Asigurarea Românească - ASIROM VIENNA INSURANCE GROUP SA

POLITICA

DE

PROTECȚIE A DATELOR CU CARACTER PERSONAL

15/11/2018

EDITIA 1/ REVIZIA 2

CONTROL DOCUMENT

CONTROL MODIFICĂRI

Editie/ revizie	Nume persoane responsabile	Modificari	Data
1.0	Doina Baron	Prima variantă	08.2014
1.1	Adrian Ioniță	Revizie și actualizare	05.2018
1.2	Adrian Ioniță	Revizie și actualizare	11.2018

AVIZARI

Status Document	Editie/ Revizie/ Nume persoane responsabile	Data
ELABORAT	1.2/ Adrian IONIȚĂ	09.11.2018
APROBAT	1.2/ Directorat	11.2018
	1.2/ Consiliu de Supraveghere	11.2018

CUPRINS

1 DEFINIȚII ȘI ABREVIERI

Datele cu caracter personal (**Date**) - orice informație referitoare la o persoană fizică identificată sau identificabilă (persoana vizată); o persoană fizică identificabilă este una care poate fi identificată, direct sau indirect, în special prin referire la un identificator cum ar fi un nume, un număr de identificare, date despre locație, un identificator online sau unul sau mai mulți factori specifici fizic, fiziologic, genetic, mental, economic, cultural sau social al acelei persoane fizice.

Categorii speciale de date cu caracter personal – orice informație care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate, date genetice, 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.

Prelucrarea datelor cu caracter personal (Prelucrare) - 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.

Sistem de evidență a datelor cu caracter personal - orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcționale sau geografice.

Persoana vizată - o persoană fizică 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. În cadrul ASIROM se pot prelucra următoarele categorii de date:

- Clienți/ potențiali clienți/ asigurați/ altele (foști clienți/ terți păgubiți etc.) - pentru datele prelucrate in scopul prestării serviciilor de asigurare;
- Angajații și colaboratorii ASIROM (inclusiv persoanele fizice care desfășoară activități în cadrul ASIROM în temeiul codului muncii) / membrii familiilor acestora - pentru datele prelucrate în scopuri de resurse umane;
- Vizitatori/ angajați - pentru datele prelucrate în scopul monitorizării/ asigurării securității persoanelor, spațiilor și/ sau bunurilor publice/ private;
- Persoanele fizice, reprezentanți ai persoanelor juridice cu care ASIROM intră în contact în calitate de clienți.

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.

Persoană împuternicită de către Operator (Împuternicit) - persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului.

Persoană autorizată să prelucreze date (Persoană autorizată) – Operatorul sau Împuternicitul sau persoanele care, sub autoritatea directă a Operatorului sau a Împuternicitului, sunt autorizate să prelucreze date.

Parte Terță - 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.

Structura de conducere - Directoratul și Consiliul de Supraveghere.

Consimțământ - 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.

ASIROM - Societatea - Asigurarea Românească - ASIROM VIENNA INSURANCE GROUP S.A.

ASF - Autoritatea de Supraveghere Financiară.

ANSPDCP – Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal.

DPO - Ofițerul pentru Protecția Datelor.

DPO – VIG - Ofițerul pentru Protecția Datelor al Grupului VIG.

GDPR – 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.

2 SCOPUL, OBIECTIVELE ȘI IMPLEMENTAREA POLITICII

2.1. SCOPUL ȘI OBIECTIVELE

Obiectivul major al Politicii de protecție a datelor cu caracter personal este de a asigura conformitatea cu legislația în domeniul protecției datelor cu caracter personal și de a minimiza riscurile prin prevenirea incidentelor de protecție a datelor cu caracter personal și reducerea impactului lor potențial.

Obiectivele generale privind protecția datelor cu caracter personal sunt:

- Asigurarea demonstrării responsabilității ASIROM privind protecția datelor cu caracter personal, în special în ceea ce privește implementarea măsurilor tehnice și organizatorice adecvate pentru a demonstra conformitatea cu GDPR;
- Îndeplinirea integrală a cerințelor privind protecția datelor cu caracter personal aplicabile, solicitate de parteneri;
- Creșterea gradului de conștientizare a importanței protecției datelor cu caracter personal în rândul angajaților;
- Asigurarea de planuri și resurse pentru supraviețuirea și revenirea în cazul unor situații de urgență;
- Asigurarea unor canale eficiente de notificare a ANSPDCP și a persoanelor vizate privind incidente de securitate în domeniul protecției datelor;
- Reducerea impactului negativ al unor potențiale riscuri privind protecția datelor cu caracter personal asupra activității societății;

- Creșterea încrederii clienților în serviciile oferite de ASIROM;
- Creșterea competitivității serviciilor prin utilizarea de tehnologii și echipamente performante pentru activitatea privind protecția datelor cu caracter personal;
- Dezvoltarea competențelor profesionale ale angajaților privind protecția datelor cu caracter personal;
- Identificarea, analizarea și evaluarea realistă a riscurilor privind datele cu caracter personal.

2.2. CONȚINUT ȘI SCOP

Politica de protecție a datelor cu caracter personal are ca scop stabilirea regulilor, a modului de organizare și a responsabilităților privind prelucrarea datelor cu caracter personal în cadrul ASIROM, în vederea asigurării conformității cu prevederile legislației și reglementărilor în vigoare, aplicabile.

