TRANDAFIR&ASSOCIATES

Conferințele CursDeGuvernare.ro

Protecția datelor cu caracter personal: normele europene, pe ultima sută de metri până la activarea automată

- 7 idei esențiale despre GDPR -

Facultatea de Drept, București, 19 martie 2018

George Trandafir
Avocat

Powerful Knowledge

1. Conștientizarea impactului GDPR

- Datele cu caracter personal sunt definite, într-o manieră extensivă, în art. 4 par. (1) GDPR.
- Exemple:

  (1) Tipice: nume, CNP, adresă/locație, adresă de email, fotografii, datele contului bancar, informații privind starea medicală.

  (2) Specifice mediului online: adresa IP, informații postate pe rețelele sociale, istoricul căutărilor pe internet, istoricul cumpărăturilor online, istoricul aplicațiilor descărcate pe telefonul mobil, traseul de jogging înregistrat de aplicațiile telefonului mobil, informații prelevate prin cookie-uri, etc.
- Încadrarea în categoria datelor personale trebuie să aibă în vedere „contextul".
- Important: informațiile privind persoana fizică, în context profesional, sunt date personale.

Aspecte practice

Cum se realizează auditul GDPR într-o organizație

- Este un proces cu o componentă internă semnificativă (i.e. necesită implicarea substanțială a organizației, prin personalul său).
- Întrebări/aspecte esențiale de urmărit:
  (1) Ce date cu caracter personal a colectat organizația de la persoanele vizate (persoane fizice)?
  (2) Cum prelucrează organizația datele cu caracter personal colectate de la persoanele vizate?
  (3) Organizația a efectuat schimburi de date cu caracter personal cu terțe părți sau a transmis aceste date către terțe părți?
  (4) A adoptat organizația vreo măsură de protecție pentru a asigura integritatea/protecția datelor cu caracter personal?
  (5) Evaluarea modului în care Clientul ar putea fi afectat în mod indirect, în baza articolului 25 GDPR?

Aspecte practice

Cum se realizează auditul GDPR într-o organizație – continuare

- Recomandări esențiale pentru audit:

(1) Pentru o inventariere completă a datelor personale, trebuie avute în vedere: interacțiunile dintre organizație și angajați (indiferent de titlul sub care sunt angajați), partenerii de afaceri (indiferent de rolul lor, de ex. furnizori, subcontractori, etc.), sau clienți/alte persoane fizice (în cazul entităților publice), atât din trecut cât și din prezent. Descrieți interacțiunile, de la inițiere până la finalizare.

(2) Stabiliți cu acuratețe și precizați care a fost scopul pentru care au fost colectate, respectiv prelucrate datele cu caracter personal, pentru fiecare categorie în parte (astfel cum există în evidențele organizației).

(3) Descrieți maniera în care datele cu caracter personal sunt prelucrate (utilizate) inclusiv prin referirea la chestiuni tehnice sau practice, circumstanțe, persoane implicate, etc. În abordarea acestei probleme, aveți în vedere definiția legală a "prelucrării", din cadrul art. 4 par. (2) GDPR.

(4) Realizați un audit tehnic, în funcție de necesități.

Aspecte practice

Minimizarea prelucrării

- Este un principiu fundamental al prelucrării datelor cu caracter personal.
- Art. 5 par. (1) lit. (a) GDPR impune ca datele procesate să fie adecvate, relevante și limitate la ceea ce este necesar prin raportare la scopul procesării.
- Aspect practic major: politica de protecție a datelor personale ale fiecărei organizații trebuie să definească ce date personale sunt colectate și procesate, în cazul fiecărei categorii de date, raportat la scopul procesării.

Aspecte practice

Pseudonimizarea

- Preambul, par. 28, GDPR: *„Aplicarea pseudonimizării datelor cu caracter personal poate reduce riscurile pentru persoanele vizate și poate ajuta operatorii și persoanele împuternicite de aceștia să își îndeplinească obligațiile de protecție a datelor. Introducerea explicită a conceptului de „pseudonimizare” în prezentul regulament nu este destinată să împiedice alte eventuale măsuri de protecție a datelor."*
- Constă în *„prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;"*.
- Impact:
  (1) În principiu, poate minimiza costurile de conformare a unui procesator.
  (2) Poate contribui în mod definitoriu la implementarea art. 25 GDPR.
  (3) Ar putea constitui o modalitate de asigurare a legalității procesării în cazurile în care consimțământul persoanelor nu a fost obținut pentru toate scopurile prelucrării; DAR, este necesar ca prelucrarea să nu vizeze o persoană determinată, ci să aibă caracter statistic.

