

FORT S.A.: Politică generală privind protecția datelor cu caracter personal

Cuprins

1. POLITICA GENERALĂ PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL.....	3
2. INTRODUCERE. OBIECTIV, SCOP ȘI UTILIZATORI.....	3
3. LEGISLAȚIE ȘI DOCUMENTE DE REFERINȚĂ	4
4. DEFINIȚII.....	5
5. ROLURI ȘI RESPONSABILITĂȚI GENERALE ÎN CADRUL SOCIETĂȚII	6
5.1. OPERATOR DE DATE CU CARACTER PERSONAL – ROLUL ȘI RESPONSABILITĂȚILE SOCIETĂȚII.....	6
5.2. PERSOANA ÎMPUTERNICITĂ DE OPERATOR. ROLUL ȘI RESPONSABILITĂȚILE SOCIETĂȚII, ÎN CALITATE DE PERSOANĂ ÎMPUTERNICITĂ	7
5.3. CONFIGURAȚIA GENERALĂ A RESPONSABILITĂȚILOR ALOCATE ÎN CADRUL SOCIETĂȚII	8
6. DISEMINAREA POLITICII ȘI MONITORIZAREA CONFORMĂRII CU ACEASTA ȘI CU LEGISLAȚIA ÎN DOMENIUL PROTECȚIEI DATELOR CU CARACTER PERSONAL	8
6.1. DISEMINAREA POLITICII.....	8
6.2. MONITORIZAREA RESPECTĂRII POLITICII ȘI A LEGISLAȚIEI PROTECȚIEI DATELOR CU CARACTER PERSONAL ȘI SANȚIUNILE APLICABILE ÎN CAZUL UNOR ÎNCĂLCĂRI	8
7. PRINCIPII DE BAZĂ LEGATE DE PRELUCRAREA DATELOR CU CARACTER PERSONAL	9
7.1. LEGALITATEA, ECHITATEA ȘI TRANSPARENTA PRELUCRĂRILOR.....	10
7.2. LIMITAREA SCOPULUI	10
7.3. REDUCEREA LA MINIMUM A DATELOR	10
7.4. EXACTITATEA DATELOR	11
7.5. LIMITAREA PERIOADEI DE STOCARE (RETENȚIE)	11
7.6. INTEGRITATEA ȘI CONFIDENȚIALITATEA DATELOR	12
7.7. RESPONSABILITATEA OPERATORULUI	12
8. LINII DIRECTOARE DE URMAT DE CĂTRE ANGAJAȚI ȘI COLABORATORI / CONTRACTORI.....	12
9. SCOPURILE PENTRU CARE SOCIETATEA PRELUCREAZĂ DATELE CU CARACTER PERSONAL ȘI PERSOANELE ALE CĂROR DATE SUNT PRELUCRATE	13
10. IMPLEMENTAREA PROTECȚIEI DATELOR ÎN ACTIVITĂȚILE ÎNTEPRINSE DE SOCIETATE.....	14
10.1. COLECTAREA DATELOR CU CARACTER PERSONAL	14
10.2. INFORMAREA PERSOANELOR VIZATE.....	14
10.3. REGISTRUL DE EVIDENȚĂ AL OPERAȚIUNILOR DE PRELUCRARE	15
10.4. TEMEIURI LEGALE DE PRELUCRARE.	15
10.5. UTILIZARE, STOCARE ȘI DISTRUGERE/ȘTERGERE.....	16
10.6. DEZVĂLUIREA CĂTRE TERȚI.....	16
10.7. TRANSFERUL TRANSFRONTALIER AL DATELOR CU CARACTER PERSONAL	17
10.8. „PRIVACY BY DESIGN” ȘI „PRIVACY BY DEFAULT”	18
11. ASIGURAREA RESPECTĂRII DREPTURILOR PERSOANELOR VIZATE	18
11.1. CERERILE PERSOANELOR VIZATE. DISPOZIȚII GENERALE	18
11.2. OBLIGAȚIA DE INFORMARE A PERSOANEI VIZATE	19
11.3. DREPTURILE PERSOANELOR VIZATE	19
12. GESTIONAREA RISCURILOR. EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR CU CARACTER PERSONAL.....	23
12.1. ASPECTE GENERALE	23
12.2. CE PRESUPUNE O EVALUARE A IMPACTULUI ASUPRA PROTECȚIEI DATELOR?	23
12.3. CÂND TREBUIE EFECTUATĂ O EVALUARE A IMPACTULUI ASUPRA PROTECȚIEI DATELOR?.....	23

13. RĂSPUNSUL LA INCIDENTE DE ÎNCĂLCARE A SECURITĂȚII DATELOR CU CARACTER PERSONAL	24
14. ORGANIZARE ȘI RESPONSABILITĂȚI	24
15. AUDIT ȘI RESPONSABILITATE.....	24
16. CONFLICTELE LEGILOR.....	25
17. AUTORIZARE ȘI DISEMINARE.....	25

1. POLITICA GENERALĂ PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL

Această Politică generală privind protecția datelor cu caracter personal a fost adoptată la nivelul FORT S.A.

De către: Delia Alina Necula

În calitate de: Director General

2. INTRODUCERE. OBIECTIV, SCOP ȘI UTILIZATORI

FORT S.A. (referită în cele ce urmează ca "*Societatea*" sau "*FORT*") este un furnizor român de servicii de cybersecurity și securitate a informațiilor, specializat în teste de penetrare, audituri de securitate, evaluări de conformitate și servicii SOC. Cu experiență în proiecte desfășurate pentru organizații din domeniul reglementat și critice, FORT furnizează servicii menite să identifice vulnerabilități, să reducă riscurile cibernetice și să sprijine conformitatea cu cerințele de securitate și reglementare aplicabile. În desfășurarea activității sale, Societatea realizează operațiuni de prelucrare de date cu caracter personal.

Având în vedere preocuparea Societății pentru respectarea legislației, în general, și a normelor destinate să asigure un nivel ridicat de protecție a persoanelor fizice în ceea ce privește datele cu caracter personal ale acestora, în special, se impune adoptarea acestei politici generale menită să reglementeze cerințele generale aplicabile la nivelul Societății cu privire la operațiuni desfășurate cu și în legătură cu date cu caracter personal, conform legislației aplicabile.

Această Politică privind protecția datelor cu caracter personal la nivelul Societății (referită în cele ce urmează ca "*Politica*") stabilește principiile de bază conform cărora Societatea prelucrează datele cu caracter personal ale asociaților, angajaților, contractorilor/colaboratorilor, reprezentanților persoane fizice ale partenerilor comerciali, angajaților și/sau ale altor persoane fizice și indică responsabilitățile departamentelor și angajaților/colaboratorilor/contractorilor în ceea ce privește prelucrarea datelor cu caracter personal.

Utilizatorii acestui document sunt toți angajații, permanenți sau temporari, precum și toți contractorii/colaboratorii care lucrează în numele Societății.

Respectarea acestei Politici, de către oricare și totți angajații și contractorii / colaboratorii care lucrează în numele Societății este deosebit de importantă atât din perspectiva consecințelor juridice pe care eventualele încălcări ale legislației privind protecția datelor cu caracter personal le pot produce (*e.g. amenzi de până la 20 milioane EUR sau 4% din cifra de afaceri a Societății sau a grupului de societăți din care Societatea face parte*), cât și din perspectiva eventualelor consecințe reputaționale de tipul publicității negative, ce pot conduce la diminuarea încrederii și renumelui pe care Societatea le-a construit în piața din România și nu numai.

