POLITICA GENERALA DE CONFIDENTIALITATE SI SECURITATE A DATELOR CU CARACTER PERSONAL

I. INTRODUCERE

1. Context

Incepand cu data de 25 mai 2018 se va aplica Regulamentul UE nr. 679/2016 privind protectia persoanelor fizice in ceeace priveste prelucrarea datelor cu caracter personal si privind libera circulatie a acestor date si de abrogare a Directivei 95/46/CE, denumit in continuare Regulamentul General de Protectie a Datelor ("GDPR"). Acest Regulament este direct aplicabil in toate statele membre ale Uniunii Europene, nefiind necesara o actualizare a legislatiei privind protectia datelor cu caracter persona. Totodata, GDPR se aplica tuturor firmelor care sunt inregistrate in Uniunea Europeana si/sau care au operatiuni pe teritoriul Uniunii Europene.

Una dintre cele mai importante si de impact modificari pe care le aduce Regulamentul General de Protectie a Datelor este ca in cazul neconformarii, societatile vor putea fi amendate cu pana la 4% din cifra de afaceri mondiala anuala sau 20.000.000 de euro, cu aplicarea celui mai mare cuantum al amenzii. Sunt introduse cerinte noi in materie de transparenta, respectiv:

- consolidarea drepturilor la informare, la acces si la stergerea date;
- Tacerea, omisiunea sau inactiunea nu mai sunt considerate drept consimtamant valabil exprimat, fiind obligatorie existenta unei actiuni pozitive, exprese in acest sens;
- Protejarea copiilor in mediul online;
- Un control sporit asupra datelor cu caracter personal.

De asemenea, Regulamentul General de Protectie a Datelor introduce doua noi drepturi ale persoanelor vizate, si anume: dreptul la portabilitatea datelor cu caracter personal si dreptul la restrictionarea operatiunilor de prelucrare a datelor cu caracter personal. Dreptul la portabilitatea datelor va permite persoanelor vizate ale caror date sunt prelucrate prin mijloace automate sa solicite unei intreprinderi sau organizatii sa primeasca inapoi datele cu caracter personal pe care le-au furnizat pe baza consimtamantului sau in temeiul incheierii sau executarii unui contract, pe de o parte, sau sa solicite ca aceste date sa fie transmise direct catre o alta intreprindere sau organizatie, daca acest lucru este posibil din punct de vedere tehnic. Dreptul la restrictionarea prelucrarii va permite persoanelor vizate sa solicite suspendarea prelucrarii datelor cu caracter personal in anumite cazuri, expres prevazute in Regulament. Totodate, Regulamentul General de Protectie a Datelor stabileste un set cuprinzator de norme privind incalcarea securitatii datelor cu caracter personal, stabilind obligatii de informare in sarcina intreprinderilor sau organizatiilor catre autoritatea de supraveghere si in anumite cazuri catre persoanele vizate, in cazul in care are loc un incident de securitate.

2. Scop

Avand in vedere faptul ca organizatia prelucreaza datele cu caracter personal in cadrul activitatilor sale curente, acest document isi propune sa stabileasca responsabilitatile si politica generala privind confidentialitatea si protectia datelor cu caracter personal.

Orice alta politica, procedura sau dispozitie interna speciala privind protectia si confidentialitatea datelor cu caracter personal nu vor contine dispozitii contrare acestei politici generale.

