Politica de protecție a datelor cu caracter personal

Rețele Electrice România S.A.
B-dul. Mircea Vodă 30, et. 3, Sector 3, București
Nr. de ordine în Registrul Comerțului J2002001859405, Cod Unic de înregistrare 14507322,
Capital social subscris și vărsat 580.355.660 lei
www.reteleelectrice.ro

Cuprins

Rețele Electrice România S.A.
B-dul. Mircea Vodă 30, et. 3, Sector 3, București
Nr. de ordine în Registrul Comerțului J2002001859405, Cod Unic de înregistrare 14507322,
Capital social subscris și vărsat 580.355.660 lei
www.reteleelectrice.ro

Rețele Electrice România S.A.
B-dul. Mircea Vodă 30, et. 3, Sector 3, București
Nr. de ordine în Registrul Comerțului J2002001859405, Cod Unic de înregistrare 14507322,
Capital social subscris și vărsat 580.355.660 lei
www.reteleelectrice.ro

PARTEA 1 – DOMENIUL DE APLICARE, SCOPUL, ADOPTAREA ȘI REVIZUIREA POLITICII

1. Domeniul de aplicare și scopul politicii

1.1. Politica de protecție a datelor cu caracter personal (denumită în continuare "Politica") stabilește principiile și regulile fundamentale care reglementează prelucrarea și protecția datelor cu caracter personal prelucrate de **RETELE ELECTRICE ROMANIA S.A.** (denumită în continuare "**Societatea**"), precum și principalele roluri și responsabilități pentru gestionarea problemelor de protecție a datelor cu caracter personal și pentru supravegherea adecvării nivelului de protecție a datelor cu caracter personal în cadrul Societății.

1.2. Politica se aplică tuturor activităților de prelucrare a datelor cu caracter personal care se încadrează în sfera activităților comerciale ale Societății.

1.3. Scopul Politicii este de a proteja datele cu caracter personal în conformitate cu cadrul legislativ și de reglementare aplicabil, de a spori încrederea părților interesate (angajați, acționari, clienți, potențiali clienți, reprezentanți legali, parteneri și alte terțe părți) și de a proteja reputația și poziția competitivă a Societății și a Grupului pe piață.

1.4. Politica se aplică membrilor Consiliului de Administrație, persoanelor care fac parte din organele administrative, de conducere sau de supraveghere ale Societății, precum și managerilor, angajaților și colaboratorilor legați de Societate prin relații contractuale de orice tip, inclusiv ocazionale și/sau exclusiv temporare.

1.5. În cazul unui conflict între obligațiile reglementate prin prezenta Politică și prevederile legislației aplicabile privind protecția datelor cu caracter personal, prevederile legislației vor prevala.

2. Adoptarea și revizuirea Politicii

2.1. Politica va intra în vigoare la aprobarea acesteia de către Consiliul de Administrație al Societății.

2.2. Politica este supusă unor revizuiri periodice (cel puțin o dată la doi ani) și este revizuită, atunci când este necesar pentru a asigura alinierea la cadrul legal și de reglementare aplicabil și la nevoile operaționale ale Societății. În plus, Politica este supusă revizuirii atunci când apar modificări semnificative în activitățile comerciale, cum ar fi modificări în practicile de afaceri ale Societății, care necesită sau implică modificări substanțiale în prelucrarea datelor cu caracter personal. Revizuirea Politicii trebuie documentată, inclusiv cazurile în care nu sunt necesare modificări.

2.3. Politicile, standardele și/sau procedurile specifice dezvoltate pentru implementarea acestei Politici sunt aprobate de Directorul General al Societății.

2.4. Politica este disponibilă pentru întregul personal al Societății prin instrumente de comunicare internă și este, de asemenea, publicată pe site-ul Societății.

PARTEA 2 – CADRUL DE GUVERNANȚĂ PENTRU PROTECȚIA DATELOR CU CARACTER PERSONAL

3. Responsabilitatea Societății

3.1. Societatea, în calitatea sa de operator de date cu caracter personal și/sau persoană împuternicită de operator, poartă întreaga responsabilitate pentru respectarea cadrului legislativ și de reglementare aplicabil pentru protecția datelor cu caracter personal, precum și a prezentei Politici și trebuie să poată demonstra conformitatea acesteia în orice moment.

4. Obligația de desemnare a responsabilului cu protecția datelor

4.1. Societatea desemnează un responsabil cu protecția datelor atunci când operațiunile sale implică prelucrarea datelor cu caracter personal care, datorită naturii, domeniului de aplicare și/sau scopurilor lor, pot prezenta un risc ridicat pentru drepturile și libertățile persoanelor vizate. Astfel de operațiuni includ, dar nu se limitează la, monitorizarea regulată și sistematică a persoanelor vizate pe scară largă

și prelucrarea categoriilor speciale de date cu caracter personal la scară largă sau a datelor referitoare la condamnări penale și infracțiuni.

Pentru a evalua dacă prelucrarea are loc pe scară largă, se iau în considerare următoarele aspecte:

4.1.1. numărul persoanelor vizate implicate, fie ca număr specific, fie ca procent din populație;

4.1.2. volumul și gama de date;

4.1.3. durata sau caracterul permanent al prelucrării;

4.1.4. extinderea geografică a prelucrării.

4.2. Societatea este obligată să pună la dispoziția responsabilului cu protecția datelor resursele financiare și umane necesare pentru îndeplinirea sarcinilor sale.

5. Sarcinile responsabilului cu protecția datelor

5.1. Responsabilul cu protecția datelor desemnat de Societate va fi implicat de Societate în toate aspectele legate de protecția datelor cu caracter personal în timp util, fără a primi instrucțiuni de la Societate atunci când își îndeplinește atribuțiile. Sarcinile principale ale responsabilului cu protecția datelor desemnat de Societate includ:

5.1.1. Informarea și consilierea Societății cu privire la obligațiile sale în conformitate cu GDPR și cadrul legislativ relevant privind protecția datelor cu caracter personal.

5.1.2. Monitorizarea respectării de către Societate a cadrului legislativ privind protecția datelor cu caracter personal și a politicilor interne de protecție a datelor și efectuarea auditurilor relevante.

5.1.3. Sprijinirea șefilor de unități organizatorice în elaborarea și actualizarea procedurilor legate de protecția datelor cu caracter personal din sfera lor de competență.

5.1.4. Asistarea în investigarea cazurilor în care persoanele vizate depun o plângere la Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal.

5.1.5. Să fie informat și să asiste în investigarea incidentelor de încălcare a securității datelor cu caracter personal și notificarea autorităților competente și/sau persoanelor vizate.

5.1.6. Desfășurarea de activități de conștientizare și formare a personalului implicat în operațiunile de prelucrare.

5.1.7. Oferirea de consultanță și sprijin cu privire la evaluările impactului asupra protecției datelor cu caracter personal/evaluările interesului legitim și monitorizarea implementării măsurilor de reducere a riscurilor stabilite în conformitate cu prezenta Politică.

