POLITICA DE CONFIDENŢIALITATE

PRIVIND PRELUCRAREA DATELOR PERSONALE

În vigoare începând cu 31.03.2026

Cuprins:

POLITICA DE CONFIDENŢIALITATE

PRIVIND PRELUCRAREA DATELOR PERSONALE

Acest document stabilește politica de confidențialitate privind procesarea datelor cu caracter personal utilizând adresa online www.roncredit.ro. Te rugăm să citești cu atenție Politica de Confidențialitate înainte de a accesa sau utiliza site-ul și serviciile oferite. Prin accesarea și utilizarea serviciilor descrise pe www.roncredit.ro, ești de acord cu Politica de Confidențialitate și cu modul de prelucrare a datelor personale prezentate, în caz contrar te rugăm să nu utilizezi site-ul nostru.

RON CREDIT IFN SA, denumită în continuare „Instituția", are obiectivul să se conformeze cu legile și reglementările aplicabile privind protecția prelucrării datelor cu caracter personal, în țările în care operează Instituția. Această Politică de protecție a prelucrării datelor cu caracter personal ("Politica") stabilește principiile de bază prin care Instituția procesează datele cu caracter personal ale clienților/consumatorilor, furnizorilor, partenerilor comerciali, angajaților și/sau ale altor persoane fizice și indică responsabilitățile departamentelor și angajaților în ceea ce privește procesarea datelor cu caracter personal.

Legislație și documente de referință:

- Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 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 – GDPR);
- Legea nr. 190/2018 privind măsuri de punere în aplicare a GDPR;
- Decizii ale Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), așa cum pot fi acestea adoptate din când în când;
- Ghidul orientativ de aplicare a Regulamentului General privind Protecţia Datelor destinat operatorilor, publicat de ANSPDCP pe website-ul autorității;
- Politica de stocare (retentie) a datelor personale a Societatii
- Nota de informare persoane vizate a Instituției
- Politica cookies a Instituției
- Politicile privind securitatea informațiilor ale Instituției
- Procedura de notificare privind încălcarea securității datelor a Instituției

Definiții

Date cu caracter personal: Orice informații privind o persoană fizică identificată sau identificabilă („**Persoana Vizată**") 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.

Categorii speciale de date cu caracter personal: Datele cu caracter personal care sunt, prin natura lor, deosebit de sensibile în ceea ce privește drepturile și libertățile fundamentale, necesită o protecție specifică, deoarece contextul prelucrării acestora ar putea genera riscuri considerabile la adresa drepturilor și libertăților fundamentale ale persoanei vizate. Aceste date cu caracter personal includ datele cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, convingerile religioase sau filozofice sau calitatea de membru într-un sindicat, datele genetice, datele biometrice în scopul de identificare unică a acelei persoane fizice, date privind sănătatea sau date privind viața sexuală sau orientarea sexuală a persoanei fizice.

Operator: 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. În sensul prezentei Politici, RON CREDIT IFN SA este operator de date cu caracter personal.

Persoană împuternicită de Operator: Persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele Operatorului.

Prelucrare: O 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.

Anonimizare: Eliminarea ireversibilă a identificării datelor cu caracter personal, astfel încât să nu se poată identifica persoana prin folosirea unei perioade de timp, costuri și tehnologie rezonabilă, fie de către Operator, fie de către orice altă persoană, pentru a identifica acea persoană fizică. Principiile de prelucrare a datelor cu caracter personal nu se aplică datelor anonimizate, întrucât nu mai sunt date cu caracter personal.

Pseudonimizare: 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. Pseudonimizarea reduce, dar nu elimină complet capacitatea de a asocia datele cu caracter personal în scopul identificării unei persoane vizate. Întrucât datele pseudonimizate sunt încă date cu caracter personal, prelucrarea datelor pseudonimizate se conformează principiilor de prelucrare a datelor cu caracter personal.

Creare de profiluri: orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea acestora pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia.

