Politica generală privind protecția datelor cu caracter personal

CUPRINS:

Politica generală privind protecția datelor cu caracter personal

Introducere

Importanța respectării legislației privind protecția datelor cu caracter personal pentru **REPUBLIKA INTERACTIVE S.R.L.**, denumita in cele ce urmeaza „Republika"

În realizarea obiectului de activitate, Republika colectează, utilizează, stochează, transmit și realizează alte operațiuni asupra datelor cu caracter personal ale diferitelor persoane fizice, cum ar fi angajații, parteneri, colaboratori, furnizori și clienti.

Având în vedere preocuparea Republika pentru respectarea legislației, în general, și a normelor destinate să protejeze datele cu caracter personal și viața privată a persoanelor fizice, în special, se impune adoptarea acestei politici care să guverneze prelucrarea datelor cu caracter personal realizată de acesta.

Scopul Politicii de prelucrare a datelor cu caracter personal este de a descrie regulile și procedurile aplicabile operațiunilor de prelucrare a datelor cu caracter personal realizate de/ în numele Republika, astfel încât personalul Republika să respecte, pe tot parcursul activității lor, următoarele reguli generale cu privire la protecția datelor cu caracter personal (fără însă a se limita la acestea):

(i) operațiunile de prelucrare să fie conforme legislației în domeniul prelucrării datelor cu caracter personal la nivelul României și al Uniunii Europene și bunelor practici și standarde în domeniu;

(ii) drepturile persoanelor vizate să fie întru totul respectate, iar aceste persoane să fie protejate împotriva riscurilor ce decurg din prelucrarea datelor lor cu caracter personal de către Republika;

(iii) adoptarea unei poziții transparentă, consecventă și previzibilă cu privire la maniera în care prelucrează datele cu caracter personal, care să ofere încredere clienților, partenerilor, angajaților și colaboratorilor actuali sau potențiali.

Dincolo de consecințele juridice ale încălcării legislației referitoare la protecția datelor cu caracter personal (de exemplu, amenzi într-un cuantum semnificativ*, Regulamentul general privind protecția datelor*[1], adoptat la nivelul Uniunii Europene, prevăzând, pentru încălcarea prevederilor sale, amenzi de până la 20 milioane EUR sau 4% din cifra de afaceri mondială totală anuală din exercițiul financiar precedent, în funcție de care dintre aceste valori este mai mare), consecințele reputaționale de tipul publicității negative sunt deosebit de însemnate și pot diminua semnificativ încrederea și renumele pe care Republika le-au obținut în piață prin serviciile oferite.

Având în vedere potențialele consecințe negative ale încălcării legislației referitoare la protecția datelor cu caracter personal, toți angajații, colaboratorii și partenerii Societăților trebuie să citească cu atenție această Politică și să se asigure că respectă deplin normele privind protecția datelor cu caracter personal.

In cazul in care suspectați că dumneavoastră sau orice alt angajat, colaborator sau partener al Societății a încălcat sau este pe punctul de a încălca această Politică sau legislația în domeniu, adresați-vă în mod neîntârziat superiorului dumneavoastra sau la adresa de e-mail dpo@republika.ro.

Legislația care guvernează operațiunile de prelucrare a datelor cu caracter personal are ca scop protejarea persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal care le privesc, care, în România și în Uniunea Europeană, este un drept fundamental al acestora.

Legislația respectivă conține prevederi care reglementează modul în care persoanele fizice și juridice trebuie să colecteze, să utilizeze, să stocheze, să transmită și să efectueze alte operațiuni asupra datelor cu caracter personal. Aceste reguli sunt aplicabile indiferent dacă datele sunt colectate și stocate electronic, pe hârtie sau pe alte materiale.

Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE creează un regim juridic unitar la nivelul Uniunii Europene aplicabil prelucrării datelor cu caracter personal și este direct aplicabil în România.

Politica generală privind protecția datelor cu caracter personal

1. SCOPUL ȘI DOMENIUL DE APLICARE

Prin această Politică, Republika se angajează să respecte reglementările Regulament European privind protecția datelor cu caracter personal și libera circulație a acestora, precum si normele de punere in aplicare a Regulamentului.

Această politică stabilește principiile de bază prin care Operatorul, Republika prelucrează datele personale ale clienților, furnizorilor, partenerilor de afaceri, angajaților, dar si a altor persoane.

2. DOCUMENTE DE REFERINȚĂ

• **Regulamentul UE 2016/679** - al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date și de abrogare a Directivei 95/46 / CE;

• **Legea nr. 190/2018** privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor);

• **Codul Muncii – Legea 53/ 2003, Art.39** – Principalele drepturi și obligații ale salariatului;

• **Registrul Evidență Prelucră Date Caracter Personal.**

3. DEFINIȚII

Următoarele definiții ale termenilor utilizați în acest document sunt extrase din Articolul 4 din Regulamentul UE privind protecția generală a datelor:

”Date personale”: orice informație referitoare la o persoană fizică identificată sau identificabilă ("persoana vizată") care poate fi identificată, direct sau indirect, în special prin referire la un identificator, cum ar fi un nume, un număr de identificare, date despre locație, un identificator online sau la unul sau mai mulți factori specifici identității fizice, fiziologice, genetice, mentale, economice, culturale sau sociale a acelei persoane fizice;

”Datele cu caracter personal sensibile”: Datele personale care, prin natura lor, sunt deosebit de sensibile în raport cu drepturile și libertățile fundamentale, merită o protecție specifică, deoarece contextul prelucrării lor ar putea crea riscuri semnificative pentru drepturile și libertățile fundamentale. Aceste date cu caracter personal includ date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, convingerile religioase sau filosofice sau calitatea de membru al sindicatelor, datele genetice, datele biometrice în scopul identificării unice a unei persoane fizice, datele privind sănătatea sau datele referitoare la sexul unei persoane fizice viața sau orientarea sexuală.