5.1.8. Colaborarea cu autoritatea de supraveghere și acționarea ca punct de contact în aspecte legate de prelucrarea datelor cu caracter personal, inclusiv furnizarea de consultanță, după caz, cu privire la orice aspecte pertinente.

5.1.9. Asistarea Societății în implementarea strategiei de protecție a datelor cu caracter personal a Grupului PPC.

5.1.10. Asistarea Societății în integrarea și adaptarea politicilor și standardelor de protecție a datelor ale Grupului PPC în procesele și operațiunile Societății, consilierea cu privire la alinierea la cadrul mai larg de conformitate al Grupului PPC.

5.1.11. Colaborarea cu responsabilul de securitate cibernetică al Societății cu privire la aspecte legate de securitatea operațiunilor de prelucrare (de exemplu,

proiectarea măsurilor tehnice și organizatorice, gestionarea incidentelor de încălcare a securității datelor cu caracter personal).

5.1.12. Oferirea de sprijin și îndrumare continuă în materie de protecție a datelor, inclusiv analiza activităților de prelucrare a datelor și consultanță cu privire la cerințele de conformitate, la cererea șefilor unităților organizaționale.

6. Responsabilul cu protecția datelor al grupului PPC (DPO-ul grupului)

6.1. Responsabilul cu protecția datelor al grupului PPC acționează ca responsabil cu protecția datelor pentru societățile din grupul PPC care sunt obligate să numească un DPO și nu au numit unul în mod independent, cu excepția cazului în care furnizarea acestor servicii intră în conflict cu cerințele legislației aplicabile sau cadrului de reglementare sau dacă există alte motive operaționale.

6.2. Responsabilul cu protecția datelor al grupului dezvoltă politici și standarde de protecție a datelor la nivel de grup, urmărind conformitatea uniformă și consecventă a tuturor societăților din grup cu cadrul de reglementare și legal aplicabil, precum și utilizarea eficientă a instrumentelor de conformitate pentru monitorizarea, documentarea și automatizarea proceselor relevante.

6.3. Responsabilul cu protecția datelor al grupului stabilește mecanismele de supraveghere a nivelului de protecție a datelor cu caracter personal în cadrul societăților din grupul PPC. Mecanismele de supraveghere pot include stabilirea indicatorilor cheie de performanță (KPI), precum și a procedurilor de autoevaluare pentru fiecare societate din grup.

6.4. Cu condiția ca acest lucru să nu fie interzis de legislația aplicabilă, Responsabilul cu protecția datelor al grupului poate efectua audituri programate și/sau ad-hoc în societățile din grup. Aceste audituri pot fi efectuate de personalul Societății și/sau de parteneri externi.

6.5. Societatea trebuie să furnizeze Responsabilului cu protecția datelor al grupului toate informațiile necesare pentru supravegherea adecvării nivelului de protecție a datelor cu caracter personal în cadrul grupului PPC și trebuie să ia măsurile adecvate pentru a remedia orice deficiențe identificate. Responsabilul cu protecția datelor al grupului monitorizează punerea în aplicare a acestor măsuri.

6.6. Responsabilul cu protecția datelor al grupului informează anual Comitetul de audit al grupului cu privire la programul de conformitate al societăților din grup cu legislația privind protecția datelor cu caracter personal.

7. Responsabilitățile Șefilor Unităților Organizaționale

7.1. Șefii unităților organizaționale care sunt responsabili pentru activitățile de prelucrare a datelor poartă responsabilitatea operațională pentru respectarea legislației privind protecția datelor și monitorizarea respectării prezentei Politici. În mod orientativ, aceștia sunt responsabili pentru:

7.1.1. Informarea responsabilului cu protecția datelor într-un stadiu incipient cu privire la activitățile noi sau modificate de prelucrare a datelor cu caracter personal, indiferent dacă decurg din planificarea strategică și/sau din cerințele operaționale urgente, pentru a se asigura că orice probleme de protecție a datelor cu caracter personal sunt examinate și evaluate.

7.1.2. Asigurarea faptului că personalul aflat sub supravegherea lor este instruit și informat în mod corespunzător în materie de protecție a datelor.

7.1.3. Asigurarea încheierii acordurilor de prelucrare a datelor cu caracter personal conform paragrafului 27 al prezentei Politici și supravegherea persoanelor împuternicite cu privire la respectarea obligațiilor de protecție a datelor stabilite în acordurile de prelucrare a datelor menționate (de exemplu, respectarea instrucțiunilor și implementarea măsurilor tehnice și organizatorice pentru securitatea prelucrării).

7.1.4. Păstrarea unei evidențe actualizate a activităților de prelucrare pentru care sunt responsabili, în conformitate cu punctele 18.2 și 18.3.

7.1.5. Asigurarea respectării principiilor de prelucrare a datelor cu caracter personal, așa cum sunt definite de legislație și de prezenta Politică, precum și a recomandărilor emise de responsabilul cu protecția datelor.

7.1.6. Asigurarea faptului că o evaluare a impactului asupra protecției datelor cu caracter personal este efectuată atunci când este necesar, înainte de începerea prelucrării și în colaborare cu responsabilul cu protecția datelor, în conformitate cu punctul 29.

7.1.7. Implementarea unor măsuri organizatorice și/sau tehnice adecvate pentru protecția datelor cu caracter personal și asigurarea respectării obligațiilor care decurg din cadrul de securitate cibernetică al Societății.

Astfel de măsuri includ, cu titlu orientativ, controlul accesului, pseudonimizarea sau criptarea, asigurarea disponibilității și integrității sistemelor, precum și capacitatea de a detecta și de a răspunde prompt la incidentele de încălcare a securității datelor.

7.1.8. Răspunsul la solicitările de furnizare de informații în contextul investigațiilor sau al altor acțiuni desfășurate de autoritățile de supraveghere competente.

8. Obligațiile angajatului

8.1. Toți angajații și furnizorii de servicii ai Societății, indiferent de statutul lor profesional, sunt obligați să adere la cadrul legal care reglementează protecția datelor cu caracter personal și la regulile relevante, așa cum sunt descrise în această Politică. De asemenea, aceștia trebuie să contribuie activ la menținerea nivelului necesar de protecție și securitate a datelor cu caracter personal.

8.2. Angajații vor primi și trebuie să participe la cursuri de formare cu privire la principiile fundamentale ale protecției datelor cu caracter personal cel puțin o dată la doi ani. Participarea la acest training este obligatorie.

8.3. Orice încălcare a acestei Politici poate avea consecințe, așa cum este stipulat în legislația aplicabilă și în cadrul de reglementare al Societății.