Având în vedere potențialele consecințe negative ale încălcării legislației referitoare la protecția datelor cu caracter personal, totți angajații, colaboratorii și / sau contractorii Societății trebuie să citească cu atenție această Politică și să se asigure că respectă pe deplin, în activitatea întreprinsă în cadrul Societății, normele privind protecția datelor cu caracter personal. Dacă va considera necesar, Societatea va comunica această Politică, ca fiind obligatoriu de urmat și respectat în desfășurarea activității, și

oricăror persoane fizice care desfășoară activități în cadrul Societății pentru perioade determinate limitate în timp, cum ar fi beneficiarii programelor de internship. Dacă suspectați că dumneavoastră sau orice alt destinatar al acestei Politici a încălcat sau este pe punctul de a încălca această Politică sau legislația aplicabilă, vă rugăm să semnalăm de îndată acest aspect în atenția persoanei desemnate la nivelul Societății ca persoană responsabilă cu asigurarea conformității cu legislația privind protecția datelor cu caracter personal.

Cu excepția cazului în care management-ul Societății decide altfel ori există o obligație legală în acest sens, dispozițiile acestei Politici sunt confidențiale și nu pot fi divulgate persoanelor din afara Societății.

Prezenta Politică se aplică tuturor operațiunilor de prelucrare a datelor cu caracter personal realizate de Societate / în numele Societății, indiferent dacă prelucrările respective sunt în curs de desfășurare la data comunicării și implementării prezentei Politici sau încep după această dată.

Angajații și contractorii/colaboratorii Societății vor fi înștiințați despre prevederile acesteia, iar angajații și contractorii/colaboratorii esențiali din punctul de vedere al activităților de prelucrare în care sunt implicați vor fi instruiți cu privire la prevederile acesteia și ale legislației României și ale Uniunii Europene privind protecția datelor cu caracter personal. Societatea poate decide oricând instruirea oricăror alți angajați cu privire la protecția datelor cu caracter personal, în funcție de necesități și de resursele disponibile.

3. 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;
- Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice;
- Decizia Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) nr. 174/2018 privind lista operațiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecției datelor cu caracter personal;
- Orice alte Decizii ale ANSPDCP, așa cum pot fi acestea adoptate din când în când;
- Ghidul orientativ de aplicare a Regulamentului General privind Protecția Datelor destinat operatorilor, publicat de ANSPDCP pe website-ul autorității;
- Politica generală a Societății privind securitatea informațiilor;
- Politica Societății de stocare (retenție) a datelor cu caracter personal ale persoanelor vizate;
- Politica de securitate privind datele cu caracter personal stocate pe suporturi fizice;
- Politica de securitate privind datele cu caracter personal stocate pe suporturi electronice;
- Procedura privind respectarea obligațiilor referitoare la informarea persoanelor vizate;
- Procedura aplicabilă în caz de încălcare a securității datelor cu caracter personal;
- Procedura Societății cu privire la recrutarea unei persoane împuternicite;
- Procedura privind evaluarea intereselor legitime ca temei al prelucrării de date cu caracter personal realizate de Societate;
- Procedura cu privire la evaluarea impactului asupra protecției datelor cu caracter personal și consultarea prealabilă a autorității de supraveghere;

- Procedura de răspuns la cererile persoanelor vizate privind exercitarea drepturilor prevăzute de legislația protecției datelor cu caracter personal.

4. DEFINIȚII

Următoarele definiții ale termenilor utilizați în acest document sunt prezentate conform articolului 4 din GDPR:

Date cu caracter personal: Orice informații privind o persoană fizică identificată sau identificabilă („**persoana vizată**”), respectiv 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.

Categoriile speciale de date cu caracter personal : Categoriile speciale de date cu caracter personal care necesită un nivel mai ridicat de protecție ar trebui prelucrate doar în scopuri limitate, conform prevederilor legale aplicabile. Sunt considerate ca aparținând categoriilor speciale de date cu caracter personal datele cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate, precum și datele genetice, datele biometrice pentru identificarea unică a unei persoanei fizice, date privind sănătatea sau date privind viața sexuală sau orientarea sexuală a unei 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, *FORT* este operator de date cu caracter personal.

Persoană împuternicită de Operator: Persoana fizică sau juridică, 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 acestea 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 stabili 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.

Autoritate de supraveghere: Autoritatea de supraveghere în domeniul datelor cu caracter personal în România este Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP).

„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.

5. ROLURI ȘI RESPONSABILITĂȚI GENERALE ÎN CADRUL SOCIETĂȚII

5.1. Operator de date cu caracter personal – Rolul și responsabilitățile Societății

Astfel cum se indică mai sus, în sensul acestei Politici, *FORT* este operator de date cu caracter personal.

În calitate de operator, Societatea determină, singură sau împreună cu alții, scopurile și mijlocele de prelucrare a datelor cu caracter personal.

Responsabilitățile principale (responsabilități de bază) ce îi incumbă Societății, în calitate de operator de date cu caracter personal includ:

(i) să stabilească un proces pentru a se asigura că angajații și/sau colaboratorii și/sau contractorii ce acționează în numele său sunt obligați să respecte secretul și confidențialitatea datelor;

(ii) să organizeze sesiuni de formare/pregătire pentru angajați în vederea asigurării unui nivel ridicat de sensibilitate cu privire la aspectele legate de protecția datelor cu caracter personal;

(iii) să asigure stabilirea și implementarea măsurilor tehnice și organizatorice adecvate pentru a asigura securitatea prelucrării datelor cu caracter personal;

(iv) să se asigure că incidentele care implică date cu caracter personal sunt gestionate în deplină conformitate cu prevederile legale aplicabile:

Responsabilitățile suplimentare (responsabilități specifice) ce îi incumbă Societății, în calitate de operator de date cu caracter personal includ:

(i) să instituie un proces pentru a asigura legitimitatea prelucrării datelor;

(ii) să instituie un proces de selectare a Persoanelor împuternicite care să ofere garanții suficiente pentru a lua măsuri tehnice și organizatorice adecvate pentru a se conforma GDPR și pentru a asigura protecția datelor cu caracter personal;

(iii) să instituie un proces pentru a asigura transparența, față de Persoana Vizată, a operațiunilor de prelucrare și a activităților de transfer de date cu caracter personal;

(iv) să instituie un proces pentru a asigura îndeplinirea drepturilor Persoanelor Vizate, astfel cum acestea sunt reglementate prin prevederile GDPR;

(v) să instituie un registru al activităților de prelucrare;

(vi) să instituie un proces care să stea la baza evaluărilor de impact a operațiunilor de prelucrare a datelor cu caracter personal, conform cerințelor GDPR;

(vii) să se asigure că încălcările securității datelor cu caracter personal pot fi notificate autorității de supraveghere în timp util, în cazul în care sunt îndeplinite condițiile GDPR. În plus, trebuie asigurat un proces adecvat care să stea la bază comunicărilor făcute către Persoanele vizate afectate de încălcări produse asupra securității datelor cu caracter personal, în cazurile prevăzute de GDPR;

(viii) să se asigure că datele sunt șterse în conformitate cu GDPR;

(ix) să atribuie responsabilități în sarcina angajaților/colaboratorilor/contractorilor în ceea ce privește gestionarea operațiunilor de prelucrare a datelor cu caracter personal, în funcție de natura și specificul acestor operațiuni, în considerarea poziției ocupate și a sarcinilor atribuite în cadrul Societății, conform GDPR;

5.2. Persoana împuternicită de Operator. Rolul și responsabilitățile Societății, în calitate de Persoană împuternicită

În îndeplinirea obiectului său principal de activitate, Societatea deține calitatea de operator.