II. DEFINTII SI TERMINOLOGIE

Termen	Definitie
Date cu caracter personal	Orice informatii privind o persoana fizica identificata sau identificabila ("persoana vizata"); o persoana fizica identificabila este o persoana care poate fi identificata, direct sau indirect, in special prin referire la un element de identificare, cum ar fi un nume, un numar de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identitatii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.
Operatiune de prelucrare	Orice operatiune sau set de operatiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fara utilizarea de mijloace automatizate, cum ar fi colectarea, inregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispozitie in orice alt mod, alinierea sau combinarea, restrictionarea, stergerea sau distrugerea.
Restrictionarea prelucrarii	Marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora.
Creare de profiluri	Orice forma de prelucrare automata a datelor cu caracter personal care consta in utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoana fizica, in special pentru a analiza sau prevedea aspecte privind performanta la locul de munca, situatia economica, sanatatea, preferintele personale, interesele, fiabilitatea, comportamentul, locul in care se afla persoana fizica respectiva sau deplasarile acesteia.
Pseudonimizare	Prelucrarea datelor cu caracter personal intr-un asemenea mod incât acestea sa nu mai poata fi atribuite unei anume persoane vizate fara a se utiliza informatii suplimentare, cu conditia ca aceste informatii suplimentare sa fie stocate separat si sa faca obiectul unor masuri de natura tehnica si organizatorica care sa asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile.
Sistem de evidenta a datelor	Orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate dupa criterii functionale sau geografice.
Operator	Persoana fizica sau juridica, autoritatea publica, agentia sau alt organism care, singur sau impreuna cu altele, stabileste scopurile si mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile si mijloacele prelucrarii sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevazute in dreptul Uniunii sau in dreptul intern.
Persoana imputernicita	Persoana fizica sau juridica, autoritatea publica, agentia sau alt organism

Termen	Definitie
de operator	care prelucreaza datele cu caracter personal in numele operatorului.
Destinatar	Persoana fizica sau juridica, autoritatea publica, agentia sau alt organism careia (caruia) ii sunt divulgate datele cu caracter personal, indiferent daca este sau nu o parte terta. Cu toate acestea, autoritatile publice carora li se pot comunica date cu caracter personal in cadrul unei anumite anchete in conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de catre autoritatile publice respective respecta normele aplicabile in materie de protectie a datelor, in conformitate cu scopurile prelucrarii.
Parte terta	Persoana fizica sau juridica, autoritate publica, agentie sau organism altul decât persoana vizata, operatorul, persoana imputernicita de operator si persoanele care, sub directa autoritate a operatorului sau a persoanei imputernicite de operator, sunt autorizate sa prelucreze date cu caracter personal.
Consimtamânt al persoanei vizate	Orice manifestare de vointa libera, specifica, informata si lipsita de ambiguitate a persoanei vizate prin care aceasta accepta, printr-o declaratie sau printr-o actiune fara echivoc, ca datele cu caracter personal care o privesc sa fie prelucrate.
Incalcarea securitatii datelor cu caracter personal	O incalcare a securitatii care duce, in mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizata a datelor cu caracter personal transmise, stocate sau prelucrate intr-un alt mod, sau la accesul neautorizat la acestea.
Date genetice	Datele cu caracter personal referitoare la caracteristicile genetice mostenite sau dobândite ale unei persoane fizice, care ofera informatii unice privind fiziologia sau sanatatea persoanei respective si care rezulta in special in urma unei analize a unei mostre de material biologic recoltate de la persoana in cauza.
Date biometrice	Date cu caracter personal care rezulta in urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei ersonae fizice care permit sau ersona identificarea unica a respectivei ersonae, cum ar fi imaginile faciale sau datele dactiloscopice.
Date privind sanatatea	Date cu caracter personal legate de sanatatea fizica sau mentala a unei persoane fizice, inclusiv prestarea de servicii de asistenta medicala, care dezvaluie informatii despre starea de sanatate a acesteia.
Reprezentant	Persoana fizica sau juridica stabilita in Uniune, desemnata in scris de catre operator sau persoana imputernicita de operator in temeiul articolului 27, care reprezinta operatorul sau persoana imputernicita in ceea ce priveste obligatiile lor respective care le revin in temeiul prezentului regulament.

Termen	Definitie
Intreprindere	O persoana fizica sau juridica ce desfasoara o activitate economica, indiferent de forma juridica a acesteia, inclusiv parteneriate sau asociatii care desfasoara in mod regulat o activitate economica.
Grup de intreprinderi	O intreprindere care exercita controlul si intreprinderile controlate de aceasta.
Autoritate de Supraveghere	O autoritate publica independenta instituita de un stat membru in temeiul articolului 51.
Responsabil cu Protectia Datelor (RPD)	Responsabilul cu protectia datelor este persoana desemnata de operator sau de persoana imputernicita de operator implicata in mod corespunzator si in timp util in toate aspectele legate de protectia datelor cu caracter personal si care trebuie sa indeplineasca cel putin sarcinile prevazute la articolul 39 din GDPR (General Data Protection Regulation).
Autoritatea Nationala pentru Supravegherea Prelucrarilor de Date cu Caracter Personal (ANSPDCP)	Autoritatea publica de supraveghere instituita la nivelul României, in temeiul articolului 51 din Regulament.
Stocarea	Pastrarea pe orice fel de suport a datelor cu caracter personal culese.
Date anonime	Date care, datorita originii sau modalitatii specifice de prelucrare nu pot fi asociate cu o persoana identificata sau identificabila.