PARTEA 3 - PRINCIPIILE DE BAZĂ ALE PRELUCRĂRII DATELOR CU CARACTER PERSONAL

9. Limitarea scopului

9.1. Datele cu caracter personal sunt colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri ("limitarea scopului").

9.2. Înainte de orice prelucrare ulterioară în alt scop, se iau în considerare următoarele criterii:

9.2.1. Orice corelație între scopurile pentru care au fost colectate datele cu caracter personal și scopurile prelucrării ulterioare preconizate,

9.2.2. Contextul în care au fost colectate datele cu caracter personal, în special în ceea ce privește relația dintre persoanele vizate și Societate în rolul său de operator de date,

9.2.3. Natura datelor cu caracter personal, în special în ceea ce privește categoriile speciale de date cu caracter personal,

92.4. Consecințele potențiale ale prelucrării ulterioare preconizate pentru persoanele vizate,

9.2.5. Prezența unor garanții adecvate, care pot include criptarea sau pseudonimizarea.

10. Minimizarea datelor

10.1. Societatea va prelucra datele cu caracter personal numai atunci când acestea sunt adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile pentru care sunt prelucrate ("principiul minimizării datelor").

10.2. La proiectarea de noi sisteme, servicii sau procese care implică prelucrarea datelor cu caracter personal, se aplică principiul minimizării datelor încă din faza de proiectare. Sunt colectate doar datele cu caracter personal strict necesare scopului definit.

11. Exactitatea datelor

11.1. Societatea va lua măsuri pentru a se asigura că datele cu caracter personal sunt exacte și, dacă este necesar, actualizate ("exactitate").

11.2. În cazul în care datele cu caracter personal sunt inexacte în ceea ce privește scopurile prelucrării, Societatea ia măsuri pentru ștergerea sau corectarea lor imediată.

12. Limitarea stocării

12.1. Societatea va lua măsuri pentru a se asigura că datele cu caracter personal sunt păstrate într-o formă care să permită identificarea persoanelor vizate numai pentru timpul necesar îndeplinirii scopului prelucrării datelor cu caracter personal ("limitarea stocării").

12.2. Atunci când scopul prelucrării datelor cu caracter personal a fost atins, datele cu caracter personal trebuie șterse sau anonimizate, cu excepția cazului în care se specifică altfel în cadrul legal aplicabil.

12.3. Perioada de păstrare a datelor cu caracter personal va fi definită pe baza scopurilor pentru care sunt prelucrate datele și a oricărei cerințe legale sau de reglementare aplicabile sau a unei nevoi comerciale documentate. Perioada de păstrare trebuie justificată în consecință.

12.4. Perioadele de păstrare prevăzute sunt documentate în evidența activităților de prelucrare ale Societății, în conformitate cu articolul 30 din GDPR, atunci când sunt disponibile sau furnizate de către unitatea organizațională.

13. Echitatea prelucrării

13.1. Prelucrarea datelor cu caracter personal se va desfășura în conformitate cu principiul echității, asigurându-se că fiecare activitate de prelucrare este echitabilă, imparțială și justă față de persoanele vizate.

13.2. Societatea se angajează să mențină practici care promovează tratamentul transparent și echitabil al tuturor persoanelor vizate, fără discriminare sau prejudecăți, indiferent de sex, vârstă, naționalitate, religie, convingeri politice sau alte caracteristici.

13.3. Echitatea este asigurată atât în conceperea procedurilor de prelucrare, cât și în punerea lor în aplicare, evitându-se practicile care conduc la rezultate inechitabile sau disproporționate în detrimentul persoanelor vizate.

14. Legalitatea prelucrării datelor cu caracter personal

14.1. Prelucrarea datelor cu caracter personal este legală numai dacă și în măsura în care este îndeplinită cel puțin una dintre următoarele condiții:

14.1.1. Persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal în unul sau mai multe scopuri specifice [GDPR, art. 6.1 (a)].

14.1.2. Prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a lua măsuri la cererea persoanei vizate înainte de încheierea unui contract (GDPR, art. 6.1 (b)).

14.1.3. Prelucrarea este necesară pentru respectarea unei obligații legale la care este supus operatorul (GDPR, art. 6.1 (c)).

14.1.4. Prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale unei alte persoane fizice [GDPR, art. 6.1 (d)).

14.1.5. Prelucrarea este necesară pentru îndeplinirea unei sarcini de interes public sau în exercitarea autorității publice cu care este învestit operatorul de date (GDPR, art. 6.1 (e)).

14.1.6. Prelucrarea este necesară în scopul intereselor legitime urmărite de Societate în calitate de operator de date sau de o terță parte, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate care necesită protecția datelor cu caracter personal, în special dacă persoana vizată este un copil (GDPR, art. 6.1 litera (f)).

14.2. Prelucrarea categoriilor speciale de date cu caracter personal este interzisă, cu excepția cazului în care:

14.2.1. Persoana vizată și-a dat consimțământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice (GDPR, art. 9.2 (a)).

14.2.2. Prelucrarea este necesară pentru îndeplinirea obligațiilor și exercitarea drepturilor specifice ale Societății, în calitate de operator de date, sau ale persoanei vizate în domeniul legislației muncii și securității sociale și al protecției sociale, în măsura în care este autorizată de legislația națională sau de un contract colectiv de muncă în temeiul legislației naționale care prevede garanții adecvate pentru drepturile și interesele fundamentale ale persoanei vizate (GDPR, art. 9.2 litera (b)).

14.2.3. Prelucrarea este necesară pentru a proteja interesele 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 [GDPR, art. 9.2 (c)].

14.2.4. Prelucrarea se referă la datele cu caracter personal care au fost făcute publice în mod manifest de către persoana vizată (GDPR, art. 9.2 (e)).

14.2.5. Prelucrarea este necesară pentru stabilirea, exercitarea sau apărarea unui drept în instanță (GDPR, art. 9.2 (f)).

14.2.6. Prelucrarea este necesară din motive de interes public major, în temeiul dreptului Uniunii sau al dreptului intern, cu condiția să fie proporțional cu obiectivul urmărit, să respecte esența dreptului la protecția datelor cu caracter personal și să includă măsuri adecvate și specifice pentru a proteja drepturile și interesele fundamentale ale persoanei vizate [GDPR, art. 9.2 litera (g)].

14.2.7. Prelucrarea este necesară în scopuri de medicină preventivă sau a muncii, evaluarea capacității de muncă a angajaților, diagnosticul medical, furnizarea de asistență sau tratament de sănătate sau socială sau gestionarea sistemelor și serviciilor de sănătate sau de asistență socială în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul unui contract cu un profesionist din domeniul sănătății (GDPR, art. 9.2 litera (h)).

14.2.8. Prelucrarea este necesară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică sau în scopuri statistice în conformitate cu dreptul Uniunii sau al dreptului intern, care trebuie să fie proporționale cu obiectivul urmărit, să respecte esența dreptului la protecția datelor cu caracter personal și să prevadă măsuri adecvate și specifice pentru a proteja drepturile și interesele fundamentale ale persoanei vizate (GDPR, art. 9.2 litera (i)).

