

1. Introducere

Protecția datelor dumneavoastră cu caracter personal este foarte importantă pentru organizația noastră ("organizația" sau "operatorul"). Ne dorim ca dumneavoastră să fiți informat corespunzător cu privire la modul și scopurile în prelucrăm datele dumneavoastră cu caracter personal.

Scopul acestei Politici de Securitate a Prelucrării Datelor cu Caracter Personal (denumită în continuare „Politica de Securitate”) este de a stabili măsurile tehnice și organizatorice adecvate și responsabilitățile angajaților organizației noastre cu atribuții de prelucrare a datelor cu caracter personal și/sau, după caz, ale persoanelor împuternicite de organizația noastră, pentru îndeplinirea obligațiilor referitoare la garantarea și protejarea drepturilor și libertăților fundamentale ale persoanelor fizice, în special a dreptului la viața intimă, familială și privată, cu privire la prelucrarea datelor cu caracter personal.

În cazul în care constatați orice erori intervenite în furnizarea datelor cu caracter personal care vă privesc, vă rugăm să ne informați în cel mai scurt timp posibil, folosind oricare dintre mijloacele indicate în secțiunea 8 din prezenta Politică de Securitate.

Principiile prelucrării datelor cu caracter personal

- Datele cu caracter personal sunt prelucrate de organizația noastră cu bună-credință și în conformitate cu dispozițiile legale în vigoare.
- Datele cu caracter personal sunt colectate de organizația noastră în scopuri bine determinate, explicite și legitime, iar prelucrarea ulterioară nu va fi incompatibilă cu aceste scopuri.
- Datele cu caracter personal sunt adecvate, pertinente și neexcesive prin raportare la scopul în care sunt colectate și ulterior prelucrate.
- Datele cu caracter personal nu se stochează de organizația noastră pentru o perioadă mai lungă decât este necesar pentru realizarea scopurilor în care au fost colectate.
- Organizația noastră a luat măsuri tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii, accesului neautorizat sau oricărei alte forme de prelucrare ilegală, precum și cu privire la ștergerea sau rectificarea datelor inexacte sau incomplete din punct de vedere al scopului pentru care sunt colectate și pentru care vor fi ulterior prelucrate.

3. Categoriile de date și scopul utilizării datelor cu caracter personal

Datele cu caracter personal la care se face referire în prezenta Politică de Securitate includ elemente de identificare de tipul nume și prenume, numele și prenumele reprezentanților legali, sex, data și locul nașterii, vârstă, cetățenie, telefon/ fax, adresa de domiciliu/ reședință, adresă de e-mail, cod numeric personal, seria și numărul actului de identitate/ pașaportului, loc de muncă, profesie, formare profesională – diplome – studii, date bancare sau alte asemenea, care servesc la identificarea dumneavoastră sau a persoanelor care vă reprezintă ori pe care le reprezentați.

Organizația noastră va colecta, utiliza, prelucra și furniza datele personale oferite de dumneavoastră în scopuri precum reclamă, marketing și publicitate, organizarea de cursuri, seminarii, alte evenimente (inclusiv delegații, conferințe și târguri), în scop educațional pentru organizarea programelor de formare profesională, pentru emiterea oricăror documente financiar-contabile, încheierea de contracte ori alte acte necesare în activitatea noastră.

Datele personale sunt destinate utilizării de către organizația noastră și sunt colectate prin persoane desemnate în acest sens. O parte din aceste date pot fi comunicate către partenerii noștri contractuali.

Colectarea și prelucrarea datelor cu caracter personal ale minorilor de către organizația noastră se vor face doar cu acordul explicit al părinților sau al altor reprezentanți legali.

4. Reguli generale

- Prezenta Politică de Securitate stabilește măsuri tehnice și organizatorice implementate de organizația noastră, pentru îndeplinirea obligațiilor referitoare la confidențialitatea și securitatea prelucrărilor efectuate în cadrul activității sale. Prin cerințe minime de securitate este avut în vedere un complex de măsuri tehnice, informatice, organizatorice, logistice și proceduri prin care se asigură un nivel de securitate al prelucrărilor în conformitate cu cerințele Regulamentului European privind Protecția Datelor Personale GDPR 679/2016.

