Politica de protecție a datelor cu caracter personal

Aprobat de

Nume	Funcție	Dată	Semnătura
Andrei Bojita	**Director General**		

Informații despre document

Creat de: *Dana Bodea*

Istoricul versiunilor

Data	Versiunea	Modificat de	Scurtă descriere

Istoricul revizuirilor

Data revizuirii	Versiunea	Revizuit de	Funcția

Cuprins

Definiții și abrevieri

date cu caracter personal: 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;

date personale sensibile: date personale care dezvăluie originea rasială sau etnică, opinii politice, credințe religioase sau filosofice sau apartenența la sindicate, date genetice și date biometrice prelucrate în scopul identificării unice a unei persoane fizice, date privind sănătatea sau date referitoare la viața sexuală a unei persoane fizice sau la sex;

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

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

creare de profiluri: orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia;

pseudonimizare: prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;

sistem de evidență a datelor: 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: 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;

persoană împuternicită de operator: persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

destinatar: 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 în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autoritățile publice respective respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării;

parte terță: 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: 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;

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

date genetice: datele cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care oferă informații unice privind fiziologia sau sănătatea persoanei respective și care rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză;

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

autoritate de supraveghere: o autoritate publică independentă instituită de un stat membru în temeiul articolului 51 din Regulament;

reprezentant: o persoană fizică sau juridică stabilită în Uniune, desemnată în scris de către operator sau persoana împuternicită de operator în temeiul articolului 27, care reprezintă operatorul sau persoana împuternicită în ceea ce privește obligațiile lor respective care le revin în temeiul prezentului regulament;

organizație internațională: o organizație și organismele sale subordonate reglementate de dreptul internațional public sau orice alt organism care este instituit printr-un acord încheiat între două sau mai multe țări sau în temeiul unui astfel de acord.

DPO: Data Protection Officer (Responsabil de Protecția Datelor cu Caracter Personal);

GDPR: Regulamentul General de Protecție a Datelor cu caracter personal, Regulamentul European 679/2016 privind protecția persoanelor fizice in ceea ce privește prelucrarea datelor cu caracter personal si privind libera circulație a acestor date;

SEE: Spațiul Economic European.

1. Introducere

Entitatea juridică Romanian Business Consult, denumită în continuare „RBC" sau „Organizația" prin natura activităților desfășurate, colectează și prelucrează date a căror utilizare si dezvăluire se face respectând nivelul de confidențialitate atribuit fiecărei categorii în funcție de sensibilitatea acesteia pentru organizație sau pentru părți terțe cu care organizația intră în contact.

Politica de protecție a datelor cu caracter personal, denumită în continuare "Politică", descrie modul în care aceste date personale trebuie colectate, manipulate și stocate pentru a respecta standardele organizației legate de protecția datelor și Regulamentul European 679/ 2016 (GDPR) privind protecția persoanelor fizice in ceea ce privește prelucrarea datelor cu caracter personal si privind libera circulație a acestor date.

Politica se referă la datele cu caracter personal ce aparțin angajaților, clienților sau persoanelor fizice reprezentante ale partenerilor de afaceri. Politica nu se aplică altor tipuri de date legate de clienții și partenerii de afaceri care sunt persoane juridice sau instituții guvernamentale.

1.1. Obiectiv

Această politică urmărește să furnizeze cadrul general cu privire la asigurarea unui nivel adecvat de protecție a datelor cu caracter personal ale angajaților, clienților și partenerilor contractuali, procesate de RBC.

Această politică oferă un cadru pentru a sprijini Organizația să:

- respecte Regulamentul European 679/ 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și respectă bunele practici în materie de protecția datelor cu caracter personal;
- protejeze drepturile angajaților, clienților și partenerilor contractuali;
- fie transparentă cu privire la modul în care sunt procesate datele cu caracter personal;
- se protejeze de riscurile ce pot surveni în urma unei încălcări de securitate a datelor cu caracter personal precum:
    - încălcarea confidențialității - de exemplu, divulgarea datelor cu caracter personal către terțe părți din cauza lipsei sau implementării ineficiente a controalelor de securitate sau care rezultă din divulgarea necorespunzătoare a informațiilor;
    - daune aduse reputației – de exemplu, reputația RBC ar putea suferi dacă persoanele neautorizate obțin acces la date sensibile sau persoanele vizate sunt afectate de modul în care organizația utilizează datele lor personale.

Pentru a preveni și a reduce riscurile asociate colectării și prelucrării datelor cu caracter personal, este obligatoriu ca toți membrii personalului care au acces la orice tip de date cu caracter personal să se asigure că toate acțiunile lor respectă regulile stabilite de prezenta politică de protecție a datelor cu caracter personal. Această politică va fi adusă la cunoștință angajaților prin e-mail și/ sau afișare pe Intranet (sistemul electronic intern de informare).

1.2. Scop

Politica stabilește reguli pentru prelucrarea datelor cu caracter personal care aparțin:

- angajați RBC;
- tuturor angajaților și subcontractorilor de personal;
- clienților și furnizorilor RBC;
- tuturor partenerilor de afaceri care lucrează în numele RBC.