15. Consimțământul persoanei vizate

15.1. Atunci când prelucrarea se bazează pe consimțământul persoanei vizate, Societatea trebuie să poată demonstra că persoana vizată și-a dat consimțământul pentru activitatea de prelucrare.

15.2. În cazul în care consimțământul persoanei vizate este dat în contextul unei declarații scrise care se referă și la alte aspecte, cererea de consimțământ trebuie

prezentată într-un mod care să se distingă clar de celelalte aspecte, într-o formă ușor de înțeles și ușor accesibilă, folosind un limbaj clar și simplu.

15.3. Consimțământul trebuie să fie dat printr-un act afirmativ clar care indică o manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a acordului persoanei vizate cu privire la prelucrarea datelor cu caracter personal care o privesc, de exemplu printr-o declarație scrisă, inclusiv prin mijloace electronice (de exemplu, bifarea unei căsuțe atunci când se vizitează un site web) sau printr-o declarație orală.

15.4. Atunci când prelucrarea are mai multe scopuri, trebuie să se acorde consimțământul pentru toate.

15.5. În cazul în care consimțământul persoanei vizate urmează să fie obținut prin mijloace electronice, cererea de consimțământ trebuie să fie clară, concisă și să nu perturbe în mod inutil utilizarea serviciului pentru care este furnizată.

15.6. Persoana vizată are dreptul de a-și retrage consimțământul în orice moment. Retragerea consimțământului nu afectează legalitatea prelucrării bazate pe consimțământ înainte de retragerea acestuia.

15.7. Înainte de a-și da consimțământul, persoana vizată este informată cel puțin despre scopul prelucrării datelor cu caracter personal și despre identitatea Societății.

15.8. Retragerea consimțământului este la fel de ușoară ca și acordarea acestuia.

15.9. Pentru a evalua dacă consimțământul este acordat în mod liber, se ține seama în cea mai mare măsură dacă, printre altele, executarea unui contract, inclusiv furnizarea unui serviciu, este condiționată de consimțământul pentru prelucrarea datelor cu caracter personal care nu este necesară pentru executarea contractului respectiv.

15.10. Pentru a se asigura că a fost dat în mod liber, consimțământul nu ar trebui să constituie un temei juridic valabil în cazul în care există un dezechilibru clar între persoana vizată și operatorul de date.

15.11. Dovada consimțământului trebuie să fie ușor accesibilă și disponibilă pentru a răspunde exercitării drepturilor persoanelor vizate și pentru a dovedi conformitatea.

16. Informarea privind prelucrarea datelor cu caracter personal

16.1. Societatea, în calitate de operator de date, trebuie să furnizeze persoanei vizate următoarele informații:

16.1.1. Identitatea și datele de contact ale Societății.

16.1.2. Datele de contact ale responsabilului cu protecția datelor sau ale DPO-ului grupului, dacă este cazul.

16.1.3. Scopurile prelucrării pentru care sunt destinate datele cu caracter personal, precum și temeiul juridic al prelucrării.

16.1.4. Sursa din care provin datele cu caracter personal și, dacă este cazul, dacă provin din surse accesibile publicului, în cazurile în care datele nu au fost obținute direct de la persoana vizată.

16.1.5. În cazul în care prelucrarea se bazează pe temeiul juridic al intereselor legitime, descrierea intereselor legitime urmărite de operator sau de o terță parte.

16.1.6. Destinatarii sau categoriile de destinatari ai datelor cu caracter personal, dacă există.

16.1.7. Dacă este cazul, informații despre transferurile de date cu caracter personal în afara Spațiului Economic European.

16.1.8. Perioada pentru care vor fi stocate datele cu caracter personal sau, atunci când acest lucru nu este posibil, criteriile utilizate pentru a determina acea perioadă.

16.1.9. Dreptul de a solicita Societății accesul, corectarea sau ștergerea datelor cu caracter personal ori restricționarea prelucrării referitoare la persoana vizată sau

de a se opune prelucrării, precum și dreptul la portabilitatea datelor cu caracter personal.

16.1.10. În cazurile în care prelucrarea se bazează pe consimțământ, dreptul de retragere a consimțământului în orice moment, fără a afecta legalitatea prelucrării bazate pe consimțământ înainte de retragerea acestuia.

16.1.11. Dreptul de a depune o plângere la autoritatea de supraveghere.

16.1.12. Dacă furnizarea datelor cu caracter personal este o cerință legală sau contractuală sau o cerință necesară pentru încheierea unui contract, precum și dacă persoana vizată este obligată să furnizeze datele cu caracter personal și posibilele consecințe ale nefurnizării acestor date.

16.1.13. Utilizarea procesului decizional automatizat, inclusiv crearea de profiluri, și informații semnificative despre logica implicată, precum și semnificația și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

16.2. În cazul în care Societatea intenționează să prelucreze în continuare datele cu caracter personal într-un alt scop decât cel pentru care au fost colectate, Societatea va furniza persoanei vizate, înainte de această prelucrare ulterioară, informații despre acel alt scop, împreună cu orice alte informații necesare, așa cum se menționează la punctul 16.1.

17. Procesul decizional individual automatizat, inclusiv crearea de profiluri

17.1. Persoana vizată are dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce efecte juridice pentru ea sau o afectează în mod similar în mod semnificativ.

17.2. În mod excepțional, luarea automată a deciziilor care produc efecte juridice sau afectează semnificativ persoana vizată este permisă atunci când decizia:

17.2.1. Este necesară pentru încheierea sau executarea unui contract între persoana vizată și Societate,

17.2.2. Este autorizată prin lege sau

17.2.3. Se bazează pe consimțământul explicit al persoanei vizate.

17.3. În cazurile de mai sus, Societatea va implementa măsuri adecvate pentru a proteja drepturile, libertățile și interesele legitime ale persoanei vizate, inclusiv dreptul de a obține intervenția umană din partea Societății, de a-și exprima punctul de vedere și de a contesta decizia.

17.4. Societatea va asigura o prelucrare corectă și transparentă, oferind informații semnificative despre logica implicată, precum și despre semnificația și consecințele preconizate ale prelucrării.

17.5. Luarea automată a deciziilor sau crearea de profiluri nu ar trebui să vizeze copiii și nici să se bazeze pe categorii speciale de date cu caracter personal, cu excepția cazului în care, în acest din urmă caz, Societatea are consimțământul explicit al persoanei vizate.

18. Evidența activităților de prelucrare

18.1. Societatea ține o evidență cuprinzătoare a tuturor activităților de prelucrare pe care le întreprinde în conformitate cu art. 30 GDPR.

18.2. Pentru activitățile în care Societatea acționează în calitate de operator de date, înregistrarea include:

18.2.1. Numele și datele de contact ale operatorului și, după caz, ale operatorului asociat, ale reprezentantului operatorului și ale responsabilului cu protecția datelor sau ale DPO-ului grupului, dacă este cazul.