- Organizația noastră a adoptat măsuri tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerilor accidentale sau ilegale, pierderii,

modificării, dezvăluirii, accesului neautorizat sau oricărei alte forme de prelucrare ilegală. În acest sens, este desemnată, la nivelul organizației noastre, o persoană responsabilă cu respectarea dispozițiilor GDPR 679/2016.

- Pentru îndeplinirea prevederilor legale aferente și în vederea satisfacerii cerințelor păstrării în siguranță a datelor și informațiilor, organizația noastră a elaborat și implementat măsuri organizatorice și tehnice orientate pe anumite direcții de acțiune:

- Identificarea și autentificarea utilizatorului;
- Tipul de acces;
- Colectarea datelor;
- Execuția copiilor de siguranță;
- Computerele și terminalele de acces;
- Fișierele de acces;
- Instruirea personalului;
- Sistemele de telecomunicații;
- Folosirea computerelor;
- Imprimarea datelor.

5. Proceduri specifice

- Identificarea și autentificarea utilizatorului

Prin utilizator se înțelege orice persoană care acționează sub autoritatea organizației noastre sau a persoanei împuternicite de noi, cu drept recunoscut de acces la bazele de date cu caracter personal.

Pentru a dobândi acces la date cu caracter personal, utilizatorii trebuie să se identifice.

În cazul prelucrărilor automatizate, identificarea se realizează prin autentificare în sistemele informatice ale organizației noastre. Autentificarea se face prin introducerea datelor de autentificare unice, constând în cont de utilizator și parolă.

Parolele sunt șiruri de caractere, adecvate din punct de vedere al securității ca lungime și compoziție, conform politicii de securitate IT a organizației noastre. La introducerea parolelor

caracterele tastate nu sunt afișate în clar pe monitor. Conform Politicii de securitate IT a organizației noastre, parolele trebuie schimbate periodic.

Organizația a implementat un sistem informatic care refuză automat accesul unui utilizator după un număr de introduceri greșite ale parolei.

Orice utilizator care primește acces la baza de date cu caracter personal este informat că trebuie să păstreze confidențialitatea datelor de autentificare și să răspundă în acest sens în fața operatorului.

Organizația noastră a stabilit o procedură de administrare și gestionare a conturilor de utilizator, prevăzută de Politica noastră de securitate IT. În conformitate cu prevederile acesteia, sunt stabilite reguli clare de acordare, respectiv anulare a drepturilor și modalităților de acces la contul de utilizator.

Accesul utilizatorilor la bazele de date cu caracter personal gestionate în sistem manual se face numai pe baza unei liste aprobate de conducerea organizației noastre.

- Tipul de acces

Utilizatorii pot accesa numai datele cu caracter personal necesare pentru îndeplinirea atribuțiilor alocate de organizația noastră. Pentru aceasta sunt stabile tipurile de acces după funcționalitate (administrare, introducere, prelucrare, salvare etc.) și după acțiuni aplicate asupra datelor cu caracter personal (scriere, citire, ștergere), precum și procedurile privind aceste tipuri de acces.

Programatorii sistemelor de prelucrare a datelor cu caracter personal au acces la datele cu caracter personal în baza unui acord de confidențialitate strict semnat cu organizația noastră, exclusiv în cazurile în care acest lucru este necesar, fiecare operațiune fiind documentată.

Compartimentul care asigură suportul tehnic poate avea acces la datele cu caracter personal

pentru rezolvarea incidentelor și a problemelor apărute în utilizarea sistemelor informatice.

Computerele și serverele care conțin bazele de date cu informații cu caracter personal se află în încăperi cu acces controlat. Documentele care conțin date cu caracter personal de tipul celor considerate categorii speciale de date sunt ținute în încăperi cu acces restricționat.

Operatorul a stabilit modalități stricte prin care se vor distruge datele cu caracter personal.

- Colectarea datelor

Organizația noastră desemnează utilizatori autorizați pentru operațiile de colectare, introducere și prelucrare de date cu caracter personal într-un sistem informatic sau în sistem manual.