IV. PRINCIPIILE GENERALE CARE GUVERNEAZA PROTECTIA SI CONFIDENTIALITATEA DATELOR CU CARACTER PERSONAL

1. Principiul legalitatii prelucrarii datelor cu caracter personal – presupune faptul ca prelucrarea datelor se face doar in baza temeiurilor legale expres si limitative prevazute in Regulament;

2. Principiul prelucrarii transparente si echitabile a datelor cu caracter personal – presupune informarea corecta si completa a persoanelor vizate cu privire la identitatea operatorului si scopurile prelucrarii, precum si orice informatie suplimentara, intr-un mod usor accesibil si usor de inteles, utilizand un limbaj simplu si clar;

3. Principiul limitarii scopurilor prelucrarii datelor cu caracter personal - presupune ca datele cu caracter personal trebuie colectate in scopuri determinate, explicite si legitime, fara sa existe prelucrari ulterioare intr-un alt scop/scopuri care nu sunt compatibile cu cel/cele initiale;

4. Principiul minimizarii datelor cu caracter personal - presupune ca datele cu caracter personal sa fie reduse la minimum posibil, raportat la scopurile pentru care sunt prelucrate;

5. Principiul exactitatii datelor cu caracter personal - presupune ca datele cu caracter personal sa fie exacte si actualizate de ori cate ori este nevoie; de asemenea, presupune adoptarea unor masuri in vederea

stergerii si/sau rectificarii imediate a datelor incorecte, tinand cont de scopurile pentru care sunt prelucrate;

6. Principiul limitarii perioadei de stocare a datelor cu caracter personal - presupune ca datele cu caracter personal trebuie sa fie stocate doar pentru perioada necesara scopurilor pentru care sunt prelucrate;

7. Principiul integritatii si confidentialitatii datelor cu caracter personal - presupune existenta unor masuri de securitate in vederea protectiei impotriva prelucrarilor neautorizate sau ilegale si impotriva pierderii, distrugerii sau deteriorarii accidentale a datelor cu caracter personal;

8. Principiul responsabilitatii privind prelucrarea datelor cu caracter personal - presupune faptul ca operatorul poate demonstra respectarea tuturor principiilor de mai sus;

9. Principiul respectarii drepturilor fundamentale ale omului – presupune ca angajatii intreprinderii sau organizatiei sunt instruiti sa respecte drepturile persoanelor cu care intra in contact, precum dreptul la viata private, dreptul la intimidate, dreptul la opinie si ii informeaza pe acestia ca se pot folosi de aceste drepturi.

10. Principiul comunicarii eficiente – presupune faptul ca intreprinderea sau organizatia va furniza informatii corecte si complete cate persoanele care le solicita.

V. DREPTURILE PERSOANELOR VIZATE

Regulamentul General de Protectie a Datelor stabileste urmatoarele drepturi de care beneficiaza persoanele vizate ale caror date sunt prelucrate de catre operator:

1. Dreptul de a fi informat – presupune faptul ca persoanle vizate trebuie informate la momentul colectarii datelor cu caracter personal in legatura cu aspect esentiale ale prelucrarii, precum: identitatea operatorului de date cu caracter personal, datele de contact ale responsabilului cu protectia datelor, scopurile prelucrarii, temeiurile prelucrarii, destinatarii sau categoriile de destinatari ai datelor, daca este cazul, transferul de date catre tari sau organizatii terte, perioada de stocare a datelor, drepturile persoanelor vizate, dreptul de a depune plangere la autoritatea de supraveghere, existenta unui proces decisional automatizat, incluzand crearea de profiluri;