În acest sens, în activitatea de prelucrare a datelor cu caracter personal ale persoanelor vizate, ASIROM asigură:

- Prelucrarea datelor cu caracter personal ale persoanelor vizate și ale angajaților săi în conformitate cu prevederile legale;
- Respectarea principiilor de protecție a datelor în activitățile operaționale ale societății;
- Transparență în legătură cu categoriile de date cu caracter personal prelucrate în cadrul ASIROM, precum și în legătură cu scopurile prelucrărilor, destinatarii datelor cu caracter personal;
- Drepturile persoanelor vizate: dreptul la informare, dreptul de acces, dreptul la rectificare, dreptul la ștergerea datelor, dreptul la restricționarea prelucrării, dreptul la portabilitatea datelor, dreptul la opoziție, dreptul de a nu face obiectul unei decizii individuale bazate exclusiv pe prelucrare automată, dreptul de a depune plângere la o autoritate de supraveghere și dreptul de a se adresa justiției;
- Implementarea unor măsuri tehnice și organizatorice adecvate pentru garantarea drepturilor și libertăților persoanelor fizice.

2.3. DOMENIUL DE APLICARE

Respectarea prevederilor prezentei politici este obligatorie pentru întreg personalul ASIROM.

2.4. REVIZIE ȘI ACTUALIZARE

Politica va fi analizată anual și va fi modificată și actualizată, după caz. Orice modificare adusă Politicii va fi supusă aprobării Structurii de conducere ASIROM.

3 PROTECȚIA DATELOR: PREVEDERI GENERALE, PRINCIPII ȘI CATEGORII DE DATE PERSONALE

3.1 PREVEDERI GENERALE

GDPR se aplică prelucrării datelor cu caracter personal prin mijloace automate și prelucrării de date personale care fac parte dintr-un sistem de păstrare a datelor sau sunt destinate să facă parte dintr-un sistem de păstrare a datelor.

GDPR se aplică prelucrării datelor cu caracter personal în contextul activităților unui Operator sau unui Împuternicit din UE (indiferent dacă prelucrarea are loc sau nu în UE) și prelucrării datelor cu caracter personal ale persoanelor

care se află în UE de către un Operator sau Împuternicit care nu este stabilit în UE și unde activitățile de prelucrare sunt legate de furnizarea de bunuri și de servicii.

Regulamentul GDPR descrie normele privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și normele privind libera circulație a datelor cu caracter personal prin protejarea drepturilor și libertăților fundamentale ale persoanelor fizice și, în special, a dreptului acestora la protecția datelor cu caracter personal .

Persoanele și organismele juridice nu sunt incluse în domeniul de aplicare al GDPR.

GDPR urmărește în primul rând să înapoieze cetățenilor și rezidenților controlul asupra datelor lor personale și să simplifice mediul de reglementare pentru afacerile internaționale prin unificarea reglementării în cadrul UE.

3.2 PRINCIPII CU PRIVIRE LA PRELUCRAREA DATELOR CU CARACTER PERSONAL

Prelucrarea datelor cu caracter personal se supune următoarelor principii:

1. Legalitate, echitate și transparență – datele vor fi prelucrate în mod legal, echitabil și transparent față de persoana vizată;
2. Limitări legate de scop – datele vor fi colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri;
3. Reducerea la minimum a datelor – datele vor fi adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate;
4. Exactitate – datele vor fi exacte și, în cazul în care este necesar, vor fi actualizate; se vor lua 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;
5. Limitări legate de stocare – datele vor fi 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, sub rezerva punerii în aplicare a măsurilor de ordin tehnic și organizatoric adecvate;
6. Integritate, disponibilitate și confidențialitate – datele vor fi 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;
7. Responsabilitate – datele vor fi prelucrate cu respectarea principiilor sus-menționate, iar ASIROM va fi responsabil să demonstreze această respectare.

3.3 REGULI GENERALE CU PRIVIRE LA PRELUCRAREA DATELOR CU CARACTER PERSONAL

ASIROM urmărește efectuarea prelucrărilor de date cu îndeplinirea următoarelor condiții de legalitate, după caz:

1. **Executarea/ Încheierea unui contract -** 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;
2. **Obligație legala -** prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine ASIROM;
3. **Consimțământul -** persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice**;** în cazul minorilor, consimțământul va fi obținut de la titularul răspunderii părintești asupra copilului;

4. **Interese legitime -** prelucrarea este necesară în scopul intereselor legitime urmărite de ASIROM sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate;
5. **Interes vital -** prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;
6. **Interes public** - prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul.

În toate cazurile, la momentul obținerii datelor, ASIROM va informa persoana vizată despre:

- identitatea Operatorului și a reprezentantului acestuia, dacă este cazul;
- scopul în care se face prelucrarea datelor, precum și temeiul juridic (dacă prelucrarea se face în temeiul intereselor legitime, se va face referire la acestea);
- existența dreptului de a-și retrage consimțământul atunci când prelucrarea se întemeiază pe consimțământ și nu mai există alt temei de prelucrare;
- destinatarii sau categoriile de destinatari ai datelor;
- dacă furnizarea tuturor datelor cerute este obligatorie și consecințele refuzului de a le furniza;
- existența drepturilor prevăzute de lege pentru persoana vizată, precum și condițiile în care pot fi exercitate;
- intenția de a transfera datele în afara UE sau către o organizație internațională, precum și menționarea garanțiilor aplicabile;
- perioada de stocare a datelor sau criteriile utilizate pentru a o determina;
- informații despre existența unui proces decizional automatizat, dacă este cazul, precum și informații utile legate de logica utilizată și importanța prelucrării;
- orice alte informații a căror furnizare este impusă prin dispoziție a ANSPDCP, ținând seama de specificul prelucrării.

