Fondul Social European Plus (FSE+)
Programul Educație și Ocupare 2021-2027
Prioritate: P02 „Valorificarea potențialului tinerilor pe piața muncii (Ocuparea forței de muncă în rândul tinerilor)“
Obiectiv specific: ESO4.1 „Îmbunătățirea accesului la piața muncii și măsuri de activare pentru toate persoanele aflate în căutarea unui loc de muncă, în special pentru tineri, îndeosebi prin implementarea Garanției pentru tineret, pentru șomerii de lungă durată și grupurile defavorizate de pe piața muncii și pentru persoanele inactive, precum și prin promovarea desfășurării de activități independente și a economiei sociale (FSE+)”
Acțiunea 2.a.2. Pregătirea şi furnizarea ofertei de servicii de formare/ocupare pentru tineri, inclusiv pentru tineri NEET, prin pachete integrate de măsuri active personalizate în funcție de profilul tinerilor
Titlu proiect: IMPULS profesional pentru tinerii din București-Ilfov, cod MySMIS2021+: 330685

POLITICA GDPR PROIECT IMPULS, COD SMIS 330685

Cuprins

Politica privind confidențialitatea

1. **DEFINIȚII**

„GDPR", „Regulamentul" - Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor, în limba engleză General Data Protection Regulation);

„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 anonime*" - reprezintă orice date ale căror origine sau în baza cărora au fost efectuate prelucrări, însă acestea nu pot fi asociate cu nicio persoană vizată identificată sau identificabilă;

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

„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;

„***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 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***" - 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;

*„**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;
„reprezentant” - înseamnă o persoană fizică sau juridică stabilită în Uniune, desemnată în scris de către operator sau persoana împuternicită de operator, care reprezintă operatorul sau persoana împuternicită în ceea ce privește obligațiile lor respective care le revin în temeiul GDPR;

„reguli corporatiste obligatorii” - înseamnă politicile în materie de protecție a datelor cu caracter personal care trebuie respectate de un operator sau de o persoană împuternicită de operator stabilită pe teritoriul unui stat membru, în ceea ce privește transferurile sau seturile de transferuri de date cu caracter personal către un operator sau o persoană împuternicită de operator în una sau mai multe țări terțe în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună;

„autoritate de supraveghere” - înseamnă o autoritate publică independentă instituită de un stat membru;

„DPIA” - evaluarea impactului asupra protecției datelor (în limba engleză, data-protection impact assessment, DPIA);

„*transmitere*” - înseamnă transmiterea în orice formă a datelor cu caracter personal spre a fi cunoscute și consultate de una sau mai multe părți;

„***persoana vizată***” - înseamnă persoana fizică la care fac referire datele cu caracter personal;

„*difuzare/divulgare*” - înseamnă aducerea la cunoștința uneia sau mai multor părți a datelor cu caracter personal, în orice formă, și de asemenea, punerea acestora la dispoziție spre a fi consultate;

„***restricționarea 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.

2. SCOPUL ȘI DOMENIUL DE APLICABILITATE

2.1. Scopul

Prezenta Politică are drept scop **stabilirea principiilor de bază** a prelucrării datelor cu caracter personal, metodologia de lucru, precum și **reguli pentru angajați pentru a se asigura confidențialitatea** datelor personale în operațiunile de prelucrare a datelor personale efectuate de **Asociația Brahma** („Compania" sau „Operatorul"), în conformitate cu legislația aplicabilă.

Respectarea confidențialității datelor cu caracter personal reprezintă o obligație a Operatorului și a Angajaților săi, având în vedere sensibilitatea datelor cu caracter personal prelucrate, dreptul la protecția datelor personale și dreptul la viața privată a persoanelor fizice.

Angajații Operatorului înțeleg și au reprezentarea deplină a faptului că încălcarea confidențialității datelor personale poate conduce la prejudicii fizice, materiale sau morale persoanelor fizice, cum ar fi pierderea controlului asupra datelor lor cu caracter personal sau limitarea drepturilor lor, discriminare, furt sau fraudă de identitate, pierdere financiară, inversarea neautorizată a pseudonimizării, compromiterea reputației, pierderea confidențialității datelor cu caracter personal protejate prin secret profesional sau orice alt dezavantaj semnificativ de natură economică sau socială adus persoanei fizice în cauză.

