Curs Formare Regulamentul UE 2016/679 și Directiva UE 2016/680

Proiect: O operațiune a UE de combatere a lacunelor din cooperarea transfrontalieră a furnizorilor de formare (*An EU operation to tackle gaps in cross-border cooperation of training providers*). Program: Justice. Numar identificare Proiect: 807014

București, 26-28 Februarie 2020

Safe Harbor

InfoCons
protectia-consumatorilor.ro

EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR CU CARACTER PERSONAL (DPIA) ȘI CONSULTAREA PREALABILĂ

Ana-Maria Baciu
SCA Simion & Baciu

București, 26-28 Februarie 2020

Cuprins:

Abstract

- Evaluarea impactului asupra protecției datelor cu caracter personal (DPIA) este o nouă cerință în cadrul GDPR, ca parte a principiului "protection by design“.

- DPIA este utilizată în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este suseptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operațiunilor de prelucrare avute în vedere asupra protecției datelor cu caracter personal.

În practică, trebuie analizată necesitatea efectuării DPIA de fiecare dată când:

i. se utilizează noile tehnologii;

ii. se urmărește locația sau comportamentul persoanelor;

iii. se monitorizează sistematic un loc accesibil publicului pe scară largă;

iv. se prelucrează date sensibile;

v. prelucrarea datelor este utilizată pentru a lua decizii automate cu privire la persoane sau dacă datele prelucrate pot duce la vătămări fizice ale persoanelor vizate în caz de divulgare neautorizată.

1. Evaluarea impactului asupra protecției datelor cu caracter personal (DPIA)

1.1. Legislație aplicabilă la nivelul Uniunii Europene

- La nivelul Uniunii Europene, sediul materiei este constituit de art. 35 din Regulamentul 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), denumit în cele ce urmează „GDPR”:

„(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.

(3) Evaluarea impactului asupra protecției datelor menționată la alineatul (1) se impune mai ales în cazul:

a) unei evaluări sistematice și cuprinzătoare a aspectelor personale referitoare la persoanele fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, și care stă la baza unor decizii care produc efecte juridice privind o persoană 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; sau

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

(…)

(7) Evaluarea cuprinde cel puțin:

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 menționate la alineatul (1);

d) măsurile preconizate în vederea abordării riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter persoanl și să demonstreze conformitatea cu dispozițiile prezentului regulament, luând în considerare drepturile și interesele legitime ale persoanelor vizate și ale altor persoane interesate.”

1.2. Ghiduri de implementare la nivelul Uniunii Europene

- În data de 4 aprilie 2017, Grupul de Lucru creat în temeiul articolului 29 din Directiva 95/46/CE, organism consultativ european independent care se ocupă cu protecția și confidențialitatea datelor, a adoptat Ghidul privind Evaluarea impactului asupra protecției datelor (DPIA) și stabiliarea dacă o prelucrare este „susceptibilă să genereze un risc ridicat” în sensul Regulamentului 2016/679, referit în cele ce urmează „Ghidul DPIA”.

- Ghidul DPIA își dorește să clarifice noțiunea de prelucrare susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, aceasta fiind situația premisă ce atrage obligativitatea unei evaluări a impactului asupra protecției datelor, precum și să furnizeze criterii pentru listele adoptate la nivel național de autoritățile de protecție a datelor.

Considerente de principiu ce trebuie avute în vedere:

i. Realizarea unei DPIA nu este obligatorie pentru fiecare operațiune de prelucrare de date personale;

ii. DPIA se poate referi doar la o singură operațiune de prelucrare sau la un set de operațiuni similare de prelucrare;

iii. DPIA se realizează anterior prelucrării, fără ca prin aceasta să se înțeleagă că efectuarea DPIA ar fi un exercițiu unic;

iv. Responsabilitatea pentru efectuarea DPIA incumbă operatorului;

v. Operatorul trebuie să solicite avizul persoanelor vizate sau al reprezentanților acestora, acolo unde este cazul, privind prelucrarea prevăzută;

vi. GDPR permite operatorului un grad ridicat de libertate în determinarea structurii și formei DPIA, tocmai pentru a permite ca aceasta să se potrivească practicilor de lucru existente.

1.3. Legislația aplicabilă la nivel național

- În completarea prevederilor art. 35 din GDPR – direct aplicabile în dreptul național fără a se impune adoptarea unor măsuri suplimentare de orice natură la nivel național – Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal („ANSPDCP”) a emis Decizia 174/2018 privind lista operațiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecției datelor cu caracter personal, referită în cele ce urmează ca „Decizia nr. 170/2018”.