În cazul în care ASIROM nu obține datele direct de la persoana vizată, ASIROM este obligată să îi furnizeze acesteia informațiile prevăzute mai sus, cu respectarea următoarelor termene:

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

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

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

Durata de prelucrare este limitată în funcție de termenele de retenție ale datelor raportat la scopul pentru care au fost colectate datele pentru activitățile de prelucrare.

3.4 REGULI SPECIALE DE PRELUCRARE

3.4.1 PRELUCRAREA ÎN SCOP DE RECLAMĂ/ MARKETING/ PUBLICITATE A DATELOR CLIENȚILOR

- ASIROM a informat persoana vizată prin documente specifice de intrare în relație cu societatea, iar persoana vizată și-a exprimat consimțământul expres și neechivoc (obținut prin bifarea opțiunii „Da” în format letric sau în format electronic) pentru primirea de comunicări din partea ASIROM în astfel de scopuri;
- Persoana vizată are dreptul de a se opune în orice moment, în mod gratuit și fără nicio justificare, ca datele care o vizează să fie prelucrate de către operator în scop de marketing direct sau să fie transmise unor terți (inclusiv din cadrul Grupului VIG) într-un asemenea scop;

- Înaintea prelucrării în scop de reclamă/ marketing/ publicitate, ASIROM va verifica să existe consimțământul valabil al persoanei vizate în acest sens pe toata durata prelucrării (de ex.: persoana vizată să nu își fi exercitat dreptul de opoziție). Anterior inițierii oricăror prelucrări de date cu caracter personal ale clienților, altele decât cele incluse în Registrul de activități de prelucrare a datelor cu caracter personal, se va solicita avizul DPO, privind condițiile de legalitate a acestor prelucrări.

3.4.2 PRELUCRAREA DATELOR APARȚINÂND PĂRȚILOR TERȚE

În cazul operațiunilor desfășurate de ASIROM cu datele unor terțe părți, anterior inițierii oricăror prelucrări de date ASIROM va obține consimțământul persoanelor vizate și/ sau furnizează informațiile cu privire la aceste prelucrări.

3.4.3 PROTECȚIA SPECIALĂ A MINORILOR

În ceea ce privește oferirea de servicii ale societății informaționale direct unui copil, atunci când prelucrarea datelor acestuia se întemeiază pe consimțământ, prelucrarea datelor cu caracter personal ale unui copil este legală în cazul în care copilul are cel puțin 16 ani. În cazul în care copilul are sub 16 ani, o astfel de prelucrare este legală numai dacă și în măsura în care consimțământul este acordat sau autorizat de titularul răspunderii părintești asupra copilului. Operatorul face eforturi rezonabile pentru a verifica, în astfel de cazuri, acordarea sau autorizarea de către titularul răspunderii părintești asupra copilului, ținând cont de tehnologia disponibilă.

3.5 PRELUCRAREA CATEGORIILOR SPECIALE DE DATE CU CARACTER PERSONAL

Prelucrarea următoarelor categorii speciale de date cu caracter personal este supusă unor cerințe stricte și este permisă numai în anumite condiții:

- rasă sau etnie,
- opinii politice,
- credința religioasă sau filosofică,
- apartenența la sindicate,
- date genetice și biometrice,
- date privind sănătatea,
- date privind viața sexuală sau orientarea sexuală a unei persoane fizice.

În cazul prelucrării unor categorii speciale de date cu caracter personal, ASIROM va realiza acest lucru doar în următoarele situații:

- persoana vizată și-a dat consimțământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice;
- 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;
- prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice, atunci când persoana vizată se află în incapacitate fizică sau juridică de a-și da consimțământul;
- prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță sau ori de câte ori instanțele acționează în exercițiul funcției lor judiciare;
- prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod manifest de către persoana vizată.

3.6 REGULI DE MONITORIZARE

3.6.1 SUPRAVEGHEREA VIDEO

- Are ca scop prevenirea și combaterea săvârșirii infracțiunilor, asigurarea pazei și protecției persoanelor, bunurilor și valorilor, a imobilelor și a instalațiilor ASIROM precum și a împrejmuirilor acestora și/ sau realizarea unor interese legitime, cu condiția să nu se prejudicieze drepturile și libertățile fundamentale sau interesul persoanelor vizate;
- Prelucrarea vizează orice imagine care permite identificarea directă sau indirectă a persoanelor fizice;
- Camerele de supraveghere video sunt amplasate în locuri vizibile și sunt semnalizate corespunzător;
- Prelucrarea datelor salariaților prin mijloace de supraveghere video (de ex. casierie, tezaur, casete valori) este permisă pentru îndeplinirea unor obligații legale exprese (asigurarea pazei și protecției bunurilor inclusiv prevenirea și combaterea săvârșirii infracțiunilor) sau în temeiul unui interes legitim, cu respectarea drepturilor salariaților, în special a informării prealabile a acestora.

