

**DIRECȚIA GENERALĂ DE EVIDENȚĂ  
A PERSOANELOR - MUNICIPIUL  
BUCUREȘTI**



tel.: 021.306.01.00 , 021.306.01.05  
fax: 021.335.06.69

**Consiliul General al Municipiului București**

Nr. 123 din 07.01.2019

ANEXĂ 3

**REGULAMENT INTERN  
referitor la conformitatea  
DIRECȚIEI GENERALE DE EVIDENȚĂ A PERSOANELOR–MUNICIPIUL BUCUREȘTI  
cu normele GDPR**

***Ce este GDPR ?***

GDPR este **Regulamentul (UE) nr. 679 din 27 aprilie 2016** al Parlamentului European și al Consiliului Uniunii Europene privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date. **Abreviat GDPR – General Data Protection Regulation, iar în limba română RGPD – Regulamentul General pentru Protecția Datelor.**

Prevederile GDPR urmăresc protejarea datelor cu caracter personal ale persoanei fizice, identificată sau identificabilă, direct sau indirect. În textul GDPR, persoana fizică este denumită generic "*persoana vizată*".

Prevederile GDPR stabilesc un **cadru comunitar unitar, nu sunt opționale și vizează toate activitățile din orice sector** sau domeniu, indiferent de dimensiunea business-ului. Măsurile prevăzute influențează toate activitățile care implică informații, mai precis, tot ceea ce ține de prelucrarea datelor cu caracter personal ale persoanelor fizice.

***Când a intrat în vigoare ?***

Regulamentul a intrat în vigoare în anul 2016, cu aplicabilitate începând cu 25 mai 2018.

***Cui se aplică regulamentul?***

Tuturor persoanelor fizice sau juridice, autorități publice, agenții sau alte organisme care procesează sau au acces la date cu caracter personal, în spațiul comunitar și nu numai. Așadar prevederile GDPR vizează orice entitate, indiferent de obiectul său de activitate, inclusiv Direcția Generală de Evidență a Persoanelor - Municipiul București.

### **Cine evaluează?**

În România, Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal – A.N.S.P.D.C.P. în calitate de autoritate publică centrală autonomă, cu competență generală în domeniul protecției datelor personale, reprezintă garantul respectării drepturilor fundamentale la viață privată și la protecția datelor personale.

A.N.S.P.D.C.P. va efectua verificările și va aplica, după caz, sancțiunile în domeniu.

### **Care sunt sancțiunile?**

Sancțiunile prevăzute de regulament sunt extrem de dure. Astfel, sancțiunile financiare prevăzute de GDPR pentru încălcarea dispozițiilor sale de către organizațiile care operează date personale ale persoanelor fizice **pot fi de până la 20 milioane euro sau de până la 4% din cifra de afaceri a anului precedent**, oricare dintre acestea este mai mare.

N.B.: sunt încurajate procesele colective

### **Cum se aplică?**

Regulamentul nu este transpus în legislația internă, până la acest moment și, drept urmare, va fi aplicat ca atare.

Regulamentul poate fi consultat pe site-ul A.N.S.P.D.C.P. [www.dataprotection.ro](http://www.dataprotection.ro)

## **A) NOȚIUNI DE BAZĂ**

### **SINTAGME RELEVANTE UTILIZATE DE GDPR**

✓ **Date cu caracter personal** - orice informație privind o persoană fizică identificată sau identificabilă ("*persoană vizată*"); o persoană fizică este identificabilă direct sau indirect prin referințe la un element de identificare, cum ar fi nume, prenume, date de localizare (*adresa*), CNP, număr de telefon, adresa mail sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale (*este suficientă o caracteristică - de ex: doar nume sau doar număr de telefon*).

✓ **Prelucrare** – orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi, colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea.

✓ **Încălcarea securității datelor** – înseamnă 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.

### **PRINCIPII GDPR**

Principiile sunt guvernate de responsabilitatea prelucrării, **prelucrare care trebuie să fie:**

- **Legală, echitabilă și transparentă**, față de persoana vizată;
- **Efectuată în scop determinat, explicit și legitim**;
- **Adecvată, limitată și relevantă** (reducerea la "*necesar*" a datelor);
- **Exactă** (informațiile să nu conțină erori);
- **Datele să fie păstrate într-o formă care permite identificarea persoanei vizate**;
- **Prelucrarea trebuie să asigure integritatea și confidențialitatea datelor**.