Datele angajatului includ, dar nu se limitează la:

- datele de identificare ale angajaților, statutul și educația angajaților (de exemplu: numele, prenumele, adresa, data nașterii, detaliile familiei, numărul de telefon, fotografiile, numărul de identificare național, seria și numărul cărții de identitate și pașaportului, certificatele și diplomele de studii, viza și alte permise de ședere, numărul permisului de conducere);
- istoricul locurilor de muncă ale angajaților și datele actuale privind locul de muncă (de exemplu: certificatele de muncă emise de foști angajatori, datele incluse în curriculum vitae, scrisoarea de ofertă, datele privind compensațiile, promoțiile, premiile și beneficiile, înregistrările disciplinare, evaluările performanțelor, numărul de înmatriculare pentru autovehicule);
- date privind cursurile de instruire ale angajaților, certificatele profesionale, inventarul de competențe (inclusiv specializările din industrie și servicii);
- pontajul și cheltuielile angajaților;
- informații despre angajați referitoare la asigurări (de exemplu: declarații medicale, certificat medical, asigurare de călătorie, pensii, alte beneficii);
- informații financiare ale angajaților (de exemplu: numărul contului bancar, fondurile de pensii, investițiile);
- datele incluse în corespondența electronică a angajaților, în comunicațiile telefonice și date rezultate în alt mod din utilizarea resurselor IT;

RBC procesează datele personale ale angajaților pe baza uneia dintre următoarele motive juridice, după caz:

- datele fiind necesare în vederea încheierea contractului de muncă (recrutare) sau pentru îndeplinirea contractului de muncă;
- datele fiind necesare pentru respectarea obligațiilor legale ale RBC (de exemplu: plata contribuțiilor sociale, obligațiile de securitate socială și protecția socială);
- datele fiind necesare pentru scopul intereselor legitime ale RBC care prevalează asupra intereselor sau a drepturilor și libertăților fundamentale ale persoanei vizate ce necesită protecție a datelor cu caracter personal;
- consimțământul angajatului.

Datele partenerilor contractuali sau angajaților partenerilor contractuali includ, dar nu se limitează la:

- date de contact (de exemplu: nume, prenume, adresă, număr de telefon, adresă de e-mail, loc de muncă / funcție, semnătură);
- toate celelalte date impuse de legile aplicabile pentru îndeplinirea unui contract sau a regulamentelor privind spălarea banilor.

2. Reguli de prelucrare a datelor cu caracter personal

RBC se angajează să adere la principiile de protecție a datelor stabilite de GDPR. Aceste principii sunt:

Legalitatea, corectitudinea și transparența: RBC trebuie să aibă o bază legitimă pentru prelucrarea datelor cu caracter personal.

RBC poate procesa datele cu caracter personal numai pe baza unuia dintre motivele oferite într-o manieră delimitată de către GDPR, în special:

- consimțământul explicit și lipsit de ambiguitate al persoanei vizate căreia aparțin datele;
- prelucrarea este necesară pentru a încheia un contract (de exemplu contractul de muncă) sau pentru a lua măsuri la cererea persoanei vizate înainte de a încheia un contract (de exemplu, analizarea unui CV depus de un candidat care solicită un loc de muncă cu RBC);
- prelucrarea este necesară pentru respectarea unei obligații legale la care RBC este supus;
- procesarea este necesară pentru scopurile intereselor legitime ale RBC; cu toate acestea, dacă acest lucru ar aduce atingere drepturilor, libertăților sau intereselor legitime ale persoanelor vizate la care se referă datele, RBC nu va prelucra datele cu caracter personal exclusiv în scopul propriilor interese legitime sau al intereselor legitime ale unei terțe părți.

În plus, prelucrarea nu trebuie să fie contrară nici unei legi aplicabile. RBC trebuie să informeze persoana vizată despre prelucrare într-o comunicare accesibilă și ușor de înțeles.

Limitarea scopului: RBC trebuie să colecteze date cu caracter personal doar în scopuri specificate, explicite și legitime și să nu proceseze datele mai mult decât pentru scopul pentru care au fost colectate sau pentru alte scopuri compatibile.

RBC trebuie să indice în mod clar scopul pentru care intenționează să prelucreze datele cu caracter personal și astfel de scopuri să nu contravină legii. Dacă RBC intenționează să utilizeze datele colectate într-un scop pentru un alt scop diferit de cel inițial, RBC trebuie să îndeplinească în prealabil toate formalitățile necesare prelucrării datelor pentru noul scop.

Minimizarea datelor: datele cu caracter personal prelucrate ar trebui să fie adecvate, relevante și limitate la ceea ce este necesar în legătură cu scopurile; asta înseamnă că RBC nu trebuie să proceseze date care nu sunt necesare pentru scopurile legitime urmărite.

Acuratețe: RBC are obligația de a se asigura că datele cu caracter personal sunt exacte și actualizate, atunci când este necesar; RBC trebuie să ia măsuri rezonabile pentru a se asigura că datele inexacte sunt șterse sau rectificate fără întârziere.

Limitarea stocării: RBC nu trebuie să păstreze datele cu caracter personal pentru o perioadă mai lungă decât este necesar pentru scopurile pentru care au fost colectate și prelucrate ulterior. RBC trebuie să stabilească perioade de retenție pentru datele cu caracter personal care sunt prelucrate.

Integritate și confidențialitate: RBC trebuie să dispună de controale de securitate adecvate pentru a proteja datele cu caracter personal împotriva prelucrării neautorizate și/ sau ilegale și împotriva pierderii accidentale, a distrugerii sau a deteriorării acestora.

Acestea includ atât măsuri tehnice, cât și organizatorice, cum ar fi procese definite, formare și conștientizare.

Transfer legal în afara SEE: RBC trebuie să transfere numai date cu caracter personal în afara SEE către țări recunoscute de Comisia Europeană pentru a asigura un nivel adecvat de protecție a datelor sau în cazul în care există garanții adecvate, cum ar fi un cadru contractual adecvat (de exemplu, pe baza clauzelor contractuale standard adoptate de Comisia UE).