„**Persoana vizata**”: persoana fizică la care se referă (căreia îi „aparțin”) anumite date cu caracter personal.

”**Operator de date”:** Persoana fizică sau juridică, autoritatea publică, agenția sau orice alt organism care, singur sau în comun cu alții, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal.

"Restricţionarea prelucrării": marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;

"Creare de profiluri": 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 prevedea aspecte privind performanta la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia;

"Pseudonimizare": prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat şi să facă obiectul unor măsuri de natură tehnică şi

organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;

"**Sistem de evidenţă a datelor**": orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcţionale sau geografice;

"Operator": persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care, singur sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal;

”Persoana imputernicita": persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

"Consimțământul persoanei vizate”: orice manifestare de voință liberă, specifică, informată şi lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;

"Încălcarea securității datelor cu caracter personal": o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea;

"Date privind sănătatea": date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia;

"Autoritate de supraveghere": o autoritate publică independentă instituită de un stat membru în temeiul articolului 51 din GDPR.

4. PRINCIPII DE BAZĂ PRIVIND PROCESAREA DATELOR CU CARACTER PERSONAL

4.1. LEGALITATE, ECHITATE, TRANSPARENȚĂ

Datele cu caracter personal trebuie prelucrate în mod legal, echitabil și transparent față de persoana vizată („legalitate, echitate și transparență”). În practică, aceasta înseamnă că in procesul de prelucrare a datelor Republika trebuie:

- să aibă motive legitime pentru colectarea și utilizarea datelor cu caracter personal;
- să nu utilizeze datele în moduri care au efecte negative nejustificate asupra persoanelor în cauză;
- să fie transparent cu privire la modul în care se intenționează să utilizeze datele și să furnizeze persoanelor vizate informări privind confidențialitatea în momentul colectării datelor lor personale;
- să gestioneze datele personale ale persoanelor vizate numai în moduri pe care acestea le-ar putea aștepta în mod rezonabil;
- și sa se asigure că nu este nimic ilicit făcut cu datele persoanelor vizate.

Principiul echității se reflectă prin faptul că toate activitățile de prelucrare de date personale, indiferent că este vorba despre clienti, furnizori sau angajați, sunt tratate cu același respect și condiții de echitate pentru persoanele vizate și datele personale ale acestora.

Principiul transparenței este asigurat prin faptul că orice informații şi comunicări referitoare la prelucrarea datelor cu caracter personal în cadrul proceselor de business în care este angrenata Republika, sunt ușor accesibile şi ușor de înțeles, prin folosirea unui limbaj simplu şi clar.

4.2. LIMITAREA SCOPULUI

În măsura în care condițiile procedurale de prelucrare a datelor personale și prevederile legale o permit, Republika va încerca limitarea prelucrării unor anumite tipuri de date personale care nu sunt neapărat necesare sau care nu reprezintă scopul unei anume activități.

Această limitare se poate face fără a afecta condițiile legale și normele interne stabilite de societate. Un bun exemplu este solicitarea limitată a datelor de cazier judiciar, doar pentru angajații sau viitorii angajați implicați în funcții de gestiune sau cu răspundere directă și ridicată pentru anumite tipuri de activități.

4.3. MINIMIZAREA DATELOR

Datele cu caracter personal trebuie sa fie adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate. În practică, acest principiu înseamnă că Republika va trebui să se asigure că:

- Deține numai datele personale care sunt absolut necesare pentru scopul pentru care au fost colectate și
- nu deține mai multe informații decât este necesar în raport cu acest scop. Republika ar trebui să identifice cantitatea minimă de date personale de care are nevoie pentru a-și îndeplini în mod corespunzător scopul.

În măsura în care condițiile procedurale de prelucrare a datelor și prevederile legale o permit, Republika poate asigura minimizarea prelucrării unor anumite tipuri de date personale care nu sunt neapărat necesare sau care nu reprezintă scopul unei anume activități. Această limitare se poate face fără a afecta condițiile legale și normele interne stabilite de Republika.

Când Republika deține prea multe date personale? Republika nu ar trebui să dețină mai multe date personale decât este necesar. Cu toate acestea, nu ar trebui nici sa dețină date care sunt irelevante pentru scopul prelucrării. Astfel, dacă este necesara detinerea unor date specifice privind anumite persoane, ar trebui să le colecteze doar acele date vizand persoanele respective, in caz contrar colectarea datelor ar putea fi considerata excesiva și irelevanta în raport cu alte persoane. Republika nu ar trebui să colecteze date cu caracter personal pentru care exista posibilitatea ca in viitor sa ii fie utile. Cu toate acestea, este permisă păstrarea informațiilor pentru un eveniment previzibil care nu poate apărea niciodată.