Prelucrare transfrontalieră a datelor cu caracter personal: Prelucrarea datelor cu caracter personal care are loc în contextul activităților sediilor din mai multe state membre ale unui operator sau ale unei persoane împuternicite de operator pe teritoriul Uniunii Europene, dacă operatorul sau persoana împuternicită de operator are sedii în cel puțin două state membre; sau prelucrarea datelor cu caracter personal care are loc în contextul activităților unui singur sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, dar care afectează în mod semnificativ sau este susceptibilă de a afecta în mod semnificativ persoane vizate din cel puțin două state membre.

Autoritate de supraveghere: O autoritate publică independentă instituită de un stat membru în temeiul articolului 51 din GDPR UE. Autoritatea de supraveghere locală este Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP).

Autoritate de supraveghere principală: Autoritatea de supraveghere cu responsabilitatea primară de a acționa în privința activității de prelucrare transfrontalieră a datelor, de exemplu atunci când o persoană vizată depune o plângere privind prelucrarea datelor cu caracter personal ale acesteia; răspunde, printre altele, de recepționarea notificărilor privind încălcarea securității informațiilor, de notificarea în privința activității de prelucrare riscantă și va deține autoritatea completă privind îndatoririle acesteia de asigurare a conformării cu prevederile din GDPR UE.

Fiecare „**Autoritate de supraveghere locală**” va menține încă în propriul teritoriu și va monitoriza orice prelucrare locală a datelor care afectează persoanele vizate sau care se desfășoară de către un operator sau o persoană împuternicită de operator din UE sau non-UE, atunci când prelucrarea acestora se referă la persoanele vizate care locuiesc în teritoriul acesteia. Îndatoririle și puterile acestora includ desfășurarea investigațiilor și aplicarea măsurilor și amenzilor, promovarea informării publice despre riscuri, reguli, securitate și drepturile privind prelucrarea datelor cu caracter personal, precum și obținerea accesului la orice locații ale Operatorului și Persoanei împuternicite de Operator, inclusiv orice echipamente și mijloace de prelucrare a datelor.

„**Ofițerul de protecție a datelor**”: persoana fizică/juridică desemnată de Instituție în baza calităților profesionale și a cunoștințelor de specialitate, pentru a îndeplini sarcinile prevăzute de art. 39 din GDPR;

„**Sediu principal în cazul unei Persoane împuternicite de Operator**” cu sedii în cel puțin două state membre, este locul în care se află administrația centrală a acestuia în Uniune sau, în cazul în care persoana împuternicită de operator nu are o administrație centrală în Uniune, sediul din Uniune al Persoanei împuternicite de Operator, în care au loc activitățile principale de prelucrare, în contextul activităților unui sediu al Persoanei împuternicite de Operator, în măsura în care aceasta este supusă unor obligații specifice în temeiul GDPR.

„**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.

Principii de bază legate de prelucrarea datelor cu caracter personal

Principiile de protecție a datelor cu caracter personal conturează responsabilitățile de bază pentru organizațiile care manevrează date cu caracter personal. Cele 7 (șapte) principii, descrise mai în detaliu în cadrul acestei Politici, pot fi sumarizate după cum urmează:

- Să fim deschiși și transparenți în legătură cu ceea ce facem cu datele și motivul pentru care le utilizăm;
- Să ne asigurăm că avem un fundament legal pentru prelucrarea datelor;
- Să colectăm și să utilizăm doar minimul necesar de date;
- Să păstrăm datele corecte, complete și actualizate;
- Să nu păstrăm datele mai mult decât este necesar;
- Să prelucrăm datele în condiții de siguranță;
- Să fim responsabili cu prelucrările pe care le facem și să putem demonstra oricând respectarea prevederilor legale.

Legalitatea, exactitatea și transparența prelucrărilor

Datele cu caracter personal trebuie prelucrate în mod legal, corect și transparent în legătură cu persoana vizată.
Astfel, Instituția, în calitate de Operator, va utiliza datele cu caracter personal astfel încât Persoana vizată care i-a încredințat datele sale personale, să cunoască această utilizare și să corespundă așteptărilor sale privind utilizarea datelor de către Instituție.