Drepturile persoanelor vizate: persoanele vizate au un număr de drepturi pe care RBC trebuie sa le respecte, ca de exemplu, dreptul de a accesa o copie a datelor pe care RBC o deține despre acestea și dreptul de a renunța la marketingul direct pentru care au optat anterior.

Atât RBC cât și oricare dintre persoanele împuternicite de operator vor asigura confidențialitatea datelor personale în conformitate cu cerințele legii. Nu va publica sau nu va dezvălui în niciun alt fel nicio informație referitoare la datele cu caracter personal și la operațiunile efectuate fără consimțământul persoanelor vizate, cu excepția cazului in care RBC sau persoana împuternicită de operatorul de date acționează în temeiul unei obligații legale sau pe un alt temei legal.

RBC adoptă politici și proceduri care definesc principiile și practicile fundamentale ale organizației pentru a asigura confidențialitatea, integritatea și disponibilitatea informațiilor în format electronic și în format tipărit și securitatea operațiunilor.

În caz de pierderi, suspiciuni de pierderi sau pierderi potențiale ale datelor cu caracter personal care ajung în posesia unor persoane neautorizate, RBC anunță autoritățile competente și persoanele relevante în conformitate cu cerințele legale.

RBC va menține securitatea datelor protejând confidențialitatea, integritatea și disponibilitatea datelor personale, definite astfel:

- **Confidențialitate**: protejarea datelor cu caracter personal împotriva dezvăluirii neautorizate sau a interceptării inteligibile;
- **Integritate**: protejarea acurateței, completitudinii și actualității datelor cu caracter personal și a sistemelor informatice sau a programelor informatice care stochează sau prelucrează date cu caracter personal;
- **Disponibilitatea**: asigurarea faptului că datele personale sunt accesibile utilizatorilor autorizați atunci când este necesar.

2.1. Prelucrarea datelor sensibile cu caracter personal

RBC interzice prelucrarea datelor cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, credințele religioase sau filosofice, datele fizice sau psihice, calitatea de membru al sindicatelor, datele biometrice și prelucrarea datelor privind sănătatea sau viața sexuală, cu excepția cazului în care:

- persoana vizată și-a dat consimțământul explicit pentru prelucrare, cu excepția cazurilor în care legea prevede că consimțământul nu poate justifica prelucrarea datelor speciale într-o anumită situație;
- legea prevede în mod expres prelucrarea pentru a asigura protecția unui interes public important, cu condiția respectării corecte a tuturor drepturilor legate de datele cu caracter personal;

- prelucrarea este necesară pentru stabilirea, exercitarea sau apărarea unui drept legal în instanță;
- prelucrarea se referă la date care sunt făcute publice în mod evident de către persoana vizată;
- prelucrarea este necesară în scopul îndeplinirii obligațiilor și drepturilor specifice ale organizației în domeniul legislației muncii, securității sociale și protecției sociale, în măsura în care aceasta este autorizată prin lege sau printr-o convenție colectivă în conformitate cu legea.

2.2. Consimțământul

Consimțământul este definit în Art. 4 pct. 11 din GDPR, ca fiind „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".

Principii fundamentale

Consimțământul trebuie să fie dat în mod liber: consimțământul ar trebui să reflecte libertatea de alegere reală și liberă a persoanei vizate fără niciun element de constrângere sau presiune nejustificată asupra acesteia, evitând orice consecințe negative în cazul refuzului.

Consimțământul trebuie să fie specific: RBC trebuie să explice în mod clar și precis domeniul de aplicare și consecințele procesării datelor pentru care se solicită consimțământul. RBC trebuie să obțină consimțământul persoanei vizate separat pentru fiecare activitate de prelucrare efectuată în același scop sau în scopuri diferite.

Consimțământul trebuie să fie informat: natura prelucrării ar trebui explicată într-o formă inteligibilă și ușor accesibilă, folosind un limbaj clar și simplu, care nu conține clauze abuzive. Persoana vizată ar trebui să cunoască cel puțin următoarele aspecte, astfel încât consimțământul să poată fi considerat informat:

- identitatea RBC în calitate de operator de date;
- scopurile pentru care datele vor fi prelucrate;
- tipul de date care trebuie prelucrate;
- existența dreptului de retragere a consimțământului;
- unde este cazul, dacă datele ar fi utilizate pentru luarea deciziei automate care produce efecte juridice sau care afectează în mod similar persoana vizată;
- riscurile posibile ale transferurilor de date în afara UE/ SEE din cauza lipsei unei decizii de adecvare și a garanțiilor adecvate.

Consimțământul trebuie să fie explicit: RBC utilizează formulare de hârtie, răspunsuri e-mail și căsuțe de bifat (în engleză: *checkbox*).

Consimțământ explicit

Consimțământul explicit este necesar numai atunci când se prelucrează categorii de date sensibile (de exemplu: datele biometrice, originea rasială sau etnică, opiniile politice, credințele religioase sau filosofice, datele privind sănătatea fizică sau psihică, calitatea de membru al sindicatelor și prelucrarea datelor privind sănătatea sau viața sexuală).

Pentru obținerea consimțământului explicit, RBC acceptă o declarație scrisă și semnată de către persoana vizată. Validarea obținerii consimțământului se va face ulterior folosind următoarele căi: e-mail, SMS, telefon, utilizarea unei semnături electronice, înregistrarea unei declarații verbale.

Înregistrarea consimțământului

Ca orice alt operator de date, RBC are obligația de a păstra evidențele ce demonstrează faptul că a fost acordat un consimțământ valabil și că persoana vizată a fost informată.