În contextul atribuțiilor și rolurilor multiple pe care Societatea le deține sau le dobândește, pe parcursul perioadei de timp pentru care această Politică este în vigoare, este posibil ca, în executarea obiectului unui contract încheiat între părți, prin raportare la operațiuni de prelucrare specifice ce ar fi întreprinse de Societate în numele și pe seama unui operator, conform instrucțiunilor acestuia din urmă Societatea să dobândească, calitatea de persoană împuternicită a unei alte entități ce acționează în calitate de operator.

Cum ne dăm seama care sunt situațiile în care Societatea acționează ca persoană împuternicită?

Situațiile în care Societatea acționează ca persoană împuternicită se disting prin aceea că operațiunile de prelucrare a datelor efectuate de Societate sunt întreprinse în numele și pe seama operatorului, care stabilește scopurile și mijloacele de prelucrare. Atenție, noțiunea "în numele și pe seama" nu presupune în mod esențial existența unui mandat între părți, în sensul dispozițiilor Codului civil.

Ce responsabilități avem?

Destinatarii acestei Politici vor înștiința de îndată coordonatorul echipei/departamentului din care fac parte ori de câte ori dețin informații potrivit cărora Societatea ar urma să dobândească calitatea de persoană împuternicită al unui alt operator. În aceste situații, Societatea va putea emite instrucțiuni de lucru specifice ce vor fi adresate către angajații/colaboratorii/contractorii ce îndeplinesc atribuții specifice în legătură cu operațiunile de prelucrare întreprinse în această calitate.

5.3. Configurația generală a responsabilităților alocate în cadrul Societății

În cadrul Societății se instituie următoarea configurație a responsabilităților alocate în scopul asigurării conformității cu legislația privind protecția datelor cu caracter personal:

(i) în cadrul fiecărui departament/fiecărei echipe constituit/e potrivit unei structuri ierarhice predeterminate, responsabilitatea generală a asigurării conformității cu legislația privind protecția datelor cu caracter personal este atribuită coordonatorului numit al departamentului/echipei;

Membrii departamentelor/echipelor au obligația de a asigura respectarea întocmai a prezentei Politici și de a adresa orice problemă sau aspecte privind/derivând din operațiuni de prelucrare de date cu caracter personal, în atenția coordonatorului de departament/echipă.

Coordonatorii departamentelor/echipelor vor asigura respectarea prezentei Politici de către toți membrii departamentului/echipei coordonate și vor asigura asistență acestora din urmă cu privire la orice aspecte privind operațiunile de prelucrare desfășurate, potrivit prevederilor acestei Politici și ale legislației aplicabile.

(ii) în cadrul unui departament/unei echipe în cadrul căreia nu este instituită o structură ierarhică, responsabilitatea asigurării conformității cu legislația privind protecția datelor revine fiecărui membru al departamentului/echipei;

Membrii departamentelor/echipelor vor asigura, în exercitarea atribuțiilor desemnate în sarcina acestora, respectarea prezentei întocmai a acestei Politici.

6. DISEMINAREA POLITICII ȘI MONITORIZAREA CONFORMĂRII CU ACEASTA ȘI CU LEGISLAȚIA ÎN DOMENIUL PROTECȚIEI DATELOR CU CARACTER PERSONAL

6.1. Diseminarea Politicii

Coordonatorul Departamentului de HR se va asigura că această Politică este transmisă în atenția fiecărui destinatar al Politicii (colaborator / contractor / angajat și orice altă persoană ce poate fi desemnată ca destinatar al Politicii, prin decizie scrisă sau verbală a Societății, cum ar fi persoana ce beneficiază de un program de internship organizat la nivelul Societății), prin e-mail. Destinatarii acestei Politici au obligația de a citi această Politică în întregime și de a confirma luarea la cunoștință a prevederilor acesteia și acordul față de prevederile acesteia. Confirmarea se va transmite în orice caz, în scris, prin e-mail. În măsura în care există întrebări, neclarități sau condiționări specifice ce ar împiedică destinatarul Politicii să confirme luarea la cunoștință și să exprime acordul față de această Politică, acesta va transmite mențiuni și informații specifice în acest sens în atenția coordonatorului Departamentului de HR.

Orice angajat/colaborator/contractor al Societății ce are orice întrebare sau nelămurire cu privire la prevederile acestei Politici în contextul desfășurării activităților desemnate în cadrul Societății le poate adresa în atenția coordonatorului departamentului din care face parte sau în atenția coordonatorului Departamentului HR, acolo nu există un coordonator de departament.

6.2. Monitorizarea respectării Politicii și a legislației protecției datelor cu caracter personal și sancțiunile aplicabile în cazul unor încălcări

Pentru a se asigura că Politica și legislația privind prelucrarea datelor cu caracter personal sunt respectate, în cazul în care echipa de management va decide în acest sens, una sau mai multe persoane desemnate în acest scop pot realiza sau, după caz, organiza, la diferite intervale de timp, potrivit deciziei emise de către echipa de management în acest sens, audituri interne. Data, durata, modul de desfășurare, concluziile și recomandările rezultate în urma auditului vor fi înregistrate în formă scrisă și vor fi prezentate în atenția echipei de management. Societatea, orice angajat sau colaborator au obligația de a sprijini persoanele desemnate în efectuarea de activități de monitorizare a respectării Politicii și a legislației protecției datelor la nivelul Societății, în realizarea acestor activități.

La nivelul departamentelor/echipelor din cadrul Societății, prevederile Secțiunii 5 de mai sus rămân aplicabile.

7. 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 întreprind activități ce presupun și/sau implică prelucrări de date cu caracter personal. Cele 7 (șapte) principii, descrise mai în detaliu în cadrul acestei Politici, pot fi sumarizate după cum urmează:

Legalitate, Echitate și Transparență.

Respectarea limitărilor legate de scop.