3.6.2 ASIGURAREA SECURITĂȚII SISTEMULUI INFORMAȚIONAL ȘI A COMUNICĂRILOR ELECTRONICE ÎN CADRUL ASIROM

- Are ca scop protejarea informațiilor confidențiale, securitatea sistemelor informatice, prevenirea și/ sau detectarea fraudelor, preîntâmpinarea scurgerii informațiilor care conțin date cu caracter personal prin metoda excluderii accesului neautorizat la acestea; preîntâmpinarea distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în rețelele de telecomunicații și resursele informaționale; respectarea cadrului normativ de folosire a sistemelor informaționale și a programelor de prelucrare a datelor cu caracter personal; asigurarea caracterului complet, integru, veridic al datelor cu caracter personal în rețelele de telecomunicații și resurselor informaționale; păstrarea posibilităților de gestionare a procesului de prelucrare și păstrare a datelor cu caracter personal, precum și protecția reputației ASIROM. Vizează, de asemenea, urmărirea evoluției amenințărilor aferente sistemelor informatice și mai ales riscurile de natură logică (intruziune, blocarea serviciilor, etc.). Prelucrările vizează doar datele de trafic și datele de acces/ transmitere a corespondentei;
- Accesarea/ monitorizarea datelor de conținut este realizată numai în circumstanțe temeinic justificate, precum și în cazurile determinate de necesitatea îndeplinirii unor prevederi legale;
- Angajații vor fi informați la angajare, precum și ori de câte ori este cazul, despre modul de utilizare a conexiunii la internet și e-mail, precum și despre excepțiile aplicabile.

3.6.3 MONITORIZAREA AUTOTURISMELOR AFLATE ÎN UTILIZAREA ASIROM

- Are ca scop securitatea autoturismelor aflate în utilizarea ASIROM (paza și protecția bunurilor). Datele care pot fi prelucrate în acest caz sunt: detaliile autovehiculului, ruta planificată, datele privind incidentul (data, ora, locul accidentului).

3.6.4 CONTROLUL ACCESULUI ANGAJAȚILOR ÎN CADRUL ASIROM

- Are ca scop asigurarea unui control al accesului în cadrul ASIROM; datele obținute în urma acestei prelucrări nu vor fi utilizate în alte scopuri.

3.6.5 DURATA DE PRELUCRARE A DATELOR MONITORIZATE IN CADRUL ASIROM

În vederea realizării scopurilor menționate la punctele 3.6.1, 3.6.2, 3.6.3 și 3.6.4, ASIROM va prelucra datele pe parcursul relației cu persoana vizată sau pe perioada impusă de prevederile legale și documentată în Nomenclatorul Arhivistic și procedurile operaționale aplicabile fiecărui departament în parte.

Ulterior încheierii operațiunilor de prelucrare a datelor în scopurile pentru care au fost colectate, acestea vor fi arhivate de către ASIROM pe durata de timp prevăzută în documentele normative interne; ulterior, la împlinirea termenului de stocare, datele vor fi distruse astfel cum este precizat în procedura aplicabilă.

4 SCOPUL TERITORIAL AL PRELUCRĂRII DATELOR CU CARACTER PERSONAL

Obiectivul major este ca ASIROM să se asigure că nivelul de protecție și securitate al datelor cu caracter personal, garantat de GDPR, nu este compromis.

4.1 PRELUCRAREA INTERNĂ A DATELOR CU CARACTER PERSONAL

Atunci când prelucrează date personale intern, ASIROM ia în considerare următoarele principii de bază:

- prelucrarea legală a datelor;
- contract valabil de prelucrare a datelor, dacă este necesar;
- respectarea GDPR sau altor prevederi legale și reglementări naționale referitoare la protecția datelor.

4.2 PRELUCRAREA DATELOR CU CARACTER PERSONAL ÎN UE

Având în vedere aplicabilitatea GDPR în cadrul UE, sunt respectate standardele și cerințele stabilite în acest sens. În același timp sunt respectate și legile și reglementarile naționale, respectiv acele reglementări care aduc clarificări cu privire la modalitatea de implementare și respectare a GDPR.

4.3 TRANSFERUL DE DATE CU CARACTER PERSONAL CĂTRE UN STAT TERȚ

Transferul poate avea loc numai dacă statul către care se intenționează transferul asigura un nivel de protecție adecvat.

Transferul de date către un stat a cărui legislație nu prevede un nivel de protecție cel puțin egal cu cel oferit de Regulament este posibil numai dacă există garanții suficiente cu privire la protecția drepturilor fundamentale ale persoanelor vizate. Aceste garanții vor fi stabilite de ASIROM în contracte încheiate cu furnizorii/ prestatorii de servicii către care se va realiza transferul datelor.

Regulile privind transferul datelor în state terțe se aplică inclusiv în cazul în care destinatarul datelor este o entitate din VIG Grup.

5 DREPTURILE PERSOANEI VIZATE

Dreptul de acces la date

Orice persoana vizată are dreptul de a obține de la ASIROM, atunci când ASIROM acționează în calitatea sa de Operator, la cerere și în mod gratuit pentru o solicitare pe an, confirmarea faptului că datele care o privesc sunt sau nu prelucrate de ASIROM, iar în caz afirmativ, se vor furniza informațiile referitoare la: scopurile prelucrării; categoriile de date vizate; destinatarii sau categoriile de destinatari ai datelor, în special destinatari din țări terțe sau organizații internaționale; acolo unde este posibil, perioada pentru care se preconizează că vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă; existența dreptului de a solicita ASIROM rectificarea sau ștergerea datelor ori restricționarea prelucrării lor sau a dreptului de a se opune prelucrării; dreptul de a depune o plângere în fața unei autorități de supraveghere; dacă datele nu sunt colectate de la persoana vizată, orice informații disponibile privind sursa acestora; existența unui proces decizional automatizat, precum și informații pertinente privind logica utilizată și importanța preconizată a unei astfel de prelucrări pentru persoana vizată.

