
POLITICA DE PRELUCRARE A DATELOR CU CARACTER PERSONAL LA NIVELUL CENTRULUI PENTRU TINERET AL MUNICIPIULUI BUCUREȘTI

1. Introducere

Această Politică privind Prelucrarea și Protecția Datelor cu Caracter Personal (denumită în continuare "Politica") definește procedura de prelucrare și protecție a datelor cu caracter personal în cadrul Centrului pentru Tineret al Municipiului București (denumită în continuare "Operator"), și stabilește procedurile care vizează prevenirea și evidențierea oricăror încălcări ale legii aplicabile cu privire la datele cu caracter personal.

Această Politică a fost elaborată în conformitate cu legislația României și a Uniunii Europene, în special cu următoarele documente:

- a) Regulamentul General de Protecția Datelor (GDPR), adoptat de Parlamentul European și de Consiliul European la 27 Aprilie 2016;
- b) Orice altă lege locală privind protecția datelor cu caracter personal ce se aplică în România.

2. Scopul politicii de protecție a datelor

Scopurile principale ale Politicii sunt următoarele:

- a) Stabilirea unei proceduri, precum și a termenilor și condițiilor privind prelucrarea datelor cu caracter personal, inclusiv procedurile care vizează prevenirea încălcării legilor și procedurilor de realizare a controlului intern în conformitate cu legislația aplicabilă privind datele cu caracter personal
- b) Prezentarea personalului Operatorului responsabil cu prelucrarea datelor cu caracter personal, a Politicii aplicabile cu privire la datele cu caracter personal și a cerințelor privind prelucrarea datelor cu caracter personal
- c) Stabilirea responsabilităților pentru personalul care prelucrează datele cu caracter personal în cazul nerespectării legii aplicabile privind datele cu caracter personal
- d) Respectarea dreptului subiecților de a fi informați asupra modalității în care operatorul prelucrează datele lor cu caracter personal

Astfel, scopul acestei Politici este să explice care sunt datele cu caracter personal pe care le prelucrăm, de ce le prelucrăm, precum și ce facem cu acestea. Având în vedere faptul că informațiile personale aparțin fiecărui utilizator, facem tot posibilul să le stocăm în siguranță și să le prelucram cu atenție. Nu oferim informații unor părți terțe fără a ne îndeplini obligația prealabilă de informare.

3. Domeniul de aplicare și modificare a politicii de protecție a datelor

Această politică de protecție a datelor se aplică operatorului și angajaților acestuia. Politica privind protecția datelor se extinde la toate prelucrările de date cu caracter personal.

Această politică de protecție a datelor poate fi modificată doar sub coordonarea directă a Responsabilului de Protecție a Datelor (DPO) desemnat la nivelul operatorului.

Cea mai recentă versiune a politicii de protecție a datelor poate fi accesată cu informațiile privind confidențialitatea datelor pe site-ul operatorului Centrul pentru Tineret al Municipiului București.

4. Definiții de bază

În sensul prezentei Politici, se folosesc următoarele definiții:

- a) “Responsabil cu Protecția Datelor (DPO)” înseamnă o persoană care este responsabilă cu monitorizarea aplicării GDPR și a altor legi aplicabile privind protecția persoanelor vizate de prelucrarea datelor cu caracter personal și care exercită funcțiile care îi sunt atribuite de prezenta Politică și de altă legislație aplicabilă, furnizează consultanța managementului Operatorului cu privire la protecția datelor cu caracter personal.
- b) “Date cu caracter personal” înseamnă orice informații privind o persoană fizică identificată sau identificabilă (“persoana vizată”); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale ale acelei persoane.
- c) “Prelucrare” înseamnă 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 alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea.
- d) “Restricționarea prelucrării” înseamnă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora.
- e) “Creare de Profiluri” înseamnă 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 performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia.
- f) “Operator” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal.
- g) “Persoana împuternicită de operator” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului.
- h) “Destinatar” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță.

- i) “Parte terță” înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucrez date cu caracter personal.
- j) “Consimțământ” al persoanei vizate 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, că datele cu caracter personal care o privesc să fie prelucrate.
- k) “Încălcarea securității datelor cu caracter personal” 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.
- l) “Date privind sănătatea” înseamnă 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.
- m) “Prelucrarea transfrontalieră” înseamnă fie prelucrarea datelor cu caracter personal care are loc în contextul activităților sediilor din mai multe state membre ale unui operator sau ale unei persoane împuternicite de operator pe teritoriul Uniunii, dacă operatorul sau persoana împuternicită de operator are sedii în cel puțin două state membre; sau fie prelucrarea datelor cu caracter personal care are loc în contextul activităților unui singur sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, dar care afectează în mod semnificativ sau este susceptibilă de a afecta în mod semnificativ persoane vizate din cel puțin două state membre.

