PATRONATUL TINERILOR ÎNTREPRINZĂTORI DIN ROMÂNIA

POLITICĂ PRIVIND PROTECTIA SI SECURITATEA DATELOR CU CARACTER PERSONAL

CUPRINS

1. OBIECTIVELE POLITICII 3
2. DEFINITII UTILIZATE 3
3. CADRUL DE REGLEMENTARE 5
4. PRINCIPIILE DE PRELUCRARE A DATELOR 6
5. TEMEIUL JURIDIC AL PRELUCRARII 6
6. PERSOANELE VIZATE 9
7. DATELE PRELUCRATE 9
8. SCOPURILE PRELUCRARII 11
9. DURATA PRELUCRARII 11
10. DREPTURILE PERSOANEI VIZATE 11
11. FLUXUL DE SOLUTIONARE AL CERERILOR PERSOANELOR VIZATE 18
12. DESTINATARI/PERSOANE IMPUTERNICITE/OPERATORI ASOCIATI 20
13. EVIDENTA ACTIVITATILOR DE PRELUCRARE 22
14. MASURI DE SECURITATE 23
15. EVALUAREA IMPACTULUI ASUPRA PROTECŢIEI DATELOR 26
16. TRATAREA INCIDENTELOR DE SECURITATE A DATELOR CU CARACTER PERSONAL 26
17. Nerespectarea politicii 27
18. RGDP IN PROIECTELE DERULATE DE PTIR 27

Operatorul prelucrează date cu caracter personal in conformitate cu prevederile Regulamentului (UE) 2016/679 al Parlamentului European si al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal si privind libera circulatie a acestor date si de abrogare a Directivei 95/46/CE (denumit in continuare "**RGDP**" sau Regulamentul general privind protectia datelor) precum si a altor acte normative aplicabile privind protectia datelor cu caracter personal.

Prezenta Politica privind protecția si securitatea datelor cu caracter personal (denumita in continuare "**Politica**") este aplicabila si obligatorie pentru toti salariatii Persoanei juridice, precum si pentru toate persoanele fizice sau juridice care prelucrează date cu caracter personal in numele sau/si pe seama Persoanei juridice, precum, dar fara a se limita la, colaboratorii sau alti parteneri ai Persoanei juridice.

1. OBIECTIVELE POLITICII

Prezenta Politica stabileste cadrul general de conformitate ale Persoanei juridice (PJ) cu obligatiile ce ii revin potrivit legislatiei din domeniul protectiei datelor cu caracter personal.

Aceasta Politica explica modul in care sunt prelucrate datele cu caracter personal pe care PJ in desfasurarea activitatii sale.

2. DEFINITII UTILIZATE

„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.

„Activitati de prelucrare a datelor personale” înseamnă orice operaţiune sau set de operaţiuni 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 dispoziţie în orice alt mod, alinierea sau combinarea, restricţionarea, ştergerea sau distrugerea datelor.

„Persoana vizata” poate fi salariatul, un client sau un colaborator – persoana fizica, inclusiv un reprezentant al unui client – persoana juridica sau al unui partener de afaceri al Operatorului.

„Sistem de evidență a datelor” înseamnă orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcționale sau geografice.

„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; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern.

In intelesul prezentei proceduri, **Persoana juridica are calitatea de Operator de date cu caracter personal.**

„Persoană împuternicită de operator” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului.

„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. Cu toate acestea, autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete, control sau investigații, în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari. Prelucrarea acestor date de către autoritățile publice respective vor respecta normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării, respectiv legislația speciala aplicabila in domeniul respective.

„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 prelucreze date cu caracter personal.

„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, ca datele cu caracter personal care o privesc să fie prelucrate. Operatiunile de prelucrare a datelor care se realizeaza in temeiul consimtamantului conform articolului 6 alineat 1) litera a) sau, dupa caz, articolului 9 alineat 2) litera a) din RGDP vor respecta intocmai prevederile RGDP, Operatorul de date avand obligatia evidentei existentei unui consimtamant valid exprimat de persoana vizata.

„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;

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

"**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 performanţa la locul de muncă, situaţia economică, sănătatea, preferinţele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia;
"**Pseudonimizare**" înseamnă 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 informaţii suplimentare, cu condiţia ca aceste informaţii 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;

"**Date genetice**" înseamnă datele cu caracter personal referitoare la caracteristicile genetice moştenite sau dobândite ale unei persoane fizice, care oferă informaţii unice privind fiziologia sau sănătatea persoanei respective şi care rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză;

"**Date biometrice**" înseamnă o date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice;

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

3. CADRUL DE REGLEMENTARE

Aceasta Politica a fost elaborata in vederea respectării cerințelor cadrului legislativ si de reglementare existent cu privire la prelucrarea datelor cu caracter personal, respectiv in special următoarele acte normative:

- Conventia privind protectia drepturilor omului si a libertatilor fundamentale, adoptata la Roma la 4 noiembrie 1950;
- Conventia pentru protejarea persoanelor fata de prelucrarea automatizata a datelor cu caracter personal, adoptata la Strasbourg la 28 ianuarie 1981, ratificata prin Legea nr. 682/2001;
- Regulamentul nr. 679 din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE;
- Directiva 2002/58/CE a Parlamentului European si a Consiliului din 12.07.2002 privind prelucrarea datelor cu caracter personal si protectia vietii private in sectorul comunicatiilor electronice, ratificata prin Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice;
- Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice;
- Ordinul nr. 52/2002 al Avocatului Poporului privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal;

- Regulamentul UE nr.910/2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE
- Recomandari, opinii si decizii relevante ale organismelor institutionale nationale si europene.

4. PRINCIPIILE DE PRELUCRARE A DATELOR

Cu ocazia realizării unei operațiuni de prelucrare a datelor cu caracter personal, Operatorul, salariații săi si orice alte persoane desemnate sau împuternicite de PJ vor respecta întocmai principiile de prelucrare a datelor prevăzute de Regulamentul general privind protecția datelor (articolul 5), asigurând după cum urmează:

Legalitatea, echitatea şi transparenţa. Datele cu caracter personal sunt prelucrate de către Operator in mod legal, corect și transparent, persoana vizată fiind informată cu privire la existenţa unei operaţiuni de prelucrare şi la scopurile acesteia legitime, stabilite pe criterii de echitate fata de drepturile si interesele fundamentale ale persoanei vizate.

Limitarea scopului operațiunii de prelucrare a datelor cu caracter personal. Datele cu caracter personal se colectează de către Operator în scopuri specifice, explicite și legitime și nu se prelucrează ulterior pentru scopuri adiționale care nu sunt compatibile cu scopul colectării datelor.

Proporționalitatea si reducerea la minim a datelor cu caracter personal. Datele se prelucrează de o maniera adecvată, relevantă și limitată la necesitatea de a realiza scopurile legitime si precis determinate pentru care sunt prelucrate.

Exactitatea datelor. Datele prelucrate sunt exacte şi, în cazul în care este necesar, acestea sunt actualizate. In acest sens, Operatorul trebuie să ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt şterse sau rectificate fără întârziere.

Limitarea legata de stocarea datelor. Datele sunt pastrate de catre Operator intr-o forma care permite identificarea persoanelor vizate pentru o perioadă care nu depășește perioada necesară pentru scopurile pentru care sunt prelucrate datele cu caracter personal.

Integritatea si confidențialitatea datelor. Datele sunt prelucrate in conditii de securitate adecvate astfel incat sa se asigure protecția acestora împotriva prelucrării neautorizate sau ilegale, respectiv împotriva pierderii, distrugerii sau deteriorării accidentale a datelor.

5. TEMEIUL JURIDIC AL PRELUCRARII

5.1. **Prelucrarea datelor cu caracter personal** de baza este legala numai daca si in masura in care se aplica cel putin una dintre urmatoarele conditii:

- persoana vizata si-a dat consimtamantul pentru prelucrarea datelor sale cu caracter
- personal pentru unul sau mai multe scopuri specifice;

- prelucrarea este necesara pentru executarea unui contract la care persoana vizata este parte sau pentru a face demersuri la cererea persoanei vizate inainte de incheierea unui contract;
- prelucrarea este necesara in vederea indeplinirii unei obligatii legale care îi revine operatorului;
- prelucrarea este necesara pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;
- prelucrarea este necesara pentru indeplinirea unei sarcini care serveste unui interes public sau care rezulta din exercitarea autoritatii publice cu care este investit operatorul;
- prelucrarea este necesara în scopul intereselor legitime urmarite de operator sau de o parte terta, cu exceptia cazului în care prevaleaza interesele sau drepturile si libertatile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizata este un copil.

5.2. Legalitatea prelucrarii datelor cu caracter special

Date cu caracter special sunt datele privind originea rasiala sau etnica, opiniile politice, confesiunea religioasa sau convingerile filozofice sau apartenenta la sindicate, datele genetice, datele biometrice privind identificarea unica a unei persoane fizice, datele privind sanatatea sau datele privind viata sexuala sau orientarea sexuala a unei persoane fizice.