Dreptul de rectificare

Persoana vizată are dreptul de a obține de la ASIROM în calitate de operator de date, fără întârzieri nejustificate, rectificarea datelor cu caracter personal inexacte care o privesc.

Ținându-se seama de scopurile în care au fost prelucrate datele, persoana vizată are dreptul de a obține completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declarații suplimentare.

Dreptul la ștergerea datelor

Persoana vizată are dreptul de a obține ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, iar ASIROM va avea obligația de a șterge datele fără întârzieri nejustificate în cazul în care:

a) datele nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;
b) persoana vizată își retrage consimțământul pe baza căruia are loc prelucrarea;
c) datele cu caracter personal au fost prelucrate ilegal;
d) persoana vizată își exercită dreptul la opoziție în condițiile Regulamentului General pentru Protecția Datelor;
e) datele trebuie șterse pentru respectarea unei obligații legale a operatorului;
f) datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale societății informaționale minorilor în condițiile Regulamentului General pentru Protecția Datelor.

ASIROM, în calitate de operator de date, poate refuza cererea de ștergere a datelor în următoarele condiții:

a) prelucrarea este necesară pentru exercitarea dreptului la liberă exprimare și la informare;
b) prelucrarea este necesară pentru respectarea unei obligații legale aplicabile operatorului;
c) prelucrarea este necesară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în condițiile Regulamentului General pentru Protecția Datelor, în măsura în care exercitarea dreptului poate face imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective;
d) prelucrarea este necesara pentru constatarea, exercitarea sau apărarea unui drept în instanță.

Dreptul la restricționarea prelucrării

Persoana vizată are dreptul de a obține din partea ASIROM în calitate de operator de date restricționarea prelucrării în următoarele cazuri:

a) persoana vizată contestă exactitatea datelor, pentru o perioadă care îi permite operatorului să verifice exactitatea datelor;
b) prelucrarea este ilegală, dar persoana vizată se opune ștergerii datelor cu caracter personal, solicitând în schimb restricționarea utilizării lor;
c) ASIROM 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;
d) 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

Persoana vizată are dreptul:

a) de a se opune în orice moment, din motive întemeiate și legitime legate de situația sa particulară, ca datele care o vizează să facă obiectul unei prelucrări, cu excepția cazurilor în care există dispoziții legale contrare. În caz de opoziție justificată, prelucrarea nu mai poate viza datele în cauză decât dacă există motive legitime și imperioase care justifică prelucrarea și care prevalează asupra drepturilor persoanei vizate sau dacă scopul este constatarea, exercitarea sau apărarea unui drept în instanță.

b) de a se opune în orice moment, în mod gratuit și fără nici o justificare, ca datele care o vizează să fie prelucrate în scop de marketing direct, inclusiv în ceea ce privește crearea de profiluri în acest scop.

Dreptul la portabilitatea datelor

Persoana vizată are dreptul de:

a) a primi datele cu caracter personal care o privesc și pe care le-a furnizat ASIROM într-un format structurat, utilizat în mod curent și care poate fi citit automat;
b) a transmite aceste date altui operator, fără obstacole din partea ASIROM căruia i-au fost furnizate datele cu caracter personal, în cazul în care: (i) prelucrarea se bazează pe consimțământ sau pe un contract; și (ii) prelucrarea este efectuată prin mijloace automate.

În exercitarea dreptului său la portabilitatea datelor, persoana vizată are dreptul ca datele sale să fie transmise direct de la un operator la altul acolo unde acest lucru este fezabil din punct de vedere tehnic.

În plus față de drepturile de mai sus, persoana vizată mai are și următoarele drepturi:

a) de a nu fi supus unei decizii individuale, respectiv dreptul de a cere si de a obține:
    1. retragerea sau anularea oricărei decizii care produce efecte juridice în privința sa, adoptată exclusiv pe baza unei activități de prelucrare a datelor efectuată prin mijloace automate, destinată să evalueze unele aspecte ale personalității sale, precum competența profesională, credibilitatea, comportamentul ori alte asemenea aspecte;

2. reevaluarea oricărei alte decizii luate în privința sa , care o afectează în mod semnificativ, dacă decizia a fost adoptată exclusiv pe baza unei activități de prelucrare care îndeplinește condițiile prevăzute la punctul (1).

b) de a depune o plângere în fața unei autorități de supraveghere precum și dreptul de se adresa justiției.

6 OBLIGAȚII GENERALE ALE ASIROM

ASIROM implementează măsuri tehnice și organizatorice adecvate pentru a se asigura că prelucrarea datelor cu caracter personal este efectuată în conformitate cu GDPR și/ sau orice alte prevederi legale.

6.1 EVIDENȚA ACTIVITĂȚILOR DE PRELUCRARE

ASIROM ține o evidență a activităților de prelucrare aflate sub responsabilitatea sa (art. 30 din GDPR), în formă scrisă și electronic, pentru a putea fi prezentată ANSPDCP, la cerere. Această evidență conține următoarele informații:

- numele și datele de contact ale Operatorului și ale DPO;
- scopul prelucrării;
- descrierea categoriilor de subiecți de date și a categoriilor de date cu caracter personal;
- categoriile de destinatari cărora le-au fost sau le vor fi dezvăluite date cu caracter personal, inclusiv destinatarii din țări terțe;
- acolo unde este cazul, transferuri de date cu caracter personal către o țară terță, inclusiv identificarea acelei țări terțe;
- dacă este posibil, termenele prevăzute pentru ștergerea diferitelor categorii de date;
- dacă este posibil, o descriere generală a măsurilor de securitate tehnică și organizatorică (cf. art. 32 GDPR).