Limitarea scopului

Datele cu caracter personal trebuie colectate pentru scopuri determinate, explicite și legitime și nu trebuie prelucrate într-un mod care este incompatibil cu aceste scopuri.
Prelucrarea ulterioară de către Instituție în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice nu va fi incompatibilă cu prelucrarea inițială, câtă vreme se face cu respectarea prevederilor GDPR (art. 89).
În cazul în care oricare din departamentele Instituției, inclusiv departamentele cu funcție de suport/funcție administrativă, intenționează să utilizeze datele personale ale clienților/angajaților etc. în scopuri secundare (alte scopuri decât cele pentru care datele personale au fost colectate inițial), va informa Ofițerul de Protecție a Datelor (DPO) in vederea identificarii posibilitatii de a utiliza aceste date personale în aceste scopuri secundare.

Reducerea la minimum a datelor

Datele cu caracter personal trebuie să fie adecvate, relevante și limitate strict la ceea ce este necesar în legătură cu scopurile pentru care se prelucrează. În cazul în care este necesar, Instituția va lua măsuri adecvate de anonimizare și/sau pseudonimizare a datelor cu caracter personal, acolo unde este posibil, pentru a reduce riscurile pentru persoanele vizate.
În acest sens, pe cât posibil, Instituția se va asigura că angajații/colaboratorii săi vor lua și respecta următoarele măsuri organizaționale:

- vor limita transferul de date cu caracter personal atât intern cât și extern și
- nu vor utiliza date cu caracter personal în comunicările pe e-mail, prin mesageria instant sau în câmpurile libere din sistemele de evidență ale Instituției, decât în măsura în care este necesar pentru desfășurarea activității Instituției, pentru a evita potențialele riscuri reputaționale sau litigioase care ar putea expune Instituția.

Exactitatea datelor

Datele cu caracter personal trebuie să fie exacte și, dacă este necesar, actualizate. În acest sens, Instituția va lua măsuri rezonabile pentru a se asigura că datele cu caracter personal care nu sunt exacte sub aspectul scopurilor pentru care se prelucrează, se șterg sau se rectifică la timp.
În cazul în care oricare din angajații/colaboratorii Instituției ia la cunoștință despre orice astfel de inexactitate a datelor cu caracter personal prelucrate de către Instituție, acesta va corecta inexactitatea identificată sau, dacă acest lucru nu este posibil, va informa persoana/echipa relevantă care poate înlătura inexactitatea constatată, in conformitate cu procedurile interne ale Societatii de actualizare a datelor cu caracter personal.

Limitarea perioadei de stocare (retentie)

Datele cu caracter personal nu trebuie menținute mai mult decât este necesar pentru îndeplinirea scopurilor pentru care se colectează și se prelucrează datele, in conformitate cu Politica de stocare (retentie) a datelor personale a Instituției.

Datele cu caracter personal vor putea fi ținute de către Instituție și după îndeplinirea scopurilor pentru care acestea au fost colectate inițial, în măsura în care datele cu caracter personal vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, cu respectarea prevederilor GDPR (art. 89), sub rezerva punerii în aplicare de către Instituție de măsuri de ordin tehnic și organizatoric adecvate în vederea respectării și garantării drepturilor și libertăților persoanelor vizate.

După îndeplinirea scopurilor pentru care datele cu caracter personal au fost colectate (și în lipsa aplicabilității situațiilor menționate la paragraful anterior), datele cu caracter personal vor fi distruse, șterse sau anonimizate din bazele de date/sistemele de evidență ale Instituției (atât electronice, cât și în format letric/hârtie), cu respectarea prevederilor legale aplicabile și a Politicii de stocare (retenție) a datelor personale a Instituției.