5. Principii de prelucrare a datelor cu caracter personal

5.1 Corectitudinea și legalitatea

Operatorul protejează drepturile individuale ale persoanelor fizice (“Persoana vizată”) cu ocazia prelucrării datelor cu caracter personal, datele cu caracter personal fiind colectate și prelucrate în mod legal și corect.

“Legalitatea” – presupune identificarea bazei legale înainte de prelucrarea datelor cu caracter personal. Acestea sunt denumite adesea „condițiile de prelucrare”, de exemplu, consimțământul.

“Corectitudinea” – pentru ca prelucrarea datelor să fie corectă, operatorul de date trebuie să facă anumite informații disponibile pentru Persoanele vizate. Aceasta se aplică indiferent dacă datele cu caracter personal au fost obținute direct de la persoanele vizate sau din alte surse.

5.2 Restricții la un anumit scop („limitări legate de scop”)

Datele cu caracter personal sunt prelucrate numai în scopul definit înainte de începerea colectării datelor. Modificările ulterioare ale scopului sunt posibile doar cu titlu excepțional, într-o măsură limitată și necesită o fundamentare.

5.3 Transparența

Persoana vizată este informată cu privire la modul în care sunt prelucrate datele sale. În general, datele cu caracter personal sunt colectate direct de la persoana în cauză. Atunci când datele sunt colectate, Persoana vizată trebuie să fie conștientă sau să fie informată despre:

- a) Identitatea Operatorului de Date
- b) Scopul prelucrării datelor
- c) Terțe părți sau categorii de terțe părți cărora le-ar putea fi transmise datele.

5.4 Reducerea prelucrării datelor și economia colectării datelor („reducerea la minimum a datelor”);

Înainte de prelucrarea datelor cu caracter personal, se va determina dacă și în ce măsură prelucrarea datelor cu caracter personal este necesară pentru atingerea scopului pentru care este efectuată. Atunci când scopul permite acest lucru și unde cheltuielile implicate sunt proporționale cu scopul urmărit, sunt utilizate date anonime sau statistice. Datele cu caracter personal nu sunt colectate în avans și stocate în scopuri potențiale viitoare, cu excepția cazului în care acest lucru este impus sau permis de legislația în vigoare.

5.5 Ștergerea

Datele personale care nu mai sunt necesare după expirarea perioadelor legate de procesele legale sau de afaceri sunt șterse. În cazul în care sunt identificate indicii cu privire la existența unor interese care necesită protejarea sau legate de importanța istorică a acestor date în cazuri individuale, este posibil ca operatorul să păstreze datele până când interesele care merită protejate au fost clarificate în mod legal, sau arhiva internă a evaluat datele pentru a determina dacă trebuie păstrate în scopuri istorice/ arhivistice. Atunci când ștergerea datelor poate avea impact asupra sistemelor informatice ale operatorului, datele vor fi anonimizate ireversibil, astfel încât să nu mai existe indicii care să poată conduce la identificarea persoanei vizate.

5.6 Precizia faptică; actualizarea datelor („exactitate”)

Datele cu caracter personal trebuie să fie corecte, complete și, dacă este necesar, să fie actualizate. Operatorul ia măsuri adecvate pentru a se asigura că datele eronate sau incomplete sunt șterse, corectate, completate sau actualizate.

5.7 Confidențialitatea și securitatea datelor („integritate și confidențialitate”).

Datele cu caracter personal sunt supuse obligațiilor legale de păstrare a secretului datelor.

Acestea trebuie să fie tratate ca fiind confidențiale de fiecare angajat al Operatorului și sunt asigurate măsuri organizatorice și tehnice adecvate pentru a preveni accesul neautorizat, prelucrarea sau distribuția ilegală, precum și pierderea accidentală, modificarea sau distrugerea.

5.8 Principiul răspunderii conform GDPR

GDPR include prevederi care promovează răspunderea și guvernanta. Acestea completează cerințele de transparență ale GDPR. Principiul răspunderii din Articolul 5 (2) din GDPR solicită ca operatorul să demonstreze că respectă principiile și specifică explicit că aceasta este responsabilitatea operatorului.

