EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR ȘI BREȘA DE SECURITATE/DPIA ȘI DATA BREACH

AVOCAT LUIZA BUDUȘAN

EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR
DPIA (DATA PROTECTION IMPACT ASSESSMENT)

- Evaluarea impactului asupra protecției datelor cu caracter personal – DPIA (data protection impact assessment) este o operațiune anterioară prelucrării datelor cu caracter personal, prin care operatorii fac o analiză completă și concretă atât a datelor pe care urmează să le prelucreze, cât și a condițiilor în care se va face prelucrarea, pentru a vedea care sunt cele mai bune metode de prelucrare a datelor, de respectare a principiilor Regulamentului, a drepturilor persoanelor vizate și, totodată, de protejare a acestor date.
- Ea le permite operatorilor să identifice măsurile optime de securitate.

- Reglementarea procedurii se regăsește în art. 35 din Regulament, care prevede:

- (1) Având în vedere natura, domeniul de aplicare, contextul și scopurile prelucrării, în cazul în care 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, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operațiunilor de prelucrare prevăzute asupra protecției datelor cu caracter personal. O evaluare unică poate aborda un set de operațiuni de prelucrare similare care prezintă riscuri ridicate similare.
- (2) La realizarea unei evaluări a impactului asupra protecției datelor, operatorul solicită avizul responsabilului cu protecția datelor, dacă acesta a fost desemnat.

EVALUAREA IMPACTULUI

- Grupul de lucru art. 29 apreciază o DPIA **poate fi utilă, de asemenea, pentru a evalua impactul unui produs al tehnologiei asupra protecției datelor**, de exemplu, al unui element de hardware sau software, atunci când este posibil ca acesta să fie utilizat de diferiți operatori de date pentru a efectua diferite operațiuni de prelucrare.

- Art. 35 alin. 3 menționează că evaluarea impactului asupra protecției datelor menționată la alin. 1 se impune **mai ales** în cazul:

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

- ***(b) prelucrării pe scară largă a unor categorii speciale de date, menționată la articolul 9 alineatul (1), sau a unor date cu caracter personal privind condamnări penale și infracțiuni, menționată la articolul 10;***

- ***(c) unei monitorizări sistematice pe scară largă a unei zone accesibile publicului.***

DECIZIA NR. 174 DIN 18 OCTOMBRIE 2018

- ANASPDCP a emis ***Decizia nr. 174 din 18 octombrie 2018 privind lista operaţiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecţiei datelor cu caracter personal***, care cuprinde o listă a operațiunilor pentru care este necesară efectuarea evaluării:

- a) prelucrarea datelor cu caracter personal în vederea realizării unei evaluări sistematice şi cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, şi care stă la baza 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, viaţa sexuală sau orientarea sexuală ale unei persoane fizice sau a datelor cu caracter personal referitoare la condamnări penale şi infracţiuni;

- 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, pieţe, parcuri sau alte asemenea spaţii;

- d) prelucrarea pe scară largă a datelor cu caracter personal ale persoanelor vulnerabile, în special ale minorilor şi ale angajaţilor, prin mijloace automate de monitorizare şi/sau înregistrare sistematică a comportamentului, inclusiv în vederea desfăşurării activităţilor de reclamă, marketing şi 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 operaţiunile respective limitează capacitatea persoanelor vizate de a-şi exercita drepturile, cum ar fi utilizarea tehnicilor de recunoaştere facială în vederea facilitării accesului în diferite spaţii;

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

- g) prelucrarea pe scară largă şi/sau sistematică a datelor de trafic şi/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 situaţii) atunci când prelucrarea nu este necesară pentru prestarea unui serviciu solicitat de persoana vizată.