6.2 EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR (ART. 35 GDPR)

În cazul în care un tip de prelucrare generează un risc ridicat pentru drepturile și libertățile persoanelor fizice sau se încadrează în cazurile enumerate la art. 1 din decizia nr. 174/2018 a ANSPDCP, ASIROM va efectua, înainte de prelucrare, o evaluare a impactului operațiunilor de prelucrare preconizate asupra protecției datelor cu caracter personal.

O singură evaluare poate aborda un set de operațiuni de prelucrare similare care prezintă riscuri ridicate similare.

6.3 ACTIVITĂȚILE DE PRELUCRARE A DATELOR REALIZATE ÎN BAZA UNUI CONTRACT DE PRESTĂRI SERVICII

În cazul activităților de prelucrare a datelor în baza unui Contract de prestări servicii încheiat între ASIROM și un prestator/ furnizor/ partener, este necesar să se respecte următoarele condiții:

- contractul se încheie în scris;
- contractul conține clauze specifice privind prelucrarea datelor, pentru următoarele situații:

  a) În cazul în care prestatorul are calitatea de Operator, în contract se vor insera clauze standard;

  b) În cazul în care prestatorul are calitatea de Împuternicit, în contract se vor insera clauze specifice; în situația în care există dificultăți în stabilirea calității furnizorului de Împuternicit, departamentele implicate se vor adresa și DPO-ului;

c) În cazul in care prelucrarea presupune un transfer al datelor în țări care, conform capitolului 4.3 din prezentul document, nu asigură un nivel adecvat de protecție, se va insera în contract clauza referitoare la transfer.

În relațiile contractuale pe care ASIROM le are cu diverși prestatori/ furnizori de servicii, departamentele implicate in negocierea și încheierea contractelor trebuie să aibă în vedere:

- optarea pentru un prestator care prezintă garanții în ceea ce privește măsurile de securitate tehnică și organizatorice cu privire la activitățile de prelucrare ce vor fi efectuate (locația serverelor, locația de back-up dacă este cazul etc.);
- să identifice dacă prestarea serviciilor ce fac obiectul contractului care urmează să fie încheiat presupune un transfer de date în afara UE (ex: date stocate de către prestator pe servere aflate în SUA etc.);
- să introducă în contract clauzele specifice activităților de prelucrare de date cu caracter personal comunicate de DPO;
- să existe posibilitatea verificării conformității furnizorului cu privire la respectarea măsurilor de protecție a datelor (verificarea documentelor, expertiza, audit etc.);
- consultarea DPO.

6.4 SECURITATEA ACTIVITĂȚILOR DE PRELUCRARE A DATELOR CU CARACTER PERSONAL. INCIDENTE DE SECURITATE ÎN DOMENIUL PROTECȚIEI DATELOR (ART. 32 – 34 GDPR)

ASIROM aplică măsuri tehnice și organizatorice adecvate pentru protejarea datelor împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, în special dacă prelucrarea respectivă comportă transmisii de date în cadrul unei rețele, precum și împotriva oricărei alte forme de prelucrare ilegală. Aceste măsuri asigură un nivel de securitate adecvat în ceea ce privește riscurile pe care le reprezintă prelucrarea, precum și în ceea ce privește natura datelor care trebuie protejate.

ASIROM are implementate politici de securitatea informației *(Politica de Securitatea Informației, PSI /PP-16)* care prezintă principiile de securitate și măsurile care trebuie respectate în cadrul societății pentru a menține siguranța informațiilor, inclusiv a datelor cu caracter personal, a procesărilor și a sistemelor informatice la un nivel adecvat.

Incidentul în domeniul protecției datelor, stocate sau transmise, reprezintă orice eveniment care afectează confidențialitatea, integritatea sau disponibilitatea acestor date.

În principal, constituie incident de protecție a datelor:

- pierderea, sustragerea, înlocuirea, alterarea sau distrugerea neautorizata ori accidentală a datelor;
- modificarea neautorizată și nejustificată a datelor;
- accesul neautorizat la mediile pe care sunt stocate date.

Reprezintă risc de incident următoarele:

- nerespectarea regulilor privind depozitarea, utilizarea sau distrugerea mediilor de stocare în uz pe care sunt păstrate date;
- orice situație de natură să afecteze confidențialitatea, integritatea sau disponibilitatea datelor.

Orice incident de protecție a datelor trebuie comunicat în cel mai scurt timp DPO, în vederea notificării ANSPDCP despre acest fapt sau a operatorului de date, în cazurile în care ASIROM acționează ca Împuternicit. Notificarea către ANSPDCP trebuie formulată în termen de 72h de la momentul la care Operatorul a luat la cunoștința despre incident.

De asemenea, ASIROM deține o procedură de securitate fizică *(Regulament privind accesul în sediile ASIROM, R2/PP-15)* inclusiv pentru asigurarea siguranței sediilor și bunurilor aflate în paza juridică a ASIROM. Securitatea fizică se asigură prin desfășurarea neîntreruptă a unor activități/ acțiuni efectuate în scopul asigurării unui nivel de securitate adecvat specificului activității fiecărui obiectiv al companiei cât și pentru adaptarea permanentă la condițiile de mediu în care își desfășoară societatea activitatea.