Marketing direct

RBC se angajează în comunicarea comercială nesolicitată (comunicare de marketing direct) numai cu acordul prealabil al persoanei vizate ("opt-in"). În orice comunicare de marketing direct care se face către persoana vizată, se oferă persoanei vizate posibilitatea de a renunța la o comunicare de marketing direct. Datele cu caracter personal colectate de RBC nu vor fi divulgate niciodată unor societăți terțe care intenționează să le utilizeze în scopuri de marketing direct, cu excepția cazului în care persoana vizată a dat un consimțământ specific.

Obiecția față de marketingul direct

Dacă o persoană vizată obiectează la primirea comunicărilor de marketing sau își retrage consimțământul de a primi astfel de materiale, RBC va lua măsuri pentru a se abține de la trimiterea altor materiale de marketing așa cum solicită în mod specific persoana vizată. Obiecția față de marketingul direct se aplică numai în măsura în care se realizează marketing direct pe baza interesului legitim al RBC. Aceasta nu se aplică în cazul în care marketingul direct se bazează pe acordul persoanei vizate (a se vedea punctul 2.2.6 de mai jos), în acest din urmă caz retragerea consimțământului fiind formalitatea necesară efectuării de către persoana vizată pentru a nu mai primi direct comunicări de marketing.

În cazul în care comunicările de marketing direct sunt trimise unei persoane vizate pe baza consimțământului acesteia și persoana vizată trimite o notificare de obiecție la prelucrarea ulterioară a datelor în acest scop, conform celor mai bune practici, RBC va limita utilizarea detaliilor de contact ale persoanei vizate privind marketingul direct până la obținerea unei clarificări clare din partea persoanei vizate, fie dacă notificarea semnifică sau nu retragerea consimțământului.

Retragerea consimțământului

Persoana vizată are dreptul să-și retragă consimțământul în orice moment, fără costuri. Retragerea consimțământului nu afectează legalitatea prelucrării pe baza consimțământului înainte de retragerea acestuia. Înainte de a da consimțământul, persoana vizată trebuie informată. Consimțământul va putea fi retras la fel de ușor cum a fost dat. RBC are obligația de a facilita retragerea de către consumatori a consimțământului.

În acest sens, RBC acceptă o declarație scrisă și semnată de către persoana vizată prin care se specifică exercitarea dreptului de retragere a consimțământului. Aceasta va fi transmisă către RBC la adresa de e-mail hr@rbc.com.ro sau prin poștă folosind următoarele date de contact :Romanian Business Consult srl, strada Promoroaca nr 3A, sector 1, Bucuresti

Validarea retragerii consimțământului se va face ulterior folosind următoarele căi: e-mail, SMS, telefon, utilizarea unei semnături electronice, înregistrarea unei declarații verbale. În

plus, RBC trebuie sa păstreze evidența pentru a demonstra că a fost acordat un consimțământ valabil și că persoana vizată a fost informată.

2.3. Informarea persoanei vizate

RBC trebuie să informeze persoanele vizate printr-o politică de protecție a datelor sau o notificare privind:

- scopurile de afaceri pentru care datele lor sunt prelucrate;
- alte informații relevante (de exemplu: natura și categoriile datelor prelucrate, categoriile de părți terțe cărora le sunt comunicate datele, dacă există și modul în care persoanele vizate își pot exercita drepturile, temeiul juridic al procesării datelor etc.).

În acest scop, RBC informează persoanele vizate sub diferite forme, în funcție de modul de interacțiune cu acestea.

2.4. Utilizarea datelor cu caracter personal

Activitățile de utilizare a datelor cu caracter personal pot rezulta în materializarea riscurilor legate de pierderea, modificarea sau furtul datelor. Având în vedere ca datele cu caracter personal nu au nicio valoare dacă organizația nu le poate utiliza, trebuie implementate măsurile necesare pentru prevenirea materializării riscurilor mai sus enunțate, astfel:

- angajații vor utiliza funcționalitatea de blocare a stațiilor de lucru ori de cate ori nu le folosesc și nu se află în apropierea acestora;
- datele cu caracter personal nu vor fi dezvăluite în mod informal;
- datele cu caracter personal trebuie să fie criptate înainte de a fi transferate electronic; Managerul IT poate explica modul de trimitere a datelor terților autorizați;
- datele cu caracter personal nu trebuie să fie dezvăluite persoanelor neautorizate, nici în cadrul organizației, nici în cadrul unor terțe părți;
- datele cu caracter personal trebuie revizuite și actualizate în mod regulat, dacă se constată că sunt inactuale; dacă aceste date nu mai sunt necesare, acestea trebuie șterse și eliminate;
- angajații trebuie să solicite asistență din partea directorului departamentului sau a DPO dacă nu sunt siguri cu privire la orice aspect al protecției datelor;
- singurele persoane capabile să acceseze datele acoperite de această politică trebuie să fie cele care au nevoie de ele pentru a-și desfășura activitățile zilnice;
- datele cu caracter personal trebuie să fie împărtășite într-o manieră formală; atunci când accesul la informații confidențiale este necesar, angajații pot solicita acest lucru din partea managerilor departamentului.

RBC va oferi instruire tuturor angajaților pentru a crește gradul de conștientizare a responsabilităților lor în ceea ce privește prelucrarea datelor cu caracter personal și a dispozițiilor prezentei politici.

2.5. Stocarea datelor cu caracter personal

Datele cu caracter personal trebuie să fie păstrate într-o formă care să permită identificarea persoanelor vizate pentru o perioadă care nu depășește perioada necesară pentru scopurile pentru care au fost colectate. Datele cu caracter personal pot fi stocate pentru perioade mai îndelungate, în măsura în care datele vor fi prelucrate exclusiv în scopuri de arhivare în

interes public sau în scopuri științifice, istorice sau statistice, sub rezerva aplicării garanțiilor adecvate.