### **LEGALITATEA PRELUCRĂRII**

Prelucrarea datelor cu caracter personal este legală, dacă **cel puțin una dintre condiții** este îndeplinită:

- **Există consimțământul** persoanei vizate;
- **Este necesară pentru executarea unui contract** în care persoana vizată este parte;
- **Este necesară pentru îndeplinirea unei obligații legale** a operatorului;
- **Este necesară pentru protejarea intereselor vitale** ale persoanei vizate;
- **Este necesară pentru îndeplinirea unei sarcini care servește un interes public**;
- **Este necesară în scopul realizării intereselor legitime urmărite de operator.**

#### **DREPTURILE PERSOANEI VIZATE**

Persoana vizată are următoarele **drepturi**, conform GDPR, astfel:

- Dreptul la **informare**;
- Dreptul la **acces**;
- Dreptul la **rectificare**;
- Dreptul la **ștergerea datelor** ("dreptul de a fi uitat");
- Dreptul la **restricționarea prelucrării**;
- Dreptul la **portabilitatea datelor**.

#### **OBLIGAȚIILE OPERATORULUI DE DATE**

Operatorul/procesatorul datelor **trebuie să asigure**:

- *Mijloacele* pentru obținerea consimțământului explicit;
- *Disponibilitatea și rezistența sistemelor* și a serviciilor de prelucrare;
- *Siguranța accesului* la date și a transferului acestora;
- *Numirea unui responsabil* cu protecția datelor;
- *Testarea și evaluarea* periodică;
- *Integritatea și confidențialitatea datelor*;
- *Pseudonimizarea și/sau criptarea datelor*;
- *Evidența prelucrării*;
- *Transmiterea notificărilor de incident* în maxim 72 ore către A.N.S.P.D.C.P.;
- *Restaurarea datelor și a accesului* la acestea în caz de incidente.

#### **B) CONFORMAREA Direcției Generale de Evidență a Persoanelor - Municipiul București LA REGULAMENT**

#### **SCOP**

Direcția Generală de Evidență a Persoanelor - Municipiul București prelucrează date cu caracter personal în **scopul**:

- administrare și prestări servicii;
- relații publice;
- plăți, contabilitate și audituri;

#### **LEGALITATE**

Prelucrarea datelor cu caracter personal se realizează în **mod transparent, cu bună credință, strict raportat la scopul pentru care sunt colectate** datele.

1. Activitatea Direcției Generale de Evidență a Persoanelor - Municipiul București este reglementată de Ordonanța nr. 84 din 30 august 2001 privind înființarea, organizarea și funcționarea serviciilor publice comunitare de evidență a persoanelor, cu modificările și completările ulterioare; OUG 97/2005 privind evidența, domiciliul, reședința și actele de identitate ale cetățenilor români; HG 1375/2006 pentru aprobarea normelor metodologice de aplicare unitară a dispozițiilor legale pentru evidența, domiciliul, reședința și actele de identitate ale cetățenilor români; Legea nr.252/2007 pentru modificarea și completarea unor acte normative care reglementează evidența

persoanelor, eliberarea actelor de identitate și activitatea serviciilor publice comunitare de evidență a persoanelor; Legea nr. 119/1996 cu privire la actele de stare civilă, modificată și completată prin Legea nr. 117/2006. Legea nr. 105/1992 cu privire la reglementarea raporturilor de drept internațional privat, cu modificările și completările ulterioare; Ordonanța nr. 41 /2003 privind dobândirea și schimbarea pe cale administrativă a numelor persoanelor fizice, aprobată prin Legea nr. 323/2003, cu modificările și completările ulterioare; H.G. nr. 839/2006 privind forma și conținutul actelor de identitate, ale autocolantului, privind stabilirea reședinței și ale cărții de imobil, modificată prin H.G. nr. 516/2009; H.G. nr. 220/2006 pentru aprobarea Normelor de lucru privind procurarea și transmiterea în străinătate a certificatelor și extraselor de pe actele de stare civilă, precum și a datelor cu privire la domiciliul și reședința unor persoane; H.G. nr. 64/2011 pentru aprobarea Metodologiei cu privire la aplicarea unitară a dispozițiilor în materie de stare civilă; Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, cu modificările și completările ulterioare; Legea nr. 544/2001 privind liberul acces la informațiile de interes public, cu modificările și completările ulterioare; Legea nr. 201/02.06.2009 pentru modificarea și completarea Legii nr. 119/1996 cu privire la actele de stare civilă, cu modificările și completările ulterioare; Legea nr. 243/23.06.2009 pentru modificarea și completarea O.U.G. nr. 97/2005 privind evidența, domiciliul, reședința și actele de identitate ale cetățenilor români, pentru modificarea O.G. nr. 84/2001 privind înființarea, organizarea și funcționarea serviciilor publice comunitare de evidență a persoanelor, precum și pentru modificarea și completarea O.G. nr. 41/2003 privind dobândirea și schimbarea pe cale administrativă a numelor persoanelor fizice; Legea nr. 329/2009 privind reorganizarea unor autorități și instituții publice, rationalizarea cheltuielilor publice, susținerea mediului de afaceri și respectarea acordurilor-cadru cu Comisia Europeană și Fondul Monetar; Legea nr. 117/1999 privind taxele extrajudiciare de timbru, cu modificările și completările ulterioare; Hotărârea 175/2010 a Consiliului General al Municipiului București.

