Școala Gimnazială, Sat Ulmetu, Comuna Copăceni, Județul Vâlcea
Cod Fiscal: **29007244**

Politica generală GDPR
Numărul 1053 din 25.07.2023

Domeniul de aplicare al Regulamentului

La data de 27 aprilie 2016 a fost adoptat de către Parlamentul European și Consiliul Uniunii Europene Regulamentul nr. 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 95/46ICE, denumit în continuare RGPD, act normativ cu aplicabilitate directă în statele membre.

În acord cu prevederile art. 99 alin. (1) și (2) din RGPD, acest act normativ a intrat în vigoare la data de 25 mai 2016 și se aplică de la 25 mai 2018.

Dispoziții relevante din Regulamentul general privind protecția datelor

Definiții

Conform art. 4 din RGPD, termenii de mai jos au următoarele semnificații:

- „date cu caracter personal" înseamnă orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată"); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

- „prelucrare" înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;

- „restricționarea prelucrării" înseamnă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;

- „pseudonimizare" înseamnă 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;

- „sistem de evidență a datelor" înseamnă orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcționale sau geografice;

- „operator" înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern;

- „persoană împuternicită de operator" înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

- „destinatar" înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Cu toate acestea, autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autoritățile publice respective respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării;

- „parte terță" înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;

- „consimțământ" al persoanei vizate înseamnă orice manifestare de voință liberă, specifică, informată și

lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;

- „organizație internațională" înseamnă o organizație și organismele sale subordonate reglementate de dreptul internațional public sau orice alt organism care este instituit printr-un acord încheiat între două sau mai multe țări sau în temeiul unui astfel de acord.

Principii legate de prelucrarea datelor cu caracter personal

Art. 5 alin. (1) din RGPD prevede faptul că datele cu caracter personal sunt:

a) prelucrate în mod legal, echitabil și transparent față de persoana vizată („legalitate, echitate și transparență");

b) colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile în conformitate cu articolul 89 alineatul (1) din RGPD („limitări legate de scop");

c) adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate („reducerea la minimum a datelor");

d) exacte și, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere („exactitate");

e) păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1) din RGPD, sub rezerva punerii în aplicare a măsurilor de ordin tehnic și organizatoric adecvate prevăzute în prezentul regulament în vederea garantării drepturilor și libertăților persoanei vizate („limitări legate de stocare");

f) prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare („integritate și confidențialitate").

Operatorul este responsabil de respectarea art. 5 alin. (1) din RGPD și poate demonstra această respectare („responsabilitate").

Legalitatea prelucrării

Astfel cum prevede art. 6 alin. (1) din RGPD, prelucrarea este legală numai dacă și în măsura în care se aplică cel puțin una dintre următoarele condiții:

a) persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;

b) prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;

c) prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;

d) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;

e) prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul;

Prelucrarea de categorii speciale de date cu caracter personal

Se interzice prelucrarea de date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice, așa cum prevede art. 9 din RGPD.

Prevederile din paragraful de mai sus nu se aplică în următoarele situații:

a) persoana vizată și-a dat consimțământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice, cu excepția cazului în care dreptul Uniunii sau dreptul intern prevede ca interdicția prevăzută la paragraful de mai sus să nu poată fi ridicată prin consimțământul persoanei vizate;

b) prelucrarea este necesară în scopul îndeplinirii obligațiilor și al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forței de muncă și al securității sociale și protecției sociale, în măsura în care acest lucru este autorizat de dreptul Uniunii sau de dreptul intern ori de un acord colectiv de muncă încheiat în temeiul dreptului intern care prevede garanții adecvate pentru drepturile fundamentale și interesele persoanei vizate.

Condiții privind consimțământul

În temeiul art. 7 din RGPD, în cazul în care prelucrarea se bazează pe consimțământ, operatorul trebuie să fie în măsură să demonstreze că persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal.

În cazul în care consimțământul persoanei vizate este dat în contextul unei declarații scrise care se referă și la alte aspecte, cererea privind consimțământul trebuie să fie prezentată într-o formă care o diferențiază în mod clar de celelalte aspecte, într-o formă inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu. Nicio parte a respectivei declarații care constituie o încălcare a RGPD nu este obligatorie.

Persoana vizată are dreptul să își retragă în orice moment consimțământul.

Retragerea consimțământului nu afectează legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia. Înainte de acordarea consimțământului, persoana vizată este informată cu privire la acest lucru. Retragerea consimțământului se face la fel de simplu ca acordarea acestuia.

Transferurile de date cu caracter personal către țări terțe sau organizații internaționale

Principiul general al transferurilor

În baza art. 44 din RGPD, orice date cu caracter personal care fac obiectul prelucrării sau care urmează a fi prelucrate după ce sunt transferate într-o țară terță sau către o organizație internațională pot fi transferate doar dacă, sub rezerva celorlalte dispoziții ale prezentului regulament, condițiile prevăzute în prezentul capitol sunt respectate de operator și de persoana împuternicită de operator, inclusiv în ceea ce privește transferurile ulterioare de date cu caracter personal din țara terță sau de la organizația internațională către o altă țară terță sau către o altă organizație internațională. Toate dispozițiile din prezentul capitol se aplică pentru a se asigura că nivelul de protecție a persoanelor fizice garantat prin prezentul regulament nu este subminat.

Prelucrarea necesară a datelor personale pentru încheierea și executarea unui contract

Elementul cheie care justifică utilizarea acestui temei juridic este necesitatea încheierii sau executării unui contract.

În acest context, prelucrarea este legală dacă:

a) Există un contract valabil, pentru a cărui executare este necesară prelucrarea de date cu caracter personal;

b) În faza pre-contractuală, la solicitarea persoanei vizate, este nevoie de prelucrarea anumitor date cu caracter personal în vederea încheierii contractului.

În mod contrar, prelucrarea nu se poate baza pe temeiul încheierii/executării contractului dacă:

a) Trebuie prelucrate datele unei persoane, alta decât cea cu care se încheie contractul;

b) Inițiativa încheierii contractului aparține operatorului sau unei terțe persoane.

Cerința necesității prelucrării pentru încheierea sau executarea unui contract nu înseamnă întotdeauna că prelucrarea este esențială în acest scop, totuși aceasta trebuie să fie limitată și proporțională cu scopul urmărit.