Aceste date cu caracter special pot fi prelucrate numai in conformitate cu prevederile 9 din Regulamentul general privind protectia datelor, respectiv in urmatoarele situatii:

- persoana vizată şi-a dat consimţământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice, cu excepțiile prevăzute de lege;
- prelucrarea este necesară în scopul îndeplinirii obligaţiilor şi al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forţei de muncă şi al securităţii sociale şi protecţiei 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 garanţii adecvate pentru drepturile fundamentale şi interesele persoanei vizate;
- 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-şi da consimţământul;
- prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod manifest de către persoana vizată;
- prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în
- instanţă sau ori de câte ori instanţele acţionează în exerciţiul funcţiei lor judiciare;

- prelucrarea este necesară din motive de interes public major, în baza dreptului Uniunii sau a dreptului intern, care este proporţional cu obiectivul urmărit, respectă esenţa dreptului la protecţia datelor şi prevede măsuri corespunzătoare şi specifice pentru protejarea drepturilor fundamentale şi a intereselor persoanei vizate;
- prelucrarea este necesară în scopuri legate de medicina preventivă sau a muncii, de
- evaluarea capacităţii de muncă a angajatului, de stabilirea unui diagnostic medical, de
- furnizarea de asistenţă medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor şi serviciilor de sănătate sau de asistenţă socială;
- prelucrarea este necesară în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1) RGDP, în baza dreptului Uniunii sau a dreptului intern, care este proporţional cu obiectivul urmărit, respectă esenţa dreptului la protecţia datelor şi prevede măsuri corespunzătoare şi specifice pentru protejarea drepturilor fundamentale şi a intereselor persoanei vizate.

5.3. Legalitatea prelucrarii datelor referitoare la condamnari penale si infractiuni

Prelucrarea datelor cu caracter personal referitoare la condamnari penale si infractiuni sau la masuri de securitate conexe se efectueaza numai in conditiile prevazute de art. 10 din Regulamentul general privind protectia datelor si numai in urmatoarele situatii:

- numai sub controlul unei autoritati de stat sau
- atunci cand prelucrarea este autorizata de dreptul Uniunii sau de dreptul intern care prevede garantii adecvate pentru drepturile si libertatile persoanelor vizate.

Orice registru cuprinzator al condamnarilor penale se tine numai sub controlul unei autoritati de stat.

5.4. Conditii privind consimtamântul

În cazul în care prelucrarea se bazeaza pe consimtamant, operatorul trebuie sa fie în masura sa demonstreze ca persoana vizatã si-a dat consimtamantul pentru prelucrarea datelor sale cu caracter personal. În cazul în care consimtamantul persoanei vizate este dat în contextul unei declaratii scrise care se refera si la alte aspecte, cererea privind consimtamantul trebuie sa fie prezentata într-o forma care o diferentiaza în mod clar de celelalte aspecte, într-o forma inteligibila si usor accesibila, utilizând un limbaj clar si simplu. Nicio parte a respectivei declaratii care constituie o încalcare a Regulamentului general privind protectia datelor nu este obligatorie.

Persoana vizata are dreptul sa îsi retraga în orice moment consimtamantul. Retragerea consimtamantului nu afecteaza legalitatea prelucrarii efectuate pe baza consimtamantului înainte de retragerea acestuia. Înainte de acordarea consimtamântului, persoana vizata este informata cu privire la acest lucru. Retragerea consimtamantului se face la fel de simplu ca acordarea acestuia.

Atunci când se evaluează dacă consimţământul este dat în mod liber, se ţine seama cât mai mult de faptul că, printre altele, executarea unui contract, inclusiv prestarea unui serviciu, este condiţionată sau nu de consimţământul cu privire la prelucrarea datelor cu caracter personal care nu este necesară pentru executarea acestui contract

6. PERSOANELE VIZATE

PJ efectueaza operatiuni de prelucrare a datelor cu caracter personal cu privire la urmatoarele categorii principale de persoane vizate:

- salariații;
- alte persoanele vizate, care intra in contact cu PJ prin prisma rolului lor in relațiile PJ cu partenerii acesteia.

7. DATELE PRELUCRATE

7.1. Datele partenerilor contractuali:

PJ prelucreaza urmatoarele date:

- numele si prenumele, data nasterii, sex; CNP,
- adresa (domiciliul/ reședința/adresa de corespondenta);
- telefonul, fax, e-mailul;
- cont bancar, date card bancar,
- imagine video;
- semnătura, etc.

7.2. Datele salariatilor:

In calitate de angajator, PJ prelucrează datele salariaților săi, dintre care enumeram:

Informaţii Generale: Numele, prenumele, numele anterior, initiala tatalui/mamei, adresa de domiciliu şi adresa de unde este prestată munca la distanţă, dacă este diferită, data naşterii, starea civilă, numărul de telefon şi adresa de email, naţionalitatea, cetăţenia, sexul, religia si detalii privind orice dezabilități sau restricţii de muncă, si fotografia persoanei vizate

Dovada identităţii şi eligibilităţii pentru angajare: Date privind cartea de identitate sau paşaportul, cum ar fi CNP, seria si numărul CI/Pașaportului, şi/sau permisul de conducere, certificat de căsătorie, sau alt document care atesta identitatea dumneavoastră după caz, atestate profesionale sau atestate emise de autorităţile de reglementare şi/sau vizele de ședere in tara, după caz.

Verificări anterioare angajării: Referinţe, note de interviu, evidenţe/rezultatele verificărilor anterioare angajării, inclusiv verificări privind cazierul judiciar, informaţii incluse în CV-ul Persoanei Vizate şi/sau în orice formulare de cerere. În cazul în care temeiul legal al prelucrării datelor referitoare la cazierul judiciar îl reprezintă consimţământul dumneavoastră (articolul 6 alineatul 1) litera a), veţi primi o notificare de informare separată, prin care vi se va solicita consimţământul în conformitate cu din Regulamentul General UE privind protecția datelor.

Condiţiile de angajare: Evidenţe privind oferta de muncă şi acceptarea acesteia, experienţa profesională, contractul de muncă al Persoanei Vizate, programul de lucru convenit, durata perioadei de probă, modificarea fişei postului şi motivul modificării, precum şi relaţia de subordonare, adresa locului de munca, funcţia, ocupația, date privind relocarea, daca este cazul, detalii referitoare la superiorul ierarhic şi persoana responsabilă de angajare, detalii privind cursurile de formare.

Date privind remuneraţia si taxele si impozitele legale: Detalii privind salariul, bonusurile, beneficiile, contul bancar, CNP-ul, numărul de pașaport,numărul permisului de ședere, detalii privind contul de retragere şi privind pensia, date privind taxele si impozitele datorate de Persoana Vizata conform legislației fiscale aplicabile.

Date privind orele de lucru si prezenta la locul de munca: Vechimea în muncă, absenţele de la locul de muncă, orele lucrate;

Date privind sănătatea: informaţii privind sănătatea, concediile medicale, date privind controlul medical la angajare, controlul medical periodic, detalii privind asigurarea obligațiilor PJ privind securitatea si sănătatea in munca;

Informaţii referitoare la performanţa Persoanei Vizate la locul de muncă: Analizele de performanţă și evaluare, îmbunătăţirea performanţei sau planurile de dezvoltare şi documentele aferente, rezultate ale testelor efectuate de către dumneavoastră la încheierea contractului de munca sau pe durata executării acestuia.

Informaţii referitoare la deplasările şi cheltuielile efectuate de Persoana Vizată în interes de serviciu: Detalii privind conturile bancare, paşaportul, permisul de conducere, înmatricularea autovehiculului şi detalii privind asigurările, facturi.

Date privind modificarea, încetarea şi desfacerea contractului de muncă: documentele sau motivele legale de modificare sau încetare a contractului individual de munca conform legislației muncii aplicabile.

Date privind copii, respectiv rudele Angajatului, pentru care acesta are calitate de reprezentant legal sau convențional. Numele, prenumele, certificatul de naștere al copiilor, reprezentanți legal de Angajat, nume, prenume, copie CI aferent celorlalți membri de familie, situația familiala, certificat de deces, daca este cazul.

Date privind executarea altor obligații contractuale din contractele/documentele încheiate cu persoana vizata: nume, prenume, adresa de e-mail.

7.3. In cazul PARTICIPANTILOR la proiectele derulate de PTIR se prelucreaza urmatoarele date:

- date de identificare: nume, prenume, data nasterii, sex, nationalitate, varsta, CNP, adresa de domiciliu sau de resedință, e-mail, telefon, loc de munca, copie C.I., copie certificat de nastere, copie certificat de casatorie, starea civila, semnatura, etnie;
- date bancare;
- date privind studiile absolvite;
- imagine;

- date referitoare la profilarea aplicantilor la proiectele derulate de PTIR in vederea admiterii acestora.

8. SCOPURILE PRELUCRARII

PTIR prelucreaza date cu caracter personal in vederea:

- derularii contractelor individuale de munca;
- indeplinirii obligatiilor legale privind raportarea angajatilor in Registrul Salariatilor si a concediilor medicale catre Casa de Sanatate;
- validarea participantilor la proiectele derulate;
- indeplinirii obligatiilor contractuale din proiectele de finantare;
- reprezentarii societatii in fata instantelor de judecata și a autoritatilor publice, realizarea procedurilor de recuperare a creantelor, dupa caz;
- desfasurarii activitatilor de recrutare/selectie pentru ocuparea posturilor vacante;
- informarii partenerilor cu privire la activitatile desfasurate (pe website, Facebook, sau alte mijloace de comunicare online);

9. DURATA PRELUCRARII

Datele cu caracter personal prelucrate de catre PJ si sunt stocate pe tot parcursul perioadei necesare indeplinirii scopului de prelucrare si/sau in conformitate cu legea. Odata ce aceasta perioada a expirat, datele pot fi stocate pentru perioada prevazuta de legislatia in vigoare/pentru perioada ceruta pentru protejarea drepturilor PJ in fata autoritatilor judiciare sau altor autoritati competente.