În conformitate cu prevederile Regulamentului, Direcția Generală de Evidență a Persoanelor - Municipiul București prelucrează date cu caracter personal în temeiul: îndeplinirii unei obligații legale, intereselor legitime, executării unui contract la care persoana vizată este parte sau consimțământului.

### **PERSOANE ȘI FLUXURI**

În perspectiva Direcției Generale de Evidență a Persoanelor - Municipiul București sunt de luat în considerare următoarele aspecte, legate de datele cu caracter personal, respectiv:

#### **Persoane fizice:**

- Clientul extern;
- Clientul intern, salariatul.

#### **Flux date cu caracter personal pe suport:**

- Electronic (stații, servere, CD/DVD, memory-stick-uri, aplicații, comunicații etc.)
- Letric (pe suport de hârtie – fișe, formulare, borderouri, dosare etc.)

## **CATEGORII DE DATE PRELUCRATE**

Date utilizate:

- ✓ În cazul *clientului extern*, Direcția Generală de Evidență a Persoanelor - Municipiul București utilizează date cu caracter personal necesare efectuării serviciilor (arătate anterior, la scop), cu precădere : nume, prenume, adresă poștală, telefon, adresă email.
- ✓ În cazul *clientului intern*, sunt utilizate date cu caracter personal necesare îndeplinirii obligațiilor Direcției Generale de Evidență a Persoanelor - Municipiul București în calitate de angajator, inclusiv date personale necesare în procesul de medicină a muncii. Gradul de senzitivitate al acestor date cu caracter personal este mai ridicat.

## **TRANSFERUL DE DATE**

Direcția Generală de Evidență a Persoanelor - Municipiul București, în calitate de operator de date cu caracter personal, nu transferă către terți baze de date cu caracter personal ale persoanelor fizice, cu excepția situațiilor în care datele cu caracter personal sunt solicitate de entități publice, în condițiile legii.

## **STOCAREA DATELOR**

Datele sunt stocate în fișete, dulapuri, cameră de arhivă etc. pe suport:

- **Letric** (hârtie, dosare, registre, registre acces clădire, etc.);
- **Electronic** ( servere, CD-uri, DVD-uri, memory-stick-uri, etc.)

Datele stocate sau arhivate trebuie protejate împotriva riscurilor de alterare în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau de accesul neautorizat.

Pentru toate zonele de stocare a datelor, vor fi dispuse măsuri concrete de securitate fizică, după caz:

- ✓ Fișete, dulapuri etc. închise – marcarea cu afișe "*Acces restricționat*";
- ✓ Camere de arhivă – control acces (electronic), inclusiv monitorizare video și/sau EMF (yale, lacăt, gratii și folie securizată pentru ferestre etc.) și completare de registru acces (în toate cazurile);
- ✓ Nominalizarea salariaților care au acces la datele cu caracter personal stocate/arhivate;
- ✓ Verificarea măsurilor anti incendiu și asigurarea împotriva inundațiilor;

Măsurile cibernetice de securitate vor viza soluții precum : malware, "*troieni*", spywares, penetrare cibernetică etc.