Stocarea datelor este operația de procesare care constă în păstrarea datelor cu caracter personal colectate de RBC pe orice tip de suport (electronic sau hârtie).

Datele cu caracter personal trebuie prelucrate într-un mod care să asigure o securitate adecvată, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, distrugerii sau deteriorării accidentale, utilizând măsuri tehnice sau organizatorice adecvate.

Măsurile de securitate pentru datele electronice sunt detaliate în politica de securitate a informațiilor și procedurile anexate acesteia.

Măsuri de securitate pentru datele pe suport de hârtie:

- utilizatorii care lucrează în departamente care manipulează documente ce conțin date cu caracter personal trebuie să blocheze și să asigure toate informațiile atunci când părăsesc incinta biroului;
- sunt implementate controale de acces pentru a monitoriza și a restricționa accesul la persoanele care necesită un astfel de acces pentru a-și desfășura activitățile de afaceri; aceste restricții sunt aplicate după cum este necesar de către angajații RBC, inclusiv furnizori, vizitatori și alte terțe părți identificate ca fiind relevante;
- RBC stabilește programe de păstrare sau de depozitare pentru anumite categorii de înregistrări pentru a asigura respectarea legală și, de asemenea, pentru a îndeplini alte obiective, cum ar fi păstrarea proprietății intelectuale și gestionarea costurilor.

2.6. Actualizarea datelor cu caracter personal

Datele cu caracter personal trebuie să fie corecte și, dacă este necesar, să fie actualizate. RBC trebuie să adoptate toate măsurile rezonabile pentru a se asigura că datele cu caracter personal care sunt neconforme cu realitate sunt fie șterse, fie rectificate imediat. Este responsabilitatea tuturor angajaților care lucrează cu date cu caracter personal să ia măsuri rezonabile pentru a se asigura că acestea sunt de actualitate.

Cele mai bune practici:

- datele cu caracter personal vor fi păstrate în cât mai puține locații; angajații RBC nu trebuie să creeze inutil seturi suplimentare de date cu caracter personal;
- angajații RBC trebuie să profite de fiecare ocazie pentru a asigura actualizarea datelor;
- RBC va oferi canale ușor accesibile persoanelor vizate pentru a le actualiza informațiile;
- datele cu caracter personal trebuie sa fie actualizate de îndată ce se descoperă neconformități ale acestora cu realitatea.

2.7. Transferul în străinătate a datelor cu caracter personal

În cazul in care este necesar transferul datelor cu caracter personal în afara spațiului Uniunii Europene, Responsabilul cu Protecția Datelor (DPO) va fi informat înainte de transfer și se va analiza oportunitatea transferului.

3. Responsabilități

Orice persoană autorizată de RBC să prelucreze datele cu caracter personal în numele său și angajații săi implicați în prelucrarea datelor cu caracter personal ale persoanelor vizate sau care au acces la date cu caracter personal în orice mod trebuie să respecte această politică.

Toți angajații RBC au responsabilități în ceea ce privește colectarea, prelucrarea și stocarea corectă a datelor cu caracter personal. Totodată, departamentele și echipele sunt responsabile de elaborarea propriilor proceduri operaționale pentru a asigura stabilirea și respectarea bunelor practici privind protecția datelor.

De asemenea, este responsabilitatea fiecărui angajat să informeze DPO în cazul în care apare o schimbare în ceea ce privește datele cu caracter personal.

Responsabil de Protecția Datelor cu Caracter Personal (Data Protection Officer - DPO)

Responsabilitățile acestei persoane includ, dar nu se limitează la:

- menținerea întregii organizații la curent cu privire la responsabilitățile, riscurile și problemele legate de protecția datelor;
- revizuirea tuturor politicilor și procedurilor de protecție a datelor și a politicilor conexe, în conformitate cu un program agreat în prealabil;
- planificarea instruirii referitoare la datele cu caracter personal și consiliere pentru angajații RBC;
- răspunde întrebărilor referitoare la protecția datelor cu caracter personal inițiate de angajați și toate persoanele pentru care se aplică prezenta politică;
- tratează solicitările din partea persoanelor vizate de a accesa datele pe care RBC le deține (numite și "solicitări ale persoanelor vizate");
- verifică și aprobă orice contract sau acord cu terțe părți care pot prelucra date cu caracter personal ale organizației;
- controlează și monitorizează conformitatea cu regulile de protecție a datelor cu caracter personal, inclusiv cu obligațiile menționate în prezenta politică (în îndeplinirea acestor obligații, DPO are dreptul de a efectua investigații interne și de a accesa informații);
- trebuie să prezinte cunoștințe de specialitate ale legislației și a practicilor privind protecția datelor cu caracter personal;
- să poată funcționa independent de conducere, fără conflicte de interese cu alte atribuții profesionale;
- cooperează cu autoritățile competente de supraveghere a protecției datelor și care acționează ca punct de contact cu aceste autorități în orice chestiune legată de prelucrarea datelor cu caracter personal.