Integritatea și confidențialitatea datelor

Ținând cont de stadiul tehnologiei și al măsurilor de securitate disponibile, de costul de implementare și probabilitatea și gravitatea riscurilor pentru datele cu caracter personal, Instituția are obligația să aplice măsuri tehnice sau organizatorice adecvate pentru a prelucra datele cu caracter personal, într-un mod care să asigure securitatea corespunzătoare a datelor, inclusiv protecția împotriva distrugerii, pierderii, modificării accidentale sau ilegale, accesul neautorizat sau dezvăluirea neautorizată.
Instituția ia măsuri tehnice și organizatorice adecvate pentru a asigura securitatea datelor cu caracter personal, cum ar fi controale de acces, încriptarea datelor, transferul cu respectarea strictă a cerințelor de confidențialitate etc., conform politicilor de securitate ale Instituției.

Responsabilitatea Operatorului

Instituția este responsabilă de conformarea cu principiile prevăzute mai sus și poate să demonstreze respectarea acestora. În acest sens, Instituția documenteaza respectarea principiilor de prelucrare a datelor personale prin întocmirea de proceduri adecvate de confidentialitate, retentie și securitate a datelor, prin pregătirea unui registru de evidență cu operațiunile de prelucrare efectuate de Instituție, prin informarea persoanelor vizate (angajați sau clienți etc.) cu privire la prelucrarea datelor cu caracter personal de către Instituție, prin postarea Informării privind prelucrarea datelor personale pe website-ul Instituției (pentru asigurarea principiului transparenței prelucrărilor), precum și prin orice alte demersuri întreprinse de către Instituție pentru a documenta respectarea principiilor de prelucrare și îndeplinirea obligațiilor legale.

Implementarea protecției datelor în activitățile comerciale

Pentru a demonstra conformarea cu principiile de protecție a datelor, Instituția are obligația să implementeze protecția datelor în activitățile comerciale ale acesteia, de la momentul colectării datelor personale (sau chiar înainte) și până la distrugerea/ștergerea acestora din sistemele de evidență a datelor deținute și organizate de Instituție.

Colectarea datelor cu caracter personal

Instituția are obligația să colecteze volumul minim necesar de date cu caracter personal. Dacă datele cu caracter personal se colectează de la un terț, angajații Instituției au obligația să se asigure că datele cu caracter personal se colectează cu respectarea prevederilor legale aplicabile prevăzute de GDPR si să informeze în prealabil Ofițerul de Protecție a Datelor (DPO) din cadrul Instituției.

Informarea persoanei vizate

În momentul colectării sau înainte de colectarea datelor cu caracter personal pentru orice tip de activități de prelucrare, incluzând, dar nelimitându-se la vânzarea produselor și serviciilor Instituției sau activitățile de marketing, Instituția va informa corespunzător persoanele vizate cu privire la următoarele:

(i) identitatea și datele de contact ale operatorului și după caz, ale reprezentantului acestuia;

(ii) datele de contact ale ofițerului pentru protecția datelor, după caz;

(iii) tipurile de date cu caracter personal colectate;

(iv) scopurile prelucrării precum și temeiul juridic al prelucrării;

(v) interesele legitime urmărite de Instituție în calitate de Operator, în cazul în care efectuează prelucrări în baza acestui temei legal;

(vi) destinatarii sau categoriile de destinatari ai datelor cu caracter personal;

(vii) drepturile Persoanelor vizate în privința datelor cu caracter personal ale acestora;

(viii) perioada de stocare a datelor sau dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;

(ix) eventualele transferuri internaționale de date către o țară terță sau o organizație internațională existența unor garanții adecvate luate de Instituție pentru a proteja datele cu caracter personal, cu o trimitere la mijloacele de a obține informatii cu privire la aceasta;

(x) existența drepturilor pe care le are persoana vizată, respectiv dreptul persoanei vizate de a-și retrage consimțământul în orice moment; dreptul de a depune o plângere în fața autorității de supraveghere competente; informarea persoanei vizate

dacă furnizarea de date cu caracter personal reprezintă o obligație legală sau contractuală sau o obligație necesară pentru încheierea unui contract, precum și dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal și care sunt consecințele nerespectării acestei obligații; dacă este cazul, existența unui proces decizional automatizat incluzând crearea de profiluri și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

Atunci când se colectează categorii speciale de date cu caracter personal, Ofițerul de Protecție a Datelor (DPO) se va asigura că Informarea privind prelucrarea datelor personale specifică în mod explicit scopul pentru care se colectează aceste date cu caracter personal și temeiul juridic al prelucrării.