Operatorul va dovedi conformitatea cu principiile de protecția datelor prin implementarea politicilor de protecția datelor, respectarea codurilor de conduită, implementarea unor măsuri tehnice și organizaționale, precum și adoptarea unor tehnici precum protecția datelor, procedura de notificare a încălcării și planuri de răspuns la incidente.

6. Temeiurile prelucrării datelor

Colectarea, prelucrarea și utilizarea datelor cu caracter personal este permisă numai în temeiurile enumerate mai jos:

a. Date despre parteneri și prestatorii de servicii

a.1. Prelucrarea datelor pentru executarea unui contract sau prestarea unui serviciu

Datele personale ale persoanelor de contact și reprezentanților prestatorilor pot fi procesate pentru a stabili, executa și înceta un contract. Înainte de semnarea contractului - în timpul fazei de inițiere a contractului - datele personale pot fi prelucrate pentru a îndeplini cerințe din perspectiva care se referă la încheierea contractului. Persoanele de contact pot fi contactate în timpul procesului de pregătire a contractului, utilizând doar informațiile pe care acestea le-au furnizat pentru contactare. Orice restricții solicitate de persoanele de contact respective trebuie să fie respectate.

a.2. Consimțământul ca temei al prelucrării datelor

Atunci când este necesar consimțământul persoanelor vizate, datele pot fi prelucrate după primirea acordului persoanei vizate. Consimțământul trebuie obținut în scris sau în format electronic în scopul documentării. În anumite circumstanțe, cum ar fi conversațiile telefonice, consimțământul poate fi dat verbal. Este obligatorie documentarea acordării consimțământului.

a.3. Prelucrarea datelor în conformitate cu obligația legală

Prelucrarea datelor cu caracter personal este permisă și în cazul în care legislația aplicabilă solicită, impune sau permite acest lucru. Tipul și amploarea procesării datelor trebuie să fie necesare pentru activitatea legală de prelucrare a datelor și trebuie să respecte dispozițiile legale relevante.

a.4. Prelucrarea datelor în conformitate cu interesele legitime

Datele cu caracter personal pot fi procesate și în cazul în care acest lucru este necesar pentru un interes legitim al operatorului. Interesele legitime sunt în general de natură juridică (de exemplu, colectarea creanțelor restante) sau comerciale (de exemplu, evitarea încălcărilor contractului). Datele cu caracter personal nu pot fi prelucrate în scopul unui interes legitim dacă, în cazuri individuale, există dovezi conform cărora interesele persoanei vizate merită

protecție și că aceasta are prioritate. Înainte de prelucrarea datelor, este necesar să se determine dacă există interese care merită protejate.

a.5. Prelucrarea datelor sensibile

Operatorul nu prelucrează nicio informație referitoare la rasă, națiune, opinii politice, credințe religioase sau filosofice, intimitate, viață privată.

Datele cu caracter personale sensibile pot fi prelucrate numai dacă legea impune acest lucru sau dacă persoana vizată și-a dat consimțământul în mod expres. Aceste date pot fi, de asemenea, prelucrate dacă o asemenea prelucrare este obligatorie pentru recunoașterea, exercitarea sau apărarea drepturilor legale referitoare la persoana vizată. Dacă în cadrul operatorului există planuri de prelucrare a datelor extrem de sensibile, Responsabilul cu Protecția Datelor trebuie informat în prealabil.

Dacă datele cu caracter personal sunt colectate, prelucrate și utilizate, persoanele vizate trebuie să fie informate despre aceasta printr-o declarație de confidențialitate și, dacă este cazul, să li se pună la dispoziție informații despre cookie-uri. Declarația de confidențialitate și orice informație privind modulele cookie trebuie să fie integrate astfel încât să fie ușor de identificat, direct accesibile și disponibile în mod consecvent pentru persoanele vizate.

b. Datele angajatului/viitorilor angajați

b.1. Prelucrarea datelor pentru relația de muncă

În relațiile de muncă, datele cu caracter personal pot fi prelucrate, dacă este necesar, pentru inițierea, executarea și încetarea contractului de muncă. La inițierea unui raport de muncă, datele personale ale solicitanților vor fi procesate. În cazul în care candidatul este respins, datele sale trebuie șterse în conformitate cu perioada de păstrare necesară, cu excepția cazului în care solicitantul a fost de acord să rămână la dosar pentru un viitor proces de selecție pentru o perioadă de 6 luni de la data aplicării. De asemenea, este necesar consimțământul pentru utilizarea datelor pentru procesele de aplicare suplimentare sau înainte de partajarea aplicației cu alte companii din grup.