Orice modificare a datelor cu caracter personal se poate face numai de către utilizatori autorizați desemnați de operator.

Operatorul a luat măsuri pentru ca sistemul informațional să înregistreze cine a făcut modificarea, data și ora modificării. Pentru o mai bună administrare, operatorul are implementate măsuri ca sistemul informațional să mențină datele șterse sau modificate.

- Execuția copiilor de siguranță

Sistemul informatic efectuează zilnic, în mod automat, un back-up al bazelor de date, pentru o eventuală recuperare a datelor, în cazul pierderii, distrugerii sau disfuncționalității sistemelor informatice.

Organizația stabilește intervalul de timp la care se vor executa copiile de siguranță ale bazelor de date cu caracter personal, precum și ale programelor folosite pentru prelucrările automatizate. Utilizatorii care execută aceste copii de siguranță sunt numiți de operator, într-un

număr restrâns. Copiile de siguranță se stochează într-un safe box cu acces restricționat, aflat într-o altă încăpere față de cea în care se efectuează copia de siguranță.

- Computerele și terminalele de acces

Computerele și alte terminale de acces sunt instalate în încăperi cu acces controlat, care se pot încuia. Dacă computerele sunt deschise și asupra lor nu se acționează o perioadă dată, stabilită de operator, sesiunea de lucru se închide automat.

Utilizatorii sunt instruiți, astfel încât bazele de date cu informațiile cu caracter personal să fie închise, în cazurile când acestea sunt deschise, dacă prin preajmă se află persoane neautorizate.

Serverele care găzduiesc bazele de date pot fi accesate doar în mod controlat, pe baza de drepturi de acces.

- Fișierele de acces

Organizația ia măsuri ca orice accesare a bazei de date cu caracter personal să fie înregistrată într-un fișier de acces (numit log la prelucrările automate) sau într-un registru pentru prelucrările manuale de date cu caracter personal, stabilit de operator.

Informațiile înregistrate în fișierul de acces sau în registru vor fi:

- codul de identificare (numele utilizatorului);
- numele fișierului accesat;
- numărul înregistrărilor efectuate;
- tipul de acces;
- codul operației executate sau programul folosit;
- data accesului (an, lună, zi);
- timpul (ora, minutul, secunda).

Pentru prelucrările automate aceste informații vor fi stocate într-un fișier de acces general sau în fișiere separate pentru fiecare utilizator.

Operatorul este obligat să păstreze fișierele de acces cel puțin 2 ani, pentru a fi folosite ca probe în cazul unor investigații. Dacă investigațiile se prelungesc, aceste fișiere se vor păstra până la finalizarea investigațiilor și a oricăror acțiuni în legătură cu acestea.

Fișierele de acces trebuie să facă posibilă identificarea de către operator sau de către persoana împuternicită a persoanelor care au accesat date cu caracter personal fără un motiv anume, în vederea aplicării unor sancțiuni sau a sesizării organelor competente.

- Sistemele de telecomunicații

Organizația, prin utilizatorii autorizați, realizează periodic controlul autentificărilor și tipurilor de acces pentru detectarea unor disfuncționalități în ceea ce privește folosirea sistemelor de telecomunicații. Prin sistemele de telecomunicații se vor transmite numai datele cu caracter personal strict necesare.

- Instruirea personalului

Utilizatorii care au acces la bazele de date cu caracter personal sunt instruiți cu privire la prevederile Regulamentului GDPR 679/2016, cu privire la dispozițiile politicii de securitate IT a organizației, precum și cu privire la importanța menținerii confidențialității acestora și riscurile pe care le comportă prelucrarea datelor cu caracter personal.

Utilizatorii care au acces la date cu caracter personal vor fi avertizați prin mesaje care vor apărea pe monitoare în timpul activității. Utilizatorii sunt obligați să își închidă sesiunea de lucru atunci când părăsesc locul de muncă.