2. Dreptul de acces la datele cu caracter personal - presupune dreptul de a putea solicita confirmarea faptului ca datele sunt prelucrare sau nu, iar in caz afirmativ, persoana vizata sa poata solicita accesul la acestea, precum si anumite informatii despre acestea;

3. Dreptul la rectificarea datelor cu caracter personal - presupune dreptul persoanei vizate de a obtine rectificarea datelor inexacte, precum si completarea datelor incomplete, inclusiv prin furnizarea de informatii suplimentare;

4. Dreptul la stergerea datelor cu caracter personal - presupune dreptul persoanei vizate de a obtine de la operator stergerea datelor, fara intarzieri nejustificate, pentru anumite motive, expres prevazute in Regulament;

5. Dreptul de a retrage consimtamantul - presupune dreptul persoanei vizate de a isi retrage, in orice moment, consimtamantul pentru prelucrarea datelor de catre operator;

6. Dreptul la opozitie - presupune dreptul persoanei vizate de a se opune prelucrarii datelor in anumite cazuri, inclusiv crearii de profiluri (marketing direct, cercetare stiintifica, istorica sau statistica, interesul legitim al operatorului, interes public sau care rezulta din exercitarea autoritatii publice cu care este investit operatorul);

7. Dreptul la portabilitatea datelor cu caracter personal - presupune dreptul persoanei vizate de a primi datele pe care le-a furnizat operatorului intr-un format structurat, care poate fi citit automat, precum si dreptul de a solicita operatorului ca datele sa fie transmise altui operator;

8. Dreptul la restrictionarea prelucrarii datelor cu caracter personal - presupune dreptul persoanei vizate de a obtine din partea operatorului restrictionarea prelucrarii in anumite cazuri expres prevazute in Regulament, precum: contestarea exactitatii datelor, ilegalitatea prelucrarii, opozitie la prelurarea datelor;

9. Dreptul de a depune plangere - presupune dreptul persoanei vizate de a depune plangere fata de modalitatea de prelucrare a datelor de catre operator la Autoritatea de Supraveghere (ANSPDCP).

Regulamentul stabileste anumite termene in care un operator de date este obligat sa raspunda unei cereri prin care o persoana vizata isi exercita unul sau mai multe drepturi dintre cele mai sus enumerate, dupa cum urmeaza:

Cererea persoanei vizate	**Termen**
Cerere de informatii privind prelucrarea datelor	O luna; termenul se poate prelungi cu inca 2 luni, justificat, in functie de complexitatea cererii
Cerere de acces la date	O luna; termenul se poate prelungi cu inca 2 luni, justificat, in functie de complexitatea cererii
Cerere de rectificare a datelor	O luna; termenul se poate prelungi cu inca 2 luni, justificat, in functie de complexitatea cererii
Cerere de stergere a datelor	De indata, fara intarzieri nejustificate
Cerere de restrictionare a prelucrarii datelor	De indata, fara intarzieri nejustificate
Cerere de portabilitate a datelor	O luna; termenul se poate prelungi cu inca 2 luni, justificat, in functie de complexitatea cererii
Cerere de opozitie la prelucrarea datelor	La data primirii cererii
Cerere de retragere a consimtamantului	De indata, fara intarzieri nejustificate
Plangere la Autoritatea de Supraveghere	Nu este cazul

VI. TEMEIURILE PRELUCRARII DATELOR CU CARACTER PERSONAL

Primul principiu de prelucrare mai sus mentionat, principiul legalitatii prelucrarii, prevede ca o intreprindere sau organizatie poate prelucra date cu caracter personal doar in cazurile expres si limitativ prevazute de Regulamentul General de Protectie a Datelor. Astfel, o intreprindere sau organizatie poate prelucra date cu caracter personal numai dup ace identifica unul din urmatoarele sase temeiuri, anterior inceperii prelucrarii:

1) Existenta consimtamantului persoanei vizate

In situatia in care nu identifica un alt temei de prelucrare, iar prelucrarea este necesara pentru indeplinirea unui scop legitim, organizatia va obtine intotdeauna acordul explicit al unei persoane pentru prelucrarea datelor sale cu caracter personal. In plus, pentru prelucrarea datelor cu carater personal ale

minorilor sub 16 ani este necesara obtinerea consimtamantului parintilor.