Consimțământul persoanei vizate

Instituția se asigură că, ori de câte ori colectează și prelucrează datele cu caracter personal ale persoanelor vizate, prelucrarea datelor cu caracter personal se face în baza unuia din următoarele temeiuri legale de prelucrare:

- consimțământul persoanei vizate;
- executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract (de exemplu, plata salariului de către Instituție, în calitate de Operator, către angajații Instituției, în calitate de persoane vizate, ca urmare a executării contractului de muncă);
- îndeplinirea unei obligații legale a Instituției, în calitate de Operator (de exemplu, îndeplinirea obligațiilor de medicina muncii și cele din domeniul ocupării forței de muncă și al securității sociale și protecției sociale, îndeplinirea obligațiilor de cunoaștere a clientelei și păstrare a documentației relevante, îndeplinirea obligațiilor de arhivare conform legislației specifice etc.);
- protejarea intereselor vitale ale persoanei vizate sau ale altei persoane fizice;
- îndeplinirea unei sarcini de interes public;
- interesele legitime ale Instituției sau ale unei părți terțe, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special când persoana vizată este un copil (de exemplu, prelucrarea de date cu caracter personal necesară în scopul prevenirii fraudelor).

Când se prelucrează date cu caracter personal în baza consimțământului persoanei vizate, Instituția răspunde de reținerea înregistrării unui asemenea consimțământ. Instituția răspunde de transmiterea către persoanele vizate a opțiunilor pentru a acorda consimțământul și are obligația să le informeze și să se asigure că se poate retrage consimțământul acestora (când se utilizează ca bază juridică pentru prelucrare), în orice moment.

Când se solicită corectarea, modificarea sau distrugerea evidențelor datelor cu caracter personal, Instituțiaare obligația să se asigure că aceste solicitări se gestionează cu respectarea procedurilor interne si legislatiei in vigoare. Instituția are de asemenea obligația să asigure înregistrarea acestor solicitări.

Datele cu caracter personal trebuie prelucrate numai în scopul pentru care s-au colectat inițial. În cazul în care Instituția vrea să prelucreze în alt scop datele cu caracter personal colectate, și nu are un alt temei legal decât consimțământul persoanei vizate, Instituția are obligația să solicite consimțământul persoanei vizate pentru scopurile secundare.

Orice asemenea solicitare trebuie să includă scopul inițial pentru care s-au colectat datele și de asemenea scopul/scopurile nou/noi sau suplimentar(e).

Instituția are obligația să se asigure că metodele de colectare se conformează cu legea relevantă, bunele practici și standardele din domeniu.

Utilizare, stocare și distrugere/ștergere

Scopurile, metodele, limitarea stocării și perioada de stocare a datelor cu caracter personal trebuie să fie concordante cu informațiile cuprinse în Informarea privind prelucrarea datelor personale, comunicată persoanelor vizate. Instituția are obligația să mențină corectitudinea, integritatea, confidențialitatea și relevanța datelor cu caracter personal în baza scopului de prelucrare. Este obligatorie utilizarea de mecanisme de securitate corespunzătoare, elaborate să protejeze datele cu caracter personal, pentru a preveni ca datele cu caracter personal să fie sustrase, utilizate abuziv sau abuzate și pentru a preveni încălcarea securității datelor cu caracter personal.

Dezvăluirea către terți

Instituția utilizează diverși furnizori de servicii/parteneri comerciali care au acces, stochează, transferă sau în orice alt fel prelucrează datele cu caracter personal în numele și pe seama Instituției. Acești furnizori de servicii/parteneri comerciali au calitatea de Persoană împuternicită de Operator, conform definiției menționate mai sus în cadrul *Secțiunii 3 – Definiții*.