10. DREPTURILE PERSOANEI VIZATE

10.1 Dreptul de acces la date cu caracter personal

Dreptul de acces la date al persoanei vizate include dreptul acesteia de a obtine in primul rand din partea PJ confirmarea ca PJ prelucreaza datele cu caracter personal ale acesteia, indiferent de temeiul juridic al unei asemenea prelucrari de date. Odata confirmata operatiunea de prelucrare a datelor cu caracter personal, PJ are obligatia de a informa persoana vizata cu privire la urmatoarele aspecte referitoare la datele sale prelucrate de PJ:

- scopurile prelucrării;
- categoriile de date cu caracter personal vizate;

- destinatarii sau categoriile de destinatari cărora datele cu caracter personal le-au fost sau urmează să le fie divulgate, în special destinatari din ţări terţe sau organizaţii internaţionale;
- acolo unde este posibil, perioada pentru care se preconizează că vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
- existenţa dreptului de a solicita Operatorului rectificarea sau ştergerea datelor cu caracter personal ori restricţionarea prelucrării datelor cu caracter personal referitoare la persoana vizată sau a dreptului de a se opune prelucrării;
- dreptul de a depune o plângere în faţa autorităţii de supraveghere – Autoritatea Nationala de Supraveghere a Prelucrării Datelor cu Caracter Personal – ANSPDCP (sau alta autoritate competenta in acest domeniu);
- în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, orice informaţii disponibile privind sursa acestora;
- existenţa unui proces decizional automatizat incluzând crearea de profiluri.

Totodata, in situatia unui transfer international de date cu caracter personal ale persoanei vizate, indeosebi catre o tara non-UE ori o organizaţie internaţională, aceasta are dreptul să fie informată cu privire la garanţiile adecvate, cum ar fi despre existenta unei decizii a Comisiei Europene de confirmare a unui nivel adecvat de protectie a datelor in tara terta, existenta unui contract care sa contina clauze standar de protectie a datelor avizate de catre Comisia Europeana sau o alta garantie dintre cele prevazute de art. 44-49 din RGDP.

Responsabilul cu protectia datelor cu caracter personal va gestiona cererea persoanei vizate, va analiza cererea persoanei vizate si va pregati un draft de raspuns. In solutionarea cererii, responsabilul va tine seama de faptul ca Operatorul are obligatia de a furniza o copie a datelor cu caracter personal care fac obiectul prelucrării cu titlu gratuit.

Raspunsul la cerere se transmite persoanei vizate la adresa de domiciliu/resedinta sau de corespondenta a acesteia. În situatia în care persoana vizată introduce cererea în format electronic şi cu excepţia cazului în care persoana vizată solicită un alt format, informaţiile sunt furnizate într-un format electronic utilizat în mod curent.

Pentru responsabilul cu protectia datelor cu caracter personal, educația solicitată vizează finalizarea unor studii superioare de minim 3 ani în unul dintre următoarele domenii: economic, științe sociale, științe politice, științe juridice, etc, nefiind solicitata experienta profesionala specifica a acestuia.

10.2 Dreptul la rectificarea datelor cu caracter personal

Unul din principiile prelucrarii datelor cu caracter personal reglementate de RGDP se refera la faptul ca Operatorul este obligat sa prelucreze datele cu caracter personal intr-o forma in care acestea sunt exacte și să asigure actualizarea acestora ori de cate ori este necesar, luand toate măsurile tehnice si organizatorice necesare pentru a se asigura că datele cu caracter personal care sunt inexacte sunt șterse sau, dupa caz rectificate fără întârziere.

Persoana vizata – salariat sau alta persoana fizica ale caror date sunt prelucrate de catre Operator, are astfel dreptul de a obține, in baza unei cereri, completarea datelor cu caracter personal care sunt incomplete. Pentru solutionarea cererii sale, persoana vizata poate furniza declarații sau informatii suplimentare, pentru a clarifica datele care sunt inexacte.

In situatia in care datele sunt rectificate, datele devenite astfel exacte vor fi comunicate si fiecărui destinatar care a primit datele, cu excepția cazului în care acest lucru se dovedește imposibil sau presupune eforturi disproporționate pentru PJ. Intr-un asemenea caz, este obligatoriu ca Operatorul, prin departamentul care a gestionat cererea persoanei vizate, sa justifice si sa argumenteze o asemenea decizie, fiind responsabila de tinerea documentatiei aferente.

Toate celelalte aspecte privind responsabilitatea redactarii, semnarii si trimiterii raspunsului catre persoana vizata prevazute la sectiunea anterioara raman aplicabile si cererilor privind dreptul la rectificarea datelor cu caracter personal.

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

Persoana vizata are dreptul de a solicita ștergerea datelor cu caracter personal, fără întârzieri nejustificate, în cazurile în care:

- datele nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;
- isi retrage consimțământul pentru operațiunea de prelucrare care se realizeaza de PJ in acest temei legal (prevazut de articolul 6 alin. 1) litera a) si art. 9, alin. 2) litera b) din RGDP) si nu exista alt temei legal pentru prelucrare;
- se opune prelucrării si nu exista motive juridice legitime care prevalează, respectiv persona vizata se opune prelucrarii de date cu caracter personal realizata de Operator in scop de marketing direct in temeiul interesului legitim prevazut de articolul 6 alin. 1, litera e) din RGDP, inclusiv creării de profiluri, în măsura în care este legată de marketingul direct respectiv;
- datele cu caracter personal au fost prelucrate ilegal;
- datele cu caracter personal trebuie șterse pentru respectarea unei obligații legale care revine PJ;
- datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale PJ informaționale[1] catre un copil, indiferent daca acordul pentru prelucrarea datelor in acest scop a fost acordat de catre copil, acesta avand capacitate de exercitiu pentru exprimarea unui consimtamant valid, sau de catre titularul raspunderii parintesti asupra copilului. Intr-un asemenea caz, copilul care are varsta de 14 ani sau copilul, cu incuviintarea reprezentantului sau legal, isi poate retrage consimtamantul privind prelucrarea datelor sale, in orice moment, fara a

[1] Prin "serviciu al societății informaționale", se intelege conform Directivei (UE) 2015/1535 a Parlamentului European și a Consiliului din 9 septembrie 2015. referitoare la procedura de furnizare de informații în domeniul reglementărilor tehnice și al normelor privind serviciile societății informaționale, articolul 1, alineat 1, litera b), orice serviciu prestat în mod normal în schimbul unei remunerații, la distanță, prin mijloace electronice și la solicitarea individuală a beneficiarului serviciului. În sensul acestei definiții: (i) „la distanță” înseamnă că serviciul este prestat fără ca părțile să fie prezente simultan; (ii) „prin mijloace electronice” înseamnă că serviciul este transmis inițial și primit la destinație prin intermediul echipamentului electronic pentru prelucrarea (inclusiv arhivarea digitală) și stocarea datelor și este transmis integral, transferat și recepționat prin cablu, radio, mijloace optice sau alte mijloace electromagnetice; (iii) „la solicitarea individuală a beneficiarului serviciilor” înseamnă că serviciul este prestat prin transmiterea datelor în urma solicitării individuale.

afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia.

In situația in care persoana vizata va transmite o cerere catre PJ, iar ca urmare a analizei acesteia conform secțiunii prezente, PJ dispune stergerea datelor, persoana vizata are dreptul ca decizia de ștergere a datelor sale sa fie comunicata si fiecărui destinatar care a primit datele, cu excepția cazului în care acest lucru se dovedește imposibil sau presupune eforturi disproporționate.

In conditiile in care datele cu caracter personal sunt necesare pentru a fi retinute in unul din temeiurile prevazute de legislația privind protectia datelor, nationala sau europeana, respectiv in cazul in care datele sunt necesare pentru constatarea, exercitarea sau apărarea unui drept în instanță al Operatorului, responsabilul cu protectia datelor cu caracter personal, va dispune ca datele sa nu fie sterse, informand intocmai persoana vizata despre aceasta decizie si despre justificarea legitima care a stat la baza acesteia, avand obligatia de a tine documentatia necesara pentru demonstrarea acesteia din punct de vedere al conformitatii sale cu drepturile persoanei vizate conform RGDP.

Toate celelalte aspecte privind responsabilitatea redactării, semnarii si trimiterii raspunsului catre persoana vizata prevazute la punctul 5.1., raman aplicabile si cererilor privind dreptul la stergerea datelor cu caracter personal.

10.4 Dreptul la restricționare a prelucrării

Restricționarea prelucrării datelor cu caracter personal înseamnă marcarea datelor cu caracter personal stocate de către PJ cu scopul de a limita prelucrarea viitoare a acestora, motivata de anumite situații mai jos descrise.