4.4. ACURATEȚEA DATELOR

Datele cu caracter personal trebuie să fie exacte și in cazul in care este necesar, să fie actualizate. Toate părțile implicate în procesarea datelor cu caracter personal din activitățile derulate în cadrul Republika sunt conștiente de importanța menținerii acurateței acestor date, începând cu faza de achiziție și trecând prin toate succesiunile de prelucrare, stocare parțială, transfer și arhivare.

Când datele personale sunt "inexacte"? Datele personale sunt inexacte dacă sunt incorecte sau înșelătoare cu privire la orice aspect de fapt.

Cum rămâne cu greșelile? Este acceptabila mentinerea unei evidențe a evenimentelor care au avut loc din greșeală, cu condiția ca aceste înregistrări să nu inducă în eroare in legătura cu faptele efectiv întâmplate. Republika ar putea sa adauge o notă la o înregistrare/evidenta pentru a clarifica faptul că s-a produs o greșeală.

Datele personale trebuie întotdeauna să fie actualizate? Aceasta depinde de scopul pentru sunt prelucrate datele. Dacă informația este utilizată într-un scop de a rămâne la curent, aceasta trebuie actualizata. De exemplu, înregistrările salariale ale angajaților ar trebui să fie actualizate atunci când există o modificare a contractului individual de munca.

Ce se întâmplă atunci când persoanele vizate contestă acuratețea datelor despre ele? Dacă se întâmplă acest lucru, Republika ar trebui să verifice dacă datele sunt corecte și, dacă nu, ar trebui să le șteargă sau să le corecteze. Uneori persoana vizata poate fi în măsură să furnizeze dovezi convingătoare că, de exemplu, data nașterii a fost înregistrată incorect. În alte circumstanțe, Republika ar putea avea nevoie să inițieze niște controale pentru a se asigura de corectitudinea datelor personale prezentate.

4.5. LIMITAREA PERIOADEI DE STOCARE

Datele cu caracter personal trebuie păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele. Nu

există perioade minime sau maxime specifice pentru păstrarea datelor cu caracter personal. În schimb, Republika trebuie sa aiba in vedere faptul că operațiunile de prelucrare în orice scop sau scopuri, nu trebuie păstrate mai mult decât este necesar în acel scop sau în acele scopuri. În practică, înseamnă că, pentru fiecare proces, Compaia va trebui:

- Sa revizuiască durata de timp pentru care va stoca datele personale;
- Sa ia în considerare scopul sau scopurile pe care entitatea deține datele pentru a decide dacă (și pentru cât timp) trebuie să le păstreze;
- să șteargă în siguranță informațiile/datele care nu mai sunt necesare pentru unul sau mai multe scopuri; și
- să actualizeze, să arhiveze sau să șteargă în siguranță datele dacă termenele de păstrare sunt depășite.

Ce abordare trebuie să iau pentru a lua decizii privind păstrarea datelor cu caracter personal? Este o bună practică revizuirea în mod regulat a datelelor personale pe care Republika le deține și să ștergeți tot ce nu mai este necesar, conform politicilor si procedurile adoptate in cadrul Republika. Informațiile care nu trebuie să fie accesate în mod regulat, dar care trebuie încă păstrate, ar trebui să fie arhivate în siguranță, in conformitate cu masurile stabilite in cadrul Republika.

In cazul in care Republika deține mai multe tipuri/categorii de date cu caracter personal, este o practică bună să se stabilească perioade de păstrare standard pentru fiecare categorie de date. Republika va trebui să țină seama de orice **norme profesionale in domeniul in care isi desfasoara activitatea si/sau cerințe de reglementare care se aplică.**

***Ce determină durata unei perioade de păstrare*?** Datele personale vor trebui să fie păstrate pentru mai mult timp în unele cazuri decât în altele. Republika va stabili durata stocării pe categorii de date personale si prin raportare la nevoile individuale ale activitatii, prin considerarea urmatoarelor:

- valoarea actuală și viitoare a informațiilor;
- costurile, riscurile și pasivele asociate cu păstrarea informațiilor; și
- ușurința sau dificultatea de a vă asigura că rămâne exactă și actualizată.

Perioada de păstrare adecvată este, de asemenea stabilita prin raportare la scopul prelucrării datelor personale. Astfel, durata pentru care Republika trebuie să păstreze datele personale depinde de scopul pentru care au fost obținute și de natura acestora. Dacă păstrarea datelor va fi necesara pentru respectarea legii, atunci Republika ar trebui să le păstreze atât timp cât se aplică acest motiv – obligația legala. Pe de altă parte, datele care nu mai sunt necesare, fiind indeplinit scopul pentru care acestea au fost colectate, iar legislatia aplicabila nu impune pastrarea acestora pentru o perioada succesiva de timp, stergerea acestor date ar trebui realizata in conformitate cu procedurile si politicile aprobate de Republika.

