**Evaluarea riscurilor prezentate de prelucrarea datelor**

**cu caracter personal din grupul țintă**

Camera de Comerţ, Industrie și Agricultură Dâmbovița cu sediul în Municipiul Târgoviste, str. Calea Câmpulung, nr. 6A, jud. Dâmbovița, tel. 0245.210.318,e-mail info@cciadb.ro**,** în calitate de ***Beneficiar***, în implementarea proiectului **IMM DIGITall** - Dezvoltarea integrată a competențelor digitale pentru angajații și specialiștii IT care activează în sectoarele SNC/domeniile SNCDI la nivelul Regiunii Sud-Muntenia **(POCU/860/3/12/141968)** respectă confidenţialitatea tuturor cursanților sau persoanelor împlicate în buna desfășurare a proiectului **IMM DIGITall** şi va trata/prelucra datele personale cu mare atenţie, în condiţii tehnice şi organizatorice de securitate adecvată.

Camera de Comerţ, Industrie și Agricultură Dâmbovița prelucrează datele cu caracter personal, primite direct de la entitatea grupului țintă, în calitate de persoane vizate sau indirect cu ocazia derulării cursurilor, organizate de către beneficiar sau unul dintre parteneri şi/sau în incinta sediului sau a altor săli de cursuri.

 Datele cu caracter personal sunt colectate numai cu acordul/acceptul entității grupului țintă și sunt oferite cu bună ştiinţă.

 Evaluarea impactului asupra protecției datelor (DPIA) este un proces destinat să descrie prelucrarea, să evalueze necesitatea și proporționalitatea acesteia și să contribuie la gestionarea riscurilor la adresa drepturilor și libertăților persoanelor vizate rezultate din prelucrarea datelor cu caracter personal , prin evaluarea acestora și stabilirea de măsuri pentru atenuarea lor.

Evaluarea impactului asupra protecției datelor (DPIA) reprezintă un instrument important pentru responsabilizare deoarece ajută operatorii de date, nu numai să respecte cerințele GDPR, ci și să demonstreze că au fost luate măsuri adecvate pentru a asigura conformitatea cu Regulamentul. Cu alte cuvinte, evaluarea impactului asupra protecției datelor (DPIA) reprezintă un proces pentru construirea și demonstrarea conformității.

      GDPR cere operatorilor să implementeze măsuri adecvate pentru a asigura și demonstra conformitatea cu RGPD, luând în considerare, printre altele, „riscurile de variație a probabilității și gravității asupra drepturilor și libertăților persoanelor fizice”. Obligația operatorilor de a realiza evaluarea impactului asupra protecției datelor în anumite situații ar trebui înțeleasă în contextul obligației lor generale de a gestiona în mod corespunzător riscurile prezentate de prelucrarea datelor cu caracter personal.

Un „risc” reprezintă un scenariu care descrie un eveniment și consecințele acestuia, estimat în termeni de severitate și probabilitate. Pe de altă parte, „managementul riscului” poate fi definit ca fiind activitățile coordonate pentru a conduce și controla o organizație cu privire la un risc.

Suplimentar, GDPR impune o procedură de revizuire periodică, analiză și evaluare a eficacității măsurilor tehnice și organizatorice (art. 32 alin. (1) lit. (d) din GDPR). GDPR oferă posibilitatea evaluării procedurilor bazate pe IT în codurile de conduită și prin mecanisme de certificare (art. 40-43 ale GDPR). Articolul 5 al GDPR / art.4 din Legea nr. 133/2011 stabilește principiile de bază pentru prelucrarea datelor cu caracter personal: datele cu caracter personal sunt prelucrate în mod legal, corect și transparent, colectate în scopuri precise, explicite și legitime, bazate pe date exacte, protejate împotriva pierderii, distrugerii sau deteriorării și într-un fel care asigură integritatea și confidențialitatea acestora.

Gestionarea riscurilor în domeniul prelucrării datelor cu caracter personal

În cazul în care au fost identificate prelucrări de date cu caracter personal susceptibile de a prezenta riscuri ridicate pentru drepturile și libertatile persoanelor fizice, operatorul va efectua o evaluare a impactului asupra protecției datelor, în condițiile art. 35 din Regulamentul General privind Protecția Datelor.

Evaluarea impactului asupra protecției datelor se realizează anterior colectării datelor cu caracter personal si efectuarii prelucrarii. 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. Evaluarea impactului asupra protecției datelor presupune:
- o descriere a prelucrării de date efectuate și a scopurilor acesteia;
- o evaluare a necesității și a proportionalității prelucrării de date efectuate;
- o estimare a riscurilor asupra drepturilor și libertăților persoanelor vizate;
- măsurile prevazute pentru a trata riscurile și a asigura conformitatea cu dispozitiile Regulamentul General privind Protecția Datelor.