- Să fim deschiși și transparenți, față de Persoanele Vizate, în legătură cu operațiunile pe care le întreprindem în legătură cu datele cu caracter personal, mijloacele utilizate în prelucrare și scopul pentru care efectuăm activități de prelucrare de date;
- Să ne asigurăm că operațiunile de prelucrare sunt legale, ceea ce presupune că orice operațiune de prelucrare trebuie să aibă un temei legal (dintre temeiurile legale prevăzute de lege și redate în cele ce urmează); *Atenție*, nu vom confunda temeiul legal al prelucrării cu obligația legală ce justifică prelucrarea; obligația legală este doar unul dintre temeiurile prevăzute de lege pentru o prelucrare legală a datelor cu caracter personal;

Reducerea la minimum a datelor

- Să colectăm și să utilizăm doar minimumul necesar de date;

Exactitate

- Să păstrăm date corecte, complete și să urmărim asigurarea actualizării acestor date;

Respectarea limitărilor legate de stocare

- Să nu păstrăm datele mai mult decât este necesar, conform prevederilor legale sau, acolo unde legea nu prevede, conform scopului declarat;

Integritate și confidențialitate

- Să prelucrăm datele în condiții de siguranță; aceasta presupune că operațiunile de prelucrare vor fi întreprinse 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;

Reponsabilitate

- Să fim responsabili cu prelucrările pe care le facem și să putem demonstra oricând respectarea prevederilor legale.

7.1. Legalitatea, echitatea și transparența prelucrărilor

Datele cu caracter personal trebuie prelucrate în mod legal, corect și transparent în legătură cu Persoana Vizată.

Societatea, în calitate de Operator, va întreprinde orice operațiune de prelucrare a datelor cu caracter personal numai cu îndeplinirea cumulativă a următoarelor condiții:

(i) a identificat un temei de prelucrare corespunzător, dintre temeiurile de prelucrare prevăzute de lege;

(ii) a identificat și a stabilit scopurile și mijloacele de prelucrare și asigură întreprinderea operațiunii de prelucrare în condiții de echitate față de Persoana Vizată;

(iii) a asigurat sau va asigura, după caz, informarea corespunzătoare a Persoanei Vizate cu privire la datele cu caracter personal ce sunt prelucrate, scopul în care și mijloacele prin care aceste date cu caracter personal sunt prelucrate, precum și cu privire la orice alte elemente prevăzute de lege.

Temeiurile legale de prelucrare sunt redate în Secțiunea 10.4. din această Politică. Este necesar să cunoaștem aceste temeiuri și să analizăm fiecare prelucrare de date cu caracter personal în considerarea acestor temeiuri. Dacă o operațiune de prelucrare nu poate fi justificată prin niciunul dintre temeiurile legale prevăzute de lege, operațiunea de prelucrare nu va fi efectuată.

7.2. 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 Societate 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 Societății, inclusiv departamentele cu funcție de suport/funcție administrativă, intenționează să utilizeze datele personale ale Persoanei Vizate în scopuri secundare (alte scopuri decât cele pentru care datele personale au fost colectate inițial), va informa Responsabilul cu protecția datelor în vederea identificării posibilității de a utiliza aceste date personale în aceste scopuri secundare, precum și a măsurilor ce trebuie întreprinse pentru astfel de utilizări.

7.3. 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, Societatea 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, Societatea 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 (aceasta se va face inclusiv prin măsuri de limitare a accesului la date) 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 Societății, decât în măsura în care este necesar pentru desfășurarea activității Societății, pentru a evita potențialele riscuri reputaționale sau litigioase care ar putea expune Societatea.

7.4. Exactitatea datelor

Datele cu caracter personal trebuie să fie exacte și, dacă este necesar, actualizate. În acest sens, Societatea 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 Societății ia la cunoștință despre orice astfel de inexactitate a datelor cu caracter personal prelucrate de către Societate, acesta va corecta inexactitatea identificată sau, dacă acest lucru nu este posibil, va informa persoana/echipa relevantă care poate înlătura inexactitatea constatată, în conformitate cu procedurile interne ale Societății de actualizare a datelor cu caracter personal.

7.5. Limitarea perioadei de stocare (retenție)

Datele cu caracter personal nu trebuie păstrate mai mult decât este necesar pentru îndeplinirea scopurilor pentru care se colectează și se prelucrează datele, în conformitate cu Politica de stocare (retenție) a datelor personale a Societății. Acolo unde perioada maximală de păstrare a datelor cu caracter personal este reglementată prin lege, în nicio situație nu se va depăși termenul legal prevăzut de lege pentru ștergerea/distrugerea datelor.

Datele cu caracter personal vor putea fi ținute de către Societate 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 Societate de măsuri de ordin tehnic și organizatoric adecvate în vederea respectării și garantării drepturilor și libertăților persoanelor vizate.

Prin excepție de la cele de mai sus, datele rezultate din activitățile de testare de securitate, inclusiv datele de testare și rapoartele aferente, vor fi păstrate pentru o perioadă de maximum trei (3) luni de la data acceptării raportului final de către client. La expirarea acestei perioade, datele de testare și rapoartele vor fi șterse în mod securizat, cu excepția cazului în care o obligație legală impune păstrarea acestora pentru o perioadă mai lungă.

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 Societății (atât electronice, cât și în format letric/hârtie), cu respectarea prevederilor legale aplicabile și a Politicii de stocare (retenție) a datelor personale a Societății.

7.6. 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, Societatea 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.

Societatea ia măsuri tehnice și organizatorice adecvate pentru a asigura securitatea datelor cu caracter personal, cum ar fi controale de acces, criptarea datelor, transferul cu respectarea strictă a cerințelor de confidențialitate etc., conform politicilor de securitate ale Societății.

7.7. Responsabilitatea Operatorului

Societatea este responsabilă de conformarea cu principiile prevăzute mai sus și trebuie să poată demonstra respectarea acestora. În acest sens, Societatea documentează respectarea principiilor de prelucrare a datelor personale prin întocmirea de proceduri adecvate de confidențialitate, retenție și securitate a datelor, prin pregătirea unui registru de evidență cu operațiunile de prelucrare efectuate de Societate, prin informarea persoanelor vizate (angajați sau clienți etc.) cu privire la prelucrarea datelor cu caracter personal de către Societate, prin postarea Politicii de confidențialitate pe website-ul Societății (pentru asigurarea principiului transparenței prelucrărilor), precum și prin orice alte demersuri întreprinse de către Societate pentru a documenta respectarea principiilor de prelucrare și îndeplinirea obligațiilor legale.

8. LINII DIRECTOARE DE URMAT DE CĂTRE ANGAJAȚI ȘI COLABORATORI / CONTRACTORI

Numai persoanele care au nevoie de acces la anumite date cu caracter personal pentru îndeplinirea sarcinilor în cadrul Societății au acces la respectivele date. O persoană are acces numai la datele necesare pentru îndeplinirea sarcinilor care îi revin.

Doar datele cu caracter personal menționate în evidența operațiunilor de prelucrare efectuate de Societate, ținută de persoana desemnată în acest sens, pot fi stocate, consultate, divulgate sau prelucrate în alt mod de angajații și colaboratorii / contractorii Societății sau de către alți destinatari desemnați ai acestei Politici. În niciun caz destinatarii acestei Politici nu vor prelucra date cu caracter personal neincluse în evidența operațiunilor de prelucrare efectuate de Societate. În cazul în care orice destinatar al acestei Politici consideră că prelucrarea anumitor date cu caracter personal suplimentare este strict necesară pentru îndeplinirea sarcinilor lor în cadrul Societății, vor informa coordonatorul departamentului din care fac parte sau direct persoana desemnată pentru ținerea registrului de prelucrare, după caz (dacă nu există un coordonator al departamentului) pentru ca acesta să modifice evidența operațiunilor de prelucrare efectuate de Societății prin adăugarea respectivei procesări. Doar ulterior modificării evidenței operațiunilor de prelucrare efectuate de Societate respectivele date cu caracter personal vor putea fi prelucrate.