Pentru ca acest consimtamant sa fie considerat valid in conformitate cu cerintele art 13 ale Regulamentului General de Protectie a Datelor, organizatia este obligata ca la momentul obtinerii consimtamantului sa furnizeze anumite informatii persoanei vizate, precum: identitatea si datele operatorului, datele de contact ale responsabilului cu protectia datelor, scopurile in care sunt prelucrate datele, temeiul prelucrarii, drepturile persoanei vizate si modalitatea in care pot fi exercitate, perioada de stocare a datelor etc.

In situatia colectarii indirecte ale datelor unei persoane vizate, toate informatiile mai sus mentionate trebuie furnizate acesteia intr-o perioada rezonabila de timp, dar care sa nu depaseasca o luna de la data colectarii datelor.

2) Incheierea sau executarea unui contract la care persoana vizata este departe

In aceasta situatie, prelucrarea datelor cu caracter personal este necesara in vederea incheierii unui contract sau indeplinirii obligatiilor unui contract aflat in derulare. De exemplu, livrarea unor produse nu se poate realiza fara a cunoaste o adresa de livrare. In aceste cazuri, nu este necesara obtinerea consimtamantului persoanelor vizate.

3) Indeplinirea unei obligatii legale

Acest temei poate fi utilizat in cazul in care organizatei ii este instituita o obligatie legala a carei indeplinire presupune prelucrare de date cu caracter personal. De exemplu Codul Muncii instituie numeroase obligatii care implica prelucrarea datelor cu caracter personal ale angajatilor. Nici in acest caz nu este necesara obtinerea consimtamantului persoanei vizate pentru a prelucra date cu caracter personal.

4) Protejarea intereselor vitale ale persoanei vizate sau unei alte persoane fizice

In cazul in care organizatia se afla intr-o situatie in care trebuie sa protejeze un interes vital al persoanei vizate sau al unei alte persoane, precum sanatatea sau integritatea fizica, va putea folosi acest temei ca baza legala pentru prelucrarea datelor cu caracter personal. Organizatia va trebui sa pastreze dovezi in acest sens.

5) Indeplinirea unei sarcini care serveste un interes public sau care rezulta din exercitarea autoritatii publice cu care este investit operatorul

In cazul in care organizatia trebuie sa indeplineasca o sarcina care deserveste un interes public sau ca parte a unei obligatii oficiale, atunci isi va baza prelucrarea datelor cu caracter personal pe acest temei, fara a solicita consimtamantul persoanei vizate. Si in acest caz organizatia trebuie sa documenteze interesul public sau obligatia oficiala pe baza caruia/careia a prelucrat datele cu caracter personal.

6) Interesul legitim urmarit de operator sau de o terta parte

Daca organizatia trebuie sa prelucreze date cu caracter personal in interesele sale legitime si poate dovedi ca drepturile si libertatile fundamentale ale persoanelor vizate nu sunt incalcate, organizatia is poate baza prelucrarea datelor cu caracter personal pe acest temei. Totusi, pentru a se putea folosi de acest temei legal, organizatia va trebui sa evaluzeze interesele legitime si sa documenteze rezultatul evaluarii.

VII. RESPONSABILUL CU PROTECTIA DATELOR

1. Desemnarea responsabilului cu protectia datelor

In cazul in care activitatile principale ale organizatiei presupun operatiuni de prelucrare care necesita o monitorizare periodica si sistematica a persoanelor vizate pe scara larga sau in cazul in care activitatile principale ale organizatiei constau in prelucrarea pe scara larga a unor categorii speciale de date expres prevazute in Regulament (date privind santatea, date privind condamnari penale, date biometrice, CNP, date privind copii etc.), organizatia este obligata sa desemneze un responsabil cu protectia datelor. Responsabilul cu protectia datelor poate fi numit din cadrul organizatiei sau din exteriorul acesteia in baza unui contract de prestari servicii. Acesta va fi desemnat pe baza unor calitati profesionale, in special pe baza detinerii unor cunostinte de specialitate in domeniul protectiei datelor cu caracter personal. Pe baza acestor criterii, organizatia va impune sau nu numirea unui responsabil cu protectia datelor.