Angajați care au acces la datele cu caracter personal

Responsabilitățile angajaților care au acces la datele cu caracter personal includ, însă nu se limitează la:

- să acceseze numai date cu caracter personal în măsura necesară pentru a servi scopurile legitime aplicabile pentru care RBC procesează date cu caracter personal și pentru a-și îndeplini funcția;
- să raporteze despre orice (posibil) incident sau problemă cu privire la datele cu caracter personal către managerul lor sau către DPO sau către dana.bodea@rbc.com.ro;

- să nu discute niciodată despre informațiile confidențiale din zonele publice sau cu persoanele care nu au nevoie să știe;
- să elimine documentele a căror perioadă de retenție s-a terminat și care conțin date cu caracter personal ;
- dispozitivele de calcul trebuie să fie oprite atunci când nu sunt utilizate pentru perioade lungi de timp (cum ar fi după lucru, în week-end, în timpul sărbătorilor și așa mai departe);
- utilizatorii care lucrează în departamente care manipulează date cu caracter personal ar trebui să blocheze și să asigure toate informațiile și echipamentele atunci când nu se află în vecinătatea biroului;
- utilizatorii ar trebui să își păstreze zonele de birou organizate și să păstreze toate documentele care conțin date cu caracter personal securizate și ascunse atunci când sunt departe de birourile lor;
- să nu partajeze parola;
- utilizatorul trebuie să raporteze prompt orice presupusă încălcare a politicii de securitate care i se aduce la cunoștință;
- să consulte DPO și / sau managerul direct ori de câte ori au probleme cu privire la confidențialitatea datelor cu caracter personal.

Consiliul de administrație

Responsabilitățile conducerii superioare a RBC includ, dar nu se limitează la:

- asigurarea faptului că există o structură organizațională adecvată, precum și canale eficiente de comunicare și raportare, pentru a se asigura că datele cu caracter personal sunt prelucrate într-o manieră clară și consecventă și în conformitate cu politicile și procedurile interne ale RBC;
- colaborarea cu DPO și facilitarea procesului de creare și menținere a unui cadru pentru elaborarea, implementarea și actualizarea politicilor și procedurilor locale de protecție a datelor cu caracter personal (inclusiv formare și educație);
- asigurarea implementării eficiente a cadrului de management al afacerii impus, inclusiv stabilirea unor mecanisme de dezvoltare și monitorizare a implementării reglementărilor interne pentru a asigura implementarea adecvată a acestei politici.

Information Security Officer (ISO)

Printre responsabilitățile pe care le are ISO se includ și următoarele, fără însă a se limita la:

- se asigură de faptul că toate sistemele, serviciile și echipamentele utilizate pentru prelucrarea / stocarea datelor cu caracter personal respectă standardele acceptabile de securitate;
- efectuează verificări și scanări periodice pentru a se asigura că hardware-ul și software-ul de securitate funcționează corespunzător;
- evaluează orice servicii ale unor terțe părți pe care organizația intenționează să le utilizeze pentru stocarea sau prelucrarea datelor cu caracter personal pentru a asigura integritatea, confidențialitatea și disponibilitatea (de exemplu: furnizorii de cloud);
- identifică și pune în aplicare măsurile tehnice pentru asigurarea securității datelor cu caracter personal stocate;
- acordă sprijin pentru investigarea potențialelor încălcări ale securității;
- furnizează instruire privind standardele tehnice și de securitate pentru prelucrarea și protecția datelor cu caracter personal.

Manager departament

Responsabilitățile managerilor de departamente includ, însă nu se limitează la:

- să se asigure că unitatea lor de afaceri va procesa date personale în conformitate cu această politică;
- să se asigure ca angajații RBC sunt informați cu privire la politicile și procedurile relevante pentru protecția datelor cu caracter personal;
- să se asigure că datele cu caracter personal sunt procesate în conformitate cu politicile și procedurile relevante pentru protecția datelor cu caracter personal;
- să notifice DPO și să îi urmeze sfaturile cu privire la riscurile și incidentele emergente;
- să se asigure ca procesul de inventariere a datelor este corect și complet; inventarul datelor cu caracter personal trebuie să fie actualizat periodic;
- să se asigure că angajații care lucrează în unitatea lui/ ei de afaceri urmează instruirile obligatorii.

Departamentul de Marketing

Responsabilitățile departamentului de Marketing includ, însă nu se limitează la:

- să se asigure ca strategiile de marketing sunt conforme cu principiile definite în prezenta procedură;
- să se asigure că bazele de date ce conțin date cu caracter personal și sunt utilizate în scopuri de marketing sunt actualizate și atunci când consimțământul este utilizat, acesta a fost obținut în mod valid;
- să lucreze împreună cu alți reprezentanți ai organizației pentru a se asigura că inițiativele de marketing respectă principiile protecției datelor cu caracter personal;
- să coordoneze orice solicitări referitoare la protecția datelor cu caracter personal venite din media;
- să avizeze orice declarație cu privire la datele cu caracter personal ce însoțește materiale publicitare sau este folosită în canalele comunicare (e-mail, scrisori).

Resurse umane

Responsabilitățile departamentului de Resurse Umane includ, însă nu se limitează la:

- să identifice necesitățile de instruire și dezvoltare ale personalului în legătură cu prelucrarea și protecția datelor cu caracter personal;
- să asigure includerea materialelor de formare în domeniul protecției datelor cu caracter personal în cadrul planului anual de formare;
- să asigure suport pentru unitățile de afaceri pentru implementarea programelor de instruire privind prelucrarea și protecția datelor cu caracter personal;
- să asigure faptul că orice acțiune întreprinsă cu privire la datele angajaților este în conformitate cu cerințele GDPR; acest lucru se aplică tuturor proceselor gestionate de echipa de resurse umane, începând cu procesul de recrutare, punerea în aplicare a contractului de muncă și terminarea acestuia.

În toate aceste cazuri, Managerul Resurselor Umane trebuie să fie implicat în procesul de luare a deciziilor și, în special, în evaluarea impactului potențialelor proiecte asupra protecției datelor angajaților. El trebuie să asigure un echilibru între interesele societății și dreptul la viața privată a angajaților.