În această situație, Instituția se asigură că Persoana împuternicită de operator va aplica măsuri de securitate adecvată pentru a proteja datele cu caracter personal corespunzătoare de riscurile asociate (de exemplu, utilizarea abuzivă a datelor cu caracter personal, o dezvăluire neautorizată a datelor cu caracter personal, încălcări ale securității datelor etc.). În acest scop, Instituția va putea utiliza Chestionarul de conformare GDPR pentru persoana împuternicită de operator.

De asemenea, Instituția încheie cu furnizorul sau partenerul comercial (în calitate de Persoană împuternicită de Operator) un contract de prelucrare date, care conține cel puțin

clauzele obligatorii prevăzute de GDPR pentru reglementarea raporturilor dintre Operator și Persoana împuternicită de Operator. Prin acest contract, Instituția are obligația să solicite furnizorului sau partenerului comercial, ca acesta din urmă să asigure același nivel de protecție a datelor cu caracter personal. Furnizorul sau partenerul comercial are obligația să prelucreze datele cu caracter personal numai pentru a îndeplini obligațiile contractuale ale acestuia față de Instituție și conform instrucțiunilor documentate ale Instituției și în niciun alt scop.

Atunci când Instituția prelucrează date cu caracter personal împreună cu o terță parte, în calitate de Operatori asociați, Instituția are obligația să specifice în mod explicit în contractul încheiat cu terțul, respectivele responsabilități ale acesteia și ale terțului în ceea ce privește îndeplinirea obligațiilor care le revin în temeiul GDPR, în special în ceea ce privește exercitarea drepturilor persoanelor vizate și îndatoririle fiecăruia privind obligația de informare a persoanelor vizate.

În situația în care Instituția transferă datele cu caracter personal către o terță parte, cele două entități neavând calitatea de Operatori asociați, acest transfer se va realiza de către Instituție în condiții de siguranță, cu luarea de măsuri tehnice adecvate și îndeplinirea obligațiilor legale prevăzute de GDPR (de exemplu, obținerea consimțământului persoanelor vizate la transfer, dacă este cazul etc.).

Transferul transfrontalier al datelor cu caracter personal

Orice transfer către o țară terță sau organizație internațională situată în afara Spațiului Economic European (EEA), și în legătură cu care Comisia Europeană nu a emis o decizie de asigurare a unui nivel adecvat de potecție a datelor cu caracter personal în conformitate cu prevederile GDPR, se va efectua de către Instituție cu luarea de garanții adecvate privind acest transfer, cum ar fi:

- clauzele standard de protecție a datelor adoptate de Comisia Europeană în conformitate cu cerințele GDPR;
- regulile corporatiste obligatorii, pentru transferurile intra-grup, adoptate de către grupul din care face parte Instituția conform cerințelor GDPR, dacă este cazul;
- un cod de conduită aprobat în conformitate cu cerințele GDPR, însoțit de un angajament obligatoriu și executoriu din partea Instituției de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate;
- un mecanism de certificare aprobat în conformitate cu cerințele GDPR, însoțit de un angajament obligatoriu și executoriu din partea Instituției de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate.

Transferul de date cu caracter personal către o țară terță sau organizație internațională în baza oricăreia dintre garanțiile menționate mai sus, se va realiza fără necesitatea autorizării din partea autorității de supraveghere competente.

Dacă niciuna dintre garanțiile menționate mai sus nu pot fi asigurate de către Instituție la data transferului de date, acest transfer de date se va face doar cu autorizarea din partea autorității de supraveghere competente și cu respectarea cerințelor GDPR.

Indiferent de situație, entitatea către care se transferă datele cu caracter personal are obligația să se conformeze principiilor de prelucrare a datelor cu caracter personal prevăzute de GDPR.