- Folosirea computerelor

Pentru menținerea securității prelucrării datelor cu caracter personal (în special împotriva virușilor informatici) organizația a luat următoarele măsuri:

- a interzis folosirea de către utilizatori a programelor software care provin din surse nesigure;
- utilizatorii nu au drepturi de administrator pe computere;
- se utilizează software cu licență;
- utilizatorii au fost instruiți cu privire la Politica de securitate IT a organizației;
- computerele sunt protejate cu programe antivirus;
- se monitorizează activitatea utilizatorului și este restricționat accesul acestuia la imprimante
- Imprimarea datelor

Imprimarea datelor cu caracter personal se va realiza numai de către utilizatorii desemnați și numai în scopul precizat în prezentele reguli.

6. Drepturile persoanelor a căror date personale sunt colectate și/sau prelucrate

Conform GDPR 679/2016, beneficiați de următoarele drepturi cu privire la prelucrarea datelor cu caracter personal care vă privesc:

- Dreptul de informare

Aveți dreptul de a obține de la organizația noastră, conform GDPR 679/2016 cel puțin următoarele informații, cu excepția cazului în care sunteți deja în posesia informațiilor respective:

1. identitatea operatorului și a reprezentantului acestuia, dacă este cazul;
 2. scopul în care se face prelucrarea datelor;
 3. informații suplimentare, precum: destinatarii sau categoriile de destinatari ai datelor;
- dacă furnizarea tuturor datelor cerute este obligatorie și consecințele refuzului de a le furniza; existența drepturilor prevăzute de prezenta lege pentru persoana vizată, în special a dreptului de acces, de intervenție asupra datelor și de opoziție, precum și condițiile în care pot fi

exercitate;

4. orice alte informații a căror furnizare este impusă prin dispoziție a autorității de supraveghere, ținând seama de specificul prelucrării.

- Dreptul de acces la date

Aveți, de asemenea, dreptul de a obține de la organizația noastră, conform Regulamentului GDPR 679/2016, la cerere și în mod gratuit pentru o solicitare pe an, confirmarea faptului ca datele care vă privesc sunt sau nu sunt prelucrate de către noi.

- Dreptul de intervenție asupra datelor

Totodată, aveți dreptul de a obține de la operator, conform Regulamentului GDPR 679/2016 la cerere și în mod gratuit, rectificarea, actualizarea, blocarea sau ștergerea datelor a căror prelucrare nu este conformă legii, în special a datelor incomplete sau inexacte.

- Dreptul de opoziție

În plus, aveți dreptul de a se opune în orice moment prelucrării datelor cu caracter personal care vă privesc de către organizația noastră, conform Regulamentului GDPR 679/2016.

- Dreptul de a nu fi supus unei decizii individuale

Conform prevederilor Regulamentului GDPR 679/2016 beneficiați de dreptul de a cere și de a obține retragerea/ anularea/ reevaluarea oricărei decizii care produce efecte juridice în privința dumneavoastră, adoptată exclusiv pe baza unei prelucrări de date cu caracter personal, efectuată prin mijloace automate, destinată să evalueze unele aspecte ale personalității dumneavoastră, precum competența profesională, credibilitatea, comportamentul ori alte asemenea aspecte.

- Dreptul de a vă adresa justiției

În conformitate cu prevederile Regulamentului GDPR 679/2016, aveți dreptul de a vă adresa justiției pentru apărarea oricăror drepturi garantate de lege, care v-au fost încălcate.

Pentru exercitarea acestor drepturi, vă puteți adresa cu o cerere scrisă, datată și semnată, transmisă prin utilizarea datelor de contact indicate la secțiunea 8 din prezenta Politică de Securitate.

7. Dezvăluirea datelor cu caracter personal către terți

Datele colectate sunt dezvăluite către terți numai în cazul în care organizația noastră este vizată de o obligație legală în acest sens. Orice dezvăluire către terți în alte condiții a datelor cu caracter personal va fi făcută numai cu acordul dumneavoastră expres, exprimat în prealabil.

8. Prevederi Finale

Pentru solicitări sau întrebări cu privire la prezenta politică vă rugăm să ne contactați utilizând coordonatele disponibile în secțiunea de contact a prezentului website.