- Publicată în Monitorul Oficial al României nr. 919 din 31 octombrie 2018

UTILIZAREA CRITERIILOR DPIA

- Grupul de lucru, în Ghidul pe care l-a elaborat, referitor la *Evaluarea impactului asupra protecției datelor (DPIA) și stabilirea dacă o prelucrare este „susceptibilă să genereze un risc ridicat" în sensul Regulamentului 2016/679,* a făcut trimitere la mai multe exemple cu privire la modul în care ar trebui să fie utilizate criteriile, pentru a stabili dacă o anumită operațiune de prelucrare necesită sau nu o DPIA.
- 1. un spital care prelucrează datele genetice și de sănătate ale pacienților; sunt astfel prelucrate date sensibile sau foarte personale, date referitoare la persoane vizate vulnerabile și este o prelucrare la scară largă;
- 2. utilizarea unui sistem de camere pentru a monitoriza comportamentul de conducere pe autostrăzi; operatorul intenționează să utilizeze un sistem inteligent de analiză video pentru a identifica autoturismele și pentru a recunoaște în mod automat plăcuțele de înmatriculare. In acest caz are loc o monitorizare sistematică și utilizarea inovatoare sau aplicarea unor soluții tehnologice sau organizaționale;
- 3. colectarea de date personale de pe platformele de comunicare pentru generarea de profiluri; in acest caz are loc o evaluare sau punctare, datele sunt prelucrate la scară largă, corelarea sau combinarea unor seturi de date; sunt date sensibile sau foarte personale.

STUDIUL DE IMPACT

- **Continutul unui studiu de impact**

  DPIA trebuie sa cuprinda:

- **(a) o descriere sistematică a operațiunilor de prelucrare preconizate și a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator;**
- **(b) o evaluare a necesității și proporționalității operațiunilor de prelucrare în legătură cu aceste scopuri;**
- **(c) o evaluare a riscurilor pentru drepturile și libertățile persoanelor vizate**
- **(d) măsurile preconizate în vederea abordării riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze conformitatea cu dispozițiile prezentului regulament, luând în considerare drepturile și interesele legitime ale persoanelor vizate și ale altor persoane interesate.**

BRESA DE SECURITATE/DATA BREACH

- Art. 4 alin. 12 din Regulament o definește după cum urmează: *încălcarea securității datelor cu caracter personal înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea.*

- Incălcările pot fi clasificate conform următoarelor trei principii:

- - *încălcarea confidențialității* - în cazul în care există o dezvăluire neautorizată sau accidentală sau acces la datele personale;
- - *incălcarea integrității* - în cazul în care există o modificare neautorizată sau accidentală a datelor cu caracter personal;
- - *incălcare a disponibilității - în cazul în care există o pierdere accidentală sau neautorizată a accesului la sau distrugerea datelor personale, de exemplu, când datele au fost șterse fie accidental, fie de către o persoană neautorizată.*

NOTIFICAREA AUTORITATII SI A PERSONEI VIZATE

- *Potrivit art. 33 din Regulament, intitulat* ***Notificarea autorității de supraveghere în cazul încălcării securității datelor cu caracter personal,*** *în cazul în care are loc o încălcare a securității datelor cu caracter personal, operatorul notifică acest lucru autorității de supraveghere competente, fără întârzieri nejustificate și, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta.*
- Notificarea autoritatii poate fi facuta si in etape, respectiv, în termenul inițial de 72 de ore, să aibă loc informarea autorității cu privire la existența brești de securitate, oferindu-se o parte dintre informațiile deținute de către operator la acel moment, iar ulterior, operatorul să revină cu una sau mai multe completări, pe măsură ce acesta culege și el informațiile legate de incident.
- În cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul informează persoana vizată fără întârzieri nejustificate cu privire la această încălcare.

- Producerea unei încălcări a securității datelor are drept cauză faptul că operatorul nu a luat toate măsurile tehnice și organizatorice necesare pentru a asigura securitatea acestora.
- Ca urmare, acesta are obligația de a revizui măsurile luate, de a le îmbunătăți și, totodată, de a verifica eficiența lor.