18.2.2. Scopurile prelucrării datelor cu caracter personal.

18.2.3. O descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal.

18.2.4. Categoriile de destinatari, inclusiv destinatarii din țări terțe.

18.2.5. Dacă este cazul, transferurile de date cu caracter personal către o țară terță, inclusiv identificarea țării terțe respective și documentarea garanțiilor adecvate.

18.2.6. Acolo unde este posibil, termenele preconizate pentru ștergerea diferitelor categorii de date cu caracter personal.

18.2.7. Dacă este posibil, o descriere generală a măsurilor de securitate tehnice și organizaționale.

18.3. Pentru activitățile în care Societatea acționează în calitate de persoană împuternicită, înregistrarea include:

18.3.1. Numele și datele de contact ale Societății, precum și ale operatorului de date în numele cărora acționează, precum și responsabilul cu protecția datelor.

18.3.2. Categoriile de activități de prelucrare efectuate în numele fiecărui operator de date.

18.3.3. Dacă este cazul, transferuri de date cu caracter personal către o țară terță, inclusiv identificarea țării terțe respective și documentarea garanțiilor adecvate.

18.3.4. Dacă este posibil, o descriere generală a măsurilor de securitate tehnice și organizaționale.

18.4. Evidența activităților de prelucrare este actualizată atunci când apar modificări în activitățile de prelucrare, iar exactitatea și completitudinea acesteia sunt revizuite periodic de către șefii unităților organizaționale.

PARTEA 4 – DREPTURILE PERSOANELOR VIZATE

19. Dreptul de acces (articolul 15 din GDPR)

19.1. Persoanele vizate au dreptul de a accesa informațiile la care se face referire la punctul 16 al prezentei Politici.

19.2. Informațiile aferente ar trebui să fie puse la dispoziția persoanei vizate într-un format inteligibil și într-un interval de timp rezonabil. Acest lucru se realizează în general prin comunicare tipărită sau electronică.

19.3. În orice caz, persoana vizată ar trebui să fie informată în termen de o lună de la primirea cererii. Această perioadă poate fi prelungită cu încă două luni, dacă este necesar, având în vedere complexitatea și numărul de cereri. Persoana vizată ar trebui să fie informată cu privire la orice astfel de prelungire.

19.4. Societatea furnizează o copie a datelor cu caracter personal supuse prelucrării. Pentru orice copii suplimentare solicitate de persoana vizată, Societatea poate percepe o taxă rezonabilă pentru costurile administrative.

20. Dreptul la rectificare (articolul 16 GDPR)

20.1. Persoana vizată are dreptul de a solicita rectificarea datelor cu caracter personal inexacte sau completarea datelor cu caracter personal incomplete care o privesc.

21. Dreptul la ștergere (articolul 17 din GDPR)

21.1. Persoana vizată poate solicita ștergerea datelor cu caracter personal, în special atunci când datele nu mai sunt necesare, atunci când persoana vizată își retrage consimțământul sau se opune prelucrării.

21.2. Ștergerea nu se aplică în cazurile în care prelucrarea este necesară pentru respectarea unei obligații legale care necesită prelucrare sau pentru stabilirea, exercitarea sau apărarea unor pretenții legale.

22.Dreptul la restricționarea prelucrării (articolul 18 GDPR)

22.1. Persoana vizată poate solicita restricționarea prelucrării în principal atunci când:

22.1.1. Exactitatea datelor cu caracter personal este contestată de persoana vizată, pentru o perioadă de timp care permite Societății să verifice exactitatea datelor cu caracter personal,

22.1.2. Prelucrarea este ilegală, iar persoana vizată se opune ștergerii datelor cu caracter personal și solicită în schimb restricționarea utilizării acestora,

22.1.3. Societatea nu mai are nevoie de datele cu caracter personal în scopul prelucrării, dar acestea sunt solicitate de persoana vizată pentru constatarea, exercitarea sau apărarea unui drept în instanță,

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

23. Dreptul la opoziție (articolul 21 GDPR)

23.1. Persoana vizată are dreptul de a se opune, în orice moment și din motive legate de situația sa particulară, prelucrării datelor sale cu caracter personal, care se bazează pe interese legitime.

23.2. Societatea nu va mai prelucra datele cu caracter personal decât dacă demonstrează motive legitime imperioase pentru prelucrare care prevalează asupra intereselor, drepturilor și libertăților persoanei vizate sau pentru stabilirea, exercitarea sau apărarea drepturilor legale.

23.3. În cazul în care datele cu caracter personal sunt prelucrate în scopuri de marketing direct, persoana vizată are dreptul de a se opune în orice moment prelucrării datelor sale cu caracter personal în scopuri specifice de marketing, care pot include crearea de profiluri în măsura în care este legată de un astfel de marketing direct.

23.4. În cazul în care persoanele vizate se opun prelucrării în scopuri de marketing direct, datele lor cu caracter personal nu vor mai fi prelucrate în astfel de scopuri.

24. Dreptul la portabilitatea datelor cu caracter personal (articolul 20 din GDPR)

24.1. Persoana vizată are dreptul de a primi datele cu caracter personal care o privesc, pe care le-a furnizat operatorului de date, într-un format structurat, utilizat în mod obișnuit și care poate fi citit automat, atunci când prelucrarea se bazează pe consimțământ sau pe un contract și se realizează prin mijloace automate.

24.2. În exercitarea dreptului la portabilitatea datelor cu caracter personal în conformitate cu punctul 24.1, persoana vizată are dreptul de a îi fi transmise datele cu caracter personal direct de la un operator la altul, acolo unde este fezabil din punct de vedere tehnic.

25.Dreptul de a retrage consimțământul (articolul 7 GDPR)

25.1. Atunci când prelucrarea se bazează pe consimțământul persoanei vizate, aceasta își păstrează dreptul de a-l retrage în orice moment, fără a afecta prelucrarea anterioară bazată pe consimțământ.

25.2. Persoana vizată are dreptul de a se opune în orice moment utilizării datelor sale cu caracter personal dacă aceste date sunt utilizate în scopuri care nu sunt prevăzute de lege.

25.3. Dreptul de opoziție se aplică chiar dacă persoana vizată și-a dat anterior consimțământul pentru utilizarea datelor sale cu caracter personal.

26. Exercitarea drepturilor persoanelor vizate

26.1. Societatea gestionează solicitările persoanelor vizate urmând proceduri specifice.

26.2. Societatea răspunde solicitărilor persoanelor vizate fără întârzieri nejustificate și, în orice caz, în termen de o lună de la primirea solicitării. Această perioadă poate fi

prelungită cu încă două luni, dacă este necesar, având în vedere complexitatea cererii și numărul de cereri formulate.

26.3. În caz de întârziere, Societatea informează persoana vizată cu privire la prelungire în termen de o lună de la primirea cererii, împreună cu motivele întârzierii.

26.4. În cazul în care persoana vizată depune cererea prin mijloace electronice, informațiile vor fi furnizate prin mijloace electronice acolo unde este posibil, cu excepția cazului în care persoana vizată solicită altfel.