## **CONDIȚII**

Pentru realizarea operațiunilor de pseudonimizare, anonimizare sau ștergere a datelor, în anumite situații individuale (decizii de impunere, somații ori diverse acte procedurale), solicitările referitoare la datele cu caracter personal trebuie adresate deținătorilor legali ai bazelor de date cu caracter personal (parteneri contractuali ai Direcției Generale de Evidență a Persoanelor - Municipiul București ).

Solicitarea persoanei vizate trebuie să fie transmisă în 48 de ore de la primire (cu celeritate) către C.M.T.I.B. S.A.

## **MINORII**

Prevederile speciale referitoare la minori: orice prelucrare de date cu caracter personal ale minorilor se va realiza numai în condițiile legii.

## **RECLAMAȚIE vs. NOTIFICARE DATE**

În relația cu clienții este important ca toți salariații Direcției Generale de Evidență a Persoanelor - Municipiul București să poată face distincția dintre o reclamație referitoare la serviciile prestate

clienților (și eventual, conținutul acestora) unde intră în funcțiune mecanismul de soluționare al reclamațiilor și o plângere/notificare referitoare la datele cu caracter personal.

Pentru soluționarea solicitărilor referitoare la prelucrarea datelor cu caracter personal adresate Direcției Generale de Evidență a Persoanelor - Municipiul București persoana vizată trebuie să facă dovada faptului că a beneficiat de serviciile Direcției Generale de Evidență a Persoanelor - Municipiul București.

În cazul în care notificarea se va dovedi întemeiată, în termen de 72 de ore, C.M.T.I.B. va informa Autoritatea de supraveghere. De asemenea, clientul se poate adresa direct Autorității sau instanței de judecată, pentru apărarea drepturilor și libertăților sale fundamentale.

### C) DATE SENSIBILE

#### **INFORMAȚII CU CARACTER GENERAL**

La nivelul fiecărei structuri organizatorice a Direcției Generale de Evidență a Persoanelor - Municipiul București se impune o revizuire a procedurilor și a instrucțiunilor de lucru pentru asimilarea modificărilor legislative apărute, inclusiv pentru cerințele Regulamentului (UE) nr. 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date.

În toate cazurile, bazele de date conținând date cu caracter personal, arhivate pe suport letric și pe suport electronic, trebuie păstrate conform termenelor legale și termenelor de arhivare. Toți salariații trebuie să verifice ce categorii de date dețin și, dacă este cazul, să ia măsurile ce se impun - securizare și arhivare, modificare, anulare sau distrugere etc.

În cazul în care deținerea anumitor date cu caracter personal nu este justificată (expirare termen de arhivare, încheiere campanie de marketing/vânzări etc.), ele trebuie modificate sau anulate prin pseudonimizare sau anonimizare, ori distruse în cazul arhivelor letrice fiind potențiale breșe de securitate.

Bazele de date electronice menținute, care conțin date cu caracter personal, vor fi asigurate împotriva: incendiilor, inundației, furtului, utilizării accidentale, malware, "troieni", spywares, penetrare cibernetică etc.

În procedura de arhivare electronică, se va evita redundanța (dublarea) bazelor de date.

În cadrul Direcției Generale de Evidență a Persoanelor - Municipiul București există/vor exista structuri organizatorice care prelucrează de date cu caracter personal ale clientului intern (salarat) și ale clientului extern.

Direcția Generală de Evidență a Persoanelor - Municipiul București deține și prelucrează datele personale ale angajaților, obținute în procesele de recrutare, angajare, executare și încetare a contractelor individuale de muncă etc.

Datele personale ale salariaților, atât cele în format electronic, cât și cele în format letric, vor fi tratate cu maximă atenție (securizare arhive, restricționarea accesului și controlul salariaților care au acces și operează cu date cu caracter personal, eliberare adeverințe etc.); datele cu caracter personal aflate pe suport letric (ex: fișe post, dosar personal al salariatului etc.) vor fi asigurate corespunzător în fișete/ dulapuri, ce pot fi închise cu cheie/ lacăt, cu mențiunea "Acces restricționat".

De asemenea, cu suportul IT, se impune securizarea aplicațiilor, serverelor și comunicațiilor utilizate, inclusiv a bazelor de date electronice.

Arhivarea documentelor de la Serviciul Resurse Umane pe suport letric sau electronic va fi efectuată pentru o perioadă corespunzătoare, conform prevederilor legale în vigoare. Vor fi implementate măsuri de asigurare a datelor arhivate împotriva distrugerii, pierderii, modificării, divulgării neautorizate sau accesului neautorizat, în mod accidental sau ilegal.