Persoanele din cadrul Societății care au nevoie de acces la anumite date cu caracter personal vor solicita și, dacă au dreptul, vor obține accesul la acestea cu respectarea tuturor procedurilor și regulilor

aplicabile în cadrul Societății. De îndată ce atribuțiile de serviciu se vor modifica și noile atribuții nu vor mai necesita acces la anumite date cu caracter personal, angajații sau colaboratorii / contractorii vor informa departamentul de IT de îndată pentru a li se restricționa accesul la datele personale care nu mai sunt necesare în exercitarea noilor atribuții.

Angajații și colaboratorii / contractorii (inclusiv orice alt destinatar al Politicii) nu vor divulga datele cu caracter personal la care au acces niciunui terț neautorizat, indiferent dacă este vorba despre persoane din cadrul Societății sau din exterior. Orice divulgare de date cu caracter personal se va face doar către persoane autorizate și doar în conformitate cu fluxul de informații aprobat.

Nu vor avea loc divulgări ale datelor cu caracter personal pe căi informale (eg, utilizând telefonul personal pentru apeluri, SMS-uri, mesaje WhatsApp, folosind contul de Facebook etc.).

Angajații și colaboratorii / contractorii vor utiliza parole puternice pentru stațiile de lucru (laptop, desktop, tabletă etc.), telefoanele mobile de serviciu și orice dispozitive personale utilizate în scop de serviciu (eg, laptop, desktop, tabletă, telefon mobil utilizate pentru accesarea contului de email de serviciu). Orice parolă este de uz strict personal și nu poate fi divulgată niciunei alte persoane. Este strict interzisă comunicarea parolei chiar și către un alt angajat sau colaborator / contractor despre care se presupune că are dreptul de acces la informațiile protejate prin respectiva parolă – fiecare angajat sau colaborator / contractor trebuie să folosească propria parolă de acces.

Orice angajat sau colaborator / contractor care constată că anumite date cu caracter personal nu mai sunt de actualitate sau necesare va informa de îndată persoana responsabilă de stocarea (prelucrarea) respectivelor date și, dacă este cazul, va consulta persoana responsabilă, spre a se lua măsurile necesare.

Pentru orice aspect în domeniul prelucrării datelor cu caracter personal cu privire la care au nelămuriri, angajații și colaboratorii / contractorii se vor adresa persoanelor relevante din cadrul Societății, conform Secțiunii 5 din această Politică.

9. SCOPURILE PENTRU CARE SOCIETATEA PRELUCREAZĂ DATELE CU CARACTER PERSONAL ȘI PERSOANELE ALE CĂROR DATE SUNT PRELUCRATE

Fără a se limita la cele de mai jos, Societatea prelucrează date cu caracter personal ale următoarelor persoane, pentru următoarele scopuri:

(i) date cu caracter personal ale angajaților și ale colaboratorilor / contractorilor, precum și ale oricăror persoane care desfășoară activități în cadrul și în numele Societății în baza unui contract cu Societate (cum ar fi beneficiarii unor programe de internship) în scopul organizării, al aducerii la îndeplinire și, după caz, al încetării relațiilor de muncă ori de colaborare, precum și în scopul îndeplinirii obligațiilor legale ce incumbă Societății;

(ii) date cu caracter personal ale reprezentanților persoane fizice ale asociațiilor și administratorilor persoane juridice, în scopul organizării, al aducerii la îndeplinire sau al încetării relației dintre fiecare dintre asociații Societății și Societate, precum și în scopul îndeplinirii oricăror obligații legale ce incumbă Societății;

(iii) date cu caracter personal ale reprezentanților, angajaților și/sau colaboratorilor partenerilor contractuali – persoane juridice orice ale partenerilor contractuali – persoane fizice, în scopul asigurării menținerii și/sau încetării colaborării, după caz;

(iv) date cu caracter personal ale persoanelor fizice prelucrate în contextul unor proiecte de studii/cercetare de piață;

Lista exhaustivă a categoriilor de date cu caracter personal, a persoanelor la care acestea se referă, a scopurilor prelucrării și a altor informații relevante în această privință este conținută în evidența operațiunilor de prelucrare efectuate de Societate, ținută de persoana desemnată în acest sens.

10. IMPLEMENTAREA PROTECȚIEI DATELOR ÎN ACTIVITĂȚILE ÎNTREPRINSE DE SOCIETATE

Pentru a demonstra conformarea cu principiile de protecție a datelor, Societatea are obligația să implementeze principiile și regulile în baza cărora se asigură protecția datelor cu caracter personal, în activitățile întreprinse de Societate, 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 Societate.

10.1. Colectarea datelor cu caracter personal

Societatea are obligația să colecteze volumul minim necesar de date cu caracter personal. Dacă datele cu caracter personal se colectează de la un terț, reprezentanții, angajații și/sau contractorii / colaboratorii ce acționează în numele Societății au obligația să se asigure că datele cu caracter personal se colectează cu respectarea prevederilor legale aplicabile prevăzute de GDPR.

10.2. Informarea Persoanelor Vizate

Colectarea de date cu caracter personal de la Persoanele Vizate atrage obligația Societății de a asigura informarea corespunzătoare a fiecărei Persoane Vizate cu privire la următoarele: (i) identitatea și datele de contact ale operatorului și după caz, ale reprezentantului acestuia; (ii) datele de contact ale Responsabilului cu 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 Societate 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 Societate pentru a proteja datele cu caracter personal, cu o trimitere la mijloacele pe care la are la dispoziție pentru a obține informații 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. Aceste informații s-au comunicat/se comunică Persoanelor vizate prin Informarea privind prelucrarea datelor personale, transmisă de către Societate către Persoanele vizate prin canalele de comunicare stabilite.

Dacă datele cu caracter personal sunt obținute direct de la Persoana Vizată, informațiile prevăzute mai sus sunt furnizate în momentul obținerii acestor date cu caracter personal.

În cazul în care datele cu caracter personal nu sunt obținute direct de la Persoana Vizată, informațiile de mai sus sunt transmise:

(i) 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;

(ii) dacă datele cu caracter personal urmează să fie utilizate pentru comunicarea cu Persoana Vizată, cel târziu în momentul primei comunicări către Persoana Vizată respectivă; sau

(iii) 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.

Modalitatea de asigurare a informării Persoanelor Vizate se va stabili în funcție de canalul de comunicare existent între Societate și Persoana Vizată.

Mai multe informații cu privire la respectarea obligațiilor referitoare la informarea Persoanei Vizate sunt disponibile în cadrul Procedurii aplicabile la nivelul Societății cu privire la respectarea obligațiilor referitoare la informarea persoanei vizate, procedură de asemenea obligatorie la nivelul Societății.

10.3. Registrul de evidență al operațiunilor de prelucrare

Societatea, în calitate de Operator, ține un Registru de evidență al operațiunilor de prelucrare (referit în cele ce urmează ca "**Registru**"), care cuprinde următoarele informații:

(i) numele și datele de contact ale Societății în calitate de Operator și ale reprezentantului Operatorului;

(ii) scopurile prelucrării;

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

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

(v) 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 documentația care dovedește existența unor garanții adecvate, și în cazul transferurilor menționate la articolul 49 alineatul (1) al doilea paragraf din GDPR;

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

(vii) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate.