26.5. Societatea utilizează toate măsurile rezonabile pentru a verifica identitatea unei persoane vizate care solicită accesul, păstrând datele de identificare numai pentru timpul necesar. Societatea nu trebuie să păstreze datele cu caracter personal exclusiv în scopul de a răspunde la potențialele solicitări viitoare ale persoanelor vizate.

26.6. Societatea își rezervă dreptul de a refuza, integral sau parțial, cererea unei persoane vizate numai atunci când aceasta intră sub incidența unei excepții GDPR sau a unei dispoziții de drept național. În orice caz, persoana vizată este informată în scris și motivat cu privire la decizia de a nu satisface cererea sa, precum și cu privire la dreptul său de a depune o plângere la Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal.

PARTEA 5 – ATRIBUIREA PRELUCRĂRII DATELOR CU CARACTER PERSONAL ȘI TRANSFERURILE DE DATE CU CARACTER PERSONAL ÎN AFARA SEE

27. Verificări prealabile (Due Diligence) și cerințe contractuale

27.1 Ori de câte ori Societatea desemnează un împuternicit pentru prelucrarea datelor cu caracter personal, prelucrează date în numele unui operator sau împreună cu un alt operator, aceasta are obligația de a se asigura, înainte de încheierea acordului relevant, că prelucrarea se va realiza în mod legal și corect, prin realizarea unor verificări prealabile (due diligence).

27.2. Societatea va utiliza numai persoane împuternicite care oferă garanții suficiente pentru a implementa măsuri tehnice și organizatorice adecvate în așa fel încât prelucrarea să îndeplinească cerințele GDPR și să asigure protecția drepturilor persoanelor vizate.

27.3. Angajarea unei persoane împuternicite va fi guvernată de un acord de prelucrare a datelor, care este obligatoriu din punct de vedere juridic pentru persoana împuternicită în ceea ce privește Societatea care acționează în calitate de operator de date și stabilește în mod clar obiectul și durata prelucrării, natura și scopul prelucrării, tipul de date cu caracter personal și categoriile de persoane vizate implicate, precum și drepturile și obligațiile Societății. În special, acordul prevede că persoana împuternicită de operator:

27.3.1. Prelucrează date cu caracter personal numai pe baza instrucțiunilor documentate din partea Societății, inclusiv instrucțiuni privind transferurile de date cu caracter personal către o țară terță sau o organizație internațională, cu excepția cazului în care acest lucru este impus de legislația Uniunii sau a unui stat membru la care este supusă persoana împuternicită. În astfel de cazuri, persoana împuternicită va informa Societatea cu privire la cerința legală înainte de prelucrare, cu excepția cazului în care legea interzice astfel de informații din motive importante de interes public.

27.3.2. Se asigură că persoanele autorizate să prelucreze datele cu caracter personal s-au angajat la confidențialitate sau au o obligație legală adecvată de confidențialitate.

27.3.3. Ia toate măsurile tehnice și organizatorice necesare.

27.3.4. Nu angajează o altă persoană subîmputernicită fără autorizație prealabilă specifică sau generală scrisă din partea Societății. În cazul unei autorizații scrise generale, persoana împuternicită informează Societatea cu privire la orice modificări intenționate cu privire la adăugarea sau înlocuirea altor

subîmputerniciți, oferind astfel Societății posibilitatea de a se opune unor astfel de modificări.

27.3.5. Atunci când persoana împuternicită de operator angajează un alt subîmputernicit pentru a efectua activități specifice de prelucrare în numele Societății, aceleași obligații de protecție a datelor cu caracter personal ca cele prevăzute în acordul dintre Societate și persoana împuternicită de operator sunt impuse acelui alt subîmputernicit prin intermediul unui contract, în special, oferind garanții suficiente pentru a implementa măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să îndeplinească cerințele GDPR.

27.3.6. Ține cont de natura prelucrării și asistă Societatea prin măsuri tehnice și organizatorice adecvate, în măsura în care acest lucru este posibil, pentru îndeplinirea obligației Societății de a răspunde solicitărilor de exercitare a drepturilor persoanei vizate.

27.3.7. Asistă Societatea în asigurarea respectării obligațiilor privind securitatea prelucrării, gestionarea incidentelor de încălcare a securității datelor cu caracter personal și efectuarea de evaluări de impact, având în vedere natura prelucrării și informațiile disponibile persoanei împuternicite de operator.

27.3.8. La alegerea Societății, șterge sau returnează toate datele cu caracter personal către Societate după încheierea furnizării serviciilor de prelucrare și șterge copiile existente, cu excepția cazului în care legislația Uniunii sau a statelor membre impune stocarea datelor cu caracter personal.

27.3.9. Pune la dispoziția operatorului toate informațiile necesare pentru a demonstra respectarea obligațiilor stabilite și permite și contribuie la audituri, inclusiv inspecții, efectuate de Societate sau de un alt auditor mandatat de Societate.

27.4. Societatea trebuie să implementeze mecanisme de monitorizare adecvate pentru a se asigura că serviciile furnizate de persoanele împuternicite sunt în conformitate cu obligațiile stabilite în contractele convenite.

27.5. În cazurile în care Societatea acționează ca operator asociat cu o altă entitate juridică, trebuie încheiat un acord între părți, care să stabilească în mod transparent responsabilitățile lor respective pentru respectarea obligațiilor GDPR, în special în ceea ce privește exercitarea drepturilor persoanelor vizate și obligațiile corespunzătoare de a furniza informații persoanelor vizate. Acordul poate specifica un punct de contact pentru persoanele vizate.

28. Transferuri de date cu caracter personal în afara SEE

28.1. Orice transfer de date cu caracter personal către o țară din afara Spațiului Economic European (SEE)[1] sau către o organizație internațională va avea loc numai dacă sunt îndeplinite condițiile prevăzute în GDPR, asigurându-se că nivelul de protecție a persoanelor fizice garantat de GDPR nu este subminat.

28.2. Transferul de date cu caracter personal în afara SEE poate avea loc în următoarele circumstanțe:

28.2.1. Comisia Europeană a emis o decizie privind caracterul adecvat confirmând că nivelul de protecție a datelor cu caracter personal într-o țară din afara SEE sau într-o organizație internațională este în esență echivalent cu cel din Spațiul Economic European.

28.2.2. Sunt furnizate garanții adecvate în ceea ce privește organizația beneficiară în conformitate cu articolul 46 din GDPR (de exemplu, clauze contractuale standard ale UE, norme corporative obligatorii), și, în același timp, entitatea juridică care acționează în calitate de exportator efectuează o evaluare a impactului

[1] Țările UE, Islanda, Norvegia și Liechtenstein

transferului pentru a stabili dacă legislația sau practicile țării din afara SEE împiedică eficacitatea garanțiilor adecvate (de exemplu, din cauza legislației care obligă accesul la datele cu caracter personal). În cazul în care evaluarea indică faptul că legile sau practicile țărilor terțe afectează eficacitatea instrumentului de transfer, atunci transferul poate avea loc numai dacă exportatorul stabilește măsuri suplimentare pentru a se asigura că nivelul de protecție a datelor cu caracter personal transferate se apropie de standardul UE de echivalență substanțială.