Drepturi specifice incidente în contextul prelucrării datelor cu caracter personal

RGPD prevede 8 drepturi specifice în materie de prelucrare a datelor cu caracter personal, care pot fi exercitate în măsura în care nu aduc atingere drepturilor și libertăților altora:

a) Dreptul de acces la date;

b) Dreptul la rectificarea datelor;

c) Dreptul la ștergerea datelor;

d) Dreptul la restricționarea prelucrării;

e) Dreptul la portabilitatea datelor;

f) Dreptul de opoziție la prelucrarea datelor;

g) Dreptul de a nu fi supus unor decizi automatizate, inclusiv profilarea;

h) Dreptul la notificarea destinatarilor privind rectificarea, ștergerea ori restricționarea datelor cu caracter personal.

Aspecte generale privind confidențialitatea și securitatea datelor

Conform art. 32 din RGPD,

Având în vedere stadiul actual al dezvoltării, costurile implementării și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscul cu diferite grade de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul și persoana împuternicită de acesta implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând printre altele, după caz:

a) pseudonimizarea și criptarea datelor cu caracter personal;

b) capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare;

c) capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natura fizică sau tehnică;

d) un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

Un rol important în evaluarea nivelului adecvat de securitate îl vor avea riscurile pe care le implică prelucrarea, riscuri ce pot fi generate, accidental ori ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.

Demonstrarea îndeplinirii condițiilor menționate se poate realiza, printre altele, prin aderarea la un cod de conduită aprobat în temeiul art. 40 din RGPD sau la un mecanism de certificare aprobat în temeiul art. 42 RGPD.

Organizarea procedurilor interne în domeniul protecției datelor

Pentru a asigura permanent un nivel ridicat de protecție a datelor cu caracter personal, operatorul trebuie să elaboreze proceduri interne care să garanteze respectarea protecției datelor în orice moment, luând în considerare toate evenimentele care pot apărea pe parcursul efectuării prelucrărilor de date, precum:

- breșe de securitate;

- solicitări privind exercitarea drepturilor persoanelor vizate;

- modificarea datelor cu caracter personal colectate;

- schimbarea prestatorului.

Organizarea procedurilor interne implică, în special:

- luarea în considerare a protecției datelor cu caracter personal încă de la momentul conceperii (privacy by design) unei aplicații sau a unei prelucrări: minimizarea colectării datelor în funcție de scop, cookie-uri, perioada de stocare, informațiile furnizate persoanelor vizate, obținerea consimțământului persoanelor vizate, securitatea și confidențialitatea datelor cu caracter personal, garantarea rolului și responsabilității părților implicate în efectuarea prelucrării datelor;

- aplicarea de măsuri tehnice și 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 (privacy by default), având în vedere: volumul de date colectate, gradul de prelucrare a acestora, perioada de

stocare și accesibilitatea lor, astfel încât datele cu caracter personal să nu fie accesate, fără intervenția persoanei, de un număr nelimitat de persoane;

- sensibilizarea și organizarea diseminării informației, în special prin stabilirea unui plan de pregătire și de comunicare cu persoanele care prelucrează date cu caracter personal;

- soluționarea plângerilor și cererilor adresate de persoanele vizate în exercitarea drepturilor lor, stabilind părțile implicate și modalitățile de exercitare a acestora; exercitarea drepturilor trebuie să se poată realiza inclusiv pe cale electronică, în cazul în care datele au fost colectate prin astfel de mijloace;

- anticiparea unei posibile încălcări a securității datelor specificând, pentru anumite cazuri, obligativitatea notificării autorității pentru protecția datelor în termen de 72 de ore și a persoanelor vizate în cel mai scurt timp;

- asigurarea confidențialității și securității prelucrării prin adoptarea de măsuri tehnice și organizatorice adecvate, incluzând printre altele, după caz:

a) pseudonimizarea și criptarea datelor cu caracter personal;

b) capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare;

c) capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;

d) un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

Protejarea datelor cu caracter personal considerate "sensibile"

Următoarele categorii speciale de date cu caracter personal sunt considerate "sensibile" și beneficiază de protecție specifică în temeiul RGPD:

- originea etnică sau rasială;

- opiniile politice;

- confesiunea religioasă sau convingerile filozofice;

- apartenența la sindicate;

- prelucrarea de date genetice;

- prelucrarea de date biometrice pentru identificarea unică a unei persoane fizice;

- sănătatea;

- viața sexuală sau orientarea sexuală.

Regula generală este că prelucrarea datelor menționate este interzisă. Pe baza anumitor derogări, o unitate ar putea, însă, să prelucreze date cu caracter personal sensibile, atunci când, de exemplu:

- v-ați făcut publice în mod manifest propriile date sensibile;

- v-ați dat consimțământul explicit;

- există o lege care reglementează un anumit tip de prelucrare de date într-un anumit scop legat de interesul public sau de sănătate;

- o lege care include garanții adecvate prevede prelucrarea datelor cu caracter personal sensibile în domenii precum sănătatea publică, ocuparea forței de muncă și protecția socială.

Colectarea datelor cu caracter personal despre copii

Pentru acest tip de date cu caracter personal s-au instituit măsuri de protecție suplimentare, deoarece copiii sunt mai puțin conștienți de riscurile și consecințele transmiterii datelor, precum și de drepturile proprii.

Orice informații adresate în mod specific unui copil ar trebui adaptate pentru a fi ușor accesibile, formulate într-un limbaj simplu și clar.

Pentru majoritatea serviciilor online este necesar consimțământul unui părinte sau al unui tutore legal pentru prelucrarea datelor cu caracter personal ale unui copil pe bază de consimțământ până la o anumită vârstă. Acest lucru este valabil pentru site-urile de rețele sociale, precum și pentru platformele pentru descărcarea de muzică și cumpărarea de jocuri online.

Limita de vârstă pentru obținerea consimțământului părinților este stabilită de fiecare stat membru al UE și poate fi între 13 și 16 ani.

Unitățile trebuie să depună eforturi rezonabile, ținând seama de tehnologiile disponibile, pentru a se asigura că respectivul consimțământ a fost într-adevăr acordat în conformitate cu prevederile legislației aplicabile. Aceste eforturi pot cuprinde implementarea unor măsuri de verificare a vârstei (de exemplu, o întrebare la care un copil mediu nu ar ști să răspundă sau solicitarea ca minorul să comunice adresa de e-mail a părintelui său pentru a face posibilă acordarea consimțământului scris).

Serviciile de prevenire sau de consiliere oferite direct copiilor sunt scutite de obligația de a obține consimțământul unui părinte, deoarece ele urmăresc protejarea intereselor copiilor.