Drepturile persoanelor vizate

Aspecte generale

Atunci când acționează în calitate de Operator, Instituția răspunde de asigurarea pentru persoanele vizate a unui mecanism de acces rezonabil pentru a le oferi posibilitatea persoanelor vizate să își exercite drepturile pe care le au în legătură cu prelucrarea datelor cu caracter personal ale acestora, respectiv:

(i) dreptul de a primi informații privind operațiunile de prelucrare a datelor personale care privesc persoana vizată;

(ii) dreptul de a solicita acces la datele cu caracter personal deținute și prelucrate de Instituție și de asemenea,

(iii) dreptul la rectificarea/completarea acestor date dacă acestea sunt inexacte/incomplete;

(iv) dreptul de a se opune prelucrării datelor cu caracter personal, în anumite condiții, inclusiv dreptul de a-și retrage consimțământul acordat;

(v) dreptul de a solicita ștergerea datelor cu caracter personal, în anumite condiții;

(vi) dreptul de a solicita restricționarea prelucrărilor datelor cu caracter personal, în anumite condiții;

(vii) dreptul la portabilitatea datelor cu caracter personal, în anumite condiții;

(viii) dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce efecte juridice care privesc persoana vizată sau care o afectează în mod similar într-o măsură semnificativă.

Având în vedere elementele de noutate aduse de GDPR în raport cu legislația anterioară de protecție a datelor cu caracter personal, mai jos sunt prezentate detalii privind dreptul la portabilitatea datelor și dreptul la ștergerea datelor („dreptul de a fi uitat”).

Portabilitatea datelor

Persoanele vizate au dreptul să primească, la cerere, datele pe care le-au transmis Instituției într-un format structurat, utilizat în mod curent și care poate fi citit automat și să transmită acele date altui operator, cu titlu gratuit, fără obstacole din partea Instituției.
Instituția se asigura că asemenea solicitări se prelucrează în termen de maxim o lună, nu sunt excesive (de exemplu, ale unei persoane vizate care transmite în fiecare zi cereri către o Instituție) și nu afectează drepturile asupra datelor cu caracter personal ale altor persoane fizice.

Dreptul la ștergerea datelor („dreptul de a fi uitat”)

Persoanele vizate au dreptul să obțină de la Instituție ștergerea datele cu caracter personal ale acestora. Atunci când Instituția acționează în calitate de Operator și când poate da curs acțiunii de ștergere a datelor personale (neexistând alte temeiuri legale pentru păstrarea datelor cu caracter personal menționate în solicitarea de ștergere), Instituția va initia acțiunile necesare (inclusiv măsurile tehnice) pentru a informa terții, care utilizează sau prelucrează acele date, să se conformeze cu solicitarea de ștergere primită de la Persoana vizată.

Necesitatea de a stabili autoritatea de supraveghere principală

Identificarea unei autorități de supraveghere principale este relevantă numai dacă Instituția desfășoară prelucrarea transfrontalieră a datelor cu caracter personal.
Transferul transfrontalier al datelor cu caracter personal se efectuează dacă:

a. *prelucrarea datelor cu caracter personal se execută de filialele Instituției cu sediul în alte state membre;*
sau
b. *prelucrarea datelor cu caracter personal care are loc la un sediu unic al Instituției, în Uniunea Europeană, dar care afectează semnificativ sau poate afecta semnificativ Persoanele Vizate în cel puțin două state membre.*

Dacă Instituția are sedii doar într-un singur stat membru și activitățile de prelucrare ale acesteia afectează doar Persoanele vizate din acel stat membru, atunci nu este necesar să se stabilească o autoritate de supraveghere principală. Singura autoritate competentă va fi

Autoritatea de Supraveghere din țara în care Instituția are sediul social (pentru România – ANSPDCP).

Răspunsul la incidente de încălcare a securității datelor cu caracter personal

Atunci când Instituția află despre o încălcare a securității datelor cu caracter personal, in cadrul Societatii se va desfășura o investigație și se vor lua măsurile adecvate de remediere, în timp util, conform Politicii privind încălcarea securității datelor a Societatii.

Atunci când există risc pentru drepturile și libertățile Persoanelor vizate, Instituția are obligația să notifice autoritățile competente de protecție a datelor, fără o întârziere nejustificată și, dacă este posibil, în termen de 72 de ore.