- Lista operațiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecției datelor adoptată prin Decizia nr. 170/2018 cuprinde, de o manieră neexhaustivă, urmatoarele situații de prelucrare:

a) prelucrarea datelor cu caracter personal în vederea realizării unei evaluări sistematice și cuprinzătoare a aspectelor personale referite la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, și care stă la baza unor decizii care producefecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;

b) prelucrarea pe scara largă a datelor cu caracter personal privind originea rasială sau etnică, opiniilor 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 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 exclusive 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);

g) prelucrarea pe scară largă și/sau sistematică a datelor de trafic și/sau 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 fizică.”

1.4. Ghidul orientativ de aplicare a GDPR emis la nivel național de către ANSPDCP

- Ghidul orientativ de aplicare a GDPR destinat operatorilor emis de către ANSPDCP tratează în mod succint evaluarea impactului asupra protecției datelor, în contextul obligației generale a operatorilor de date de asigurare a gestionării riscurilor, prin enunțarea cerințelor legale principale stabilite prin GDPR.

- Se subliniază că în efectuarea unei evaluări a impactului asupra protecției datelor se „va pune accent pe estimarea riscurilor asupra protecției datelor din punctul de vedere al persoanelor vizate, luând în considerare natura datelor, domeniul de aplicare, contextul și scopurile prelucrării și utilizarea noilor tehnologii.”

2. Consultarea prealabilă

2.1. Sediul legal

- Legislația națională adoptată în baza GDPR nu conține dispoziții mai restrictive decât cele ale actului normativ european, acolo unde acesta permite.
- Conform art. 36 din GDPR:

(1) Operatorul consultă autoritatea de supraveghere înainte de prelucrare atunci când evaluarea impactului asupra protecției datelor prevăzută la articolul 35 indică faptul că prelucrarea ar genera un risc ridicat în absența unor măsuri luate de operator pentru atenuarea riscului.

(2) Atunci când consideră că prelucrarea prevăzută menționată la alineatul (1) ar încălca prezentul regulament, în special atunci cînd riscul nu a fost identificat sau atenuat într-o măsură suficientă de către operator, autoritatea de supraveghere oferă consiliere în scris operatorului și, după caz, persoanei împuternicite de operator, în cel mult opt săptămâni de la primirea cererii de consultare, și își poate utiliza oricare dintre competențele menționate la articolul 58.

Această perioadă poate fi prelungită cu șase săptămâni, ținându-se seama de complexitatea prelucrării prevăzute. Autoritatea de supraveghere informează operatorul și, după caz, persoana împuternicită de operator, în termen de o lună de la primirea cererii, cu privire la orice astfel de prelungire, prezentând motivele întârzierii. Aceste perioade pot fi suspendate până când autoritatea de supraveghere a obținut informațiile pe care le-a solicitat în scopul consultării.

(3) Atunci când consultă autoritatea de supraveghere în conformitate cu alineatul (1), operatorul îi furnizează acesteia:

a) dacă este cazul, responsabilitățile respective ale operatorului, ale operatorilor asociați și ale persoanelor împuternicite de operator implicate în activitățile de prelucrare, în special pentru prelucrarea în cadrul unui grup de întreprinderi;

b) scopurile și mijloacele prelucrării preconizate;

c) măsurile și garanțiile prevăzute pentru protecția datelor și libertăților persoanelor vizate, în conformitate cu prezentul regulament;

d) dacă este cazul, datele de contact ale responsabilului cu protectia datelor;

e) evaluarea impactului asupra protecției datelor prevăzută la articolul 35;

f) orice alte informații solicitate de autoritatea de supraveghere.

(4) Statele membre consultă autoritatea de supraveghere în cadrul procesului de pregătire a unei propuneri de măsură legislativă care urmează să fie adoptată de un parlament național sau a unei măsuri de reglementare întemeiate pe o astf de măsură legisativă, care se referă la prelucrare.

(5) În pofida alineatului (1), dreptul intern poate impune operatorilor să se consulte cu autoritatea de supraveghere și să obțină în prealabil autorizarea din partea acesteia în legătură cu prelucrarea de către un operator în vederea îndeplinirii unei sarcini exercitate de acesta în interes public, inclusiv prelucrarea în legătură cu protecția socială și sănătatea publică.”

2.2. Ghiduri de implementare și aplicare

- În abordarea problematicii consultării autorității de supraveghere conform art. 36 din GDPR, Ghidul DPIA oferă o serie de exemple relevante de risc ridicat inacceptabil:

i. accesul ilegal la datele care duc la amenințarea vieții persoanelor vizate, concediere, risc financiar;

ii. inaptitudinea de a reduce numărul de persoane care accesează datele datorită modalităților de partajare, de utilizare, de distribuție sau atunci când vulnerabilitatea bine cunoscută nu este înlăturată.

- Aceste exemple practice derivă din caracterul evident al faptului că riscul va avea loc.

Întrebări ?

Va mulțumim!

Str. Maior Alexandru Câmpeanu nr. 11, etj. 1
Bucharest 011235, Romania

e-mail: office@simionbaciu.ro

Tel/Fax: +40-31 419 04

București, 26-28 Februarie 2020