Astfel, dreptul de restrictionare a datelor cu caracter personal, poate fi exercitat de catre persoana vizata in urmatoarele situatii:

- se contesta exactitatea datelor, fiind necesara verificarea corectitudinii datelor; astfel, pe perioada care permite Companiei verificarea corectitudinii datelor, se va dispune restrictionarea datelor cu caracter personal;
- prelucrarea este ilegala, iar persoana se opune ștergerii datelor cu caracter personal, solicitând in schimb restricționarea utilizării lor;
- PJ nu mai are nevoie de datele cu caracter personal în scopul prelucrării pentru care datele au fost colectate sau copiate, arhivate, utilizate, etc., dar persoana i le solicită pentru constatarea, exercitarea sau apărarea unui drept în instanță;
- persoana vizata s-a opus prelucrării datelor sale cu caracter personal realizata fie in interesul legitim al PJ sau al unei terte parti conform art. 6 alin. 1) litera f) din RGDP sau prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public realizat de PJ conform art. alin. 1) litera e) din RGDP, pentru intervalul de timp în care se verifică dacă drepturile fundamentale si interesele legitime ale operatorului prevalează asupra celor ale persoanei respective.

In situatia în care prelucrarea a fost restricționată conform cazurilor mai sus mentionate, datele cu caracter personal ale persoanei vizate pot fi prelucrate numai in urmatoarele situatii:

- pentru stocarea datelor conform temeiurilor juridice ale unei asemenea operatiuni;

- numai cu consimțământul persoanei vizate;
- pentru constatarea, exercitarea sau apărarea unui drept în instanță al PJ sau pentru protecția drepturilor unei alte persoane fizice sau juridice sau din motive de interes public important al Uniunii sau al unui stat membru.

Persoana vizata va fi informata cu privire la decizia de restricționare a datelor sau la refuzul întemeiat al PJ de a restricționa datele, prin responsabilul cu protectia datelor cu caracter personal. Responsabilul va informa, de asemenea, persoana vizata înainte de ridicarea restricției de prelucrare.

Responsabilul cu protectia datelor cu caracter personal are obligatia de a tine documentatia necesara pentru demonstrarea conformitatii PJ cu prevederile RGDP privind drepturile persoanei vizate.

Toate celelalte aspecte privind responsabilitatea redactarii, semnarii si trimiterii raspunsului catre persoana vizata prevazute la punctul 5.1., raman aplicabile si cererilor privind dreptul la restrictionarea datelor cu caracter personal.

10.5 Dreptul la portabilitate a datelor

Persoana vizata are dreptul de a primi datele sale cu caracter personal într-un format standard, structurat, utilizat în mod curent și care poate fi citit automat și dreptul ca datele să fie transmise altui Operator fara obstacole din partea PJ.

Dreptul de portabilitate poate fi exercitat de catre persoana vizata in urmatoarele cazuri:

- datele sale cu caracter personal sunt prelucrate, prin mijloace automate, in temeiul consimtamantului exprimat conform articolului 6 alineat 1) litera a) sau articolului 9 alineat 1) litera a) din RGDP (ultimul caz referindu-se la date cu caracter special);
- datele sale cu caracter personal sunt prelucrate, prin mijloace automate, in temeiul unui contract conform articolului 6 alineat 1) litera b) din Regulamentul General UE privind protecția datelor.

Persoanele vizate pot solicita ca datele lor personale să fie transferate acestora sau unui alt Operator, într-un format structurat, utilizat în mod curent și care poate fi citit automat. Tertul care primeste datele, fiind posibila transmiterea din punct de vedere tehnic catre cel de-al doilea Operator, poate fi un contabil sau alt furnizor de servicii, persoana vizata neavând obligația de a motiva solicitarea sa către acestia.

Prin exercitarea acestui drept de catre persoana vizata nu se poate aduce atingere drepturilor si libertatilor altor persoane vizate. Astfel, ori de cate ori portabilitatea datelor implica si operatiuni de prelucrare a datelor cu caracter personal ale altor persoane, aceste situatii vor fi analizate de Departamantul responsabil de gestionarea cererii prsoanei vizate, cu suport din partea departamentelor tehnice, si cu avizul Responsabilului cu protectia datelor.

Toate celelalte aspecte privind responsabilitatea redactarii, semnarii si trimiterii raspunsului catre persoana vizata prevazute la punctul 5.1., raman aplicabile si cererilor privind dreptul la portabilitatea datelor cu caracter personal.

10.6 Dreptul la opoziție

Dreptul la opoziție se refera la dreptul persoanei vizate de a se opune, din motive legate de situația sa particulară în care se afla, prelucrării datelor cu caracter personal care o privesc, inclusiv creării de profiluri pe baza respectivelor date, atunci când prelucrarea se realizează in temeiul articolului 6 alineat 1) literele e) si f) din RGDP, respectiv:

- pentru realizarea unui interes legitim al Operatorului sau de o terta persoana; sau
- pentru realizarea unei sarcini care servește unui interes public;
- in scop de marketing direct, inclusiv crearii de profiluri in masura in care este legata de marketingul direct respectiv.

In situatia primelor doua cazuri, PJ prin Departamentul responabil va analiza cererea persoanei vizate, dispunand oprirea operatiunii de prelucrare a datelor, cu exceptia cazului cand, cu avizul Responsabilului cu protectia datelor, se poate demonstra că PJ are motive legitime și imperioase care justifică prelucrarea in continuare a datelor pentru scopurile mentionate și care prevalează asupra intereselor, drepturilor și libertăților persoanei vizate sau că scopul este constatarea, exercitarea sau apărarea unui drept în instanță.

In situatia in care persoana se opune prelucrarii de date realizate in scop de marketing direct, inclusiv pentru crearea de profiluri in acest scop, PJ prin Responsabilul cu protectia datelor cu caracter personal va informa de indata organizatia care realizeaza operatiunile de marketing direct pentru stoparea acestei activitati de prelucrare fata de persoana vizata, aceasta avand dreptul de a se opune in orice moment pentru o asemenea prelucrare.

In situatia in care operatiunile de marketing direct sunt realizate in baza consimtamantului persoanei vizate, persoana vizata are dreptul de a-si retrage oricand consimtamantul, PJ urmand a trata cererea persoanei vizate conform sectiunii aplicabile dreptului de retragere a consimtamantului mai jos mentionata.

In situatia prelucrarilor de date cu caracter personal in scop statistic, istoric, sau de cercetare stiintifica, persoana vizata are dreptul de a se opune prelucrării datelor cu caracter personal care o privesc, cu excepția cazului în care prelucrarea este necesară pentru îndeplinirea unei sarcini din motive de interes public.

In situatia de exceptie prevazuta, Departamentul responsabil cu gestionarea sesizarii va solicita avizul Responsabilului cu protectia datelor al PJ, pentru transmiterea unui raspuns documentat persoanei vizate.

Ca in toate celelelate cazuri, Departamentul responsabil de gestionarea sesizarii persoanei vizate, are obligatia de a tine documentatia necesara pentru demonstrarea conformitatii PJ cu prevederile RGDP privind drepturile persoanei vizate.

De asemenea, toate celelalte aspecte privind responsabilitatea redactarii, semnarii si trimiterii raspunsului catre persoana vizata prevazute la punctul 5.1., raman aplicabile si cererilor privind dreptul la opozitie.

10.7 Dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrare automata, inclusiv crearea de profiluri

Persoana vizată are dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă, cu

excepția urmatoarelor situatii:

- prelucrarea este strict necesara pentru încheierea sau executarea unui contract intre PJ si persoana vizata, cum ar fi analiza de risc pentru creditarea sau finantarea persoanei vizate;
- prelucrarea este autorizata de prevederile legale aplicabile Operatorului, prevazand măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate;
- prelucrarea datelor se realizează pe baza consimtamantului liber exprimat al persoanei vizate, cu mentiunea ca aceasta are dreptul de a-si retrage oricand consimtamantul conform sectiunii urmatoare.

Dacă datele sunt utilizate pentru a lua decizii automate cu privire la persoana vizată, persoana vizata are dreptul sa solicite informatii cu privire la logică utilizata de sistemul/sistemele interne de prelucrare a datelor cu caracter personal ale PJ.

In legatura cu acest tip de prelucrari de date, realizate pentru încheierea sau executarea unui contract cu persoana vizata sau in baza consimtamantului persoanei vizate, aceasta are urmatoarele drepturi, ce pot face obiectul unei cereri adresate PJ:

- dreptul de a obtine din partea PJ intervenția umană asupra modului de prelucrare a datelor, rezultatele analizei si deciziei bazate exclusiv pe prelucrarea automata, inclusiv constand in profilarea sa;
- dreptul de a-si exprima punctul sau de vedere cu privire la cele de mai sus;
- dreptul de a contesta decizia astfel adoptata de PJ.

Responsabilul cu protectia datelor cu caracter personal va solicita opinia departamentului operational din cadrul PJ responsabil de realizarea operatiunii de prelucrare a datelor in mod automat si de luarea deciziei de afaceri pe baza acestei prelucrari. Toate celelalte aspecte privind responsabilitatea redactarii, semnarii si trimiterii raspunsului catre persoana vizata prevazute la punctul 5.1., raman aplicabile si cererilor privind dreptul reglementat in acesta sectiune.

10.8 Dreptul de retragere a consimtamantului

Atunci când prelucrarea datelor cu caracter personal se realizează in temeiul acordului persoanei vizate, potrivit art. 6 alineat 1) litera a) sau, dupa caz, art. 9 alineat 2) litera a) din RGDP, aceasta are dreptul de a-si retrage in orice moment consimtamantul, fara a afecta legalitatea prelucrării efectuate pe baza consimtamantului înainte de retragerea acestuia. Atat PJ cat si departamentele responsabile cu operatiunea de prelucrare realizata in temeiul consimtamantului au obligatia de a lua, fara intarziere, toate masurile necesare pentru realizarea dreptului persoanei vizate, respectiv pentru incetarea operatiunii de prelucrare pentru care aceasta si-a retras consimtamantul.