În raportul de muncă existent, prelucrarea datelor trebuie să se refere întotdeauna la scopul contractului de muncă dacă nu se aplică niciuna dintre următoarele circumstanțe pentru prelucrarea datelor autorizate.

Dacă în timpul procedurii de solicitare ar trebui să fie necesară colectarea de informații despre un solicitant de la o terță parte, trebuie respectate cerințele legilor naționale corespunzătoare. În caz de îndoială, trebuie obținut un acord de la persoana vizată.

Trebuie să existe o autorizație legală pentru prelucrarea datelor cu caracter personal care au legătură cu relația de muncă, dar care nu a făcut parte inițial din executarea contractului de muncă. Acestea pot include cerințe legale, reglementari colective cu reprezentanții angajaților, consimțământul angajatului sau interesul legitim al companiei.

b.2. Prelucrarea datelor în conformitate cu obligația legală

Prelucrarea datelor personale ale angajaților este permisă și în cazul în care legislația națională solicită și impune acest lucru. Tipul și amploarea procesării datelor trebuie să fie necesare pentru activitatea legală de prelucrare a datelor și trebuie să respecte dispozițiile legale relevante. Dacă există o anumită flexibilitate juridică, trebuie luate în considerare interesele angajatului care merită protejate.

b.3. Consimțământul la prelucrarea datelor

Acolo unde este necesar, datele angajatului pot fi prelucrate după consimțământul persoanei în cauză. Declarațiile de consimțământ trebuie prezentate în mod voluntar. Acordul involuntar este nul. Declarația de consimțământ trebuie obținută în scris sau în format electronic și va fi păstrată de operator. În anumite circumstanțe, consimțământul poate fi dat verbal, caz în care trebuie să fie documentat ulterior corespunzător. În cazul furnizării informate și voluntare de date de către partea relevantă, se poate presupune existența unui acord, dacă legislația națională nu solicită consimțământul expres.

Prin „consimțământ” se înțelege că persoana vizată și-a dat acordul pentru prelucrarea datelor cu caracter personal cu privire la propria persoană. Persoana vizată își poate retrage consimțământul în orice moment prin trimiterea unui email la: contact@ctmb.eu

b.4. Prelucrarea datelor în baza unui interes legitim

Datele personale pot fi procesate și în cazul în care este necesar să se impună un interes legitim al operatorului. Interesele legitime sunt în general de natură juridică (*de exemplu, depunerea, aplicarea sau apărarea împotriva unor acțiuni legale*) sau financiare (*de exemplu, evaluarea întreprinderilor*).

Datele cu caracter personal nu pot fi prelucrate pe baza unui interes legitim dacă, în cazuri individuale, există dovezi că interesele angajatului merita protecție. Înainte de procesarea datelor, trebuie să se determine dacă există interese care merită protejate.

Măsurile de control care necesită prelucrarea datelor angajatului pot fi luate numai dacă exista o obligație legală în acest sens sau dacă există un motiv legitim. Chiar dacă există un motiv legitim, trebuie examinată și proporționalitatea măsurii de control. Interesele justificate ale Operatorului (de exemplu, respectarea dispozițiilor legale și a reglementărilor interne ale instituției) trebuie să fie cântărite în raport cu interesele angajatului care trebuie protejate și care pot fi afectate de măsura de control ce urmează a fi adoptată. Interesul legitim al instituției și orice interese ale angajatului care merită protejat trebuie să fie identificate și documentate înainte de luarea oricăror măsuri. În plus, trebuie luate în considerare orice cerințe suplimentare din legislația națională (de exemplu, drepturile de co-decizie pentru reprezentanții angajaților și drepturile de informare ale persoanelor vizate).

b.5. Prelucrarea datelor personale sensibile

Datele personale sensibile pot fi procesate numai în anumite condiții. Datele personale sensibile sunt date despre originea rasială și etnică, convingerile politice, convingerile religioase sau filozofice, calitatea de membru al unei uniuni/formațiuni și sănătatea și viața

sexuală a persoanei vizate. În conformitate cu legislația națională, alte categorii de date pot fi considerate sensibile sau conținutul categoriilor de date poate fi completat diferit. Mai mult, datele care se referă la o infracțiune pot fi procesate numai în conformitate cu cerințele speciale din legislația națională.