În cazul în care datele cu caracter personal sunt păstrate pentru mai mult de un scop, nu este nevoie să ștergeți datele daca acestea sunt încă necesare pentru oricare dintre aceste scopuri. Cu toate acestea, datele cu caracter personal nu ar trebui să fie păstrate pe termen nelimitat.

Republika nu trebuie să șteargă toate datele personale atunci când încetează un raport juridic, intrucat exista posibilitatea ca unele informații sa fie necesare tocmai pentru a confirma existența raportului juridic – incheierea/incetarea acestuia. În unele cazuri, Republika va putea pastra datele cu caracter personal in eventualitatea unor revendicări legale viitoare. Cu toate acestea, Republika ar putea în continuare să șteargă date care nu ar putea fi relevante pentru o astfel de revendicare.

In situatia in care există diverse cerințe legale și orientări profesionale privind păstrarea anumitor tipuri de evidențe - cum ar fi informațiile necesare pentru impozitul pe venit și scopurile auditului sau informații privind aspectele legate de sănătate și securitate, conformarea cu acest tip de cerinta nu va fi considerată perioada excesiva de pastrare a datelor.

Ce ar trebui să se întâmple cu datele personale la sfârșitul perioadei de păstrare? La sfârșitul perioadei de păstrare sau a duratei de viață a unei evidente, datele trebuie revizuite și eliminate, cu excepția cazului în care există un motiv special pentru păstrarea acestora.

Intrucat există o diferență semnificativă între ștergerea definitivă a unei evidente de date și arhivarea acesteia, dacă o înregistrare este arhivată sau stocată offline, aceasta ar trebui să reducă disponibilitatea acesteia și riscul de utilizare greșită sau de eroare.

Cu toate acestea, Republika va arhiva doar acea evidenta a datelor pe care trebuie să o păstreze potrivit prevederilor legale, pentru a se asigura respectarea si solutionarea cererilor persoanelor vizate in ceea ce priveste drepturile acestora prevazute de Regulament.

Cum rămâne cu păstrarea datelor partajate cu terțe persoane? În cazul în care datele cu caracter personal sunt împărțite între organizații, acele organizații trebuie să fie de acord cu privire la ce trebuie să facă atunci când nu mai au voie să împărtășească informațiile.

Societățile implicate in procesul de partajare/divulgare a informațiilor vor trebui să-și stabilească propriile perioade de păstrare, in functie de motivele si necesitatile fiecareia. Cu toate acestea, dacă informațiile partajate trebuie șterse, intrucat scopul urmarit a fost indeplinit, iar legislatia nu prevede un termen de pastrare, toate organizațiile care detin informatiile respective le vor sterge.

4.6. INTEGRITATEA ȘI CONFIDENȚIALITATEA

Datele cu caracter personal trebuie prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare.

În vederea asigurării securității datelor, nu există o soluție "potrivită pentru toți". Măsurile de securitate adecvate pentru o organizație vor depinde de abordarea Republika cu privire la evaluări bazate pe riscuri pentru a decide de ce nivel are nevoie. În special, Republika va trebui:

- să își elaboreze și să-și organizeze securitatea pentru a se potrivi cu datele personale pe care le deține și prejudiciul care poate rezulta dintr-o încălcare a securității;
- sa stabileasca un responsabil de asigurarea securității informațiilor;
- sa ia masurile tehnice si organizatorice rezonabile pentru a se asigura securitatea fizică și tehnică potrivită, susținută de politici și proceduri solide și de un personal bine instruit.

Ansamblul de măsuri care are ca scop asigurarea conformității GDPR la nivelul întregii Companii are ca obiectiv major asigurarea condițiilor necesare pentru asigurarea integrității și confidențialității datelor cu caracter personal.

4.7. RESPONSABILITATEA

Responsabilitatea pentru integritatea proceselor de business pe care le desfășoară Republika, este extinsă în mod automat și neunivoc și asupra prelucrării datelor personale. Prin natura acestora, datele personale care sunt prelucrate in cadrul Republika pot fi încadrate în trei mari categorii de date:

1. Date ale persoanelor de contact care reprezintă partenerii, colaboratori si furnizorii, acumulate în mod natural prin relațiile comerciale și de parteneriat derulate încă de la înființarea entității;
2. Datele personale ale clientilor, colectate și prelucrate prin diverse mijloace;
3. Date personale ale propriilor angajați, candidați sau foști angajați acumulate prin procesele de recrutare, angajare și administrare a statelor de salarii și dosarelor de personal.

Indiferent de natura și de particularitățile acestor date, Republika își asumă responsabilitatea pentru asigurarea celor mai depline condiții de integritate și confidențialitate pentru prelucrarea, transferul, stocarea și arhivare acestor date, pe tot parcursul fluxurilor de date.

Un rol foarte important în prelucrarea datelor personale la nivelul Republika îl au chiar angajații care sunt implicați – prin natura funcției lor – în activități legate de prelucrarea datelor personale ale persoanelor vizate. Din această perspectivă, fiecare angajat care are o astfel de funcție trebuie să fie conștient de importanța acesteia pentru entitate și, în același timp, să fie conștient de rolul și responsabilitatea sa în respectarea tuturor condițiilor necesare pentru asigurarea integrității și confidențialității datelor personale ale persoanelor vizate.