Drepturile persoanelor fizice instituite de GDPR

Aveți dreptul:

- să primiți informații privind prelucrarea datelor dvs. cu caracter personal;

- să obțineți acces la datele cu caracter personal deținute în legătură cu dvs.;

- să solicitați corectarea datelor cu caracter personal incorecte, inexacte sau incomplete;

- să solicitați ștergerea datelor cu caracter personal când acestea nu mai sunt necesare sau dacă prelucrarea acestora este ilegală;

- să vă opuneți prelucrării datelor dvs. cu caracter personal în scopuri de marketing sau din motive legate de situația particulară în care vă aflați;

- să solicitați restricționarea prelucrării datelor dvs. cu caracter personal în anumite cazuri;

- să primiți datele dvs. cu caracter personal într-un format care poate fi citit automat și să le trimiteți altui operator („portabilitatea datelor");

- să solicitați ca deciziile bazate pe prelucrarea automată a datelor dvs. cu caracter personal care vă privesc sau care vă afectează într-o măsură semnificativă să fie luate de către persoane fizice, nu exclusiv de computere. În acest caz, aveți și dreptul de a vă exprima punctul de vedere și de a contesta decizia.

Pentru a vă exercita drepturile, ar trebui să contactați unitatea care vă prelucrează datele (adică operatorul de date). În cazul în care unitatea are un responsabil cu protecția datelor (RPD), îi puteți adresa cererea acestui RPD. Unitatea trebuie să răspundă cererilor fără întârzieri nejustificate și cel târziu în termen de o lună. Dacă nu intenționează să se conformeze la cererea dvs., unitatea trebuie să motiveze refuzul. Vi se poate cere să furnizați informații pentru a vă confirma identitatea (de exemplu, să faceți click pe un link de verificare, să introduceți un nume de utilizator sau o parolă) pentru a vă exercita drepturile.

Aceste drepturi se aplică în întreaga UE, indiferent unde se prelucrează datele și unde își are sediul unitatea. Aceste drepturi se aplică și când cumpărați produse și servicii de la unități din afara UE care își desfășoară activitatea în UE.

Cum pot fi accesate datele cu caracter personal pe care le deține o unitate

Aveți dreptul de a obține din partea unității o confirmare că se prelucrează sau nu date cu caracter personal care vă privesc.

În cazul în care unitatea are datele dvs. cu caracter personal, aveți dreptul să accesați datele respective, să primiți o copie și să obțineți orice informații suplimentare relevante (cum ar fi motivul prelucrării datelor dvs. cu caracter personal, categoriile de date cu caracter personal utilizate etc.).

Acest drept de acces ar trebui să poată fi exercitat cu ușurință și să fie posibil la „intervale de timp rezonabile". Unitatea ar trebui să vă furnizeze gratuit o copie a datelor dvs. cu caracter personal. Eventualele copii suplimentare pot fi supuse unei taxe rezonabile. Dacă efectuați cererea prin mijloace electronice (de exemplu, printr-un e-mail) și nu solicitați un alt format, informațiile ar trebui furnizate într-un format electronic utilizat în mod curent.

Acest drept nu este unul absolut, exercitarea dreptului de acces la datele dvs. cu caracter personal nu ar trebui să afecteze drepturile și libertățile altora, inclusiv secretele comerciale sau proprietatea intelectuală.

Evidența gestionării cererilor de exercitare a drepturilor persoanelor cărora le sunt prelucrate datele personale

Atât cât acționează ca operator cât și ca persoană împuternicită, este recomandabilă păstrarea de către operator a unei evidențe clare a răspunsurilor date în contextul cererilor persoanelor vizate de exercitare a drepturilor specifice în materie de prelucrare a datelor cu caracter personal. Astfel:

a) Operatorul trebuie să aibă dovezi clare scrise (inclusiv conținând răspunsurile și data transmiterii acestora) care să ateste îndeplinirea obligațiilor specifice în materie; recomandăm păstrarea evidenței pe două paliere: solicitări primite cu toate informațiile aferente cu evidențierea datei primirii acestora și respectiv răspunsuri transmise, cu evidențierea datei transmiterii răspunsurilor, iar unde este cazul de prelungire a termenului de răspuns după o lună, cu indicarea clară a motivului prelungirii.

b) Persoana împuternicită trebuie să aibă dovezi scrise care să susțină transmiterea în termen util a informațiilor solicitate respectiv implementarea în mod rezonabil a măsurilor necesare pentru conformarea cu drepturile specifice ale persoanelor vizate a operatorilor care le solicită informații/luarea de măsuri specifice.

Este preferabilă păstrarea dovezilor în formă scrisă. Cu toate acestea, dacă persoana vizată solicită anumite informații oral, este admisibilă și păstrarea unor dovezi ale înregistrărilor care să ateste răspunsul acordat unor asemenea solicitări.

Îndeplinirea obligației privind ținerea evidențelor prelucrărilor datelor

Din interpretarea art. 30 alin. 5 din RGPD, rezultă că obligația menținerii unei evidențe a activităților de prelucrare a datelor cu caracter personal este obligatorie de principiu, instituțiilor cu peste 250 de angajați.

Instituțiile cu mai puțin de 250 de angajați sunt obligați să țină această evidență doar dacă prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate, prelucrarea nu este ocazională sau prelucrarea include categorii speciale de date, astfel cum se prevede la articolul 9 alineatul (1), sau date cu caracter personal referitoare la condamnări penale și infracțiuni, astfel cum se menționează la articolul 10 din RGPD.

Deși cele mai multe unități s-ar afla sub pragul de 250 de angajați, categoriile de date prelucrate determină, în principiu, existența unui registru de prelucrare a datelor personale.

Externalizarea gestiunii datelor utilizate în activitatea operatorilor (servicii de cloud, servicii de gestiune a datelor/documentelor)

Executarea în practică a acestor obligații ce derivă din externalizarea gestiunii datelor cu caracter personal este lăsată la latitudinea operatorilor, motiv pentru care nu poate fi exclusă utilizarea unor metode și proceduri de externalizare a datelor prin servicii de cloud sau de gestiune a datelor/documentelor.

Specificul acestor proceduri și mecanisme ce presupun transferul unor date din evidența operatorilor către serverele administrate de terțe persoane (denumite generic în continuare prestatorii de servicii de gestiune a datelor, persoane împuternicite în accepțiunea RGPD) impun o atenție sporită pentru respectarea RGPD și pentru evitarea oricăror breșe de securitate.