Organizare și responsabilități

Responsabilitatea pentru asigurarea prelucrării corespunzătoare a datelor cu caracter personal revine fiecărei persoane care lucrează pentru Instituție sau cu aceasta și are acces la datele cu caracter personal prelucrate de Instituție.
Domeniile principale de responsabilitate pentru prelucrarea datele cu caracter personal revin următoarelor roluri organizatorice:

Directoratul ia deciziile în privința strategiilor generale ale Instituției privind protecția datelor cu caracter personal și le aprobă.

Ofițerul de Protecție a Datelor (DPO) (Data Protection Officer), impreuna cu Managerul privind Securitatea Informatiei, Ofiterul privind Securitatea Informatiei sau orice alt angajat relevant, răspund de gestionarea programului de protecție a datelor cu caracter personal și răspund de dezvoltarea și promovarea politicilor de protecție a datelor cu caracter personal complete, după cum se definesc în fișa postului.

Rolul principal al ofițerului de protecţie a datelor va fi:

- să informeze și să consilieze Instituția, precum și angajaţii acesteia cu privire la obligaţiile existente în domeniul protecţiei datelor cu caracter personal;
- să monitorizeze respectarea GDPR și a legislaţiei naţionale în domeniul protecţiei datelor;
- să consilieze Instituția în legătură cu realizarea de studii de impact privind protecţia datelor și să verifice efectuarea acestora;

- să coopereze cu autoritatea pentru protecţia datelor și să reprezinte punctul de contact în relaţia cu aceasta.

Departamentul Juridic împreună cu Ofițerul de Protecție a Datelor (DPO) monitorizează și analizează legile privind datele cu caracter personal și modificările regulamentelor, elaborează cerințe de conformare și asistă departamentele comerciale la realizarea obiectivelor acestora privind datele cu caracter personal.

Directorul Departamentului IT răspunde de:

- Asigurarea că toate sistemele, serviciile și echipamentele utilizate pentru stocarea datelor se conformează standardelor de securitate acceptabile.
- Efectuarea verificărilor și scanărilor periodice pentru asigurarea că hardware-ul și software-ul de securitate funcționează în mod corespunzător.

Directorul Departamentului Marketing răspunde de:

- Aprobarea oricăror declarații de protecție a datelor atașate la comunicări, cum ar fi mesaje de e-mail sau adrese.
- Replicarea la orice întrebări privind protecția datelor din partea jurnaliștilor sau canalele de mass media, cum ar fi ziarele.
- Dacă este cazul, colaborarea cu Ofițerul de Protecție a Datelor (DPO) pentru a se asigura că inițiativele de marketing respectă principiile de protecție a datelor.

Directorul Departamentului Resurse Umane răspunde de:

- Îmbunătățirea informării tuturor angajaților despre protecția datele cu caracter personal ale utilizatorilor.
- Organizarea instruirilor de competență și informare privind datele cu caracter personal pentru angajații care lucrează cu date cu caracter personal.
- Protecția completă a datelor cu caracter personal ale angajaților. Acesta are obligația să se asigure că datele cu caracter personal ale angajaților se prelucrează în scopuri comerciale legitime ale angajatorului și în funcție de necesitățile acestuia.

Managerul Compartimentului Achiziții răspunde de înaintarea responsabilităților de protecție a datelor cu caracter către furnizori și îmbunătățirea nivelurilor de informare ale furnizorilor în privința protecției datelor cu caracter personal, precum și cerințele de transmitere descendentă a datelor cu caracter personal către orice terț utilizat de un furnizor. Compartimentul de Achiziții are obligația să se asigure că Instituția își rezervă dreptul de a audita furnizorii.

Conflictele legilor

Scopul acestei Politici este să se conformeze cu legile și reglementările existente la locația sediului și din țările în care funcționează Instituția. În cazul oricărui conflict între această Politică și legile și reglementările aplicabile, vor prevala acestea din urmă.

Prin utilizarea acestui site, vizitatorul/ utilizatorul/ Solicitantul de credit/ Împrumutatul confirmă că a citit și este de acord cu Politica de Confidentialitate privind procesarea datelor cu caracter personal.