7 MANAGEMENTUL PROTECȚIEI DATELOR

Managementul protecției datelor acoperă rolurile și responsabilitățile conform celor menționate mai jos:

7.1 ACTIVITĂȚI DPO

- Furnizarea de informații (ex. apariție/ modificare cerințe legale/ de reglementare, clauze contractuale, acorduri de prelucrare/ de confidențialitate) și consilierea Directoratului ASIROM și a angajaților ASIROM în ceea ce privește obligațiile care le revin în materia protecției datelor;
- Menținerea Registrului activităților de prelucrare a datelor;
- Menținerea Registrului de evidență a cererilor prin care își exercită drepturile persoanele vizate conform procedurii specifice;
- Evaluarea impactului schimbărilor legislative în domeniul protecției datelor asupra activităților ASIROM;
- Monitorizarea respectării dispozițiilor legale, atât din legislația primară, cât și cea secundară privind protecția datelor;
- Elaborarea, implementarea și monitorizarea respectării politicilor și procedurilor ASIROM în ceea ce privește protecția datelor cu caracter personal;
- Propunerea rolurilor și responsabilităților în ceea ce privește protecția datelor cu caracter personal;
- Identificarea, evaluarea, controlul și raportarea riscurilor de conformitate privind protecția datelor; promovarea acțiunilor de aducere la cunoștința/ sensibilizare și de formare a personalului implicat în operațiunile de prelucrare;
- Efectuarea auditurilor de protecție a datelor cu caracter personal, raportarea rezultatelor și formularea recomandărilor către Directorat;
- Furnizarea de informații la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia;
- Cooperarea cu autoritatea de supraveghere/ ANSPDCP;
- Persoană de contact pentru ANSPDCP, DPO - VIG, precum și pentru persoanele vizate;
- Îndeplinirea obligațiilor de raportare prevăzute de legislația în vigoare;
- Întreprinderea de măsuri pentru publicarea datelor de contact ale DPO pe site-ul ASIROM și transmiterea lor către ANSPDCP ;
- Cooperarea cu Grupul VIG, conform celor mentionate în Cap. 7.3;
- Raportarea, conform celor mentionate în Cap. 7.4.

7.2 POZIȚIONAREA DPO ȘI LINII DE RAPORTARE

DPO își îndeplinește sarcinile în mod independent, nu este influențat și nu primește instrucțiuni privind exercitarea sarcinilor și activităților menționate.

DPO raportează direct Directoratului ASIROM.

În conformitate cu GDPR, datele de contact ale DPO sunt publicate și comunicate ANSPDCP.

În principiu, DPO poate îndeplini alte sarcini și responsabilități în cadrul ASIROM, dacă acestea nu conduc la un conflict de interese.

7.3 COOPERAREA CU VIG GRUP

Cooperarea periodică și standardizată în cadrul VIG Grup include următoarele:

- participarea la întâlnirile de lucru ale Grupului VIG, în special pentru schimbul de experiență privind exemple de bune practici,
- comunicarea regulată cu DPO-VIG,
- furnizarea Raportului anual de activitate către DPO-VIG,
- furnizarea unui raport trimestrial privind incidentele de securitate către DPO-VIG ,
- notificarea DPO-VIG în cazul oricăror probleme de urgență legate de protecția datelor.

7.4 RAPORTAREA

La nivelul ASIROM, DPO va raporta în mod regulat Directoratului ASIROM.
În plus, va elabora un Raport anual de activitate, care să includă cel puțin următoarele elemente:

- Rezultatele auditurilor/ vizitelor ANSPDCP și, dacă este cazul, implementarea măsurilor;
- Un sumar al notificărilor adresate ASIROM de către persoanele vizate;
- Schimbări majore în cadrul sistemului de management al protecției datelor.

La nivelul VIG Grup DPO va transmite către DPO- VIG, în baza formularelor primite de la VIG:

- Raportul anual de activitate, până la sfârșitul trimestrului 1 al anului următor;
- Incidentele de securitate și impactul acestora – ad-hoc, fără întârziere.

7.5 COOPERAREA ȘI INTERACȚIUNEA CU ALTE DEPARTAMENTE

În cadrul desfășurării activității sale, DPO interacționează cu alte departamente. Având în vedere faptul că, în special în cadrul îndeplinirii atribuțiilor și responsabilităților sale, DPO acționează independent fără a fi implicat în activitatea operativă, sunt definite următoarele modalități de cooperare precum și resposanbilitățile celorlalte departamente din cadrul ASIROM:

7.5.1 RESPONSABILITĂȚI GENERALE

Toate structurile ASIROM au obligația:

- să cunoască și să respecte prevederile politicilor și procedurilor interne privind prelucrarea datelor;
- să identifice și să transmită DPO activitățile desfășurate de respectiva structură ce presupun prelucrare de date și să actualizeze informațiile ori de câte ori intervin modificări;
- să comunice către DPO incidentele de securitate care sunt de natură să conducă la o dezvăluire a datelor către persoane neautorizate.