Prelucrarea trebuie permisă în mod expres sau prescrisă de legislația națională. În plus, prelucrarea poate fi permisă dacă este necesar ca autoritatea responsabilă să își îndeplinească drepturile și obligațiile în domeniul dreptului muncii. Angajatul poate, de asemenea, să consimtă în mod expres prelucrarea.

Dacă există planuri de prelucrare a datelor personale sensibile, Responsabilul cu Protecția Datelor (DPO) trebuie informat în prealabil.

b.6. Telecomunicații și internet

Echipamentele telefonice, adresele de e-mail, intranetul și internetul împreună cu rețelele sociale interne sunt furnizate de instituție în primul rând pentru misiuni legate de muncă. Ele sunt un instrument și o resursă a companiei. Acestea pot fi utilizate în cadrul reglementarilor legale aplicabile și al politicilor interne ale companiei. În cazul utilizării autorizate în scopuri personale, legile privind secretul telecomunicațiilor și legile naționale privind telecomunicațiile trebuie să fie respectate, dacă este cazul.

Operatorul nu va prelucra date cu caracter personal în absența unuia dintre motivele de mai sus. Aceeași regulă se aplică, de asemenea, în cazul în care scopul colectării, prelucrării și utilizării datelor cu caracter personal trebuie să fie modificat față de scopul inițial.

c. Date despre beneficiari

c.1 Prelucrarea datelor pentru desfășurarea activităților, proiectelor, programelor instituției.

Datele personale ale persoanelor vizate pot fi prelucrate pentru ca operatorul să poată să desfășoare activitățile, proiectele și programele la care persoanele vizate participă. Înainte de colectarea datelor persoana vizată este notificată cu privire la intenția de prelucrare a datelor cu caracter personal. Persoana vizată poate fi contactată ulterior utilizând doar informațiile pe care aceasta le-au furnizat pentru contactare. Orice restricții solicitate de persoanele de contact respective trebuie să fie respectate.

c.2 Acordul/ consimțământul ca temei al prelucrării datelor

Acordul/ consimțământul persoanelor vizate este necesar pentru ca datele cu caracter personal să poată fi prelucrate. Acordul/ consimțământul trebuie obținut în scris sau în format electronic în scopul documentării. În anumite circumstanțe, cum ar fi conversațiile telefonice, acordul poate fi dat verbal. Este obligatorie documentarea acordării consimțământului.

c.3 Prelucrarea datelor în conformitate cu obligația legală

Prelucrarea datelor cu caracter personal este permisă și în cazul în care legislația aplicabilă solicită, impune sau permite acest lucru. Tipul și amploarea procesării datelor trebuie să fie necesare pentru activitatea legală de prelucrare a datelor și trebuie să respecte dispozițiile legale relevante.

c.4 Prelucrarea datelor în conformitate cu interesele legitime

Datele cu caracter personal pot fi procesate și în cazul în care acest lucru este necesar pentru un interes legitim al operatorului. Interesele legitime sunt în general de natură juridică. Datele cu caracter personal nu pot fi prelucrate în scopul unui interes legitim dacă, în cazuri individuale, există dovezi conform cărora interesele persoanei vizate merită protecție și că aceasta are prioritate. Înainte de prelucrarea datelor, este necesar să se determine dacă există interese care merită protejate.

c.5 Prelucrarea datelor sensibile

Datele cu caracter personale sensibile pot fi prelucrate numai dacă legea impune acest lucru sau dacă persoana vizată și-a dat consimțământul în mod expres. Aceste date pot fi, de asemenea, prelucrate dacă o asemenea prelucrare este obligatorie pentru recunoașterea, exercitarea sau apărarea drepturilor legale referitoare la persoana vizată. Dacă în cadrul operatorului există planuri de prelucrare a datelor extrem de sensibile, Responsabilul cu Protecția Datelor trebuie informat în prealabil.

Dacă datele cu caracter personal sunt colectate, prelucrate și utilizate, persoanele vizate trebuie să fie informate despre aceasta printr-o declarație de confidențialitate și, dacă este cazul, să li se pună la dispoziție informații despre cookie-uri. Declarația de confidențialitate și orice informație privind modulele cookie trebuie să fie integrate astfel încât să fie ușor de identificat, direct accesibile și disponibile în mod consecvent pentru persoanele vizate.

7. Transmiterea datelor cu caracter personal

Transmiterea datelor cu caracter personal către destinatarii din afara sau în interiorul operatorului face obiectul cerințelor de autorizare pentru prelucrarea datelor cu caracter personal în conformitate cu cerințele Regulamentului. Beneficiarul datelor trebuie să fie obligat să utilizeze datele numai în scopurile definite.