4. Drepturile persoanelor vizate

4.1. Dreptul la informare

Atunci când colectează date privind angajații sau date referitoare la orice persoană vizată, direct de la persoana vizată la care se referă, RBC se va asigura că acele persoane sunt informate cu privire la următoarele (cu excepția cazului în care acestea sunt evidente) în momentul obținerii datelor cu caracter personal:

- identitatea și datele de contact ale operatorului de date și, după caz, ale reprezentantului operatorului de date;
- datele de contact ale responsabilului cu protecția datelor;
- scopul prelucrării și baza juridică;
- interesele legitime urmărite de către operatorul de date sau de o terță parte, după caz;
- destinatarii sau categoriile de destinatari ai datelor cu caracter personal, după caz;
- faptul că operatorul de date intenționează să transfere date cu caracter personal către o țară terță sau o organizație internațională și existența sau absența unei decizii de adecvare sau, după caz, garanția corespunzătoare pentru transfer și mijloacele prin care o copie a garanțiilor poate să fie obținută;
- perioada pentru care vor fi stocate datele cu caracter personal sau criteriile utilizate pentru a determina acea perioadă;
- existența drepturilor persoanei vizate: dreptul de a solicita accesul și rectificarea sau ștergerea datelor cu caracter personal sau de a limita prelucrarea sau de a se opune prelucrării, dreptul la portabilitatea datelor, dreptul de retragere a consimțământului în orice moment (acolo unde este aplicabil) și dreptul de a depune o plângere la o autoritate de supraveghere;
- dacă este cazul, existența unui proces automat de luare a deciziilor, inclusiv profilarea, informații relevante despre logica implicată, precum și semnificația și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată;
- dacă furnizarea de date cu caracter personal este o cerință legală sau contractuală sau o cerință necesară pentru a încheia un contract, precum și dacă persoana vizată este obligată să furnizeze datele cu caracter personal și consecințele posibile ale neîndeplinirii acestor date.

Informațiile menționate mai sus trebuie furnizate, de asemenea, în cazul în care datele nu au fost obținute direct de la persoana vizată la care se referă, cu următoarele informații suplimentare:

- categoriile de date prelucrate;
- din ce surse proveneau datele personale și
- dacă este cazul, dacă datele provin din surse disponibile publicului.

Atunci când datele cu caracter personal nu sunt obținute direct de la persoana vizată, informațiile trebuie furnizate în termen rezonabil după obținerea datelor cu caracter personal (cel târziu în termen de o lună) sau cel târziu în momentul primei comunicări către respectivul subiect sau cel mai târziu, când datele cu caracter personal sunt divulgate pentru prima dată, dacă se prevede divulgarea către alt destinatar.

RBC nu va furniza informații privind prelucrarea în cazul în care consideră în mod rezonabil că acest lucru ar putea face imposibilă sau poate afecta serios realizarea obiectivelor

procesării respective (de exemplu: prevenirea, investigarea, descoperirea sau urmărirea penală a încălcărilor eticii profesionale sau a infracțiunilor).

4.2. Dreptul de acces

RBC va lua măsurile adecvate pentru a furniza persoanei vizate orice informație referitoare la prelucrare într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, folosind un limbaj clar și simplu.

Persoana vizată are dreptul de a confirma dacă RBC procesează de fapt datele lor cu caracter personal. Dacă răspunsul este afirmativ, RBC trebuie să îi pună la dispoziție persoanei vizate următoarele:

- Scopul procesării;
- Categoria de date cu caracter personal în cauză (de exemplu: nume, adresă, istoric, comportament de navigare online);
- destinatarii sau categoriile de destinatari cărora le-au fost sau le vor fi dezvăluite datele cu caracter personal, în special destinatarii din țări terțe (adică țări din afara UE / SEE) sau organizații internaționale;
- dacă este posibil, perioada prevăzută pentru care vor fi stocate datele cu caracter personal sau, dacă nu este posibil, criteriile utilizate pentru stabilirea acestei perioade;
- existența dreptului de a solicita de la RBC rectificarea sau ștergerea datelor cu caracter personal sau restricționarea procesării datelor cu caracter personal ale persoanei vizate, să se opună unei astfel de procesări sau să înregistreze o plângere la autoritatea de supraveghere;
- în cazul în care datele cu caracter personal nu sunt colectate direct de la persoana vizată, orice informații disponibile cu privire la sursa acestora;
- dacă are loc luarea automată a deciziilor sau profilarea și, dacă da, logica implicată, semnificația și consecințele posibile ale unei astfel de procesări.

La cererea persoanei vizate, RBC furnizează, de asemenea, o copie a datelor cu caracter personal care fac obiectul unei prelucrări în conformitate cu cerințele de mai jos:

- **copie gratuită**: prima solicitare de copie a datelor personale prelucrate va fi gratuită;
- **copii ulterioare**: pentru alte solicitări poate fi percepută "o taxă rezonabilă";
- **copii electronice**: cu excepția cazului în care persoana vizată solicită altfel, cererile electronice de copiere a datelor vor fi furnizate în formă electronică utilizată în mod obișnuit (cum ar fi .csv / .txt / .xml).

Mai mult decât atât, RBC se va asigura că dreptul persoanei vizate de a obține o copie nu afectează negativ drepturile și libertățile celorlalți.