De aceea, se impune luarea unor măsuri minime de siguranță:

a) Analiza tehnologiei care stă la baza infrastructurii cloud/de gestiune a datelor folosite în scopul determinării nivelului de securitate a datelor, îndeplinirea cerințelor impuse de RGPD etc.

b) Pentru a permite exercitarea drepturilor persoanelor vizate (dreptul de a fi uitat, dreptul de acces la informații, dreptul de a fi informat etc) operatorul trebuie să se asigure că prestatorii de servicii de gestiune a datelor cunosc locația fizică a fiecărui server prin care administrează bazele de date în discuție. Aceasta se impune întrucât documentele electronice sunt mai greu de găsit decât documentele în format fizic, primele putând fi transferate prin sisteme backup, arhive sau către terțe părți/entități (ex.: Dropbox). În scopurile respectării RGPD, atât operatorul, cât și persoana împuternicită trebuie sa aibă o evidență clară cu privire la localizarea fiecărei informații. În același scop (exercitarea drepturilor de către persoanele vizate), se impune revizuirea de către operator a protocoalelor de backup și stocare utilizate de către prestatorii de servicii de gestiune a datelor.

c) Asumarea expresă de către prestatorii de servicii de gestiune a datelor, a obligațiilor ce le incumbă în temeiul RGPD și a legislației aplicabile în raport atât cu operatorul cât și cu persoanele vizate.

d) Determinarea locației exacte a serverelor este utilă și pentru a determina legislația aplicabilă diferitelor operațiuni.

e) Pentru a evita compromiterea datelor în integralitatea lor și a breșelor de securitate cu impact major, este recomandabilă împărțirea datelor pe diverse categorii și stocarea lor pe servere diferite.

f) Reiterarea în contractele și acordurile încheiate între operatori și prestatorii de servicii de gestiune a datelor (în calitate de persoane împuternicite) ca prelucrarea datelor cu caracter personal transmise către cei din urmă se face în numele operatorilor, aceștia menținând controlul constant asupra informațiilor.

g) Crearea unor proceduri de verificare și de analiză de risc cărora să le fie supuși prestatorii de servicii

de gestiune a datelor și testarea periodică a respectării legislației aplicabile în domeniul prelucrării datelor cu caracter personal (spre exemplu, dar fără a se limita la, art. 28 din RGPD)

Desemnarea responsabilului cu protecția datelor (DPO)

Pentru a îndruma modul în care sunt gestionate datele cu caracter personal în cadrul unui operator sau al unei persoane împuternicite de operator, în anumite situații, este necesară o persoană care să exercite o misiune de informare, de consiliere și de control în plan intern: responsabilul cu protecția datelor.

Desemnarea unui responsabil cu protecția datelor este obligatorie din 25 mai 2018, raportat la dispozițiile art. 37 - 39 din RGPD, în cazul în care operatorul sau persoana împuternicită de operator:

- este o autoritate publică sau un organism public, cu excepția instanțelor în exercitarea funcției lor jurisdicționale;

- desfășoară o activitate principală care conduce la realizarea unei monitorizări constante și sistematice pe scara largă a persoanelor;

- desfășoară o activitate principală care constă în prelucrarea pe scara largă de date sensibile (cum ar fi: date privind originea rasială sau etnică, convingerile religioase, apartenența sindicală, date genetice, biometrice, privind starea de sănătate) sau referitoare la condamnări penale și infracțiuni.

Chiar dacă entitatea nu are obligația expresă de a desemna un responsabil cu protecția datelor, ANSPDCP recomandă numirea acestuia, în considerarea efectului benefic al activității responsabilului în vederea asigurării respectării RGPD de către operatorul respectiv sau persoana împuternicită de operator.

Un responsabil cu protecția datelor reprezintă un avantaj major pentru operator în vederea înțelegerii și respectării obligațiilor prevăzute de RGPD, dialogului cu autoritățile pentru protecția datelor și reducerii riscurilor apariției unor litigii.

Rolul responsabilului cu protecția datelor (DPO)

Conform art. 39 din RGPD, responsabilul cu protecția datelor are rolul:

- să informeze și să consilieze operatorul sau persoana împuternicită de operator, precum și angajații acestora cu privire la obligațiile existente în domeniul protecției datelor cu caracter personal;

- să monitorizeze respectarea RGPD și a legislației naționale în domeniul protecției datelor;

- să consilieze operatorul sau persoana împuternicită în legătură cu realizarea de studii de impact privind protecția datelor și să verifice efectuarea acestora;

- să coopereze cu autoritatea pentru protecția datelor și să reprezinte punctul de contact în relația cu aceasta.

Cartografierea prelucrărilor de date cu caracter personal

Toți operatorii din sistemul public, persoanele împuternicite de operator, precum și operatorii din sistemul privat cu peste 250 de angajați, au obligația cartografierii prelucrărilor de date cu caracter personal efectuate, raportat la prevederile art. 30 din RGPD.

Chiar și operatorii din sistemul privat cu mai puțin de 250 de angajați au obligația cartografierii prelucrărilor în cazurile în care prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate, în cazul în care prelucrarea nu este ocazională sau prelucrarea include categorii speciale de date ori date cu caracter personal referitoare la condamnări penale și infracțiuni.

În acest sens pentru a evalua în mod eficient impactul RGPD asupra activității entității, este necesară identificarea prelucrărilor de date cu caracter personal efectuate și păstrarea evidenței activităților de prelucrare.

Pentru a avea o evidență completă și exactă a prelucrărilor de date cu caracter personal efectuate și pentru a răspunde noilor exigențe, trebuie identificate, în prealabil, cu precizie:

- diferitele prelucrări de date cu caracter personal;

- categoriile de date cu caracter personal prelucrate;

- scopurile urmărite prin operațiunile de prelucrare a datelor;

- persoanele care prelucrează aceste date;

- fluxurile de date, indicând originea și destinația datelor, în special pentru a identifica eventualele

transferuri de date în afara Uniunii Europene.

Evidența păstrată de operator va cuprinde:

a) numele și datele de contact ale operatorului și, după caz, ale operatorului asociat, ale reprezentantului operatorului și ale responsabilului cu protecția datelor;

b) scopurile prelucrării;

c) o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal;

d) categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe sau organizații internaționale;

e) dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și, în cazul transferurilor menționate la articolul 49 alin. (1) paragraful 2 din RGPD, documentația care dovedește existența unor garanții adecvate;

f) acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date;

g) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 32 alin. (1) din RGPD.