În cazul în care datele sunt transmise unui destinatar din afara operatorului către o țară terță, această țară trebuie să accepte să mențină un nivel de protecție a datelor echivalent cu această politică de protecție a datelor. Acest lucru nu se aplică în cazul în care transmiterea se bazează pe o obligație legală.

În cazul în care datele sunt transmise către o terță parte sau în Uniunea Europeană / Spațiul Economic European, operatorul trebuie să se asigure că datele pot fi utilizate în scopul dorit.

8. Prelucrarea datelor privind contractele

Prelucrarea datelor în numele său înseamnă că un prestator este angajat să proceseze date cu caracter personal, fără a-și asuma responsabilitatea pentru procesul de afaceri afiliat. În aceste cazuri, un acord privind prelucrarea datelor în numele acestuia trebuie încheiat între prestatorul extern (care devine împuternicit) și operator (care devine beneficiar). Împuternicitul poate procesa date personale numai conform instrucțiunilor beneficiarului.

9. Drepturile persoanei vizate

Persoana vizată ale cărei date cu caracter personal sunt prelucrate de Operator are dreptul de a fi informată și poate solicita Operatorului următoarele informații cu privire la:

- a) Dreptul de acces la datele cu caracter personal - să obțină de la Operator confirmarea dacă datele cu caracter personal sunt prelucrate și dreptul de a primi o copie a oricărei înregistrări care conține datele sale cu caracter personal.
- b) Dreptul la rectificare - să obțină de la Operator fără întârzieri nejustificate rectificarea unor date cu caracter personal inexacte cu privire la el/ea, completarea datelor cu caracter personal incomplete, inclusiv prin furnizarea unei declarații suplimentare.
- c) Dreptul la ștergerea datelor ("dreptul de a fi uitat") - să obțină de la Operator ștergerea datelor cu caracter personal fără întârzieri nejustificate (dacă datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate; persoana vizată își retrace consimțământul; datele cu caracter personal au fost prelucrate ilegal etc.).
- d) Dreptul la restricționarea prelucrării dacă datele cu caracter personal sunt inexacte; prelucrarea este ilegală și persoana vizată solicită restricționarea utilizării datelor cu caracter personal în locul ștergerii lor; datele cu caracter personal nu mai sunt necesare în scopul prelucrării, dar ele sunt solicitate pentru constatarea, exercitarea sau apărarea unui drept în instanță; persoana vizată s-a opus prelucrării pentru intervalul de timp când se verifică dacă drepturile legitime ale operatorului prevalează asupra celor ale persoanei vizate.
- e) Dreptul la portabilitatea datelor – să primească datele cu caracter personal într-un format structurat, utilizat în mod curent și care poate fi citit automat și are dreptul de a transmite aceste date cu caracter personal unui alt operator fără obstacole din partea Operatorului (dacă prelucrarea se bazează pe consimțământ sau pe un contract, iar prelucrarea este efectuată prin mijloace automate).
- f) Dreptul la opoziție în orice moment al prelucrării datelor cu caracter personal (inclusiv crearea de profiluri).
- g) Dreptul la retragerea consimțământului în orice moment, fără a afecta legalitatea prelucrării bazate pe consimțământ, înainte de retragerea sa. Astfel persoana vizată înțelege și este de acord ca, în cazul retragerii, nu se poate ajunge la scopul prelucrării datelor cu caracter personal.
- h) Dreptul de a depune o plângere la o autoritate de supraveghere, în cazul în care persoana vizată decide că drepturile sale sunt încălcate.
- i) Dreptul la o cale de atac eficientă împotriva unei autorități de supraveghere, Operatorului sau alt procesator.
- j) Dreptul la despăgubiri de la Operator sau de la un alt procesator pentru prejudiciul suferit.

10. Confidențialitatea procesării

Datele personale sunt considerate informații confidențiale și vor fi tratate ca atare. Orice colectare, prelucrare sau utilizare neautorizată a acestor date de către angajați este interzisă. Prelucrarea datelor cu caracter personal este confidențială. Ea va fi efectuată numai de

persoanele care acționează sub autoritatea Operatorului și numai pe baza instrucțiunilor acestuia.

