea respectării GDPR** și a altor dispoziţii legale referitoare la protecţia datelor

- **consiliere în realizarea unei evaluări de impact** asupra protecţiei datelor şi **monitorizarea executării acesteia**

- **cooperare cu Autoritatea de Supraveghere și punct de contact cu aceasta**

Cartografierea - art. 30 din GDPR

Se aplică:

- Operatorilor din sistemul public
- Persoanelor împuternicite de operator
- Operatorilor din sectorul privat cu peste 250 de angajați

1. numele și coordonatele operatorului
2. prelucrări de date efectuate
3. **scopul**
4. categoriile de date
5. perioada de stocare
6. destinatarii, transferuri – fluxuri de date
7. măsuri de securitate

Evaluarea de impact – art. 35

Analiză step by step a activităților de prelucrare care ajută operatorul să identifice și să analizeze toate riscurile pe care acestea le pot genera; analiză făcută de operator **cu sprijinul DPO**.

În cazul prelucrărilor susceptibile să genereze un **risc ridicat**:

- evaluare sistematică și cuprinzătoare prin mijloace automate care stau la baza unei decizii care produce efecte juridice asupra persoanei fizice (ex. profiling, predicting)

- prelucrare **pe scară largă** a unor categorii speciale de date cu caracter personal (ex. date biometrice, date genetice) sau date privind condamnările penale și infracțiuni

- monitorizare sistematică **pe scară largă** a unei zone accesibile publicului (ex. CCTV).

Evaluarea de impact

- Listă a tipurilor de operațiuni pentru care este necesară evaluarea întocmită și publicată de autoritatea de supraveghere

- **Criterii** pentru stabilirea prelucrărilor cu **risc ridicat**:
  - prelucrarea este de tip evaluare, scoring, profiling, predicting;
  - produce efecte juridice asupra persoanei fizice;
  - presupune monitorizare sistematică;
  - presupune date personale cu caracter special;
  - presupune prelucrare la scară largă (număr de persoane vizate, volum de date, durata prelucrării, întinderea geografică a prelucrării);
  - presupune combinarea unor date provenite din prelucrări diferite;
  - privește persoane vulnerabile (angajați, minori);
  - presupune tehnologii noi;
  - presupune transfer în afara UE.

- **Cuprinde**: descrierea operațiunilor de prelucrare și a scopurilor; evaluarea necesității și proporționalității operațiunilor de prelucrare; evaluarea riscurilor pentru drepturile și libertățile persoanelor vizate; măsurile avute în vedere pentru abordarea riscurilor.

- Atunci când nu sunt stabilite măsuri suficiente pentru atenuarea riscurilor ridicate **se consultă autoritatea de supraveghere.**

Încălcări de securitate – art. 33 - 34

- Operatorul înștiințează ANSPDCP

Termen: cel mult **72 ore** de la data la care a luat la cunoștință de încălcare

- Persoana împuternicită înștiintează operatorul

- În cazul în care încălcarea securităţii datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, operatorul informează persoana vizată fără întârzieri nejustificate cu privire la aceasta

Privacy by design and by default - art. 25

- **operatorul**, la momentul stabilirii mijloacelor de prelucrare şi al prelucrării în sine, **aplică măsuri tehnice şi organizatorice adecvate** (pseudonimizarea); acestea sunt destinate să pună în aplicare în mod eficient principiile de protecţie a datelor, precum reducerea la minimum a datelor, şi să integreze garanţiile necesare în cadrul prelucrării, pentru a îndeplini cerinţele GDPR şi a proteja drepturile persoanelor vizate;

- operatorul aplică măsuri tehnice şi organizatorice adecvate pentru a asigura că, în mod implicit, **sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării**; această obligaţie se aplică volumului de date colectate, gradului de prelucrare a acestora, perioadei lor de stocare şi accesibilităţii lor - astfel de măsuri asigură că, în mod implicit, datele cu caracter personal nu pot fi accesate, fără intervenţia persoanei, de un număr nelimitat de persoane.

Drepturile persoanelor vizate

- Dreptul la informare (art. 13, 14)
- Dreptul de acces (art. 15)
- Dreptul la rectificare (art. 16, 19)
- Dreptul la ștergere (art. 17, 19) – ”dreptul de a fi uitat”
- Dreptul la restricționarea prelucrării (art. 18, 19)
- Dreptul la portabilitate (art. 20)
- Dreptul la opoziție (art. 21)
- Dreptul de a nu face obiectul unei decizii automate, profilare (art. 22)

Condiții de exercitare a drepturilor

Transparență

Condiții:

- **limbaj clar, simplu (copil)**
- **formă concisă, transparentă, inteligibilă și ușor accesibilă**
- **în scris/electronic/oral**
- **gratuit (excepții – refuz, taxă rezonabilă)**

Facilitarea exercitării drepturilor

Termene:

30 zile

se poate prelungi până la **maximum 3 luni**

1 lună – prelungire termen/refuz adoptare măsuri; motivat; cu drept de a depune plângere la Autoritatea națională de supraveghere și de a depune acțiune în instanță

Responsabilitatea operatorului - art. 24

- operatorul pune în aplicare măsuri tehnice şi organizatorice adecvate pentru a garanta şi a fi în măsură să demonstreze că prelucrarările se efectuează în conformitate cu GDPR; măsurile se revizuiesc şi se actualizează, dacă este necesar

- operatorul poate demonstra conformitatea cu GDPR prin aderarea la **coduri de conduită** aprobate de ANSPDCP

Responsabilitatea împuternicitului - art. 28

- **oferă garanţii suficiente** pentru punerea în aplicare a unor măsuri tehnice şi organizatorice adecvate, astfel încât prelucrarea să respecte cerinţele prevăzute în GDPR şi să asigure protecţia drepturilor persoanei vizate

- prelucrarea de către o persoană împuternicită este reglementată printr-un **contract** care are **caracter obligatoriu** pentru părți şi care stabileşte obiectul şi durata prelucrării, natura şi scopul prelucrării, tipul de date cu caracter personal şi categoriile de persoane vizate şi obligaţiile şi drepturile operatorului

Concluzii

Responsabilizarea operatorului:

- nu mai are obligația notificării prelucrării la ANSPDCP

- respectarea drepturilor persoanelor vizate, inclusiv dreptul de a fi uitat și dreptul la portabilitatea datelor

- studiu de impact - în cazul prelucrărilor ce presupun un risc ridicat pentru viață privată a persoanelor - permite identificarea de riscuri specifice și adoptarea de măsuri de securitate

- numirea unui responsabil pentru protecția datelor

- **sancţiuni severe** - până la 10 – 20 milioane de euro sau între 2% şi 4% din cifra de afaceri la nivel internaţional (în mediul privat)

www.dataprotection.ro - secțiune dedicată GDPR

- Ghid orientativ de aplicare a Regulamentului General privind Protecţia Datelor destinat operatorilor (ANSPDCP)

- Ghidul privind responsabilul cu protecția datelor (WP Art. 29)
- Ghid privind dreptul la portabilitatea datelor
- Ghid pentru stabilirea autorității de supraveghere principale a operatorului sau a persoanei împuternicite de operator

- Ghidul privind notificarea încălcărilor de securitate
- Ghidul privind deciziile automate individuale și profilare
- Ghidul privind consimțământul
- Ghidul privind transparența

AUTORITATEA NAŢIONALĂ DE SUPRAVEGHERE A PRELUCRĂRII DATELOR CU CARACTER PERSONAL

e-mail: anspdcp@dataprotection.ro

www.dataprotection.ro

Simona – Nicoleta ZANFIR