2. Relația cu persoanele ale căror date sunt colectate/prelucrate

- Drepturile persoanelor vizate pot fi exercitate individual, însă și în mod colectiv.
- Profilul unei persoane

  (1) Este o colecție de date personale, în privința căreia sunt aplicabile pe deplin toate principiile cuprinse în art. 5 GDPR cu privire la legalitatea procesării, inclusiv minimizarea și limitarea în timp a stocării datelor.

  (2) Este relevant pentru o multitudine de servicii ale societății informaționale, precum și pentru exercitarea dreptului la portabilitate.

  (3) Impact practic: în caz de neutilizare a unui profil într-o anumită perioadă de timp, dezactivați-l.
- Profiling-ul

  (1) Este o colecție de date personale, dar și modalitate de procesare automată a datelor personale.

  (2) Impact practic: orice servicii oferite în baza unei analize de tip profiling trebuie să aibă în vedere respectarea art. 22 GDPR.

Aspecte practice

Dreptul la portabilitatea datelor personale

- Element de noutate în reglementarea europeană a protecției datelor personale.
- Practic, dreptul la portabilitate impune obligația unui furnizor, ale cărui bunuri și servicii sunt disponibile în baza creării unui profil și a utilizării acestuia în cadrul contractării de bunuri și servicii, de a asigura stocarea și punerea la dispoziția persoanei fizice, la solicitarea acesteia, a profilului astfel creat, în vederea utilizării în relațiile cu un alt furnizor.
- Impact: major, asupra serviciilor societății informaționale, similar portabilității resurselor de numerotație telefonică.

Aspecte practice

GDPR în raporturile cu angajații

- Politica privind protecția datelor personale a fiecărei organizații trebuie să definească categoriile de date colectate de la angajați și modul de prelucrare a acestora.
- GDPR permite legiuitorilor naționali să adopte reguli specifice în privința procesării datelor angajaților. Atenție la legislația internă, care ar putea introduce limitări în privința monitorizării activității angajaților.
- Aspecte practice importante:

(1) Datele personale ale angajaților nu pot fi reținute de către angajator pe perioadă nelimitată, după încetarea raporturilor de muncă. Definiți prin politica organizației o perioadă optimă în decursul căreia să fie păstrate datele personale.

(2) Profilul unui angajat, prelucrat de către angajator și făcut public, în interiorul organizației, de exemplu prin intranet, reprezintă un model de prelucrare a datelor personale, cu privire la care sunt aplicabile toate drepturile și garanțiile oferite de GDPR.

3. Relația cu autoritățile de resort

- Autoritatea de resort în domeniul datelor personale poate dispune două categorii de măsuri în privința operatorilor:
  (1) sancțiuni – amenzile administrative, în condițiile legislației privind contravențiile (OG nr. 2/2001), la care face trimitere în mod explicit 83 (inclusiv prin art. 83 par. (9) GDPR);
  (2) măsuri corective (cf. art. 58 par. (2) GDPR) - cu caracter preventiv sau de remediere a unor încălcări ale GDPR.
- Raporturile dintre persoanele vizate și autoritățile de resort:
  (1) Art. 80 GDPR reglementează posibilitatea exercitării acțiunilor colective, de către ONG-uri, în numele persoanelor vizate, chiar și fără mandatul acestora.
  (2) Art. 80 GDPR reglementează posibilitatea exercitării colective a drepturilor persoanelor vizate, prin depunerea unei plângeri la autoritatea de resort (art. 77 GDPR), respectiv prin dreptul de a exercita o cale judiciară de atac împotriva deciziei autorității de resort (art. 78 GDPR).