Toți angajații implicați în activități de prelucrare a datelor personale ale pacienților sau ale propriilor angajați trebuie să participe periodic la ședințe de instruire sau să studieze materiale dedicate condițiilor de prelucrare a datelor cu caracter personal GDPR, cu atenție specială pentru tot ceea ce face referire la responsabilitățile individuale și să semneze că a luat cunoștință de rolul său și de responsabilitatea sa individuală.

Pe lângă măsurile interne, Republika are în vedere asigurarea condițiilor de responsabilitate asociate activităților derulate de partenerii externi, în special cei care efectuează servicii externalizate. Procedura de inventariere și de actualizare a relațiilor contractuale acordă o atenție specială clauzelor contractuale care garantează asumarea răspunderii de fiecare dintre partenerii de procesare a datelor personale în raport cu tipul de activități executate.

5. ASIGURAREA PROTECȚIEI DATELOR PERSONALE PE TOT PARCURSUL PROCESELOR DE BUSINESS

5.1. COLECTAREA

Procesul de implementare a condițiilor de conformitate cu GDPR a avut în vedere asigurarea celor mai eficiente condiții de siguranță încă din etapa de colectare a datelor și a vizat atât modul în care se colectează datele, cât și canalele de comunicare folosite pentru această achiziție.

Toate datele personale ale clientilor au ca temei legal legitimul interes al Republika de a oferi servicii la cele mai ridicate standarde precum și întregul set de norme și prevederi legislative specifice domeniului de activitate, iar acolo unde este necesar – consimțământul persoanei vizate.

5.2. UTILIZAREA, RETENȚIA ȘI ȘTERGEREA

Toate datele personale care sunt prelucrate de entitate sunt utilizate numai în scopurile pentru care au fost colectate, au ca suport temeiurile legale prevăzute de Regulamentul GDPR, dar si alte prevederi legale în vigoare specifice domeniului de activitate, precum si interesul legitim al Republika.

Retenția și ștergerea acestor date se fac în funcție de normele si regulile impuse de cadrul legal aplicabil, dar si de procedurile interne, iar persoanele vizate sunt informate de acest lucru încă din momentul colectării datelor.

5.3. TRANSFERUL INTERNAȚIONAL DE DATE PERSONALE

Datele cu caracter personal nu vor fi transferate către o țară sau un teritoriu din afara UE, cu excepția cazului în care țara sau teritoriul respectiv asigură un nivel adecvat de protecție a drepturilor și libertăților persoanelor vizate în ceea ce privește prelucrarea datelor cu caracter personal. În cazul în care nu este posibil să se facă o apreciere daca transferul preconizat oferă un nivel adecvat de protecție, este necesar să se instituie "garanții adecvate". Atunci când se instituie garanții adecvate, drepturile persoanelor fizice continuă să fie protejate chiar și după ce datele lor au fost transferate în afara SEE. Aceste garanții pot consta în contracte, clauze etc.

5.4. NOTIFICAREA PERSOANELOR VIZATE

Atât angajații, cât și clientii Republika pot beneficia de transparența metodologiilor de prelucrare a datelor cu caracter personal încă din procesul de colectare. Aceleași condiții transparente de notificare se regăsesc în procesul de angajare sau în orice relație comercială de achiziție sau de vânzare.

Procedura de anunțare a breșelor de securitate include toate activitățile care trebuie derulate de echipa tehnică de intervenție în cazul apariției unor incidente care au afectat integritatea datelor personale, in conformitate cu procedurile si masurile adoptate de Republika.

6. DREPTURILE PERSOANELOR VIZATE

6.1. Dreptul de acces

Persoana vizată are dreptul de a obține de la Republika confirmarea că se prelucrează sau nu datele sale cu caracter personal. In situatia in care Republika îi prelucrează datele cu caracter personal, persoana vizată are dreptul de acces la datele respective și la informațiile următoare:

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

Persoana vizată trebuie să își poată exercita acest drept cu ușurință și la intervale de timp rezonabile, iar daca cererea persoanei vizate este în format electronic și nu solicită să i se răspundă într-un alt format, răspunsul Republika va fi transmis într-un format electronic utilizat în mod curent.

6.2. Dreptul la rectificare

Dacă datele sale cu caracter personal sunt inexacte ori incomplete, persoana vizată are dreptul ca acestea să fie rectificate de Republika, fără întârzieri nejustificate. În funcție de scopul prelucrării datelor cu caracter personal, persoana vizată are dreptul ca datele sale prelucrate de Republika să fie completate (dacă este cazul), inclusiv în urma oferirii declarații suplimentare de către persoana vizată.

6.3. Dreptul la ștergerea datelor („dreptul de a fi uitat”)

Persoana vizată are posibilitatea de a solicita ca datele sale cu caracter personal să fie șterse fără întârzieri nejustificate dacă nu mai este necesar ca acestea să fie prelucrate de către Republika, in calitate de operator de date cu caracter personal).