2. Roluri si responsabilitati

Responsabilul cu protectia datelor va avea urmatoarele atributii:

a) Se va implica in mod corespunzator si in timp util in toate aspectele legate de protectia datelor cu caracter personal;

b) Va solicita toate resursele necesare pentru indeplinirea sarcinilor sale, iar organizatia il va sprijini in acest sens;

c) Nu va primi nicio instructiune in indeplinirea sarcinilor sale, acesta raspunzand direct in fata celui mai inalt nivel al conducerii organizatiei;

d) Este obligat sa respecte confidentialitatea sau secretul profesional in indeplinirea sarcinilor sale; e) Informeaza si consiliaza organizatia, precum si angajatilor acesteia care sunt implicati in operatiunile de prelucrare a datelor cu caracter personal, cu privire la obligatiile ce le revin in temeiul Regulamentului General de Protectie a Datelor si altor dispozitii legale privind protectia datelor cu caracter personal;

f) Monitorizeaza respectarea Regulamentului General de Protectie a Datelor si altor dispozitii legale privind protectia datelor cu caracter personal, precum si a politicilor de protectie a datelor adoptate in cadrul organizatiei;

g) Aloca responsabilitati, actiuni de sensibilizare si de formare a personalului implicat in operatiunile de prelucrare a datelor cu caracter personal si realizeaza auditurile aferente;

h) Ghideaza organizatia in cadrul procesului de management datelor cu caracter personal;

i) Furnizeaza consiliere, la cerere, in cee ace priveste evaluarea impactului asupra protectiei datelor cu caracter personal, in conformitate cu art. 35 din Regulament;

j) Furnizeaza consiliere la crearea inventarului operatiunilor de prelucrare;

k) Raspunde la solicitari din partea persoanelor vizate;

l) Coopereaza cu autoritatea de supraveghere;

m) Isi asuma rolul de punct de contact cu autoritatea de supraveghere privind toate aspectele legate de prelucrarea datelor cu caracter personal, inclusive consultarea prealabila prevazuta la art. 36 din Regulament, precum si, daca este cazul, consultarea cu privire la orice alte chestiuni;

n) In indeplinirea tuturor sarcinilor sale, va tine cont in mod corespunzator de riscul asociat operatiunilor de prelucrare, luand in considerare natura, domeniul de aplicare, contextual si scopurile prelucrarii datelor cu caracter personal.

VIII. CARTOGRAFIEREA PRELUCRARII DATELOR CU CARACTER PERSONAL

In conformitate cu cerintele art. 30 din Regulamentul General de Protectie a Datelor, organizatia va mentine o evidenta a tuturor activitailor de prelucrare. Aceasta evidenta va include cel putin urmatoarele informatii:

- Descrierea operatiunii de prelucrare a datelor cu caracter personal;
- Departamentul in care are loc prelucrarea datelor cu caracter personal;
- Scopurile prelucrarii datelor cu caracter personal;
- Documentele colectate;
- Categorii de persoane vizate;
- Categorii de date cu caracter personal prelucrate;
- Categorii de destinatari ai datelor cu caracter personal;
- Locatia de stocare a datelor cu caracter personal;
- Durata de stocare a datelor cu caracter personal;
- Temeiul legal al prelucrarii datelor cu caracter personal;
- Masuri de securitate.

IX. INFORMAREA PERSOANELOR VIZATE

In conformitate cu prevederile art. 12 din Regulamentul General de Protectie a Datelor, organizatia va raspunde oricaror cereri de informare din partea persoanelor vizate intr-o forma concise, transparenta, inteligibila si usor accesibila, utilizand un limbaj clar si simplu. Informatiile vor fi furnizate in scris, in format fizic sau electronic in functie de solicitarea persoanei vizate. De asemenea, organizatia va putea furniza oral informatiile, la solicitarea persoanei vizate, cu conditia sa verifice identitatea persoanei vizate prin alte mijloace care sa nu fie excesive in raport cu scopurile prelucrarii.

Organizatia va raspunde unei cereri din partea persoanei vizate in termen de maximum o luna de la primirea cererii. Acest termen va putea fi prelungit cu inca doua luni, justificat, in functie de complexitatea cererii persoanei vizate. Organizatia va informa persoana vizata in legatura orice prelungire a termenului de raspuns, in termen de maximum o luna de la primirea cererii.