Consimțământul necesar prelucrării datelor cu caracter personal. Condiții de valabilitate

În lumina noilor prevederi ale RGPD, prelucrarea datelor pe bază de consimțământ presupune respectarea unor standarde legale specifice.

A prelucra date pe baza consimțământului, înseamnă a da persoanei vizate reala libertate de alegere și control sporit asupra prelucrării. Câteva din cele mai importante reguli de obținere și gestionare a consimțământului sunt:

a) Consimțământ explicit. Consimțământul trebuie să fie exprimat în mod explicit, într-o manieră clară și specifică (manifestare pozitivă a consimțământului). Utilizarea unor metode de exprimare implicită/tacită a consimțământului (căsuțe de acord pre-bifate) nu este o practică legală;

b) Consimțământ nelegat. Furnizarea unui serviciu solicitat de / oferit persoanei vizate nu poate fi condiționată de acordarea consimțământului pentru prelucrare din partea respectivei persoane, întrucât astfel, consimțământul nu ar fi liber exprimat;

c) Consimțământ separat. Consimțământul trebuie solicitat în mod separat de termeni și condiții ori alte documente de informare și prezentare și în mod specific pentru fiecare scop pentru care se face prelucrare pe acest temei juridic;

d) Consimțământ documentat. Consimțământul trebuie documentat și dovada acestuia trebuie păstrată. Ca principiu, operatorul trebuie să poată demonstra cine a dat consimțământul, când, prin ce metodă și ce informații au fost furnizate cu ocazia preluării consimțământului;

e) Consimțământ revocabil. Persoana vizată are dreptul de a retrage consimțământul în orice moment (forma de manifestare a dreptului de a fi uitat), iar operatorul trebuie să ofere un mecanism de retragere facil și să acționeze pentru a da eficiență retragerii în cel mai scurt timp posibil.

Procedura de solicitare a consimțământului pentru prelucrarea datelor cu caracter personal

Cererea privind consimțământul trebuie prezentată într-o formă clară și concisă, într-un limbaj ușor de înțeles, și trebuie să se diferențieze în mod clar de alte informații, cum ar fi termenele și condițiile.

Cererea trebuie să precizeze cum vor fi utilizate datele dvs. cu caracter personal și să includă datele de contact ale unității care prelucrează datele. Consimțământul trebuie să fie o manifestare liber exprimată, specifică, în cunoștință de cauză și clară. Consimțământul „în cunoștință de cauză" înseamnă că trebuie să vi se ofere informații cu privire la prelucrarea datelor dvs. cu caracter personal, inclusiv cel puțin:

- identitatea unității care prelucrează datele;

- scopurile în care sunt prelucrate datele;

- tipul de date care se vor prelucra;

- posibilitatea de retragere a consimțământului (de exemplu prin trimiterea unui e-mail pentru a vă retrage consimțământul);

- dacă este cazul, faptul că datele vor fi utilizate pentru luarea de decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri;

- în cazul în care consimțământul se referă la un transfer internațional al datelor dvs., riscurile posibile ale transferurilor de date în țări din afara UE, dacă nu există o decizie privind caracterul adecvat al nivelului de protecție sau garanții adecvate în privința acestor țări.

Când se face informarea cu privire la prelucrarea datelor cu caracter personal?

În cazul datelor cu caracter personal colectate direct de la persoana vizată, informarea se face în momentul obținerii datelor.

Raportat la art. 14 alin. (3) din RGPD, în cazul datelor cu caracter personal colectate din alte surse, informarea se face:

a) într-un termen rezonabil după obținerea datelor cu caracter personal, dar nu mai mare de o lună, ținându-se seama de circumstanțele specifice în care sunt prelucrate datele cu caracter personal;

b) dacă datele cu caracter personal urmează să fie utilizate pentru comunicarea cu persoana vizată, cel târziu în momentul primei comunicări către persoana vizată respectivă;

c) dacă se intenționează divulgarea datelor cu caracter personal către un alt destinatar, cel mai târziu la data la care acestea sunt divulgate pentru prima oară.

Informații ce trebuie transmise când se cere acordul privind prelucrarea datelor cu caracter personal

Informațiile minime ce ar trebui transmise în cazul primirii unor cereri de acces vizează:

1) scopurile prelucrării

2) destinatarii sau categoriile de destinatari cărora datele le-au fost sau urmează să le fie divulgate

3) categoriile de date cu caracter personal vizate, acolo unde este posibil, perioada pentru care se preconizează ca vor fi stocate datele cu caracter personal sau criteriile utilizate pentru a stabili aceasta perioadă, după caz

4) existența drepturilor specifice; orice informații disponibile privind sursa datelor (dacă este cazul)

5) existența unui proces decizional automatizat incluzând crearea de profiluri și informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

6) unde datele sunt transferate către state terțe ori organizații internaționale (din afara UE/SEE)

Consimțământul salariaților pentru utilizarea datelor cu caracter personal

Situația angajator-angajat este considerată, în general, o relație dezechilibrată, în care angajatorul dispune de mai multă putere decât angajatul.

Deoarece consimțământul trebuie să fie liber și având în vedere caracterul dezechilibrat al relației, angajatorul nu poate, în majoritatea cazurilor, să se bazeze pe consimțământul dvs. pentru a vă utiliza datele.

S-ar putea să existe situații în care este legală prelucrarea datelor cu caracter personal ale unui angajat pe baza consimțământului acestuia, în special dacă prelucrarea se face în interesul angajatului. De exemplu, dacă o unitate acordă beneficii angajatului sau membrilor familiei acestuia (cum ar fi reduceri la serviciile oferite de unitate), prelucrarea datelor cu caracter personal ale unui angajat este permisă și legală, dacă s-a acordat consimțământul prealabil în cunoștință de cauză.

Informații ce trebuie furnizate când se solicită date cu caracter personal

Informații de primit:

- denumirea unității care prelucrează datele dvs. (inclusiv datele de contact ale RPD, dacă există unul);

- scopurile în care unitatea va utiliza datele dvs.;

- categoriile de date cu caracter personal în cauză;

- temeiul juridic al prelucrării datelor dvs. cu caracter personal;

- perioada de timp pentru care datele dvs. vor fi stocate;

- alte unități care vor primi datele dvs.;

- o eventuală transferare a datelor în afara UE;

- drepturile de bază în ceea ce privește prelucrarea datelor (de exemplu, dreptul de a accesa și transfera datele sau de a dispune ștergerea acestora);

- dreptul de a depune o plângere în fata unei autorități de protecție a datelor (APD);

- dreptul de a retrage consimțământul în orice moment;

- existența unui proces decizional automatizat și logica utilizată, inclusiv consecințele.