Retragerea consimtamantului trebuie sa se poata realiza in mod facil de catre persoana vizata, fara ca PJ sa aiba dreptul de a conditiona in vreun fel acest drept sau de a implementa masuri care sa ingreuneze exercitarea facila a acestui drept de catre persoana vizata.

In situatia unei asemenea cereri din partea persoanei vizate, care se poate exercita pe orice cale, inclusiv verbal, Departamentul responsabil cu solutionarea cererii persoanei vizate va informa de indata departamentul care gestioneaza operatiunea de prelucrare a

datelor in cauza despre retragerea consimtamantului persoanei vizate si despre obligatia acestuia de a inceta operatiunea de prelucrare realizata in baza consimtamantului pana la retragerea acestuia conform celor de mai sus.

Toate celelalte aspecte privind responsabilitatea redactarii, semnarii si trimiterii raspunsului catre persoana vizata prevazute la punctul 5.1., raman aplicabile si cererilor persoanei vizate privind dreptul la retragerea consimtamantului.

11. FLUXUL DE SOLUTIONARE AL CERERILOR PERSOANELOR VIZATE

11.1 Persoanele responsabile de gestionarea cererii persoanei vizate

Cererile persoanei vizate se pot transmite de catre aceasta pe canalele de comunicare cu PJ, respectiv:

- adresa sediului PJ, din Bucuresti, Str. Spatarului nr. 30;
- adresa de email a PJ[2] office@ptir.ro, cererea putând fi introdusa in format electronic de catre persoana vizata;

In cazul in care persoana vizata va transmite o cerere de exercitare a drepturilor sale prevazute de articolul 15-22 din RGDP, asfel cum au fost descrise in sectiunea 10 a prezentei politici, aceasta va fi transmisa catre Departamentul responsabil.

11.2 Identificarea persoanei vizate

Pentru a putea răspunde în timp util solicitărilor persoanei vizate, Departamentul responsabil cu gestionarea cererii persoanei vizate va solicita persoanei vizate, dupa caz, furnizarea unor informații minime, dar necesare pentru a valida identitatea (de ex. pentru a se asigura că persoana care solicită informațiile este persoana vizată sau persoana autorizată sa obtina informatiile solicitate). Astfel, se pot solicita persoanei vizate să furnizeze doua sau mai multe categorii de date cu caracter personal care sa permita Companiei identificarea: de ex. o categorie obligatorie priveste furnizarea numelui complet, dar pot fi solicitate/transmise si alte date cu caracter personal, cum ar fi un cod unic de angajat, informatii legate de adresa sau data nasterii.

În cazul în care solicitantul nu are, totodata, si calitatea de persoana vizată este necesară confirmarea scrisă că solicitantul este autorizat să acționeze în numele persoanei vizate, PJ fiind indreptatita sa solicite evidente conform legislatiei aplicabile cu privire la calitatea acesteia.

11.3 Analiza cererii si solutionarea acesteia

Dupa identificarea persoanei vizate se va trece la analiza pe fond a cererii acesteia.

In situatia in care sunt necesare informatii sau analize, opinii, etc. de la alte departamente din cadrul PJ, acestea vor asigura, pe baza cererii Departamentului responsabil de soluționarea

[2] Prin considerentul 59 din RGPD se recomandă Operatorilor de date să se ofere mijloacele necesare pentru ca cererile persoanelor vizate să fie făcute pe cale electronică, în special în cazul în care datele cu caracter personal sunt prelucrate prin mijloace electronice.

cererii, sprijinul necesar identificarii persoanei vizate si solutionarii cererii acesteia, fara întârziere.

De asemenea, in cazul in care este necesar suportul persoanelor imputernicite ale PJ (de ex. furnizorii de servicii IT), acestia vor fi implicati de catre Departamentului responsabil de solutionarea cererii, inca de la inregistrarea cererii, astfel incat sa nu se intarzie nejustificat din punct de vedere legal solutionarea acesteia.

Raspunsul redactat de catre Departamentului responsabil de solutionarea cererii, pe baza analizei sale, a documentelor si informatiilor primite, a opiniilor departamentelor de specialitate, va fi trimis persoanei vizate.

Raspunsul la cerere se transmite persoanei vizate la adresa de domiciliu/reședința sau de corespondenta a acesteia. În situația în care persoana vizată introduce cererea în format electronic şi cu excepţia cazului în care persoana vizată solicită un alt format, informaţiile sunt furnizate într-un format electronic utilizat în mod curent.

Termenul de raspuns la cererea persoanei vizate este de cel mult o luna de la primirea cererii. Cu toate acestea, Departamentul responsabil cu gestionarea cererii persoanei vizate va avea in vedere ca PJ are obligatia de a-i furniza persoanei vizate informatii relevante privind acțiunile întreprinse în urma unei cereri de exercitarea a drepturilor acesteia conform articolelor 15-22 din RGDP, fără întârzieri nejustificate.

Termenul de 1 luna este un termen maxim in care PJ trebuie sa raspunsa persoanei vizate. Această perioadă de 1 luna poate fi prelungită cu două luni numai in cazuri exceptionale, respectiv atunci când este necesar, ținându-se seama de complexitatea și numărul cererilor.

Intr-o asemenea situatie, PJ prin Departamentul responsabil cu gestionarea cererii persoanei vizate va informa persoana vizată cu privire la orice astfel de prelungire, în termen de o lună de la primirea cererii, prezentând și motivele întârzierii.

In situatia in care PJ nu a dat curs cererii persoanei vizate, respingand-o ca nefundamentata, Departamentul responsabil cu gestionarea cererii persoanei vizate va explica in raspunsul adresat persoanei vizate, motivele care au stat la baza respingerii cererii sale.

Totodata, in situatia in care PJ poate demonstra că nu este în măsură să identifice persoana vizată, desi au fost solicitate persoanei vizate informatii suplimentare c are sa permita identificarea acesteia, Departamentul responsabil cu gestionarea cererii persoanei vizate, va informa, de indata, persoana vizată în mod corespunzător, despre acest lucru, cu exceptia cazului în care nu este posibila transmiterea unui raspuns catre persoana vizata din motive strict obiective (de ex. persoana vizata nu este clientul companiei si nu a lasat o adresa la care sa poata fi contactata).

Totodată, persoana vizata are dreptul de a primi răspuns la cererea sa in mod gratuit.

In cazul în care cererile din partea unei persoane vizate sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, operatorul poate: (a) fie să perceapă o taxă rezonabilă ținând cont de costurile administrative pentru furnizarea informațiilor sau a comunicării sau pentru luarea măsurilor solicitate; (b) fie să refuze să dea curs cererii.

În aceste cazuri, operatorului îi revine sarcina de a demonstra caracterul vădit nefondat sau excesiv al cererii, astfel ca Departamentul responsabil cu gestionarea cererii persoanei vizate va asigura documentarea corespunzatoare a acestor situatii.

11.4 Evidenta si arhivarea cererii persoanei vizate

Departamentul responsabil cu gestionarea cererii persoanei vizate este obligat sa tina documentatia necesara si evidentele referioare la modul de solutionare a cererii pe o perioada necesara in functie de scopul operatiunilor de prelucrare si de regulile aplicabile arhivarii documentelor privind cererile si sesizarile primite de PJ, dar nu mai putin de 3 ani, conform termenului de prescriptie extinctiva, cu exceptia cazului in care nu exista un temei justificativ pentru pastrarea documentatiei pe durata acestui termen (de ex. situatia in care operatiunea de prelucrare inceteaza ca urmare a retragerii consimtamantului persoanei vizate, iar PJ nu are un temei juridic pentru pastrarea datelor dupa retragerea consimtamantului).

In cazul in care se aplica alte dispozitii legale pentru arhivare, ce impun termene specifice de prelucrare, vor fi avute in vedere aceste dispozitii speciale ce reglementeaza in mod expres perioada pentru care Operatorul de date este obligat sa stocheze si sa prelucreze/puna la dispozitia altor autoritati ale statului datele cu caracter personal prelucrate.

De asemenea pentru inregistrarea cererilor persoanei vizate si a solutiilor adoptate de PJ, Departamentul responsabil de gestionarea cererilor persoanelor vizate va tine un Registru jurnal al acestora.

12. DESTINATARI/PERSOANE IMPUTERNICITE/OPERATORI ASOCIATI

Datele cu caracter personal ale persoanelor vizate pot fi dezvaluite catre si respectiv prelucrate de către următoarele persoane, cu respectarea întocmai a legislației privind protecția datelor cu caracter personal:

- persoana vizata/ reprezentanții persoanei vizate;
- furnizorii de prestări servicii, precum furnizorii din domeniul muncii (de exemplu furnizorii de cursuri de formare profesionala sau servicii de consultanta Resurse Umane), furnizori de servicii si sisteme IT, furnizori de servicii juridice, de curierat, contabili, cenzori, executori judecătorești, precum și toate societățile din aceste categorii de destinatari de la care Operatorul va contracta servicii si produse și care au luat măsuri adecvate de protecţie, conform prevederilor legale, pentru a asigura că aceştia îşi respectă obligaţiile privind protecţia datelor cu caracter personal
- Părţile contractante ale PJ, care au calitatea de operator asociat conform art. 26 din RGDP, pentru îndeplinirea unor servicii externalizare acestora
- Alte societăţi din UE/EEA, cum ar fi auditori ai PJ.
- Autorităţile statului precum ITM, autoritatea fiscala, etc. pe baza competenţelor acestora prevăzute de legea aplicabilă.