Societatea ține acest Registru în versiune electronică.

10.4. Temeiuri legale de prelucrare.

Societatea 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:

a) consimțământul Persoanei vizate;

b) 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 Societate, în calitate de Operator, către angajații Societății, în calitate de Persoane vizate, ca urmare a executării contractului de muncă);

- c) îndeplinirea unei obligații legale a Societății, 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 clienței și păstrare a documentației relevante, îndeplinirea obligațiilor de arhivare conform legislației specifice etc.);
- d) protejarea intereselor vitale ale Persoanei vizate sau ale altei persoane fizice;
- e) îndeplinirea unei sarcini de interes public;
- f) interesele legitime ale Societății 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, Societatea răspunde de documentarea consimțământului obținut din partea Persoanei Vizate, în deplină conformitate cu cerințele legale instituite în acest sens. Societatea 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 temei legal pentru prelucrare), în orice moment.

Când se solicită corectarea, modificarea sau distrugerea evidențelor datelor cu caracter personal, Societatea are obligația să se asigure că aceste solicitări se gestionează cu respectarea procedurilor interne și legislației în vigoare. Societatea 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 Societatea vrea să prelucreze în alt scop datele cu caracter personal colectate, și nu are un alt temei legal decât consimțământul Persoanei vizate, Societatea are obligația să solicite consimțământul Persoanei vizate pentru scopurile secundare (noi). Orice asemenea solicitare trebuie să includă scopul inițial pentru care s-au colectat datele și de asemenea scopul/scopurile nou/noi sau suplimentar(e).

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

10.5. 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. Societatea 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 sustrate, utilizate abuziv sau abuzate și pentru a preveni încălcarea securității datelor cu caracter personal.

10.6. Dezvăluirea către terți

Societatea 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 Societății, conform

instrucțiunilor specifice furnizate de Societate și potrivit mijloacelor de prelucrare stabilite de Societate. 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, Societatea se asigură că Persoana împuternicită de operator va aplica măsuri de securitate adecvate 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.).

De asemenea, Societatea 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, Societatea are obligația să solicite furnizorului sau partenerului comercial, ca acesta din urmă să asigure un nivel de protecție a datelor cu caracter personal pe deplin corespunzător exigențelor legale aplicabile în materie. Furnizorul sau partenerul comercial are obligația să prelucreze datele cu caracter personal numai pentru a îndeplini obligațiile contractuale ale acestuia față de Societate și conform instrucțiunilor documentate ale Societății și în niciun alt scop.

Atunci când Societatea prelucrează date cu caracter personal împreună cu o terță parte, în calitate de Operatori asociați, Societatea 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 Societatea transferă datele cu caracter personal către o terță parte, cele două entități neavând calitatea de Operatori asociați, acest transfer se va realiza de către Societate 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.).

10.7. 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 protecție a datelor cu caracter personal în conformitate cu prevederile GDPR, se va efectua de către Societate cu acordarea consimțământului persoanei vizate, și cu luarea de garanții adecvate privind acest transfer, cum ar fi:

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

10.8. „Privacy by design” și „Privacy by default”

Societatea asigură luarea în considerare a protecției datelor cu caracter personal încă de la momentul conceperii (Privacy by design) unei aplicații sau a unei prelucrări, prin aplicarea de măsuri tehnice și organizatorice adecvate și având în vedere următoarele elemente: 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.

De asemenea, Societatea aplică 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.

11. ASIGURAREA RESPECTĂRII DREPTURILOR PERSOANELOR VIZATE

11.1. Cererile persoanelor vizate. Dispoziții generale

GDPR prevede anumite drepturi pe care persoanele vizate le au în legătură cu prelucrarea datelor cu caracter personal care se referă la acestea. Este esențial ca toate persoanele din cadrul Societății să fie conștiente de aceste drepturi și de regulile generale privind respectarea acestora, astfel încât toți angajații și colaboratorii / contractorii au obligația de a parcurge informațiile din această secțiune.

În sensul prezentei secțiuni, sunt considerate cereri ale Persoanelor Vizate solicitările scrise sau verbale, realizate direct sau prin reprezentant, ale persoanelor fizice, cu privire la: dreptul de acces, dreptul la rectificare; dreptul la ștergerea datelor („dreptul de a fi uitat”); dreptul la restricționarea prelucrării; dreptul la portabilitatea datelor; dreptul la opoziție; dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri.

Cererile din partea Persoanelor Vizate pot fi depuse fie fizic, fie electronic. Depunerea fizică a cererilor poate avea loc la sediul Societății, sau prin poștă, către adresa sediului social al Societății.

Depunerea cererilor în format fizic se va face la adresa sediului social al Societății.

Depunerea electronică a cererilor va avea loc prin poștă electronică, la adresa de e-mail instituită în acest sens la nivelul Societății.

În cazul în care orice persoană din cadrul Societății primește o cerere din partea Persoanei Vizate și consideră că este de domeniul prezentei secțiuni, o va înainta de îndată recepției (în cazul în care cererea a fost primită în formă fizică) sau o va transmite la adresa de e-mail indicată mai sus și va informa Persoana Vizată în acest sens.

Cu excepția Persoanei Responsabile, niciun alt angajat sau colaborator / contractant din cadrul Societății nu are dreptul să răspundă unei cereri din partea Persoanei Vizate și se va limita la a informa Persoana Vizată că cererea sa a fost înaintată către departamentul competent care o va soluționa în cel mai scurt timp posibil.

11.2. Obligația de informare a Persoanei Vizate

Societatea, în calitate de operator de date cu caracter personal, are obligația de a informa corect și complet Persoanele Vizate cu privire la prelucrările datelor personale ale acestora realizate de Societate.

11.3. Drepturile Persoanelor Vizate

Drepturile prevăzute în cele ce urmează vor fi aduse la cunoștința Persoanelor Vizate, în mod expres, clar și separat de alte informații, cel mai târziu la momentul primei comunicări a Societății cu Persoana Vizată.

Dreptul de acces

Persoana Vizată are dreptul de a obține de la Societate confirmarea că se prelucrează sau nu datele sale cu caracter personal. Dacă Societatea îi prelucrează datele cu caracter personal, persoana vizată are dreptul de acces la datele respective și la informațiile următoare:

- scopurile prelucrării;
- categoriile de date cu caracter personal vizate;
- destinatarii/ categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele, în special destinatari din State Terțe ori organizații internaționale;
- perioada pentru este preconizată stocarea datelor sau, dacă nu este posibil, criteriile utilizate pentru stabilirea perioadei de stocare;
- faptul că persoana vizată are dreptul de a solicita Societate rectificarea, ștergerea datelor sau restricționarea prelucrării datelor și dreptul de a se opune prelucrării;
- dreptul persoanei vizate de a depune o plângere la autoritatea de supraveghere a prelucrării datelor cu caracter personal;
- dacă datele nu sunt colectate de la persoana vizată, orice informații referitoare la sursă;
- existența unui proces decizional automatizat (inclusiv crearea de profiluri) și informații privind logica utilizată și importanța și consecințele preconizate ale prelucrării pentru persoana vizată.