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

- datele sale cu caracter personal nu mai sunt necesare pentru realizarea scopurilor pentru care Republika le-a colectat (prelucrat);
- persoana vizată și-a retras consimțământul în temeiul căruia a avut loc prelucrarea și nu există un alt temei pe care Republika se poate baza pentru a îi prelucra datele;
- persoana vizată se opune prelucrării (în temeiul dreptului său la opoziție) și nu există motive legitime care să dea Republika dreptul de a prelucra datele în continuare;
- Republika a prelucrat datele în mod ilegal;

- există o obligație legală a Republika pentru care este necesară ștergerea datelor;
- colectarea datelor a avut loc în legătură cu oferirea de servicii unui minor.

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

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

- pentru exercitarea dreptului la liberă exprimare și informare;
- pentru a respecta o obligație legală de prelucrare, pentru a îndeplini o sarcină executată în interes public sau în cadrul exercitării unei autorități oficiale cu care Republika este învestită;
- pentru motive de interes public în domeniul sănătății publice;
- în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu GDPR, în măsura în care dreptul la ștergerea datelor este susceptibil să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective;
- pentru constatarea, exercitarea sau apărarea unui drept în instanță.

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

6.4. Dreptul la restricționarea prelucrării

Republika va da curs unei solicitări exprese de restricționare a prelucrării datelor dacă cel puțin una dintre următoarele condiții este îndeplinită:

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

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

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

- persoana vizată este de acord cu prelucrarea;
- prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță;

- prelucrarea este necesară pentru protecția drepturilor unei alte persoane fizice sau juridice;
- prelucrarea este necesară din motive de interes public important al Uniunii Europene sau al unui stat membru al Uniunii Europene.

Înainte de a ridica restricționarea prelucrării, persoana vizată va fi informată.

6.5. Dreptul la portabilitatea datelor

Persoanele vizate pot obține de la Republika datele cu caracter personal pe care aceasta le prelucrează, spre a le utiliza în scopurile în care doresc și a putea să le transfere dintr-un mediu în altul, într-un mod sigur și facil. Astfel, persoana vizată are dreptul la portabilitate numai în privința datelor pe care Republika le prelucrează în temeiul consimțământului său, pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri înainte de încheierea unui contract.

6.6. Dreptul la opoziție

Persoanele vizate au dreptul de a se opune prelucrării datelor lor cu caracter personal care este necesară pentru îndeplinirea unei sarcini care servește unui interes public, rezultă din exercitarea autorității publice cu care este învestită Republika sau este necesară pentru interesele legitime ale Republika sau ale unui terț. De asemenea, persoanele vizate au dreptul de a se opune prelucrării în scop de marketing direct.

Nu in ultimul rand, persoanele vizate au dreptul de a se opune prelucrării în scopuri de cercetare științifică ori istorică sau în scopuri statistice, mai puțin în cazul prelucrarea respectivă este necesară pentru îndeplinirea unui sarcini realizate din motive de interes public.

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

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

Persoanele vizate nu vor beneficia însă de dreptul de mai sus atunci când decizia (i) este necesară pentru încheierea sau executarea unui contract între persoana vizată și Republika, (ii) este prevăzută de lege, în condițiile GDPR sau (iii) este întemeiată pe consimțământul explicit al persoanei vizate.

În cazul în care decizia este necesară pentru încheierea ori executarea unui contract între persoana vizată și Republika sau este întemeiată pe consimțământul explicit al persoanei vizate, persoana vizată are următoarele drepturi: (i) dreptul de a obține intervenție umană în luarea deciziei, (ii) dreptul de a își exprima punctul de vedere și (iii) dreptul de a contesta decizia.

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

7. ROLUL ÎN PROCESAREA DATELOR PERSONALE

7.1. IMPORTANȚA ROLURILOR DE OPERATOR ȘI PROCESATOR

Esența unui bun început în elaborarea planului de conformitate GDPR este poziția pe care Republika o are în fiecare dintre activitățile pe care le derulează și care implică procesarea de date personale: operator sau persoana imputernicita.

„Operator” – este persoana fizică sau juridică, autoritatea publică, agenție sau alt organism care - singur sau împreună cu altele - stabilește scopurile şi mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile şi mijloacele prelucrării sunt stabilite print-o prevedere a Uniunii Europene sau o prevedere a legislației naționale, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul UE sau în dreptul intern;

„Persoana imputernicita” – este persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului, printr-o împuternicire de partea acestuia;

Operatorul joacă un rol crucial în asigurarea conformității. GDPR definește clar modul în care organizațiile trebuie să mențină cadrul legal în toate activitățile de procesare. Persoana imputernicita și Operatorul trebuie să fie de încredere și răspunzători pentru rolul lor. Ambele posturi implică implementarea măsurilor tehnice și organizaționale apte a demonstra că procesarea datelor este asigurată în conformitate cu GDPR.

La implementarea măsurilor tehnice și operaționale, Operatorul trebuie să țină cont de natura, scopul, contextul și motivul procesării, precum și de riscurile care pot amenința drepturile și libertățile persoanelor vizate.