A. PERSOANA IMPUTERNICITA

În cazul în care prelucrarea urmează să fie realizată în numele unui Operator, Operatorul recurge doar la persoane împuternicite care oferă garanţii suficiente pentru punerea în aplicare a unor măsuri tehnice şi organizatorice adecvate, astfel încât prelucrarea să respecte cerinţele prevăzute în Regulamentul general privind protecția datelor şi să asigure protecţia drepturilor persoanei vizate.

Persoana împuternicită de operator nu recrutează o altă persoană împuternicită de operator fără a primi în prealabil o autorizaţie scrisă, specifică sau generală, din partea operatorului.

Prelucrarea de către o persoană împuternicită de un operator va fi reglementată printr-un contract sau alt act juridic în temeiul dreptului Uniunii sau al dreptului intern care are caracter obligatoriu pentru persoana împuternicită de operator în raport cu operatorul şi care stabileşte obiectul şi durata prelucrării, natura şi scopul prelucrării, tipul de date cu caracter personal şi categoriile de persoane vizate şi obligaţiile şi drepturile operatorului.

Respectivul contract sau act juridic prevede în special că persoană împuternicită de operator:

a)prelucrează datele cu caracter personal numai pe baza unor instrucţiuni documentate din partea operatorului, inclusiv în ceea ce priveşte transferurile de date cu caracter personal către o ţară terţă sau o organizaţie internaţională, cu excepţia cazului în care această obligaţie îi revine persoanei împuternicite în temeiul dreptului Uniunii sau al dreptului intern care i se aplică; în acest caz, notifică această obligaţie juridică operatorului înainte de prelucrare, cu excepţia cazului în care dreptul respectiv interzice o astfel de notificare din motive importante legate de interesul public;

b)se asigură că persoanele autorizate să prelucreze datele cu caracter personal s-au angajat să respecte confidenţialitatea sau au o obligaţie statutară adecvată de confidenţialitate;

c)adoptă toate măsurile necesare în conformitate cu articolul 32 din Regulamentul general privind protecția datelor cu caracter personal;

d)respectă condiţiile menţionate in art 28 din Regulamentul general privind protecția datelor privind recrutarea unei alte persoane împuternicite de operator;

e)ţinând seama de natura prelucrării, oferă asistenţă operatorului prin măsuri tehnice şi organizatorice adecvate, în măsura în care acest lucru este posibil, pentru îndeplinirea obligaţiei operatorului de a răspunde cererilor privind exercitarea de către persoana vizată a drepturilor persoanei vizate;

f)ajută operatorul să asigure respectarea obligaţiilor prevăzute la articolele 32-36 din Regulamentul general privind protectia datelor cu caracter personal, ţinând seama de caracterul prelucrării şi informaţiile aflate la dispoziţia persoanei împuternicite de operator;

g)la alegerea operatorului, şterge sau returnează operatorului toate datele cu caracter personal după încetarea furnizării serviciilor legate de prelucrare şi elimină copiile existente, cu excepţia cazului în care dreptul Uniunii sau dreptul intern impune stocarea datelor cu caracter personal;

h)pune la dispoziţia operatorului toate informaţiile necesare pentru a demonstra respectarea obligaţiilor prevăzute de ar. 28 din Regulamentul general privind protectia datelor, permite desfăşurarea auditurilor, inclusiv a inspecţiilor, efectuate de operator sau alt auditor mandatat şi contribuie la acestea.

B. OPERATOR ASOCIAT

In cazul in care un partener contractual stabilește in comun cu PJ scopurile si mijloacele de prelucrare, aceștia au calitatea de operatori asociati.

In acest caz, operatorii asociati au obligatia conform art. 26 din Regulamentul general privind protectia datelor sa stabileasca in mod transparent responsabilitatile fiecaruia in ceea ce priveste indeplinirea obligatiilor ce revin potrivit Regulamentului general de protectia datelor, in special in cee ace priveste exercitarea drepturilor persoanelor vizate si indatoririle fiecaruia de furnizare a informatiilor prevazute de art. 13 si 14 din Regulamentul general privind protectia datelor.

Operatori asociați se vor asigura ca persoanelor vizate li se va aduce la cunostinta cuprinsul acestui acord.

De asemenea, prin acordul incheiat intre operatorii asociati, se va respecta dreptul persoanei vizate de a-si exercita drepturile prevazute de Regulamentul general privind protectia datelor cu privire la si in raport cu fiecare dintre operatori.

13. EVIDENTA ACTIVITATILOR DE PRELUCRARE

Operatorul păstrează o evidenţă a activităţilor de prelucrare desfăşurate sub responsabilitatea sa. Aceasta evidenţă cuprinde toate următoarele informaţii:

- scopurile prelucrării;
- o descriere a categoriilor de persoane vizate şi a categoriilor de date cu caracter personal;
- categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din ţări terţe sau organizaţii internaţionale;
- dacă este cazul, transferurile de date cu caracter personal către o ţară terţă sau o organizaţie internaţională, inclusiv identificarea ţării terţe sau a organizaţiei internaţionale respective şi, daca este cazul, documentaţia care dovedeşte existenţa unor garanţii adecvate;
- acolo unde este posibil, termenele-limită preconizate pentru ştergerea diferitelor categorii de date;
- acolo unde este posibil, o descriere generală a măsurilor tehnice şi organizatorice de securitate.

Evidenţa activităților de prelucrare se formulează în scris, inclusiv în format electronic si se actualizează permanent.

Fiecare sef de Departament din cadrul PJ are obligația de a informa persoana responsabila cu protecția datelor cu privire la operațiunile sale de prelucrare a datelor cu caracter personal si de a-si actualiza operațiunile din Registrul activităților de prelucrare la nivelul departamentului său.

Operatorul pune aceasta evidenţa la dispoziţia ANSPDCP, la cererea acesteia.

14. MASURI DE SECURITATE

PJ asigura implementarea unor masuri tehnice si organizatorice adecvate pentru prevenirea riscurilor prezentate de operațiunile de prelucrare a datelor cu caracter personal, generate în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.

Masurile de securitate vor fi adoptate luându-se in calcul cel puțin următoarele aspecte:

- stadiul actual al dezvoltării tehnologice, aplicațiilor, bazelor de date, precum si a altor elemente in funcție de operațiunea de prelucrare si de mijloacele realizării acesteia,
- costurile implementării masurilor de securitate,
- natura, domeniul de aplicare, contextul și scopurile prelucrării datelor cu caracter personal,
- riscul cu diferite grade de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice.

PJ, avand in vedere elementele analizate mai sus, va asigura cel puțin următoarele masuri tehnice:

- capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare;
- capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;
- un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

Totodată, PJ va asigura urmatoarele cerinte minime de securitate:

- **Controlul accesului**

Accesul persoanelor neautorizate la computerele şi terminalele de acces prin care sunt prelucrate sau accesate date cu caracter personal este interzis. Măsurile privind restricţionarea sau securizarea accesului sunt efectuate prin cartelă magnetică, cheie, uşă securizată, personal de securitate sau dispozitive de monitorizare precum sistem alarmă, supraveghere vídeo.

- **Identificarea şi autentificarea utilizatorului unei baze de date sau sisteme IT** se realizează prin coduri de acces unice, fiecare utilizator autorizat având propriul nume de utilizator si propria parola pe care o tastează personal, nefiind permisa impartasirea codurilor de acces către alți salariați sau alte persoane. Niciodată mai mulţi utilizatori nu pot să aibă acelaşi cod de identificare.

Parolele sunt şiruri de caractere, fiind compuse dintr-o combinație de caractere mari, mici, precum si alte simboluri (e.g. %#&), astfel incat sa se asigure cel puțin un şirul de 8

caractere. La introducerea parolelor acestea nu pot fi afişate în clar pe monitor. Parolele trebuie schimbate periodic, respectiv dupa trecerea unei perioade de 6 luni Schimbarea periodică a parolelor se face numai de către salariatii / utilizatori autorizaţi de operator. In cazul introducerii de 5 introduceri greşite ale parolei, se va refuza automat accesul acelui utilizator la sistemul informatic.

PJ va autoriza anumiţi salariati / utilizatori pentru a revoca sau a suspenda un cod de identificare şi autentificare acordat unui salariat conform fisei sale de post, dacă acesta şi-a dat demisia ori a fost concediat, şi-a încheiat contractul individual de munca, a fost transferat la alt serviciu şi noile sarcini nu îi solicită accesul la date cu caracter personal, a abuzat de codurile primite sau dacă va absenta o perioadă îndelungată stabilită de entitate.

Orice salariat/ utilizator care primeşte un cod de identificare şi un mijloc de autentificare este obligat sa păstreze confidenţialitatea acestora şi să răspundă în acest sens în faţa operatorului.

- **Tipul de acces**

Salariații accesează numai datele cu caracter personal necesare pentru îndeplinirea atribuţiilor lor de serviciu, conform fisei de post sau altor documente aplicabile. In funcție de atribuțiile fiecarui salariați, aceștia vor primi drepturi de acces de după funcţionalitate (cum ar fi: administrare, introducere, prelucrare, salvare a datelor etc.) şi după acţiuni aplicate asupra datelor cu caracter personal (cum ar fi: scriere, citire, ştergere).