✓ procedura de recrutare derulată prin Serviciul Resurse Umane presupune consimțământul expres și neechivoc al candidatului anterior și în scopul participării la procedura de selecție. Acordul poate fi luat în baza unei declarații sau a unui formular tipizat, predefinit. Serviciul Resurse Umane va decide și va comunica formularul de acordare a consimțământului;

- ✓ datele personale ale salariaților vor fi comunicate terților (instituții bancare, campanii de marketing etc.) doar cu consimțământul prealabil al angajaților, cu excepția situațiilor expres prevăzute de lege (solicitări scrise - poliție, parchet, instanță etc)
- ✓ orice prelucrare sau transmitere, în orice mod, a datelor cu caracter personal care excede obligației legale a angajatorului, presupune consimțământul prealabil al salariatului/salariaților.

O alta categorie de date cu caracter personal prelucrate sunt:

- state salarii,
- adeverințe venit,
- fișe fiscale etc.

În prelucrarea acestor date se impune respectarea unor proceduri clare, care prevăd sau trebuie să prevadă securitatea operațiunilor, prin: desemnarea nominală a salariaților care au acces la aceste date, securizarea stațiilor de lucru, a token-urilor și a aplicațiilor, acordarea de parole etc.

Și în acest caz, datele cu caracter personal, aflate pe suport letric sau electronic, vor fi asigurate corespunzător în fișete/ dulapuri, ce pot fi închise cu yală/ lacăt, cu mențiunea "Acces restricționat".

Arhivarea documentelor care conțin aceste tipuri de date pe suport letric sau electronic va fi făcută conform prevederilor legale în vigoare și procedurilor de arhivare, în încăperi încuiate, cu acces limitat și monitorizat. Vor fi implementate măsuri de asigurare a datelor arhivate împotriva distrugerii, pierderii, modificării, divulgării neautorizate sau accesului neautorizat, în mod accidental sau ilegal.

✓ Este recomandat a fi utilizat formularul pentru consimțământul angajatului elaborat de Serviciul Resurse Umane cu mențiunea că salariatul va trebui să indice clar și neechivoc scopul pentru care și-a dat consimțământul;

✓ Comunicațiile dintre Direcția Generală de Evidență a Persoanelor - Municipiul București și instituțiile bancare, în legătură cu datele cu caracter personal se vor face într-un mod securizat. În principiu, vor fi utilizate canale de comunicare securizate, fișiere criptate, token-uri etc.

Direcția Generală de Evidență a Persoanelor - Municipiul București asigură prelucrarea datelor cu caracter personal în condiții de siguranță prin implementarea de politici, proceduri, echipamente și soluții software și hardware care să elimine posibilitatea accesului neautorizat la baze de date, comunicații sau informații ce conțin date cu caracter personal ale persoanelor fizice, client intern și/sau client extern.

În procedura de arhivare electronică, se va evita redundanța (dublarea) bazelor de date.

Din punct de vedere IT se vor implementa/actualiza politicile și procedurile de lucru pentru conformarea la normele GDPR.

Totodată, din punct de vedere tehnic se va asigura o politică de dezvoltare a capabilităților Direcției Generale de Evidență a Persoanelor - Municipiul București în sensul reducerii „riscurilor prezentate de prelucrarea datelor, generate în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau de accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod”.

Direcția Generală de Evidență a Persoanelor - Municipiul București deține și prelucrează date contractuale cuprinse în convențiile încheiate de Direcția Generală de Evidență a Persoanelor - Municipiul București cu partenerii săi, persoane juridice sau persoane fizice autorizate, în general.

Sub acest aspect sunt reglementate contractual, operațiunile de prelucrare a datelor cu caracter personal:

- ✓ La încheierea contractelor se vor insera în cuprinsul acestora prevederi prin care se vor stabili drepturi și obligații ale părților contractante referitoare la protecția datelor cu caracter personal ori se va propune partenerilor Direcției Generale de Evidență a Persoanelor - Municipiul București agrearea unor anexe tehnice;
- ✓ Actualizarea contractelor existente prin agrearea unor anexe tehnice care conțin clauze în concordanță cu prevederile GDPR;
- ✓ Oricare altă situație referitoare la prevederile GDPR în raporturile contractuale va avea suportul structurilor menționate anterior.