Operatorul trebuie să apeleze numai la Persoane imputernicite care prezintă suficiente garanții, cu care să încheie un contract în care să fie prevăzute cu claritate întreaga gamă de operațiuni de procesare pe care au voie să le execute. Mentionam in acest sens faptul ca o Persoana imputernicita trebuie să aibă autorizarea clară a Operatorului pentru fiecare activitate de procesare, precum și autorizarea de a apela la alti subimputerniciti (subcontractanti) acolo unde e nevoie.

7.2. CLAUZE CONTRACTUALE OBLIGATORII DEPRELUCRARE A DATELOR PERSONALE

În relația cu o Persoana imputernicita, orice Operator (spre exemplu Republika) este obligat ca pe lângă contractul cadru, sa încheie o convenție care sa reglementeze protecția datelor cu caracter personal, cuprinzând specificații precum:

- Să acționeze numai în conformitate cu instrucțiunile documentate ale Operatorului;
- Să respecte regulile de transfer internațional al datelor;
- Să impună obligativitatea confidențialității tuturor angajaților care lucrează cu date relevante;
- Să adopte măsuri tehnice și organizatorice pentru asigurarea unui nivel de securitate apropiat de riscurile asociate procesării;
- Să respecte regulile legate de angajarea unor sub-procesatori;
- Să adopte măsuri prin care să îi asiste pe Operatori să fie conformi cu drepturile subiecților vizați;
- Să asiste Operatorul în activitățile cheie de asigurare a securității procesării, precum notificarea breșelor și evaluarea de impact;
- La decizia Operatorului, trebuie să returneze sau să distrugă datele personale la încheierea relației de parteneriat;
- Să permită și să contribuie la auditări și inspecții;
- Să furnizeze Operatorului orice informații necesare pentru demonstrarea conformității cu GDPR.

8. CONDITIILE DE RESPECTAT PENTRU PRELUCRAREA DATELOR CU CARACTER PERSONAL

In vederea aprecierii condițiilor de prelucrare se va ține cont de natura datelor cu caracter personal în cauză. Condițiile care trebuie îndeplinite pentru prelucrarea unor date sensibile sunt mult mai exigente, cum ar fi de exemplu prelucrarea unor date despre sănătatea unei persoane sau cazierul judiciar.

Care sunt condițiile de prelucrare legala? Prelucrarea este legală numai dacă și în măsura în care se aplică cel puțin una dintre următoarele condiții:

(a) persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;

(b) prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;

(c) prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;

(d) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;

(e) prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul;

(f) prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.

Ce condiții trebuie îndeplinite pentru prelucrarea legala a datelor sensibile? Cu titlu de regula generala, se interzice prelucrarea de date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, **de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea** sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice. Cu toate acestea, datele sensibile vor fi prelucrate daca intervine una dintre situațiile de mai jos:

(a) persoana vizată și-a dat consimțământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice, cu excepția cazului în care dreptul Uniunii sau dreptul intern prevede ca interdicția prevăzută la alineatul (1) să nu poată fi ridicată prin consimțământul persoanei vizate;

(b) prelucrarea este necesară în scopul îndeplinirii obligațiilor și al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forței de muncă și al securității sociale și protecției sociale, în măsura în care acest lucru este autorizat de dreptul Uniunii sau de dreptul intern ori de un acord colectiv de muncă încheiat în temeiul dreptului intern care prevede garanții adecvate pentru drepturile fundamentale și interesele persoanei vizate;

(c) prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice, atunci când persoana vizată se află în incapacitate fizică sau juridică de a-și da consimțământul;

(d) prelucrarea este efectuată în cadrul activităților lor legitime și cu garanții adecvate de către o fundație, o asociație sau orice alt organism fără scop lucrativ și cu specific politic, filozofic, religios sau sindical, cu condiția ca prelucrarea să se refere numai la membrii sau la foștii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente în legătură cu scopurile sale și ca datele cu caracter personal să nu fie comunicate terților fără consimțământul persoanelor vizate;

(e) prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod manifest de către persoana vizată;

(f) prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță sau ori de câte ori instanțele acționează în exercițiul funcției lor judiciare;

(g) prelucrarea este necesară din motive de interes public major, în baza dreptului Uniunii sau a dreptului intern, care este proporțional cu obiectivul urmărit, respectă esența dreptului la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate;

(h) prelucrarea este necesară în scopuri legate de medicina preventivă sau a muncii, de evaluarea capacității de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistență medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor și serviciilor de sănătate sau de asistență socială, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul unui contract încheiat cu un cadru medical și sub rezerva respectării condițiilor și garanțiilor prevăzute la alineatul (3);

(i) prelucrarea este necesară din motive de interes public în domeniul sănătății publice, cum ar fi protecția împotriva amenințărilor transfrontaliere grave la adresa sănătății sau asigurarea de standarde ridicate de calitate și siguranță a asistenței medicale și a medicamentelor sau a dispozitivelor medicale, în temeiul dreptului Uniunii sau al dreptului intern, care prevede măsuri adecvate și specifice pentru protejarea drepturilor și libertăților persoanei vizate, în special a secretului profesional; sau

(j) prelucrarea este necesară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1), în baza dreptului Uniunii sau a dreptului intern, care este proporțional cu obiectivul urmărit, respectă esența dreptului la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate.