Persoana vizată trebuie să își poată exercita acest drept cu ușurință și la intervale de timp rezonabile.

Dacă cererea persoanei vizate este în format electronic și nu solicită să i se răspundă într-un alt format, răspunsul Societății va fi transmis într-un format electronic utilizat în mod curent

Dreptul la rectificare

Dacă datele sale cu caracter personal sunt inexacte ori incomplete, Persoana Vizată are dreptul ca acestea să fie rectificate de Societate (în calitate de operator), fără întârzieri nejustificate.

În funcție de scopul prelucrării datelor cu caracter personal, Persoana Vizată are dreptul ca datele sale prelucrate de Societate să fie completate (dacă este cazul), inclusiv în urma oferirii declarații suplimentare de către Persoana Vizată.

Dreptul la ștergerea datelor ("dreptul de a fi uitat")

Persoana Vizată are posibilitatea de a solicita ca datele sale cu caracter personal să fie șterse fără întârzieri nejustificate dacă nu mai este necesar ca acestea să fie prelucrate de către Societate (ca operator de date cu caracter personal).

Persoana Vizată are dreptul la ștergerea datelor care o privesc în următoarele situații:

- datele sale cu caracter personal nu mai sunt necesare pentru realizarea scopurilor pentru care Societatea le-a colectat (prelucrat);
- Persoana Vizată și-a retras consimțământul în temeiul căruia a avut loc prelucrarea și nu există un alt temei pe care Societatea se poate baza pentru a îi prelucra datele;
- Persoana Vizată se opune prelucrării (în temeiul dreptului său la opoziție) și nu există motive legitime care să dea Societății dreptul de a prelucra datele în continuare;
- Societatea a prelucrat datele în mod ilegal;
- există o obligație legală a Societății pentru care este necesară ștergerea datelor;
- colectarea datelor a avut loc în legătură cu oferirea de servicii ale societății informaționale unui minor.

Persoana Vizată are dreptul la ștergerea datelor pe care Societatea le prelucrează chiar dacă prelucrarea nu i-a cauzat niciun prejudiciu sau inconvenient.

Societatea poate refuza să dea curs unei solicitări de ștergere a datelor cu caracter personal dacă prelucrarea este necesară:

- pentru exercitarea dreptului la liberă exprimare și informare;
- pentru a respecta o obligație legală de prelucrare, pentru a îndeplini o sarcină executată în interes public sau în cadrul exercitării unei autorități oficiale cu care Societatea este investită;
- pentru motive de interes public în domeniul sănătății publice;
- în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu GDPR, în măsura în care dreptul la ștergerea datelor este

susceptibil să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective;

- pentru constatarea, exercitarea sau apărarea unui drept în instanță.

În cazul în care Societatea a făcut publice datele cu caracter personal ale persoanei vizate în cauză și trebuie să dea curs solicitării de ștergere din partea persoanei vizate, va lua măsurile rezonabile disponibile pentru a informa operatorii care prelucrează acele date că persoana vizată a solicitat ștergerea de către aceștia din urmă a link-urilor către sau, după caz, a reproducerilor acelor date.

Dreptul la restricționarea prelucrării

Societatea va da curs unei solicitări de restricționare a prelucrării datelor cu caracter personal dacă cel puțin una dintre următoarele condiții este îndeplinită:

- Persoana Vizată contestă exactitatea datelor pe care Societatea le prelucrează – în acest caz, Societatea va opri prelucrarea până când va verifica exactitatea acelor date;
- prelucrarea este ilegală – caz în care Persoana Vizată, deși are dreptul ca datele sale să fie șterse (vedeți secțiunea referitoare la *Dreptul la ștergerea datelor („dreptul de a fi uitat”)*), se opune ștergerii și, în schimb, solicită Societății restricționarea utilizării lor;
- Societatea nu mai are nevoie de datele cu caracter personal, dar Persoana Vizată solicită datele în cauză în scopul constatării, al exercitării sau al apărării unui drept în instanță;
- Persoana Vizată s-a opus prelucrării necesare pentru îndeplinirea unei sarcini de interes public sau care rezultă din exercitarea autorității publice cu care Societatea (ca operator) este învestită sau Persoana Vizată s-a opus prelucrării necesare în scopul intereselor legitime ale Societății (ca operator) ori ale unui terț – în toate aceste cazuri, Societatea va opri prelucrarea datelor persoanei vizate pe parcursul perioadei în care verifică dacă motivele legitime care întemeiază prelucrarea datelor de către Societate prevalează asupra drepturilor persoanei vizate.

În astfel de situații, în calitate de operator, Societatea are dreptul de a stoca datele respective, dar nu le va mai prelucra mai departe. La rândul său, stocarea datelor trebuie să aibă loc numai în măsura necesară pentru ca Societatea să se asigure că restricționarea prelucrării acelor date va fi respectată și în viitor, *ie*, dacă Persoana Vizată își exercită dreptul la restricționarea prelucrării, activitățile Societății de prelucrare a acelor date vor fi blocate.

Cu toate acestea, Societatea va putea continua să prelucreze (și altfel decât prin stocare) datele a căror prelucrare a fost restricționată de Persoana Vizată dacă și în măsura în care:

- persoana vizată este de acord cu prelucrarea;
- prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță;
- prelucrarea este necesară pentru protecția drepturilor unei alte persoane fizice sau juridice;
- prelucrarea este necesară din motive de interes public important al Uniunii Europene sau al unui Stat Membru al Uniunii Europene.

Înainte de a ridica restricționarea prelucrării, Persoana Vizată va fi informată.

Cu titlu exemplificativ, în funcție de modul concret în care prelucrează datele în cauză, pentru a da curs cererii de restricționare a prelucrării, Societatea poate muta temporar într-un alt sistem de prelucrare datele a căror prelucrare este restricționată, poate bloca accesul utilizatorilor la acele date sau adopta orice măsuri cu efect similar.

De asemenea, se va indica într-un mod clar în sistem și în evidența operațiunilor de prelucrare ținută de Societate (de exemplu, în rubrica *Alte comentarii*) că prelucrarea datelor respective a fost restricționată, pentru a se asigura că datele în cauză nu vor face obiectul prelucrării (inclusiv prin modificarea lor) ulterior restricționării. În acest sens, vor fi informate persoanele responsabile cu prelucrarea datelor în cauză și persoana responsabilă.

Dreptul la portabilitatea datelor

Persoanele Vizate pot obține de la Societate datele cu caracter personal pe care Societatea le prelucrează, spre a le utiliza în scopurile în care doresc și a putea să le transfere dintr-un mediu în altul, într-un mod sigur și facil.

Persoana Vizată are dreptul la portabilitate numai în privința datelor pe care Societatea le prelucrează în temeiul consimțământului său, pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri înainte de încheierea unui contract, la cererea persoanei vizate.

Dreptul la opoziție

Persoanele Vizate au dreptul de a se opune prelucrării datelor lor cu caracter personal care este necesară pentru îndeplinirea unei sarcini care servește unui interes public, rezultă din exercitarea autorității publice cu care este învestită Societatea sau este necesară pentru interesele legitime ale Societății sau ale unui terț.

De asemenea, Persoanele Vizate au dreptul de a se opune prelucrării în scop de marketing direct.