De exemplu, un salariat care are acces in sistem doar pentru consultarea datelor cu caracter personal, neavând atribuțiuni de realizare al actor activitati, va primi doar drepturi de acces de citire a datelor, si nu de scriere sau ștergere a acestora.

Departamentul de IT care asigură suportul tehnic al sistemelor informatice poate avea acces la datele cu caracter personal, conform fisei de post, numai pentru rezolvarea unor cazuri excepţionale.

- **Colectarea datelor cu caracter personal se va realiza numai in baza unui temei juridic astfel cum se prevede in prezenta politica si in GDPR**

PJ desemnează anumiți salariați / utilizatori ai sistemelor informatice ale PJ pentru operatiile de colectare si introducere de date cu caracter personal in sistemul informațional, care vor putea fi modificate doar de utilizatori autorizați in acest sens.

PJ va introduce un sistem informatic care sa permită identificarea si înregistrarea utilizatorului care a facut modificarea in cadrul bazei de date, data si ora modificarii, precum si mentinerea datelor șterse sau modificate.

- **Copii de siguranța (back-up)**

PJ va desemna anumiți utilizatori care vor executa copii de siguranța ale bazelor de date cu caracter personal, precum si ale programelor folosite pentru prelucrările automatizate, cu respectarea prevederilor legale. Copiile de siguranța vor fi stocate in alte camere, in fișete metalice cu sigiliu aplicat, iar accesul la acestea va fi limitat si monitorizat.

- **Computerele si terminalele de acces**

Computerele si terminalele de acces vor fi instalate in incaperi cu acces restrictionat. Terminalele de acces folosite in relatia cu publicul pe care apar date cu caracter personal vor fi pozitionate astfel incat sa nu poata fi vazute de public.

- **Operatorul va stabili modalităţile stricte prin care se vor distruge datele cu caracter personal.**

În conformitate cu dispozițiile art. 5 lit. e) din Regulamentul European nr. 679/2016, se va stabili durata de stocare a datelor prelucrate pentru fiecare operațiune identificată în Registrul privind evidența operațiunilor de prelucrare a datelor cu caracter personal, având în vedere dispozițiile legale obligatorii conform Legii nr. 16/1996 privind Arhivele Naționale, Legii nr. 82/1991 privind contabilitatea, etc. Autorizarea pentru această prelucrare de date cu caracter personal trebuie limitată la câţiva utilizatori.

La expirarea perioadei de prelucrare sau de retenție / arhivare a datelor, acestea se vor gestiona in mod corespunzător, conform regulilor interne. In cazul in care aceste documente urmează a fi distruse, la fel ca si in cazul documentelor care nu mai sunt de actualitate sau sunt în copie şi care conţin date cu caracter personal se va utiliza doar distrugătorul de hârtie.

Astfel, in situația proceselor de recrutare, după finalizarea acestora, prin încheierea contractului individual de munca cu candidatul selectat, CV-urile celorlalți candidați se vor distruge, cele electronic prin ștergerea fișierului electronic, cele imprimate pe suport de hartie prin tocarea acestora cu tocător special pentru tăierea documentelor confidențiale. In situația in care exista un temei justificativ legal pentru tinerea acelui document in format electronic, cum ar fi păstrarea CV-urilor intr-o baza pe date, ținuta in format electronic, pe un termen suplimentar de 12 luni, cu acordul persoanei vizate, copiile documentelor imprimate pe suport de hârtie care nu mai sunt necesare se vor distruge, in timp ce fișierele in format electronic se vor arhiva intr-un sistem informațional criptat.

- **Sistemele de telecomunicații**

Accesul la reţea se face doar prin conexiuni securizate. Toate aceste sisteme sunt trecute prin teste riguroase şi aprobate pentru utilizare. Responsabilul de aplicaţie verifică lunar ştergerea conturilor de utilizator şi a drepturilor de acces pentru salariații care au părăsit PJ.

Sistemul de email este astfel conceput încât datele transmise în reţea sa nu poată fi interceptate, serverul de email fiind criptat. De asemenea, documentele conținând date cu caracter personal se trimit parolate, parola urmărind criteriile mai sus menționate. Parola se comunică telefonic destinatarului sau prin sms, fiind verificat înainte destinatarul/utilizatorul telefonului.

- **Folosirea computerelor**

In vederea menținerii securității prelucrării datelor cu caracter personal, in special împotriva virușilor informatici, PJ:

  - interzice folosirea de catre utilizatori a programelor software care provin din surse externe sau dubioase;

- informeaza periodic utilizatorii cu privire la daunele provocate de catre virusii informatici;
- implementeaza sisteme automate de devirusare si de securitate a sistemelor informatice, precum si alte masuri tehnice si organizatorice adecvate pentru protectia si securitatea datelor.

- **Instruirea personalului**

PJ va organiza cursuri de pregătire a utilizatorilor bazelor de date, iar in cadrul acestora va furniza informații cu privire la prevederile GDPR si la legislația națională si europeana aplicabila in domeniul protecției si securității datelor cu caracter personal.

Salariații PJ sunt obligați sa participe la cursurile de pregătire profesionala organizate de PJ. Coordonatorii selectie grup tinta din proiectele finantate din fonduri nerambursabile vor urma obligatoriu aceste cursuri, inante de inceperea activitatii in proiect.

Totodata, salariații PJ sunt obligați sa pastreze confidentialitatea si integritatea datelor cu caracter personal si sa prelucreze date cu caracter personal numai in conformitate cu prezenta Politica, cu Regulamentul General UE privind protecția datelor (nr. 679/2016), precum si alte reglementari legale in vigoare.

15. EVALUAREA IMPACTULUI ASUPRA PROTECŢIEI DATELOR

Având în vedere natura, domeniul de aplicare, contextul şi scopurile prelucrării, în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, Operatorul efectuează, înaintea prelucrării, o evaluare a impactului operaţiunilor de prelucrare prevăzute asupra protecţiei datelor cu caracter personal conform art. 35 RGDP. In cazul in care riscurile reziduale au un nivel ridicat deși PJ implementează masuri tehnice si organizatorice adecvate pentru protecția datelor, PJ este obligata sa consulte ANSPDCP conform art. 36 din RGDP.

Evaluarea impactului asupra protectiei datelor si, dupa caz, consultarea ANSPDCP, se va realiza conform Politicii de evaluare a impactului asupra protectiei datelor.

16. TRATAREA INCIDENTELOR DE SECURITATE A DATELOR CU CARACTER PERSONAL

Tratarea incidentelor de securitate a datelor cu caracter personal se realizeaza in conformitate cu prevederile art. 33 si 34 din Regulamentul General privind protectia datelor.

Astfel, in cazul în care are loc un incident de securitate ce are un impact asupra protectiei datelor cu caracter personal, Operatorul notifică acest lucru Autoritatii fără întârzieri nejustificate şi, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoştinţă de aceasta, cu excepţia cazului în care nu este susceptibilă să genereze un risc pentru drepturile şi libertăţile persoanelor fizice.

Responsabilul cu protectia datelor va lua masurile necesare depunerii Notificarea ANSPDCP, cu aprobarea Reprezentantului legal.

Totodata, daca încălcarea securităţii datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, operatorul informează persoana vizată fără întârzieri nejustificate cu privire la această încălcare.

Tratarea cazurilor de incalcare a securitatii datelor va face obiectul Politicii privind incidentele de securitate a datelor cu caracter personal.

17. NERESPECTAREA POLITICII

Nerespectarea acestei proceduri reprezinta o abatere grava disciplinara, putând conduce la sanctionarea disciplinara a salariatilor care se fac vinovati de incalcarea sa si a legislației aplicabile, indeosebi RGDP, inclusiv cu masura incetarii contractului individual de munca conform legislației muncii aplicabile.

18. RGDP IN PROIECTELE DERULATE DE PTIR

In implementarea proiectelor, se vor respecta prevederile Regulamentului nr. 679 din 27 aprilie 2016 privind protectia persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal si privind libera circulatie a acestor date (Regulamentul general privind protectia datelor), precum si prevederile Directivei 2002/58/CE privind prelucrarea datelor personale si protejarea confidentialitatii in sectorul comunicatiilor publice (Directiva asupra confidentialitatii si comunicatiilor electronice), transpusa in legislatia nationala prin Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal si protectia vietii private in sectorul comunicatiilor electronice, cu modificarile si completarile ulterioare. Astfel, toti participantii la activitatile proiectului vor fi informati despre obligativitatea de a furniza datele lor personale si despre faptul ca datele lor personale vor fi prelucrate in aplicatiile electronice SMIS/MySMIS, in toate fazele de evaluare/ contractare/ implementare/ sustenabilitate a proiectului, cu respectarea dispozitiilor legale mentionate. Responsabilii grup tinta vor face dovada ca au obtinut consimtamantul pentru prelucrarea datelor cu caracter personal de la fiecare participant, in conformitate cu prevederile legale mentionate.