4.3. Dreptul la rectificare

Persoana vizată are dreptul de a obține de la operator, fără întârzieri nejustificate, rectificarea datelor cu caracter personal inexacte care o privesc. În urma unei solicitări de rectificare, RBC va lua măsuri rezonabile pentru a se asigura că datele sunt corecte și pentru a rectifica datele, dacă este necesar, luând în considerare argumentele și dovezile furnizate de persoana vizată.

4.4. Dreptul la ștergerea datelor sau "dreptul de a fi uitat"

Dreptul la ștergere sau dreptul de a fi uitat acordă persoanelor vizate posibilitatea de a șterge datele lor personale dacă nu mai doresc ca acestea să fie procesate și când RBC nu mai are interese legitime pentru a le păstra.

Persoanele vizate au dreptul să ceară ștergerea datelor cu caracter personal dacă:

- datele cu caracter personal nu mai sunt necesare pentru scopul pentru care RBC le-a colectat și procesat inițial;
- organizația se bazează pe consimțământ ca bază legală pentru deținerea datelor, iar persoana își retrage consimțământul și nu există alt motiv juridic pentru procesare;
- RBC se bazează pe interesele legitime ca bază pentru procesare, obiectele individuale la prelucrarea datelor lor și nu există niciun interes legitim de a continua această procesare;
- RBC prelucrează datele cu caracter personal în scopuri de marketing direct, bazate pe interes legitim și obiectele individuale pentru prelucrarea respectivă;
- datele cu caracter personal au fost prelucrate ilegal;
- datele cu caracter personal trebuie să fie șterse pentru respectarea unei obligații legale în legislația Uniunii sau a statului membru la care este supusă operatorul de date;
- datele cu caracter personal ale unui copil, care au fost colectate în legătură cu oferta de servicii a societății informaționale.

RBC nu va asigura dreptul de ștergere dacă procesarea este necesară din unul dintre următoarele motive:

- să exercite dreptul la libertatea de exprimare și la informare;
- să respecte o obligație legală;
- pentru îndeplinirea unei sarcini îndeplinite în interes public sau în exercitarea autorității publice;
- în scopuri de arhivare în interes public, cercetare științifică istorică sau scopuri statistice, în cazul în care ștergerea este de natură să facă imposibilă sau să afecteze serios realizarea acestei prelucrări; sau
- pentru stabilirea, exercitarea sau apărarea revendicărilor legale.

4.5. Dreptul la restricționarea prelucrării

Ca alternativă la solicitarea ștergerii datelor, persoanele au dreptul să restricționeze prelucrarea datelor lor cu caracter personal în anumite circumstanțe.

Persoanele vizate au dreptul de a solicita RBC să restricționeze procesarea datelor lor cu caracter personal în următoarele circumstanțe:

- persoana vizată contestă acuratețea datelor sale personale, iar organizația verifică corectitudinea datelor;
- datele cu caracter personal au fost procesate ilegal (adică încălcând cerința de legalitate a primului principiu al GDPR), iar individul se opune ștergerii și solicită în schimb restricții;
- RBC nu mai are nevoie de datele cu caracter personal, dar persoana vizată cere organizației să o păstreze pentru a stabili, exercita sau a apăra o reclamație legală; sau

- persoana vizată a formulat obiecții cu privire la prelucrarea datelor sale în conformitate cu articolul 21 alineatul (1) din GDPR, în temeiul verificării dacă motivele legitime ale societății RBC au o prioritate față de cele ale persoanei vizate.

4.6. Dreptul la portabilitatea datelor

Persoana vizată are dreptul de a primi datele personale cu privire la aceasta pe care le-a furnizat către RBC, într-un format structurat, utilizat în mod obișnuit și care poate fi încărcat și/ sau prelucrat de un sistem informatic.

RBC va acorda doar dreptul la portabilitatea datelor atunci când:

- baza legală de prelucrare a datelor cu caracter personal ale persoanei este consimțământul sau executarea unor clauze contractuale; și
- organizația efectuează prelucrarea prin cu ajutorul resurselor informatice(i.e., informația este stocată și prelucrată în cadrul sistemelor informatice și nu pe hârtie).

4.7. Dreptul la opoziție

RBC va permite persoanelor să-și exercite dreptul de a se opune la:

- procesarea bazată pe interese legitime sau îndeplinirea unei sarcini de interes public / exercitarea autorității publice (inclusiv profilarea) - în acest caz, cu excepția cazului în care RBC demonstrează motive legitime convingătoare pentru prelucrare care depășesc interesele, drepturile și libertățile datelor sau cu excepția cazului în care RBC are nevoie de datele necesare pentru stabilirea, exercitarea sau apărarea revendicărilor legale;
- marketingul direct (inclusiv profilarea) atunci când este efectuat pe baza unui interes legitim (nu consimțământul); și
- prelucrarea în scopuri științifice / istorice de cercetare și statistici - în acest caz, cu excepția cazului în care prelucrarea este necesară pentru îndeplinirea unei sarcini îndeplinite din motive de interes public.

4.8. Drepturi privind procesul decizional individual automat

Persoana vizată are dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automatizată, inclusiv profilarea, care produce efecte juridice legate de aceasta sau, în mod similar, afectează semnificativ persoana vizată.

RBC va efectua numai decizii automatizate cu efecte juridice sau semnificative similare, dacă decizia este:

- necesară pentru încheierea sau executarea unui contract între o organizație și persoana vizată; sau
- pe baza consimțământului explicit al persoanei vizate; sau
- autorizată prin lege (de exemplu, în scopul combaterii fraudei sau evaziunii fiscale).

În primele două cazuri, astfel de decizii pot fi luate numai dacă operatorul de date pune în aplicare măsuri adecvate pentru a proteja drepturile și libertățile persoanei vizate și interesele legitime.