Informațiile ar trebui prezentate într-o formă concisă, transparentă și inteligibilă și redactate într-un limbaj clar și simplu.

Stocarea datelor cu caracter personal

Acest principiu care guvernează prelucrarea datelor cu caracter personal prevede că datele cu caracter personal trebuie să fie păstrate pe o perioadă care nu depășește perioada necesară prelucrării pentru scopul identificat.

Principiul stocării limitate a datelor cu caracter personal derivă din principiile:

- datele cu caracter personal trebuie să fie adecvate, relevante și neexcesive;

- datele cu caracter personal trebuie să fie exacte și actualizate.

În mod evident, datele cu caracter personal stocate pentru perioade mai lungi decât cele necesare prelucrării pentru scopul identificat vor deveni în mod automat excesive. Totodată, ele ar putea deveni nerelevante și chiar inexacte.

RGPD nu stabilește perioada standard de stocare a datelor cu caracter personal și nici reguli detaliate care să ajute operatorii ori persoanele împuternicite să stabilească aceasta perioadă.

Revine așadar operatorilor sarcina să stabilească perioadele de reținere a datelor cu caracter personal prelucrate.

Stabilirea perioadei de stocare a datelor trebuie să asigure un just echilibru între nevoia operatorului de a reține datele cu caracter personal pe de o parte și drepturile și interesele legitime ale persoanelor vizate pe de altă parte.

Ștergerea datelor prea devreme, în contextul în care operatorul ar putea avea (încă) nevoie să le prelucreze, l-ar putea pune pe acesta într-o situație dificilă. Totodată, stocarea datelor personale pentru mai mult timp decât este necesar riscă să încalce principiile prelucrării datelor cu caracter personal, astfel cum acestea sunt prevăzute în RGPD.

De asemenea, în cazul în care datele cu caracter personal sunt stocate mai mult decât este nevoie, va crește inutil volumul de date pentru care va trebui asigurarea securității datelor și posibilitatea exercitării drepturilor de către persoanele vizate.

În contextul prelucrării datelor cu caracter personal, pentru a se conforma regulilor privind retenția datelor, operatorii vor implementa două tipuri de reguli interne:

a) politici de arhivare, în baza cărora datele cu caracter personal care nu sunt prelucrate în activitatea curentă, dar pentru reținerea cărora există o justificare, să fie arhivate cu respectarea garanțiilor privind securitatea datelor.

b) politici de ștergere, în baza cărora se vor revizui datele cu caracter personal prelucrate și se vor șterge, sau, după caz, se vor anonimiza acele date cu caracter personal de care nu mai este nevoie.

Politici de arhivare a datelor cu caracter personal

Scopul politicilor de arhivare va fi acela de a asigura un flux corespunzător al dosarelor sau lucrărilor inactive și al datelor cu caracter personal din aceste dosare/lucrări.

Fără ca enumerarea să fie limitativă, următoarele sunt cazuri în care datele devin inactive:

- necesitatea/contractul referitor la cauza respectivă a încetat, altfel decât prin reziliere pentru culpa uneia dintre părți;

- chiar dacă nu a survenit încetarea contractului/necesității, în cauza respectivă nu s-au mai făcut

demersuri în ultimele (12) luni;

Atunci când o necesitate de prelucrare a devenit inactivă, operatorul:

- va verifica situația specifică și va identifica datele cu caracter personal prelucrate în situația respectivă;

- va analiza, pentru fiecare categorie de date prelucrate, dacă există motive justificate pentru reținerea lor în continuare. În cazul în care se vor identifica date cu caracter personal care nu mai sunt necesare, acestea se vor anonimiza sau se vor șterge. Datele din situațiile/cauzele inactive pentru reținerea cărora există temei vor fi arhivate, cu respectarea garanțiilor privind securitatea datelor.

Important, datele cu caracter personal arhivate nu au un regim juridic derogatoriu, acestora aplicându-li-se toate prevederile privind prelucrarea datelor cu caracter personal.

Politici de ștergere a datelor cu caracter personal

Scopul politicilor de ștergere va fi acela de a stabili, pentru fiecare categorie de date cu caracter personal, perioada de stocare și procedura ce urmează a fi aplicată după expirarea acestei perioade - ștergerea definitivă sau, după caz, anonimizarea.

La stabilirea perioadelor de retenție se vor avea în vedere în primul rând prevederile din legislația privind organizarea și exercitarea activității operatorilor. Ori de câte ori există un termen de retenție stabilit în legislația aplicabilă sau în actele emise de organele profesiei, operatorii nu vor stoca datele pentru perioade mai lungi decât perioada legală.

Perioada de retenție a datelor cu caracter personal trebuie stabilită de la caz la caz, în funcție de scopul pentru care au fost colectate respectivele date. Astfel, odată ce datele nu mai sunt necesare scopului pentru care au fost colectate, acestea vor fi șterse sau anonimizate.

Contextul prelucrării datelor cu caracter personal oferă de cele mai multe ori elemente relevante pentru stabilirea perioadei de stocare a datelor.

De cele mai multe ori, operatorii prelucrează date cu caracter personal în contextul serviciilor prestate clienților. Din acest punct de vedere, atunci când contractul de prestări servicii încetează, operatorul va trebui să analizeze care sunt datele de care nu mai are nevoie (acestea urmând a fi șterse sau anonimizate) respectiv care sunt datele care trebuie menținute în continuare, în ce scop și pentru cât timp.

La încetarea contractului de prestări servicii, operatorul va trebui să rețină în continuare date cu caracter personal pentru a răspunde eventualelor plângeri sau pretenții ale clientului.

Consecințele dezvăluirii datelor cu caracter personal

Se produce o încălcare a securității datelor cu caracter personal atunci când există o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea sau divulgarea neautorizata a datelor cu caracter personal prelucrate sau la accesul neautorizat la acestea.

Dacă se întâmplă acest lucru, unitatea care deține datele cu caracter personal trebuie să anunțe autoritatea de supraveghere fără întârzieri nejustificate.