Orice procesare de date efectuată de un angajat, care nu a fost autorizată să fie desfășurată ca parte a îndatoririlor sale legitime, este considerată ca fiind neautorizată. Se aplică principiul “*necesitatea de a cunoaște*”. Angajații pot avea acces la informații personale în funcție de adecvarea acestui acces la tipurile de date și de scopul determinat. Acest lucru se bazează pe defalcarea și separarea atentă a atribuțiilor angajaților operatorului și presupune punerea în aplicare a rolurilor și responsabilităților pentru fiecare angajat.

Angajaților li se interzice să utilizeze date cu caracter personal în scopuri private sau comerciale, să le dezvăluie persoanelor neautorizate sau să le pună la dispoziție în orice alt mod. Superiorii ierarhici își informează angajații la începutul relației de muncă cu privire la obligația de a proteja secretul datelor.

În cazul utilizării neautorizate a datelor personale, angajații pot fi sancționați în conformitate cu legislația aplicabilă și cu reglementările în vigoare în cadrul operatorului.

Obligația menținerii confidențialității datelor personale rămâne în vigoare și după încheierea perioadei de angajare, sancțiunile aplicabile în caz de încălcare a obligației de confidențialitate fiind cele prevăzute de cadrul legislativ în vigoare.

11. Securitatea prelucrării

Datele personale sunt protejate împotriva accesului neautorizat și împotriva prelucrării sau divulgării ilegale, precum și pierderii accidentale, modificării sau distrugerii. Acest lucru se aplică indiferent dacă datele sunt prelucrate electronic, pe suport de hârtie sau prin alte mijloace. Înainte de introducerea noilor metode de prelucrare a datelor, în special a noilor sisteme informatice, sunt definite și implementate măsuri tehnice și organizatorice de protecție a datelor cu caracter personal. Aceste măsuri trebuie să se bazeze pe stadiul tehnicii, pe riscurile procesării și pe necesitatea de a proteja datele (determinate de procesul de clasificare a informațiilor).

Accesul la datele cu caracter personal este oferit numai acelor angajați ai Operatorului care au nevoie de astfel de date cu caracter personal pentru a-și îndeplini sarcinile legate de oricare dintre scopurile prelucrării menționate mai sus (inclusiv departamentul resurse umane, departamentul Juridic, departamentul Financiar, IT, Administrativ). Orice acces la datele cu caracter personal pentru alți angajați care nu au drepturi de accesare în conformitate cu prezenta Politică este interzis.

Angajații Operatorului care au acces la datele cu caracter personal au dreptul să prelucreze numai acele date de care au nevoie pentru a-și îndeplini responsabilitățile specifice de muncă legate de oricare dintre scopurile de prelucrare menționate mai sus.

Documentele care conțin date cu caracter personal sunt stocate în departamentele structurale ale Operatorului ai căror angajați au acces la datele cu caracter personal legat de îndeplinirea atribuțiilor lor oficiale și sunt responsabili de interacțiunea datelor relevante ale persoanei vizate.

O persoană care prelucrează date cu caracter personal în numele Operatorului respectă principiile și regulile de prelucrare a datelor cu caracter personal stabilite prin prezenta Politică.

Dacă Operatorul autorizează o altă persoană cu prelucrarea datelor cu caracter personal, Operatorul este responsabil față de persoana vizată de prelucrarea datelor cu caracter personal pentru faptele sau omisiunile acelei persoane. O persoană care prelucrează date cu caracter personal în numele Operatorului este responsabilă față de Operator.

Toate datele cu caracter personal trebuie să fie tratate cu cea mai înaltă securitate și trebuie păstrate:

- a) într-o camera închisă cu cheia cu acces controlat; și/sau
- b) într-un sertar sau dulap închis cu cheia; și/sau
- c) dacă sunt computerizate, parola protejată conform cerințelor din politica de control al accesului; și/sau
- d) stocate în medii de calculator (detașabile) care sunt criptate în conformitate cu standardele în domeniu;

12. Controlul protecției datelor

Respectarea politicii de protecție a datelor și a legilor aplicabile privind protecția datelor este verificată în mod regulat prin intermediul auditurilor de protecție a datelor precum și al altor controale. Realizarea acestor controale este responsabilitatea Responsabilului cu Protecția Datelor.

Rezultatele controalelor privind protecția datelor sunt raportate managementului operatorului. La cerere, rezultatele controalelor privind protecția datelor vor fi puse la dispoziția autorității responsabile de protecția datelor. Autoritatea responsabilă cu protecția datelor poate efectua propriile controale de conformitate cu reglementările din aceasta politică, conform legislației naționale.