De asemenea, se va avea în vedere că datele cu caracter personal ale persoanelor fizice care sunt stocate și nu au acordul persoanelor conform GDPR, să fie modificate sau anulate prin pseudonimizare sau anonimizare, ori distruse, în cazul arhivelor letrice, acestea fiind potențiale breșe de securitate.

### **COMPARTIMENT SSM, PSI**

Volumul mare de date cu caracter personal este colectat în procesul de medicină a muncii și conține date ale clientului intern, salariați ai Direcției Generale de Evidență a Persoanelor - Municipiul București.

Având în vedere că datele de medicină a muncii sunt extrem de sensitive, măsurile trebuie să prevadă:

- ✓ prin contractul/actele adiționale încheiate cu prestatorul de servicii de medicină a muncii, respectarea prevederilor GDPR (UE) nr. 679/ 2016;
  - ✓ salariații Direcției Generale de Evidență a Persoanelor - Municipiul București cu atribuții SSM trebuie nominalizați și monitorizați pentru ca datele cu caracter personal ale angajaților Direcției Generale de Evidență a Persoanelor - Municipiul București să fie utilizate potrivit scopului;
  - ✓ stațiile de lucru (PC) care stochează baze de date sensitive să aibă un acces și o utilizare controlate;
  - ✓ fișierele conținând date sensitive vor trebui securizate individual, prin parole complexe, astfel încât datele să nu fie distruse sau comunicate ilegal, în mod accidental sau intenționat;
  - ✓ de asemenea, datele cu caracter personal aflate pe suport letric/ CD/ DVD/ memory-stick vor fi asigurate corespunzător în fișete/ dulapuri, ce pot fi închise cu cheie/ lacăt, cu mențiunea "Acces restricționat".
  - ✓ camerele (birouri) de lucru vor fi asigurate împotriva efracției.
- Serviciul prevenire, protecție și PSI va asigura suportul în menținerea măsurilor PSI implementate, cu precădere arhive.

### **INFORMAREA PUBLICULUI**

În vederea informării persoanelor care apelează la serviciile Direcției Generale de Evidență a Persoanelor - Municipiul București, vor fi transmise afișe de comunicare/atenționare cu privire la intrarea în vigoare a Regulamentului, în toate spațiile Direcției.

Informarea publicului referitoare la intrarea în vigoare a Regulamentului va fi disponibilă și pe site-ul Direcției Generale de Evidență a Persoanelor - Municipiul București sau prin intermediul salariaților.

### **INFORMAREA SALARIAȚILOR**

Va fi asigurată prin e-mail.



## D) CUM VERIFICĂM CONFORMITATEA?

### **RESPONSABILITATEA**

Responsabilitatea este elementul definitoriu al conformării; responsabilitatea se demonstrează prin dovezi obiective.

Într-o primă etapă, se impune implementarea de măsuri de informare, instruire și conștientizare – client intern (și client extern).

În a doua etapă, sunt analizate procesele derulate în cadrul fiecărei structuri.

Atunci când sunt prelucrate date cu caracter personal, verificați:

- ✓ Instruirea salariaților pe care îi coordonați (PV arhivat în cadrul structurii);
- ✓ Existența și respectarea procedurilor; în cazul în care se impune, revizuiți procedurile;
- ✓ Limitarea fluxului de date cu caracter personal, la "strictul necesar" pentru executarea activității; acest aspect trebuie avut în vedere și la încheierea contractelor;
- ✓ Limitarea numărului de salariați care au acces la date cu caracter personal, precum și a celor care prelucrează date cu caracter personal;
- ✓ Determinați care salariați prelucrează date cu caracter personal și ce fel de date prelucrează (cât de sensibile sunt acele date), precum și dacă sunt transferate sau recepționate date cu caracter personal ale persoanelor fizice;
- ✓ Păstrați dovezi ale prelucrării conform politicilor, procedurilor, normelor și instrucțiunilor în vigoare;
- ✓ Cum sunt arhivate datele electronice și cele în format letric și care este perioada de arhivare;
- ✓ Securitatea fizică a spațiilor de lucru/birouri etc. – yale, extincitoare, senzori mișcare și anti incendiu, camere video, control acces, extincitoare etc., după caz;
- ✓ Respectarea politicilor și procedurilor IT comunicate.