28.2.3. Transferul are loc în baza uneia dintre derogările prevăzute la articolul 49 din GDPR, după cum urmează:

a) persoana vizată și-a dat consimțământul expres pentru transferul propus, fiind informată cu privire la riscurile potențiale pe care astfel de transferuri le prezintă pentru drepturile persoanei vizate în absența unei decizii de adecvare și a unor garanții adecvate;

b) transferul este necesar pentru executarea unui contract între persoana vizată și operator sau pentru punerea în aplicare a măsurilor precontractuale luate la cererea persoanei vizate;

c) transferul este necesar pentru încheierea sau executarea unui contract încheiat în beneficiul persoanei vizate între operatorul de date și o altă persoană fizică sau juridică;

d) transferul este necesar din motive importante de interes public;

e) transferul este necesar pentru constatarea, exercitarea sau apărarea unor drepturi legale;

f) transferul este necesar pentru a proteja interesele vitale ale persoanei vizate sau ale altor persoane în cazul în care persoana vizată nu are capacitatea fizică sau juridică de a-și da consimțământul;

g) transferul se efectuează dintr-un registru care, în conformitate cu dreptul Uniunii sau al statului membru, este destinat să furnizeze informații publicului și este deschis pentru consultare fie de către publicul larg, fie de către orice persoană care se poate prevala de un interes legitim, dar numai dacă sunt îndeplinite condițiile prevăzute de dreptul Uniunii sau de dreptul statului membru în fiecare caz.

PARTEA 6 – PROTECȚIA DATELOR PERSONALE ÎNCEPÂND CU MOMENTUL CONCEPERII ȘI SECURITATEA PRELUCRARII

29. Evaluarea impactului asupra protecției datelor (EIPD)

29.1. În cazul în care un tip de prelucrare, în special cu utilizarea noilor tehnologii, având în vedere natura, domeniul de aplicare, contextul și scopurile prelucrării, este susceptibil să conducă la un risc ridicat pentru drepturile și libertățile persoanelor fizice, Societatea va efectua, înainte de prelucrare, o evaluare a impactului operațiunilor de prelucrare avute în vedere asupra protecției datelor cu caracter personal.

29.2. O evaluare poate acoperi un set de operațiuni de prelucrare similare care prezintă riscuri la fel de ridicate.

29.3. O evaluare a impactului asupra protecției datelor este necesară în special în cazurile:

29.3.1. Evaluarea sistematică și extinsă a aspectelor personale referitoare la persoanele fizice, pe baza prelucrării automate, inclusiv crearea de profiluri, și pe care se bazează deciziile care produc efecte juridice asupra persoanei fizice sau care o afectează în mod similar într-o măsură semnificativă.

29.3.2. Prelucrarea pe scară largă a categoriilor speciale de date sau a datelor cu caracter personal referitoare la condamnări penale și infracțiuni.

29.3.3. Monitorizarea sistematică a unei zone accesibile publicului la scară largă.

29.3.4. Orice operațiune de prelucrare inclusă în lista stabilită de autoritatea competentă pentru protecția datelor cu privire la tipurile de operațiuni de prelucrare supuse cerinței unei EIPD.

29.4. Evaluarea conține cel puțin:

29.4.1. O descriere sistematică a operațiunilor de prelucrare avute în vedere și a scopurilor prelucrării, inclusiv, dacă este cazul, interesele legitime urmărite de Societate.

29.4.2. O evaluare a necesității și proporționalității operațiunilor de prelucrare în raport cu scopurile.

29.4.3. O evaluare a riscurilor la adresa drepturilor și libertăților persoanelor vizate.

29.4.4. Măsurile avute în vedere pentru abordarea riscurilor, inclusiv garanții, măsuri de securitate și mecanisme de asigurare a protecției datelor cu caracter personal și de demonstrare a respectării cadrului legislativ, ținând seama de drepturile și interesele legitime ale persoanelor vizate și ale altor părți interesate.

29.5. EIDP se desfășoară sub autoritatea șefului unității organizaționale responsabil cu supravegherea activităților de prelucrare relevante. La efectuarea unei EIPD, se solicită avizul responsabilului cu protecția datelor cu privire la:

29.5.1. Dacă este necesară sau nu o EIPD pentru prelucrarea datelor cu caracter personal.

29.5.2. Ce metodologie ar trebui urmată pentru efectuarea EIPD.

29.5.3. Dacă EIPD va fi efectuată intern sau de către un partener extern. În cazul externalizării, selecția părții externe se face cu aprobarea responsabilului cu protecția datelor sau a DPO-ului grupului, după caz.

29.5.4. Tipul de garanții (inclusiv măsuri tehnice și organizatorice) pe care Societatea ar trebui să le aplice pentru a atenua riscurile la adresa drepturilor și intereselor persoanelor vizate.

29.5.5. Dacă EIPD a fost efectuată corect și dacă concluziile sale (cu privire la continuarea sau nu a prelucrării și garanțiile de implementat) sunt în concordanță cu legislația relevantă.

29.6. În cazul în care EIPD indică faptul că operațiunea de prelucrare ar avea ca rezultat un risc rezidual ridicat, Societatea trebuie, conform articolului 36 GDPR, să consulte autoritatea de supraveghere competentă înainte de prelucrare.

30. Securitatea prelucrării

30.1. Ținând cont de stadiul actual al tehnologiei, de costurile de implementare și de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscul de diferite grade de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, Societatea implementează măsuri tehnice și organizatorice adecvate pentru a asigura un nivel adecvat de protecție a datelor cu caracter personal împotriva riscurilor.

30.2. Atunci când se evaluează nivelul adecvat de securitate, se acordă o atenție deosebită riscurilor prezentate de prelucrare, în special de distrugere, pierdere, modificare, dezvăluire neautorizată sau acces accidental sau ilegal la datele cu caracter personal transmise, stocate sau prelucrate în alt mod.

30.3. Măsurile ar trebui să includă, dar nu se limitează la:

30.3.1. Măsuri pentru a împiedica persoanele neautorizate să acceseze sistemele de prelucrare a datelor cu caracter personal.

30.3.2. Măsuri pentru a se asigura că persoanele autorizate pentru sistemele de prelucrare a datelor cu caracter personal au acces numai la datele cu caracter personal pe care sunt autorizate să le gestioneze.

30.3.3. Măsuri pentru a se asigura că datele cu caracter personal nu pot fi citite, copiate, modificate sau șterse de persoane neautorizate în timpul prelucrării (de exemplu, criptare sau pseudonimizare).