13. Reținerea și eliminarea datelor

Operatorul nu va păstra datele personale într-o formă care permite identificarea persoanelor vizate pentru o perioadă mai lungă decât este necesar, în legătură cu scopurile pentru care datele au fost colectate inițial.

Operatorul poate stoca datele perioade mai lungi conform termenelor imperative de prescripție aplicabile și cu implementarea unor măsuri tehnice și organizaționale adecvate pentru a proteja drepturile și libertățile persoanelor vizate.

Datele personale trebuie să fie eliminate în siguranță în conformitate cu al șaselea principiu al GDPR – prelucrate într-un mod adecvat pentru a menține securitatea, cu protejarea „drepturilor și libertăților” persoanelor vizate. Orice eliminare a datelor va fi efectuată în conformitate cu procedura de eliminare sigură.

14. Incidente de protecție a datelor

Toți angajații sunt obligați să informeze imediat superiorul lor, Responsabilului cu Protecția Datelor (DPO) cu privire la cazurile de încălcare a acestei politici de protecție a datelor sau alte reglementări privind protecția datelor cu caracter personal (incidente de protecție a datelor), indiferent dacă este vorba despre o încălcare a confidențialității, a integrității datelor sau a disponibilității acestora.

În următoarele cazuri vor fi luate măsuri urgente pentru limitarea afectării titularilor de date cu caracter personal și pentru respectarea obligațiilor de raportare și notificare a incidentelor către autoritatea de supraveghere:

- a) Transmitere necorespunzătoare a datelor cu caracter personal către terțe părți
- b) Acces neadecvat la datele cu caracter personal
- c) Pierdere, distrugere sau alterare a datelor cu caracter personal

15. Responsabilități și sancțiuni

Conducerea operatorului precum și angajații și prepușii acestora sunt responsabili de prelucrarea datelor în zona lor de responsabilitate. Prin urmare, aceștia sunt obligați să se asigure că sunt îndeplinite cerințele legale pentru protecția datelor și cele conținute în politica de protecție a datelor (de exemplu, obligațiile naționale de raportare).

Organele de conducere au responsabilitatea de a se asigura că există măsuri organizaționale, resurse umane și tehnice pentru ca orice prelucrare a datelor să fie efectuată în conformitate cu protecția datelor. Respectarea acestor cerințe reprezintă responsabilitatea conducătorilor de structuri organizatorice.

Responsabilul cu Protecția Datelor (DPO) este persoana de contact local din cadrul operatorului. Acesta poate efectua verificări și familiarizează angajații operatorului privind conținutul politicilor de protecție a datelor. Managerii trebuie să se asigure că angajații lor sunt suficient de instruiți în protecția datelor.

Prelucrarea necorespunzătoare a datelor cu caracter personal sau alte încălcări ale legilor privind protecția datelor pot conduce la cereri de despăgubire pentru prejudicii. Încălcările pentru care angajații individuali sunt responsabili pot conduce la sancțiuni prevăzute în dreptul muncii.

16. Responsabilul cu Protecția Datelor (DPO)

Responsabilul cu Protecția Datelor (DPO) numit la nivelul operatorului, fiind independent din punct de vedere al ordinilor profesionale, își desfășoară activitatea pentru respectarea legislației în vigoare privind protecția datelor. El este responsabil pentru politica de protecție a datelor și supraveghează respectarea acesteia.

Orice persoană vizată poate aborda Responsabilul cu Protecția Datelor (DPO) pentru a solicita informații sau să depună plângeri legate de protecția datelor sau de problemele de securitate a datelor. Dacă se solicită, preocupările și plângerile vor fi tratate în mod confidențial.

Pentru orice detalii suplimentare referitoare la prelucrarea datelor personale poate fi contactat Responsabilul cu Protecția Datelor cu Caracter Personal la adresa de e-mail gdpr@helpsiasociatii.ro sau poate fi adresată o cerere scrisă la adresa Calea 13 Septembrie, nr. 168-184, Sector 5, București.

Operatorul poate schimba sau modifica prezenta politică periodic. Acest lucru se poate întâmpla, de exemplu, din cauza schimbărilor de lege, sau dacă Operatorul își modifică domeniul de activitate sau practicile sale.

Prezenta politică se aplică începând cu data de 27 iulie 2020, persoana responsabilă de revizuirea periodică, cel puțin anuală a prezentei proceduri fiind Responsabilul cu Protecția Datelor.

Întocmit,
Responsabil cu Protecția Datelor
Daniela Helwig – Reprezentant Help si Asociații

Aprobat,
Reprezentant legal unitate
Georgiana Trifu – Director General