De asemenea, Persoanele Vizate au dreptul de a se opune prelucrării în scopuri de cercetare științifică ori istorică sau în scopuri statistice, mai puțin în cazul în care prelucrarea respectivă este necesară pentru îndeplinirea unei sarcini realizate din motive de interes public.

Dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată (inclusiv cu privire la crearea de profiluri)

În cazul prelucrărilor automate de date cu caracter personal pe care Societatea le realizează, Persoanele Vizate au dreptul de a nu fi supuse unor decizii întemeiate pe astfel de prelucrări, care produc efecte juridice cu privire la persoanele vizate sau le afectează altfel în mod semnificativ.

Persoanele Vizate nu vor beneficia însă de dreptul de mai sus atunci când decizia (i) este necesară pentru încheierea sau executarea unui contract între acestea și Societate, (ii) este prevăzută de lege, în condițiile RGPD sau (iii) este întemeiată pe consimțământul explicit al persoanelor vizate.

În cazul în care decizia este necesară pentru încheierea ori executarea unui contract între persoana vizată și Societate sau este întemeiată pe consimțământul explicit al persoanei vizate, persoana vizată

are următoarele drepturi: (i) dreptul de a obține intervenție umană în luarea deciziei, (ii) dreptul de a își exprima punctul de vedere și (iii) dreptul de a contesta decizia.

Deciziile întemeiate pe prelucrări automate, atunci când sunt permise, nu vor avea la bază categoriile speciale de date cu caracter personal, cu excepția cazului în care persoana vizată a consimțit expres sau prelucrarea acelor date este necesară pentru motive de interes public major, în temeiul legii.

12. GESTIONAREA RISCURILOR. EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR CU CARACTER PERSONAL

12.1. Aspecte generale

În cazul în care Societatea identifică prelucrări de date cu caracter personal susceptibile de a prezenta riscuri ridicate pentru drepturile și libertățile persoanelor fizice, Societatea va efectua o evaluare a impactului acelor prelucrări asupra protecției datelor, în condițiile art. 35 din GDPR.

Evaluarea impactului asupra protecției datelor se realizează anterior colectării datelor cu caracter personal și efectuării prelucrării. Societatea pune accent pe estimarea riscurilor asupra protecției datelor din punctul de vedere al Persoanelor vizate, luând în considerare cel puțin următoarele elemente: (i) natura datelor, (ii) domeniul de aplicare, (iii) contextul și scopurile prelucrării și (iv) utilizarea noilor tehnologii.

12.2. Ce presupune o evaluare a impactului asupra protecției datelor?

În situația în care Societatea va efectua evaluarea impactului asupra protecției datelor, se va asigura că această evaluare acoperă următoarele aspecte:

- 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 GDPR.

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 GDPR sunt respectate.

12.3. Când trebuie efectuată o evaluare a impactului asupra protecției datelor?

Evaluarea impactului asupra protecției datelor este obligatorie, în special în următoarele cazuri:

(a) 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;

(b) prelucrării pe scară largă a unor categorii speciale de date, menționată la articolul 9 alineatul (1), sau a unor date cu caracter personal privind condamnări penale și infracțiuni, menționată la articolul 10 din GDPR;

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

(d) prelucrării pe scară largă a datelor cu caracter personal ale persoanelor vulnerabile prin mijloace automate de monitorizare și/sau înregistrare sistematică a comportamentului acestora;

(e) prelucrării pe scară largă a datelor cu caracter personal prin utilizarea inovatoare sau implementarea unor tehnologii noi, în special în cazul în care operațiunile respective limitează capacitatea persoanelor vizate de a-și exercita drepturile;

(f) prelucrării pe scară largă a datelor generate de dispozitive cu senzori care transmit date prin internet sau prin alte mijloace;

(g) prelucrării pe scară largă și/sau sistematică a datelor de trafic și/sau de localizare a persoanelor fizice atunci când prelucrarea nu este necesară pentru prestarea unui serviciu solicitat de persoana vizată.

Când evaluarea de impact indică riscuri ridicate, în absența unor măsuri luate de Societate pentru atenuarea acestora, Societatea va consulta Autoritatea locală de supraveghere (ANSPDCP) conform cerințelor GDPR.

13. RĂSPUNSUL LA INCIDENTE DE ÎNCĂLCARE A SECURITĂȚII DATELOR CU CARACTER PERSONAL

Atunci când Societatea află despre o încălcare a securității datelor cu caracter personal, în cadrul Societății se va desfășura o investigație și se vor lua măsurile adecvate de remediere, în timp util, conform Procedurii aplicabile la nivelul Societății în caz de încălcare a securității datelor cu caracter personal.

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

Fluxul de acțiune și comunicare ce trebuie urmat atunci când un angajat/colaborator/contractor al Societății ia la cunoștință despre producerea unei încălcări a securității datelor cu caracter personal este reglementat în cadrul *Procedurii în caz de încălcare a securității datelor cu caracter personal*, disponibilă la Cap. 5 din Procedurile aplicabile la nivelul FORT S.A. în materia asigurării protecției datelor cu caracter personal.

14. ORGANIZARE ȘI RESPONSABILITĂȚI

Responsabilitatea pentru asigurarea prelucrării corespunzătoare a datelor cu caracter personal revine fiecărei persoane care lucrează pentru Societate sau cu aceasta și are acces la datele cu caracter personal prelucrate de Societate.

Domeniile principale de responsabilitate pentru prelucrarea datele cu caracter personal sunt redată în cadrul Secțiunii 5 din această Politică.

15. AUDIT ȘI RESPONSABILITATE

Persoanele desemnate la nivel intern în scopul efectuării de audituri și/sau societatea terță angajată de Societate pentru efectuarea procesului / proceselor de audit impus / impuse de lege și de rigorile aplicabile la nivelul Societății răspunde de auditarea modului în care departamentele implementează această Politică.

Orice angajat și/sau contractor / colaborator și / sau orice alt destinatar desemnat al acestei Politici care încalcă această Politică va face obiectul unei acțiuni disciplinare și sau al unei acțiuni în răspundere contractuală și angajatul / contractorul / colaboatorul poate răspunde de asemenea din punct de vedere civil sau penal, în cazul în care conduita acestuia încalcă legi sau regulamente.

16. CONFLICTELE LEGILOR

Scopul acestei Politici este să se conformeze cu legile și reglementările existente și aplicabile în jurisdicția în care Societatea desfășoară activitate, respectiv în România. În cazul oricărui conflict între această Politică și legile și reglementările aplicabile, vor prevala acestea din urmă.

17. AUTORIZARE ȘI DISEMINARE

Aprobarea și autorizarea acestei Politici au fost realizate conform mențiunilor redată în cadrul Secțiunii 1 din această Politică. Revizuirea Politicii se realizează anual sau ori de câte ori este nevoie având în vedere dinamica operațiunilor de prelucrare de date cu caracter personal realizate de către Societate sau la schimbarea cadrului de reglementare.

Această Politică generală privind protecția datelor cu caracter personal a fost adoptată la nivelul FORT S.A.:

De către: Delia Alina Necula

În calitate de: Director General

Actualizată în data de: 01.06.2026

Aplicabilă în această versiune din data de: 01.06.2026