Dreptul la restricționarea prelucrării datelor cu caracter personal

Persoana vizată are dreptul de a obține din partea operatorului restricționarea prelucrării, respectiv limitarea acesteia (cu excepția stocării propriu-zise) strict la prelucrările cu care persoana vizată este de acord și /sau strict la prelucrările necesare în scopul constatării, exercitării sau apărării unui drept în instanță sau pentru protecția drepturilor unei alte persoane fizice sau juridice sau din motive de interes public important al Uniunii sau al unui stat membru. Conform art. 18 din RGPD, restricționarea se aplică în unul din următoarele cazuri:

1) persoana vizată contestă exactitatea datelor, pentru o perioadă care îi permite operatorului să verifice exactitatea datelor

2) prelucrarea este ilegală, iar persoana vizată se opune ștergerii datelor cu caracter personal, solicitând în schimb restricționarea utilizării lor

3) operatorul nu mai are nevoie de datele cu caracter personal în scopul prelucrării, dar persoana vizată i le solicită pentru constatarea, exercitarea sau apărarea unui drept în instanță

4) persoana vizată s-a opus prelucrării, pentru intervalul de timp în care se verifică dacă drepturile legitime ale operatorului prevalează asupra celor ale persoanei vizate

Dreptul de opoziție la prelucrarea datelor cu caracter personal

Raportat la art. 21 din RGPD, persoanele vizate pot să se opună oricând la prelucrarea datelor lor cu caracter personal:

a) din motive legate de situația particulară în care se află, operațiunilor de prelucrare desfășurate în temeiul necesității prelucrării pentru îndeplinirea unei sarcini care servește unui interes public cu care este investit operatorul; și/ sau prelucrărilor efectuate în temeiul intereselor legitime urmărite de operator sau de o parte terță a datelor cu caracter personal, inclusiv creării de profiluri;

b) fără motive și justificare, în cazul prelucrării datelor în scopuri de marketing direct;

Operatorul nu mai poate prelucra datele cu caracter personal în cazul opunerii, cu excepția cazului în care demonstrează că are motive legitime și imperioase care justifică prelucrarea și care prevalează asupra intereselor, drepturilor și libertăților persoanei vizate sau ca scopul prelucrării este constatarea, exercitarea sau apărarea unui drept.

Date personale incorecte. Procedura de corectare

În cazul în care considerați că datele dvs. cu caracter personal ar putea fi incorecte, incomplete sau inexacte, puteți cere unității să vă corecteze datele.

Unitatea trebuie să facă acest lucru fără întârzieri nejustificate („în principiu, în termen de o lună") sau să explice în scris motivele pentru care nu poate da curs cererii.

Exercitarea dreptului la restricționarea prelucrării datelor cu caracter personal

În general, în cazurile în care nu este clar dacă și când vor trebui șterse datele cu caracter personal, va puteți exercita dreptul la restricționarea prelucrării.

Acest drept poate fi exercitat când:

- este contestată exactitatea datelor în cauza;

- nu doriți să fie șterse datele;

- datele nu mai sunt necesare în scopul inițial, dar nu pot fi șterse încă din motive juridice;

- se așteaptă o decizie cu privire la obiecția dvs.

„Restricționare" înseamnă că - exceptând stocarea - datele dvs. cu caracter personal pot fi prelucrate numai cu consimțământul dvs. pentru constatarea, exercitarea sau apărarea unui drept în justiție, pentru protecția drepturilor altei persoane fizice sau juridice sau din motive de interes public.

Procesul decizional individual automatizat de prelucrare a datelor, inclusiv al creării de profiluri

Crearea de profiluri are loc atunci când se evaluează aspectele dvs. personale pentru a face previziuni în legătura cu dvs., chiar dacă nu se ia nicio decizie.

De exemplu, dacă o unitate vă evaluează caracteristicile (cum ar fi vârsta, sexul, înălțimea) sau vă încadrează într-o categorie, acest lucru înseamnă că vi se creează un profil.

Procesul decizional exclusiv automatizat are loc atunci când se iau decizii în privința dvs. prin mijloace tehnologice și fără nicio implicare umană: aceste decizii se pot lua chiar și fără crearea de profiluri.

Crearea de profiluri și procesul decizional automatizat sunt practici obișnuite în diferite sectoare, cum ar fi sectorul bancar și cel financiar, sectorul fiscal și al sănătății. Aceste practici pot fi mai eficiente, dar și mai puțin transparente și vă pot restricționa alegerea.

Deși, de regulă, nu puteți face obiectul unei decizii bazate exclusiv pe prelucrare automată, acest tip de proces decizional poate fi permis, în mod excepțional, dacă legea permite utilizarea algoritmilor și prevede garanții adecvate.

Mecanisme de răspuns la cererile de exercitare a drepturilor persoanelor cărora le sunt prelucrate datele cu caracter personal

Pentru a asigura tratarea cu celeritate a cererilor persoanelor vizate pentru exercitarea drepturilor specifice, respectiv a cererilor altor entități (pentru cazurile în care operatorul acționează în calitate de persoană împuternicită), următoarele mecanisme pot fi avute în vedere:

a) Alocarea unei/unor persoane care să se ocupe de tratarea în timp util a cererilor persoanelor vizate, care să răspundă în scris la asemenea solicitări;

b) Redactarea unor formulare de exercitare a drepturilor/răspuns tipizate care să fie utilizate atunci când clienții/angajații/alte persoane vizate își exercită drepturile specifice;

c) Dacă cererile sunt transmise prin mijloace electronice, răspunsul trebuie transmis prin aceleași mijloace, dacă persoanele vizate nu solicită altfel;

d) Implementarea unor secțiuni specifice pentru exercitarea drepturilor persoanelor vizate online, în special în cazurile în care colectarea datelor se realizează online;

e) Pentru formele de exercitare cu personal numeros, conceperea unei proceduri specifice cu reguli clare de urmat în cazul primirii unor astfel de cereri, inclusiv cu principiile de avut în vedere în contextul conceperii răspunsurilor la cererile specifice.

Modalități de a proceda în cazul în care nu au fost respectate drepturile privind protecția datelor cu caracter personal

În cazul în care credeți ca v-au fost încălcate drepturile privind protecția datelor, aveți trei opțiuni:

- depunerea unei plângeri la autoritatea de protecție a datelor (APD)

Autoritatea efectuează investigații și vă informează cu privire la progresele sau la soluționarea plângerii dvs. în termen de trei luni.

- acționarea în justiție a APD

În cazul în care considerași că APD nu a tratat corect plângerea dvs. sau dacă nu sunteți mulțumit(ă) de răspunsul acesteia ori dacă aceasta nu vă informează cu privire la progresele sau la soluționarea plângerii în termen de trei luni de la data depunerii puteți introduce direct o acțiune în justiție împotriva APD.