Coordonatorul selecție grup tinta/managerul de proiect din fiecare proiect va fi responsabil cu protectia datelor cu caracter personal si va indeplini cel putin urmatoarele sarcini:

- elaborarea si aprobarea unei proceduri de notificare a incalcarii securitatii datelor cu caracter personal
- realizarea si mentinerea unei evidente a activitatilor de prelucrare a datelor cu caracter personal
- informarea persoanelor participante la proiect cu privire la datele sale de contact, scopurile prelucrarii datelor, a temeiului juridic, perioada de stocare a datelor si potentialii destinatari ai datelor cu caracter personal – Anexa 1 la prezenta politica
- verificarea consimtamantului pentru prelucrarea datelor cu caracter personal de la fiecare participant la proiect, in conformitate cu prevederile legale
- evaluarea riscurilor prezentate de prelucrarea datelor cu caracter personal din proiectul respectiv

Anexa 1

NOTA DE INFORMARE PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL

Avand in vedere Regulamentul (UE) 2016/679 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 (RGPD), ASOCIAȚIA PATRONATUL TINERILOR INTREPRINZATORI DIN ROMANIA, înregistrată în Registrul asociațiilor și fundațiilor sub nr. 151/16.02.2006, cu sediul în Bucuresti, Str. Spatarului nr. 30, sector 2, România, telefon: 0318241592, fax:-, poștă electronică: office@ptir.ro,

va aducem la cunostinta urmatoarele:

Datele cu caracter personal pe care le prelucram

In cazul ANGAJATILOR:

- date de identificare: nume, prenume, data nașterii, sex, naționalitate, vârstă, CNP, adresa de domiciliu sau de reședință, e-mail, telefon, loc de muncă, copie C.I., starea civila, semnătura;
- date bancare;
- date privind studiile absolvite;
- imagine;
- date privind sanatatea si capacitatea de munca.

In cazul MEMBRILOR DE FAMILIE AI ANGAJATILOR:

- date de identificare: nume, prenume, data nasterii, sex, nationalitate, varsta, CNP, copie certificat de nastere (pentru minorii aflati in intretinere)

In cazul PARTICIPANTILOR la proiectele derulate de PTIR:

- date de identificare: nume, prenume, data nasterii, sex, nationalitate, varsta, CNP, adresa de domiciliu sau de resedință, e-mail, telefon, loc de munca, copie C.I., copie certificat de nastere, copie certificat de casatorie, starea civila, semnatura, etnie;
- date bancare;
- date privind studiile absolvite;
- imagine;
- date referitoare la profilarea aplicantilor la proiectele derulate de PTIR in vederea admiterii acestora.

Scopurile in care prelucram datelor cu caracter personal

PTIR prelucreaza date cu caracter personal in vederea:

- derularii contractelor individuale de munca;
- indeplinirii obligatiilor legale privind raportarea angajatilor in Registrul Salariatilor si a concediilor medicale catre Casa de Sanatate;
- validarea participantilor la proiectele derulate;
- indeplinirii obligatiilor contractuale din proiectele de finantare;
- reprezentarii societatii in fata instantelor de judecata și a autoritatilor publice, realizarea procedurilor de recuperare a creantelor, dupa caz;
- desfasurarii activitatilor de recrutare/selectie pentru ocuparea posturilor vacante;
- informarii partenerilor cu privire la activitatile desfasurate (pe website, Facebook, sau alte mijloace de comunicare online);

OBSERVATIE: Orice prelucrare de date efectuata in alte scopuri decat cele declarate initial va fi adusa la cunostinta printr-o nota de informare care va fi realizata separat.

Temeiurile juridice in baza carora prelucram datelor cu caracter personal:

- executarea unui contract. In aceasta categorie intra si demersurile realizate in vederea incheierii contractului
- indeplinirea unor obligații legale de către PTIR;
- interesul legitim atunci cand se are in vedere: organizarea activitatii pentru indeplinirea obiectivelor organizatiei; demararea si desfasurarea litigiilor pe rolul instantelor de judecata si (eventual) al altor autoritati publice; proceduri de recuperare a creantelor;
- consimtamantul dumneavoastra acordat in mod neconditionat si in scris, atunci cand ne aflam in situatii de prelucrari de date care necesita expres consimtamtul.

Pentru categoriile speciale de date prelucrate (datele privind sanatatea), temeiurile prelucrarii sunt următorele:

- scopuri legate de medicina preventiva sau a muncii, de evaluare a capacitatii de munca a angajatului,

Perioada pe care prelucram datele cu caracter personal:

- datele prelucrate in vederea executarii contractelor acestea vor fi stocate pe perioada contractului cat si pe o perioada de 5 ani de la data incetarii acestora. Exceptie fac contractele individuale de munca care se vor pastra pe perioada impusa de catre Nomenclatorul arhivistic, contractele de furnizare semnatura electronica ce se pastreaza timp de 10 ani conform Regulamentului UE 910/2014 si contractele de subventie/finantare nerambursabila care se pastreaza pe o perioada de 10 ani de la finalizarea proiectelor finantate. Termenele mentionate mai sus se calculeaza incepand cu data de 1 ianuarie a anului urmator celui in care are loc incetarea.

- datele prelucrate în scopuri contabile, în special cele legate de facturare si plati, vor fi stocate pe o perioadă de 10 ani, cu incepere de la data de 1 ianuarie a anului urmator incheierii exercitiului financiar in cursul caruia au fost intocmite, conform prevederilor Legii contabilitatii nr. 82/1991, cu modificarile si completarile ulterioare, inclusiv cele aduse prin Legea nr. 163/2018;

- datele privind procesul de recrutare vor fi pastrate pe o perioadă de 12 luni de la data de 1 ianuarie a anului ce urmeaza celui in care a avut loc procesul de recrutare/selecție;

- datele prelucrate in baza consimtamantului vor fi pastrate pe perioada mentionata in cuprinsul acestuia;

In cazul retragerii consimtamantul acordat, datele dumneavoastra cu caracter personal nu vor mai fi prelucrate in scopurile pentru care v-ati retras consimtamantul, din momentul retragerii consimtamantului, fara a afecta insa valabilitatea prelucrarii datelor efectuata inainte de acest moment;

OBSERVATIE: Datele cu caracter personal vor fi prelucrate și pe durata existenței unor obligații legale de pastrare a anumitor categorii de date ori de documente justificative, in funcție de reglementarile in vigoare,.

Cui divulgam datele cu caracter personal:

Datele pot fi divulgate catre furnizorii nostri de servicii doar daca acest lucru este imperios necesar pentru indeplinirea obiectului de activitate si numai in cazul oferirii unor garantii in ceea ce priveste securitatea datelor la care vor avea access.

Pentru raportările către autoritățile statului, potrivit obligațiilor legale în vigoare, va fi necesară transmiterea datelor dumneavoastră către diverse instituții publice, cum ar fi, spre exemplu: Agentia Nationala de Administrare Fiscala, Inspectoratul Teritorial de Munca, Casa Națională de Asigurări de Sănătate (CNAS) etc.

In cazul proiectelor ce beneficiaza de finantare europeana sau din bugetul de stat, datele dumneavoastra, in calitate de beneficiari vor fi comunicate catre entitatile de control si supraveghere a derularii proiectelor.

In cazul promovarii activitatii desfasurate de PTIR datele dumneavoastra vor fi divulgate catre furnizori de mass-media, numai in cazul in care exista o obligaţie contractuala sau daca exista un consimtamant expres.

Drepturile pe care le aveti în legătură cu prelucrarea datelor cu caracter personal:

- Dreptul de a primi informații cu privire la prelucrarea datelor și o copie a datelor procesate (dreptul de acces, articolul 15 RGPD),

- Dreptul de a solicita rectificarea datelor inexacte (dreptul la rectificare, art. 16 RGPD),

- Dreptul de a solicita ștergerea datelor cu caracter personal, cu exceptia situatiei in care acestea sunt prelucrate pentru indeplinirea unei obligatii legale, respectiv contractuale (dreptul de ștergere, articolul 17 RGPD),

- Dreptul de a solicita restrictionarea prelucrarii datelor (dreptul la restrictionarea prelucrarii, articolul 18 RGPD),

- Dreptul de a primi datele personale intr-un format structurat și de a solicita transmiterea acestor date catre un alt operator (dreptul la portabilitatea datelor, articolul 20 RGPD),

- Dreptul de a se opune prelucrarii datelor cu intentia de a înceta prelucrarea pe o perioada determinata (dreptul la obiecție, articolul 21 RGPD),

- Dreptul de a solicita si de a obţine retragerea, anularea si reconsiderarea oricarei decizii care produce efecte juridice asupra dumneavoastra, adoptata exclusiv in baza unei operatiuni de prelucrare a datelor cu caracter personal prin mijloace automatizate, in scopul evaluarii unor trasaturi de personalitate, precum abilitatile profesionale, credibilitatea, comportamentul dumneavoastra la locul de munca, interesele ș.a.. (dreptul de a nu fi supus unei decizii individuale automatizate, articolul 22 RGPD)

Totodata, mentionam ca in conformitate cu prevederile RGPD aveti dreptul de a retrage oricand un consimtamant dat (art.7 RGPD) si dreptul de a depune o plangere la o autoritate de supraveghere (art.77 RGPD) daca considerati ca prelucrarea datelor este o încălcare a RGPD. Retragerea consimtamantului nu va afecta legalitatea prelucrarii pe baza consimtamantului acordat inainte de retragere.

Exercitarea drepturilor de mai sus se poate realiza prin transmiterea unei adrese la sediul operatorului sau pe adresa de email office@ptir.ro. Mentionam ca pentru informatii cu privire al prelucrarea de date cu caracter personal ne puteti contacta si la numarul de telefon 0318241592.

Vă asigurăm că datele dumneavoastra personale sunt protejate, prelucrate și gestionate de noi, prin implementarea de măsuri tehnice, proceduri interne și organizatorice specifice, precum și prin aplicarea unor bune practici de protecție a datelor.

PRESEDINTE PTIR

Iuliana Postaru