7.5.2 RESPONSABILITĂȚI SPECIFICE

A. RESPONSABILITĂȚILE STRUCTURILOR/ SALARIAȚILOR ASIROM CARE AU ACCES LA/ PRELUCREAZĂ DATE:

- să cunoască și să respecte prevederile politicilor și procedurilor interne privind protecția datelor, precum și a celor care privesc securitatea informației (să păstreze confidențialitatea datelor, a user-ului, a parolei/ codului de acces la sistemele informatice/ baze de date prin care sunt gestionate/ stocate date etc.);

- să prelucreze numai datele minime necesare îndeplinirii atribuțiilor de serviciu și să acorde sprijin DPO pentru realizarea evaluărilor/ auditurilor specifice;
- să comunice de îndată orice situație de încălcare a prevederilor legale sau a procedurilor interne ale ASIROM referitoare la protecția datelor;
- să acorde suport DPO (în funcție de responsabilități) în formularea răspunsurilor la solicitările ANSPDCP.

B. RESPONSABILITĂȚILE STRUCTURILOR CARE ÎNCHEIE CONTRACTE DE PRESTARE/ FURNIZARE SERVICII ÎN BAZA CĂRORA SE PRELUCREAZĂ DATE:

- să solicite opinia DPO în situația în care clauzele standard privind prelucrarea datelor cu caracter personal nu sunt acceptate/ sunt modificate de potențialul prestator;
- să comunice prestatorului necesitatea ștergerii/ modificării datelor unei anumite persoane după caz (în baza informațiilor primite de la DPO, în cazul în care persoana vizata își manifestă unul dintre drepturile conferite de lege, în vederea respectării solicitării acesteia);
- să gestioneze Acordurile de confidențialitate ale colaboratorilor care au acces la date în baza contractului respectiv.

C. RESPONSABILITĂȚILE STRUCTURILOR CARE GESTIONEAZĂ CONTRACTE/ FORMULARE ÎN RELAȚIA CU CLIENȚII CARE REALIZEAZĂ CAMPANII COMERCIALE, DE MARKETING:

- să solicite opinia DPO în cazul în care prestatorul are calitatea de Împuternicit, pentru comunicarea clauzelor specifice ce se vor insera în contractele/ formularele încheiate cu clienții sau utilizate în orice regulament de campanie comerciala/ de marketing și care presupune o prelucrare de date;
- să furnizeze clienților informațiile privind prelucrarea datelor cu caracter personal;
- să verifice existența acordului persoanei vizate cu privire la prelucrarea datelor, inclusiv în scop de marketing;
- să elimine, la solicitarea DPO, din lista de prelucrare, persoanele care și-au manifestat dreptul de opoziție a prelucrării datelor în scop de marketing.

D. RESPONSABILITĂȚILE STRUCTURILOR CARE LANSEAZĂ PRODUSE NOI:

- Să solicite opinia DPO, după caz, cu privire la elaborarea și pregătirea lansării produsului nou, din perspectiva prelucrării datelor și să furnizeze informațiile relevante în acest scop.

E. RESPONSABILITĂȚILE STRUCTURILOR CARE TRANSFERA DATE ÎN ȚĂRI TERȚE:

- să realizeze transferul numai în baza unui contract semnat între ASIROM și respectivul furnizor/ prestator către care se transmit datele, contract în care să existe o clauză privind prelucrarea datelor, conform precizărilor din prezenta politică.

F. RESPONSABILITĂȚILE DEPARTAMENTULUI JURIDIC:

- să avizeze, din perspectivă juridică, clauzele privind prelucrarea datelor din modelele de contracte, din orice alte documente în baza cărora ASIROM desfășoară activitate comercială/ de marketing;
- să ofere consultanță juridica cu privire la orice activitate din cadrul ASIROM care presupune prelucrarea de date, la solicitarea structurilor care gestionează activitatea respectivă.

G. RESPONSABILITĂȚILE DEPARTAMENTULUI IT:

- să asigure implementarea măsurilor, aprobate de Directorat, pentru securitatea tehnică și informatică a datelor cu caracter personal;
- să comunice către DPO incidentele de securitate care sunt de natură să conducă la o dezvăluire a datelor către persoane neautorizate.

H. RESPONSABILITĂȚILE DEPARTAMENTULUI RESURSE UMANE:

- să asigure formarea profesională a salariaților ASIROM implicați în procesul de prelucrare. În acest scop, DPO va acorda Departamentului Resurse Umane suport în vederea realizării materialelor de sensibilizare și formare.

I. RESPONSABILITĂȚILE DEPARTAMENTULUI LOGISTICĂ

- ia măsuri pentru semnalarea existenței sistemului de supraveghere video în toate sediile ASIROM.

Din punct de vedere organizațional, DPO este integrat în managementul riscului și conformității al ASIROM, ceea ce poate conduce la participarea la reuniunile Comitetului de Conformitate, după caz.

8 DATE DE CONTACT

Orice întrebari aveți cu privire la această Politică, le puteți adresa către dpo@asirom.ro.

Nerespectarea prevederilor prezentului document pentru situațiile în care au fost aduse prejudicii societății, poate atrage răspunderea disciplinară a angajatului conform procedurilor interne.

În cazul în care Asirom va fi sancționat de către autoritățile competente pentru nerespectarea legislației privind protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, salariații care se fac vinovați de încălcarea reglementărilor legale care a avut drept consecință aplicarea sancțiunii, pot răspunde disciplinar, material sau penal, după caz.

ANEXA NR. 1

DOCUMENTE DE REFERINŢĂ:

- Legea 237/ 2015 privind autorizarea și supravegherea activității de asigurare și reasigurare;
- 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;
- Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice;
- Decizia ANSPDCP nr. 174 din 18.10.2018 privind lista operațiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecției datelor cu caracter personal;
- Legea 190/2018 privind măsuri de punere în aplicare a Regulamentului (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.
- Politica VIG privind protectia datelor.