Ce este "interesul legitim"? Republika poate avea motive legitime de procesare a datelor dacă sunt îndeplinite anumite cerințe. Una dintre acestea este necesitatea entității de a avea un interes legitim de prelucrare, iar a doua este ca acest interes legitim trebuie să fie echilibrat cu interesele persoanei vizate. Astfel, condiția "interesului legitim" nu va fi îndeplinită dacă prelucrarea nu este justificată din cauza efectului său prejudiciabil asupra drepturilor și libertăților sau intereselor legitime ale persoanei vizate. Interesele legitime ale Republika nu trebuie să fie în armonie totala cu cele ale persoanei vizate. Cu toate acestea, în cazul în care există o nepotrivire gravă între interesele concurente, interesele legitime ale persoanei vizate vor veni pe primul loc. În cele din urmă, prelucrarea datelor in temeiul interesului legitim trebuie să fie corectă și legală și trebuie să respecte toate principiile de protecție a datelor.

Când prelucrarea este "necesara"? Multe dintre condițiile de prelucrare a datelor depind de faptul daca prelucrarea este "necesară" pentru scopul anume la care se referă condiția. Acest lucru impune o cerință strictă, deoarece condiția nu va fi îndeplinită in cazul in care Republika poate atinge acest scop prin alte mijloace rezonabile sau dacă procesarea este necesară doar prin decizia Republika de a desfășura activitatea într-un anumit mod.

Ce se înțelege prin "consimțământ"? Una dintre condițiile pentru prelucrare este aceea ca persoana vizata sa-și fi dat acordul pentru colectarea și folosirea datelor personale în scopurile si mijloacele stabilite de operator si care nu pot fi prelucrate in alte temeiuri legale. Consimțământul înseamnă “orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate”.

Consimțământul trebuie, de asemenea, să fie adecvat vârstei și capacității persoanei și circumstanțelor particulare ale cazului. Chiar și atunci când a fost acordat consimțământul, acesta nu va dura neapărat pentru totdeauna. Cu toate că în majoritatea cazurilor consimțământul va dura până când procesarea la care se referă continuă, Republika ar trebui să recunoască faptul că persoana poate să retragă consimțământul, în funcție de natura consimțământului acordat și de circumstanțele în care au fost colectate si utilizate datele. Retragerea consimțământului nu afectează validitatea oricărui lucru deja făcut, înțelegându-se că a fost acordat consimțământul.

Consimțământul obținut prin constrângere sau prin înșelătorii nu satisface în mod adecvat condiția de prelucrare a datelor in baza consimțământului. Un aspect de reținut este ca in cazul în care prelucrarea se bazează pe consimțământ, Republika trebuie să fie în măsură să demonstreze că persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal. Atunci când consimțământul persoanei vizate este dat în contextul unei declarații scrise care se referă și la alte aspecte, cererea privind consimțământul va fi prezentată într-o formă care o diferențiază în mod clar de celelalte aspecte, într-o formă inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu.

Este important de menționat ca persoana vizată are dreptul să își retragă în orice moment consimțământul si ca atare, are dreptul de a fi informata asupra acestui lucru, anterior exprimării acordului. Cu toate acestea, retragerea consimțământului nu afectează legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia. Înainte de acordarea consimțământului, persoana vizată

este informată cu privire la acest lucru. Retragerea consimțământului se face la fel de simplu ca acordarea acestuia.

9. IMPLEMENTAREA CULTURII GDPR

GDPR este începutul unui proces care trebuie să devină ireversibil, și pentru asta are nevoie de o sursă de energie care să îl mențină în mișcare. Sursa de energie pentru menținerea condițiilor de conformitate GDPR pentru întreg ciclul de viață al unui business este capacitatea internă a Republika de a menține nivelul de compatibilitate, iar acest lucru se numeste Cultură GDPR.

Succesul unui proiect GDPR pe termen lung se bazează pe crearea unei culturi la nivel de Republika, în care oamenii – angajatii, se gândesc în primul rând la modul în care ar dori ca informațiile lor personale să fie procesate.

Pentru crearea unei culturi GDPR la nivel de organizatie, Republika a adoptat o abordare proactivă, metodică și responsabilă cu privire la conformitate, o cultură de confidențialitate și de protecție a datelor personale.

Odată construită cultura de confidențialitate a datelor, aceasta trebuie incorporată și susținută prin câteva acțiuni conjugate:

- Definirea de atribuții periodice și punctuale clare;
- Crearea de campanii periodice de informare;
- Instruiri periodice;
- Mesaje de informare privind anumite evenimente cu impact asupra modalitatii de prelucrare a datelor cu caracter personal;
- Asigurarea cadrului optim pentru ca toate politicile create să fie înțelese, asimilate și respectate;
- Discutarea problemelor de GDPR la întâlnirile de lucru cu angajații;
- Rularea periodică de audituri, rapoarte de analiză GAP și analiza a riscurilor;
- Acțiuni de simulare internă sau externă a unor breșe de securitate pentru a vedea gradul de pregătire a echipei de intervenție.

ADMINISTRATOR/DIRECTOR GENERAL,