- acționarea în justiție a unei unități

Introduceți direct o acțiune în justiție împotriva unei unități în cazul în care considerați că aceasta v-a încălcat drepturile privind protecția datelor.

Dezvăluiri de date personale la solicitarea autorităților publice

Art. 6 alin. (1) lit. c) din RGPD prevede că prelucrarea datelor cu caracter personal este legală dacă, printre altele, „prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului".

Ca atare, operatorii pot transmite date cu caracter personal pe care le prelucrează către autorități publice doar dacă și în măsura în care, în principal:

a) Aceasta se manifestă într-o obligație legală pentru aceștia;

b) Autoritatea care solicită aceste informații are competență în domeniu, verificată în prealabil de către operatorul căruia i se solicită transferul;

c) Operatorul asigură un nivel de protecție adecvat al datelor prelucrate și astfel transmise;

d) Transferul se realizează cu respectarea principiilor prevăzute de RGPD și sintetizate în art. 5 din acesta: legalitate, echitate și transparență; principiul limitării transferului în funcție de scop; principiul reducerii la minimum a datelor transferate; principiul exactității datelor; principiul limitării legate de stocarea datelor; principiul asigurării integrității și confidențialității datelor; principiul responsabilității.

Breșele de securitate a datelor cu caracter personal

Conform art. 5 din RGPD, unul din principiile de bază care guvernează prelucrarea datelor cu caracter personal este acela că datele trebuie să fie prelucrate într-un mod care asigură securitatea adecvată a acestora.

Operatorii sunt obligați să implementeze măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător, în temeiul prevederilor art. 32 din RGPD. Astfel, aceștia trebuie să stabilească măsurile necesare și suficiente pentru a asigura securitatea datelor.

Totodată, chiar dacă art. 33 din RGPD nu o prevede în mod expres, operatorii trebuie să implementeze

măsuri tehnice și organizatorice care, în cazul apariției unei breșe de securitate, asigură componența reactivă a politicilor interne privind securitatea datelor.

Aceste măsuri trebuie să ajute operatorul:

a) să stabilească imediat dacă s-a produs o breșă de securitate;

b) dacă este cazul, să notifice autoritatea de supraveghere a prelucrării datelor cu caracter personal (art. 33 din RGPD);

c) după caz, să informeze persoana sau persoanele vizate afectate de apariția breșei de securitate (art. 34 din RGPD).

Nu în ultimul rând, incidentele de securitate trebuie documentate conform art. 33 alin. (5) din RGPD.

Art. 4 punctul 12 din RGPD definește breșa de securitate: o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea sau divulgarea neautorizată a datelor cu caracter personal (...) sau la accesul neautorizat la acestea.

Există diferite exemple de breșe de securitate: atacuri informatice tip ransomware, pierderea cheii de criptare a datelor, nefuncționarea sistemelor informatice, pierderea unor documente, transmiterea unei corespondențe la adresa greșită etc.).

Breșele de securitate pot avea cauze diferite: de la nefuncționarea sau funcționarea necorespunzătoare a sistemelor informatice până la erori umane.

Informarea persoanelor vizate în cazul breșelor de securitate a datelor cu caracter personal

Art. 34 din RGPD reglementează obligația operatorului de a informa persoanele vizate cu privire la breșele de securitate.

Scopul informării este ca persoanele vizate să își poată lua măsuri de protecție.

Informarea persoanelor vizate este obligatorie numai dacă incidentul de securitate este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor vizate. Dacă notificarea autorității de supraveghere este obligatorie ori de câte ori există un risc privind drepturile și libertățile persoanelor vizate, informarea persoanelor vizate este obligatorie atunci când există un risc ridicat pentru drepturile și libertățile acestora.

RGPD nu prevede criterii obiective în funcție de care se determină nivelul riscului generat de incidentul de securitate. Conform Ghidului privind notificarea încălcării securității datelor, la analiza nivelului de risc, operatorul va avea în vedere criteriile de mai jos:

a) tipul incidentului;

b) natura, contextul, volumul datelor afectate;

c) posibilitatea de a identifica persoanele vizate;

d) consecințele incidentului asupra persoanelor vizate;

e) circumstanțele persoanelor vizate;

g) circumstanțele operatorului în cauză;

h) numărul persoanelor afectate.

În analiza sa, operatorul va avea în vedere severitatea riscului, însă în același timp va ține cont de probabilitatea apariției acestuia. Astfel, posibilitatea ca incidentul de securitate să genereze un risc ridicat cu privire la drepturile și libertățile persoanei/persoanelor vizate crește atunci când severitatea riscului crește, dar și atunci când, chiar dacă riscul nu este foarte ridicat, totuși probabilitatea apariției sale este mai mare.

În cazurile în care informarea persoanelor vizate este obligatorie, aceasta trebuie făcută fără întârziere. RGPD nu prescrie un anume formalism pentru informarea persoanelor vizate. Dacă circumstanțele concrete nu reclamă o altă abordare, informarea se va face printr-o comunicare adresată direct persoanei vizate, printr-un mijloc de comunicare corespunzător (poșta electronică, SMS etc.). Cu titlu de excepție, doar în situația în care contactarea directă a persoanei/persoanelor vizate ar presupune un efort disproporționat, se poate face o informare publică.

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 libertățile persoanelor fizice, operatorul va efectua o evaluare a impactului

asupra protecției datelor.

Evaluarea impactului asupra protecției datelor se realizează anterior colectării datelor cu caracter personal și efectuării prelucrării. 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 proporționalității prelucrării de date efectuate;

- o estimare a riscurilor asupra drepturilor și libertăților persoanelor vizate;

- măsurile prevăzute pentru a trata riscurile și a asigura conformitatea cu dispozițiile RGPD. Evaluarea impactului asupra protecției datelor permite:

- realizarea unei prelucrări de date cu caracter personal sau a unui produs care respectă viața privată;

- estimarea impactului asupra vieții private a persoanelor vizate;

- demonstrarea faptului că principiile fundamentale ale RGPD 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 stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă; prelucrării pe scară largă a unor categorii speciale de date sau a unor date cu caracter personal privind condamnări penale și infracțiuni, sau unei monitorizări sistematice pe scară largă 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.

Întocmit,
Administrator
POPA CONSTANTIN MARIUS

Aprobat,
Director
TIMPLARESCU GHEORGHE