Evaluarea impactului asupra protectiei datelor permite:
- realizarea unei prelucrari de date cu caracter personal sau a unui produs care respecta viata privata;
- estimarea impactului asupra vietii private a persoanelor vizate;
- demonstarea faptului ca principiile fundamentale ale Regulamentul General privind Protectia Datelor sunt respectate. Evaluarea impactului asupra protecției datelor se impune, mai ales, în cazul:

* unei evaluări sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, și care sta la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afecteaza în mod similar într-o măsură semnificativă;
* prelucrării pe scara larga a unor categorii speciale de date sau a unor date cu caracter personal privind condamnari penale si infractiuni;
* unei monitorizari sistematice pe scara larga a unei zone accesibile publicului. Când evaluarea de impact indică riscuri ridicate, în absența unor măsuri luate de operator pentru atenuarea acestora, se consultă Autoritatea națională de supraveghere.

În calitate de responsabil în domeniul protecției datelor cu caracter special, am înțeles importanța evaluării riscurilor asociate prelucrării datelor cu caracter personal din grupul țintă.

Evaluarea riscurilor reprezintă un pilon esențial în implementarea unui cadru robust de protecție a datelor. În cadrul acestui proces, identificarea și analiza atentă a potențialelor amenințări și vulnerabilități devin cruciale.

Grupul țintă, ca entitate distinctă, aduce cu sine particularități și sensibilități specifice, impunând o abordare personalizată a evaluării riscurilor.

Un aspect esențial constă în identificarea datelor cu caracter personal prelucrate în cadrul grupului țintă, precum și în evaluarea modului în care aceste informații sensibile sunt colectate, stocate, prelucrate și partajate.

Riscurile pot rezulta din diverse surse, inclusiv procesele interne, tehnologiile utilizate și factorii umani implicați în manipularea datelor.

Evaluarea trebuie să țină cont de conformitatea cu legislația privind protecția datelor, asigurând că toate prevederile legale sunt respectate în mod riguros. În plus, se impune luarea în considerare a potențialelor impacturi asupra individului, precum și a consecințelor reputaționale și financiare pentru organizație în cazul producerii unui incident de securitate.

Clarificarea scopului prelucrării datelor în cadrul proiectului: o direcție bine definită.

În contextul activităților proiectului în care persoana din grupul țintă este implicată, este imperativ să avem un scop clar definit pentru prelucrarea datelor cu caracter personal. Aceasta nu este doar o cerință legală, ci și un pilon esențial al respectului față de confidențialitatea individului și al asigurării unei colaborări etice și transparente.

Scopul prelucrării datelor trebuie să fie aliniat cu obiectivele specifice ale proiectului, iar această aliniere trebuie să fie evidentă și comprehensibilă pentru persoanele din grupul țintă. Fiecare activitate de prelucrare trebuie să servească unui scop bine definit și să fie justificată în contextul proiectului respectiv.

Claritatea în stabilirea scopului prelucrării datelor este esențială pentru a evita ambiguitățile și pentru a construi încrederea în rândul participanților din grupul țintă. Aceasta presupune comunicare deschisă și transparentă, în care fiecare persoană implicată să înțeleagă modul în care datele lor vor fi utilizate în cadrul proiectului și cum contribuie la realizarea obiectivelor stabilite.

În același timp, este crucial să se respecte principiile de minimizare a datelor, adică să se colecteze și să se proceseze doar informațiile strict necesare pentru atingerea scopurilor stabilite. Astfel, se asigură că prelucrarea datelor este eficientă și proporțională în raport cu activitățile proiectului.

Măsuri de securitate pentru asigurarea prelucrării

 datelor cu caracter personal:

Asigurarea securității prelucrării datelor cu caracter personal reprezintă un aspect crucial în protecția informațiilor sensibile. Astfel au fost luate câteva măsuri esențiale pentru garantarea unui mediu sigur:

* Formarea și conștientizarea grupului țintă: educația continuă a grupului țintă, cu privire la practici sigure în manipularea datelor și la riscurile de securitate cibernetică este crucială. Un grup țintă bine informat reprezintă o linie de apărare eficientă.
* Actualizări și patch-uri de securitate: menținerea sistemelor și software-urilor la zi prin aplicarea regulată a actualizărilor și patch-urilor de securitate este esențială pentru a remedia vulnerabilități cunoscute.
* Conformitate cu reglementările:\* asigurarea conformității cu reglementările privind protecția datelor, cum ar fi GDPR sau alte norme regionale, este fundamentală. Monitorizarea schimbărilor în legislație și ajustarea practicilor în consecință este esențială.

 Adoptarea acestor măsuri contribuie la crearea unui mediu sigur și încrezător pentru prelucrarea datelor cu caracter personal, protejând astfel informațiile sensibile și respectând drepturile individuale.

În concluzie, scopul prelucrării datelor trebuie să fie nu doar legal și etic, ci și orientat către atingerea cu succes a obiectivelor proiectului, contribuind astfel la construirea unei fundații solide pentru colaborarea în cadrul grupului țintă.

Prin abordarea metodică a evaluării riscurilor, organizarea poate dezvolta strategii eficiente de gestionare a acestora, contribuind la întărirea securității datelor cu caracter personal în cadrul grupului țintă.

Responsabil GDPR și protecția datelor cu caracter special:

Dodan Simona Mihaela