30.3.4. Măsuri pentru a se asigura că datele cu caracter personal prelucrate de terți/persoane împuternicite sunt prelucrate numai în conformitate cu instrucțiunile operatorului.

30.3.5. Măsuri pentru a se asigura că datele cu caracter personal sunt protejate împotriva distrugerii sau pierderii accidentale (de exemplu, copii de rezervă, planuri de recuperare a sistemului etc.).

30.3.6. Măsuri pentru a se asigura că datele cu caracter personal colectate în scopuri diferite sunt prelucrate separat.

30.4. În plus, Societatea aplică măsuri tehnice și organizatorice adecvate pentru a se asigura că, în mod implicit, sunt prelucrate numai datele cu caracter personal necesare pentru fiecare scop specific al prelucrării. Această obligație se aplică cantității de date cu caracter personal colectate, întinderii prelucrării, perioadei de stocare și accesibilității acestora. Mai exact, aceste măsuri asigură că, în mod implicit, datele cu caracter personal nu sunt puse la dispoziția unui număr nedeterminat de persoane fără intervenție umană.

31. Încălcarea securității datelor cu caracter personal

31.1. Societatea trebuie să fie capabilă să evalueze riscul care decurge dintr-un incident de încălcare a securității datelor cu caracter personal privind drepturile și libertățile persoanelor fizice. În acest context, trebuie să dispună de proceduri pentru identificarea și gestionarea în timp util și eficace a incidentelor de încălcare a securității datelor.

31.2. Atunci când se evaluează riscul unui incident pentru drepturile și libertățile persoanei vizate, sunt examinate circumstanțele specifice ale încălcării, inclusiv gravitatea și impactul potențial al acesteia. Evaluarea trebuie să ia în considerare în special următoarele criterii:

31.2.1. Tipul de încălcare.

31.2.2. Natura, sensibilitatea și volumul datelor cu caracter personal afectate.

31.2.3. Gradul de identificare a persoanei vizate.

31.2.4. Gravitatea consecințelor pentru persoana vizată.

31.2.5. Caracteristicile speciale ale persoanei vizate.

31.2.6. Numărul persoanelor vizate afectate.

32. Notificarea încălcărilor privind securitatea datelor cu caracter personal

32.1. În cazul unei încălcări privind securitatea datelor cu caracter personal, Societatea, acționând în calitate de operator, trebuie să notifice autoritățile de supraveghere relevante în conformitate cu GDPR și legislația națională.

32.2. În cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să aibă ca rezultat un risc ridicat pentru drepturile și libertățile persoanelor, Societatea trebuie să notifice imediat persoana vizată cu privire la încălcarea securității datelor cu caracter personal.

32.3. În cazul în care Societatea acționează în calitate de persoană împuternicită de operator, aceasta va notifica operatorul fără întârzieri nejustificate după ce a luat cunoștință de o încălcare a securității datelor cu caracter personal.

33. Documentarea încălcărilor privind securitatea datelor cu caracter personal

33.1. Societatea menține o evidență adecvată a incidentelor de încălcare a securității datelor cu caracter personal.

33.2. Această evidență include toate detaliile privind incidentul (data, acțiunile, părțile implicate, planul de acțiune etc.), precum și detalii despre evaluarea acestuia și notificarea către autoritățile de supraveghere și/sau persoanele vizate.

DEFINIȚII:

Operator de date cu caracter personal

Persoana juridică sau fizică sau altă entitate care stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal și atribuie prelucrarea datelor cu caracter personal Societății.

Consimțământul persoanei vizate

Orice manifestare liberă, specifică, informată și lipsită de ambiguitate a voinței persoanei vizate, prin care aceasta, printr-o declarație sau printr-o acțiune afirmativă clară, își exprimă acordul pentru prelucrarea datelor cu caracter personal care o privesc.

Persoana vizată

O persoană fizică identificată sau identificabilă la care se referă datele personale.

Criptare

Procesul de conversie a datelor cu caracter personal din forma lor originală într-o formă codificată care poate fi citită numai de cei care dețin cheia criptografică adecvată pentru a le decripta.

Operator asociat

Persoana fizică sau juridică care, alături de operator, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal.

Date personale

Orice informații referitoare la o persoană fizică identificată sau identificabilă ("persoana vizată"); O persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un identificator precum un

nume, un număr de identificare, date de localizare, un identificator online sau la unul sau mai mulți factori specifici identității fizice, fiziologice, genetice, mentale, economice, culturale sau sociale a persoanei fizice respective.

Încălcarea securității datelor cu caracter personal

O încălcare a securității care duce la distrugerea, pierderea, modificarea, dezvăluirea neautorizată sau accesul accidental sau ilegal la datele cu caracter personal transmise, stocate sau prelucrate în alt mod.

Prelucrarea datelor cu caracter personal

Orice operațiune sau set de operațiuni care se efectuează asupra datelor cu caracter personal sau a seturilor de date cu caracter personal, prin mijloace automate sau nu, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, recuperarea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminarea sau punerea la dispoziție în alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea.

Persoană împuternicită de operator

Persoana juridică sau fizică sau altă entitate care prelucrează date cu caracter personal în numele operatorului.

Profilare

Orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prezice aspecte referitoare la performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locația sau mișcările acelei persoane fizice.

Pseudonimizare

Prelucrarea datelor cu caracter personal în așa fel încât datele cu caracter personal să nu mai poată fi atribuite unei anumite persoane vizate fără utilizarea de informații suplimentare, cu condiția ca aceste informații suplimentare să fie păstrate separat și să fie supuse unor măsuri tehnice și organizatorice pentru a se asigura că datele cu caracter personal nu sunt atribuite unei persoane fizice identificate sau identificabile.

Destinatar

O persoană fizică sau juridică, o autoritate publică, o agenție sau un alt organism căruia îi sunt dezvăluite date cu caracter personal, indiferent dacă este vorba sau nu de un terț.

Categorii speciale de date cu caracter personal

Acestea sunt date cu caracter personal legate de:

- Origine rasială sau etnică;
- Opinii politice;
- Credințe religioase sau filozofice;
- Apartenența la sindicat;
- Date genetice;
- Date biometrice;
- Date de sănătate;
- Viața sexuală sau orientarea sexuală a unei persoane fizice.

Autoritatea de supraveghere

O autoritate publică independentă înființată de un stat membru responsabilă cu monitorizarea aplicării legislației privind protecția datelor cu caracter personal pentru a proteja drepturile și libertățile fundamentale ale persoanelor vizate în ceea ce privește prelucrarea și pentru a facilita libera circulație a datelor cu caracter personal în cadrul Uniunii.

Terț

O persoană fizică sau juridică, o autoritate publică, o agenție sau un organism, altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub autoritatea directă a operatorului sau a persoanei împuternicite, sunt autorizate să prelucreze date cu caracter personal.

Prezenta Politică va intra în vigoare la aprobarea acesteia de către Consiliul de Administrație al Societății, respectiv la 29.10.2025.