4. GDPR în raporturile cu partenerii de afaceri

- GDPR este aplicabil în relațiile cu partenerii de afaceri, întrucât acestea pot implica procesarea de date cu caracter personal, aparținând unor persoane fizice.
- GDPR reglementează această ipoteză, întrucât stabilește, prin art. 6 par. (1) lit. (b), că datele personale sunt procesate în mod legal atunci când procesarea acestora este necesară pentru executarea unui contract.
- Recomandări practice (raportat la condițiile impuse prin art. 5 GDPR):
  (1) Aplicați principiul minimizării procesării (nu colectați și nu procesați mai multe date decât ceea ce este necesar pentru managementul raporturilor de afaceri).
  (2) Solicitați consimțământul explicit al persoanelor ale căror date de contact doriți să le păstrați, după finalizarea contractului, pentru relații de afaceri viitoare.
  (3) Stabiliți o durată maximă de păstrare a datelor, după încetarea raporturilor contractuale.

5. GDPR și entitățile publice

- Entitățile publice au obligația stabilirii unor politici/proceduri în domeniul protecției datelor (cf. art. 24 par. (1) & (2) GDPR).
- Politicile/procedurile în domeniul protecției datelor personale constituie informații de interes public, conform Legii nr. 544/2001; pot fi accesate de către ONG-uri având drept scop protecția datelor personale și care pot exercita, în numele persoanelor vizate, drepturile recunoscute acestora, chiar fără mandat (cf. art. 80 GDPR).
- Entitățile publice au obligația numirii unui DPO (intern sau extern), cu excepția instanțelor de judecată (raportat la activitatea jurisdicțională) – cf. art. 37 par. (1) lit. (a). GDPR.
- În cazul contractării serviciilor unui DPO, sunt aplicabile prevederile OUG nr. 26/2012 (cf. art. 37 par. (6) GDPR).
- Proiectul de lege privind unele măsuri pentru aplicarea GDPR [aflat în procedură parlamentară] stabilește, în baza art. 83 paragraful (7) din GDPR, regimul sancționator aplicabil entităților publice; amenzile pot ajunge la 200.000 lei; sunt aplicabile prevederile OG nr. 2/2001, însă în contextul art. 83 par. 8 GDPR.
- Atenție la concilierea obligațiilor stabilite prin Legea nr. 544/2001 și GDPR (cf. art. 86 GDPR) – GDPR nu împiedică, în principiu, comunicarea informațiilor de interes public (cf. preambul 154 GDPR).

6. Data protection by design and by default

- Un principiu esențial al GDPR, reglementat de art. 25 („*Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit*").
- Textul evidențiază impactul transversal și multidisciplinar al GDPR.
- Impactul practic:
  (1) Orice obiect, aplicație IT sau tehnologie care folosește date personale va trebui să respecte cerințele GDPR (e.g. platforma de operare a unui magazin online, împreună cu orice software asociat acesteia).
  (2) Contractele care privesc asemenea „obiecte" trebuie să includă clauze privind respectarea GDPR (i.e. garanții, în sensul art. 1714 din codul civil cu privire la garanțiile pentru lipsa calităților convenite).
  (2) Se pot implementa sisteme de certificare a conformității GDPR (cf. art. 42 GDPR), care să suplinească prevederile contractuale.

7. Aplicabilitatea în timp a GDPR

- Problemă: în ce măsură GDPR are un efect retroactiv?
- Exemple practice:
  (1) Este necesar să se obțină din nou consimțământul persoanelor vizate, ale căror date sunt procesate, dacă au fost colectate anterior intrării în vigoare a GDPR (cf. art. 7 GDPR)?
  (2) Este necesar să se țină evidențe ale operațiunilor de prelucrare a datelor personale realizate anterior intrării în vigoare a GDPR (cf. art. 30 GDPR)?
- Principiul de drept al încrederii legitime (Eng. *protection of legitimate expectation*, Fr. *Principe de confiance legitime*) se opune, în principiu, efectului retroactiv al dreptului comunitar; excepțiile sunt însă permise (cf. CJCE, cauzele conexate C-260/91 și C-261/91).
- Concluzie: doar practica poate să confirme în ce măsură un efect retroactiv al GDPR există; în orice caz, existența unei perioade de tranziție (între data intrării în vigoare și data aplicării GDPR) este un argument pentru efectul (pseudo)retroactiv.