Atunci când considerați că măsurile luate nu acoperă toate riscurile potențiale la adresa securității prelucrării datelor cu caracter personal ale persoanelor fizice – salariați, clienți și/sau furnizorilor, dați-vă răspunsul la următoarele **3 întrebări**, valabile în toate cazurile:

- Măsurile tehnice și organizatorice există și sunt adecvate? În caz contrar vă rugăm să vă adresați superiorului ierarhic sau cu e-mail către DPO.
- Măsurile tehnice și organizatorice sunt utilizate? Aspectele de organizare (instruire/informare, verificarea respectării instrucțiunilor/procedurilor) țin de șeful locului de muncă, iar cele tehnice de zonele: IT sau departamentul GDPR.
- Măsurile tehnice și organizatorice funcționează așa după cum au fost proiectate ? În caz contrar identificați cauza și dați dispozițiile necesare sau vă adresați structurii tehnice abilitate ori transmiteți un e-mail.

### **CODUL DE CONDUITĂ**

Prin textul Regulamentului sunt încurajate demersuri pentru:

- Realizarea de Coduri de conduită ce reprezintă norme de implementare a GDPR, elaborate de asociații organizaționale sau alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori
- Instituirea de Mecanisme de certificare în domeniul protecției datelor, precum și sigilii și mărci în acest domeniu, care să permită demonstrarea faptului că operațiunile de prelucrare efectuate de operatori și de persoanele împuternicite de operatori respectă Regulamentul.

Normele de conduită profesională prevăzute de Codul de conduită sunt obligatorii pentru toate persoanele care lucrează în cadrul instituției.

## **RESPONSABILUL CU PROTECȚIA DATELOR**

Conform Regulamentului acesta trebuie numit și comunicat intern și extern, inclusiv în relația cu Autoritatea de Supraveghere.

La nivelul Direcției Generale de Evidență a Persoanelor - Municipiul București, responsabilul cu protecția datelor va fi nominalizat și comunicat de către persoana împuternicită – C.M.T.I.B. S.A. .

**Atribuțiile responsabilului cu protecția datelor sunt:**

- **Informare și consiliere internă** cu privire la dispozițiile Regulamentului
- **Monitorizarea** respectării RGDP în cadrul Direcției Generale de Evidență a Persoanelor - Municipiul București
- **Consiliere în evaluarea impactului** asupra datelor (analiză de risc/de impact)
- **Cooperare cu Autoritatea de supraveghere**
- **Deschiderea unui registru unic** de incidente privind protecția datelor cu caracter personal în cadrul Direcției Generale de Evidență a Persoanelor - Municipiul București
- **Efectuarea de evaluări și audituri** interne în cadrul Direcției Generale de Evidență a Persoanelor - Municipiul București

## **EVALUARE ȘI CONTROL**

Evaluarea va fi efectuată prin misiuni de audit intern și extern. Este de menționat faptul că, în afara auditurilor externe de certificare și a celor de supraveghere, pot exista și audituri solicitate de partenerii contractuali ai Direcției Generale de Evidență a Persoanelor - Municipiul București.

Scopurile auditului vor fi : evaluarea impactului măsurilor implementate de Direcția Generală de Evidență a Persoanelor - Municipiul București asupra prelucrării datelor cu caracter personal, respectiv modul de gestionare a riscurilor din acest domeniu, precum și calitatea actului de control.

În final, menționăm faptul că nici o măsură de securitate nu este 100% sigură, însă un mix de măsuri tehnice și organizatorice, monitorizate constant, pot limita semnificativ expunerea la risc a Direcției Generale de Evidență a Persoanelor - Municipiul București în ceea ce privește prelucrarea datelor cu caracter personal ale persoanelor fizice.

Acest Regulament intern abordează intrarea în vigoare a Regulamentului GDPR și identificarea potențialelor zone de risc în activitatea curentă a Direcției Generale de Evidență a Persoanelor - Municipiul București.

*DIRECȚIA EVIDENȚA PERSOANELOR*  
DIRECTOR EXECUTIV AD. II INCT

*DIRECȚIA STARE CIVILĂ*  
DIRECTOR EXECUTIV ADJUNCT

*DIRECȚIA ECONOMICĂ*

*SERVICIUL RESURSE UMANE*

*BIROUL JURIDIC*

*SERVICIUL RELAȚII PUBLICE*