Daca este cazul, organizatia va motiva orice refuz de a raspunde unei cereri din partea persoanei vizate si va prezenta motivele unei astfel de deicizii in termen de maximum o luna de la data primirii cererii. De asemenea, organizatia va informa persoana vizata in legatura cu posibilitatea depunerii unei plangeri in fata autoritatii de supraveghere si introducerii uneicai de atac judiciare.

Toate informatiile vor fi puse la dispozitia persoanelor vizate gratuit. In cazul in care cererile persoanelor vizate sunt vadit excesive sau nefondate, organizatia poate fie sa perceapa o taxa rezonabila pentru furnizarea informatiilor, fie sa refuse sa raspunda cererilor.

In situatia in care are dubii cu privire la identitatea persoanei vizate, organizatia poate solicita informatii suplimentare din partea persoanelor vizate.

Pentru modalitatea exacta deraspuns, se va consulta politica de raspuns la cererile persoanelor vizate.

X. MASURI DE SECURITATE

1. Confidentialitate prin design

Organizatia adopta principiul confidentialitatii prin designul sistemelor informatice si va defini si planifica in conformitate cu acest principiu de lucru toate sistemele noi sau modificate semnificativ care prelucreaza date cu caracter personal.

In acest scop, vor fi efectuate evaluari de impact asupra protectiei datelor, care vor include cel putin urmatoarele aspecte:

- examinarea modului in care vor fi prelucrate datele cu caracter personal si scopurile;
- evaluarea necesitatii si proportionalitatii prelucrarii datelor cu caracter personal;
- evaluarea riscurilor pentru persoanele fizice in prelucrarea datelor cu caracter personal;
- identificarea controalelor necesare pentru a aborda riscurile identificate si a demonstra respectarea Regulamentului General de Protectie a Datelor.

2. Masuri tehnice si organizatorice de protectie a datelor cu caracter personal

Organizatia va implementa cel putin urmatoarele masuri tehnice si organizatorice in vederea protectiei datelor cu caracter personal:

- pseudonimizarea si criptarea datelor cu caracter personal;
- capacitatea de a asigura confidentialitatea, integritatea, disponibilitatea si rezistenta continue ale sistemelor si serviciilor de prelucrare;
- capacitatea de a restabili disponibilitatea datelor cu caracter personal si accesul la acestea in timp util in cazul in care are loc un incident de natura fizica sau tehnica;
- implementarea unui proces pentru testarea, evaluarea si aprecierea periodice ale eficacitatii masurilor tehnice si organizatorice pentru garantarea securitatii prelucrarii datelor cu caracter personal.

3. Acorduri cu privire la prelucrarea datelor cu caracter personal

Organizatia se asigura ca va incheia acorduri de prelucrare a datelor cu caracter personal cu toti partenerii contractuali, care va cuprinde cerintele minime prevazute in Regulamentul General de Protectie a Datelor.

4. Transferurile internationale de date cu caracter personal

Organizatia poate efectua transferuri de date cu caracter personal catre tari terte sau organizatii international doar cu respectarea uneia din urmatoarele conditii:

- Existenta unei decizii privind caracterul adecvat al nivelului de protectie emisa de Comisia Europeana in tara terta sau organizatia internationala; sau
- Existenta unor garantii adecvate pentru protectia datelor cu caracter personal si existenta unor drepturi opozabile si cai de atac eficiente pentru persoana vizata; sau
- Aderarea la reguli corporatize obligatorii aprobate de autoritatea de supraveghere in care sunt prevazute regulile efectuarii unui transfer.

5. Anuntarea incidentelor de securitate

In cazul in care organizatia constata producerea unui incident de securitate care poate conduce la producerea unui risc pentru drepturile persoanelor vizate, va notifica autoritatea de supraveghere in termen de maximum 72 de ore de la data la care a luat cunostinta de acesta. In cazul in care incidentul de securitate este susceptibil sa produca un risc ridicat pentru drepturile si libertatile persoanelor vizate, organizatia va informa persoanele vizate fara intarzieri nejustificate.

Acest aspect va fi gestionat in conformitate cu Politica speciala de raspuns la incidente de securitate.


TEH 2001 SERVICE SRL