2.2. Destinatari

Prevederile prezentei Politici sunt obligatorii pentru salariații permanenți și temporari ai **Asociația** Brahma, precum și pentru orice alte persoane care, deși nu sunt salariații **Asociația Brahma** pot fi asimilați unui personal dedicat CEDO (*toate aceste persoane fiind denumite în acest document în mod generic „Angajați"*).

Prezenta Politică va fi considerată ca având caracter general și se va aplica tuturor prelucrărilor efectuate de Operator. Acest document stabilește modul în care vor fi protejate datele personale pe care Operatorul le deține și le prelucrează în îndeplinirea activităților sale comerciale.
În cazul în care se constată existența anumitor aspecte legate de confidențialitate pentru care prezenta Politică nu oferă directive corespunzătoare, Angajații trebuie să solicite imediat consiliere din partea persoanei responsabile cu protecția datelor dacă a fost numit, sau a reprezentantului legal al Operatorului.

2.3. Sfera datelor personale

Datele clienților
Operatorul prelucrează următoarele date cu caracter personal aparținând **clientului și/sau celorlalte** persoane vizate, astfel cum acestea sunt comunicate:
(i) prin intermediul formularelor de cerere privind acordarea serviciului solicitat și a anexelor acestora;
(ii) prin intermediul propunerii pentru încheierea contractului și anexelor acesteia;
(iii) prin intermediul **comunicărilor transmise** Operatorului după data încheierii contractului *(în formă scrisă, în formă electronică, completate la întrebările formulate telefonic de angajații Operatorului/Împuterniciți și prin alte procedee acceptate de persoana vizată)*, precum: prenume, nume, **numele anterior, pseudonimul, sexul, adresa de domiciliu și de reședința, data, locul și țara nașterii, codul numeric personal, seria și numărul actului de identitate/pașaportului, alte date ale** actului de identitate**, alte date din actele de stare civilă, cetățenia, semnătura, datele din permisul** de conducere/certificatul de înmatriculare, date de contact *(adrese, numere de telefon, fax, adrese **electronice și nr. de telefon mobil),*** **profesia, locul de muncă, numărul dosarului de pensie, situație**

militară, situație economică și financiară ale clientului sau, după caz, ale celorlalte persoane vizate.
În unele cazuri, este posibil să fie solicitate date conținute în cazierul judiciar, **inclusiv situația litigiilor** în care clientul este implicat, acestea fiind necesare Operatorului pentru evaluarea clienților și/sau garanțiilor pe care le prezintă aceștia.
Operatorul poate colecta și utiliza datele personale ale clienților și potențialilor clienți (de ex. nume, vârsta, data nașterii, adresa, rezidența, e-mail etc.), pentru realizarea scopurilor de afaceri.

Datele angajaților

Asociația Brahma colectează și utilizează datele personale ale angajaților săi (actuali și foști) în cadrul desfășurării raporturilor de muncă inclusiv a obligațiilor care decurg din acestea, în temeiul **legii și numai** în scopuri relevante, corespunzătoare și uzuale. Departamentul Resurse Umane va comunica Angajaților informații în legătură cu motivele și metodele de prelucrare a datelor respective.

Asociația Brahma recunoaște și respectă drepturile de confidențialitate ale angajaților săi, limitând **colectarea, accesul și utilizarea** datelor personale aferente angajării. **Asociația Brahma** ia măsuri **preventive suplimentare înainte de divulgarea către părțile terțe legitime** a informațiilor oricărui angajat. Respectivele divulgări pot avea loc numai în condițiile în care există înțelegerea deplină a faptului că accesul și utilizarea datelor sunt limitate, și că datele trebuie să fie protejate.

3. PRINCIPII GENERALE

3.1. Soluțiile de organizare

Asociația Brahma, în calitate de Operator, a adoptat următoarele soluții de organizare în ceea ce privește confidențialitatea datelor:

- ✓ aspectele tehnice de securitate a datelor intră în responsabilitatea Departamentului IT și trebuie gestionate atât în baza liniilor directoare definite, a proceselor și procedurilor, cât și prin controale efectuate la nivelul sistemelor informatice;
- ✓ responsabilitatea privind prelucrarea datelor în acord cu prezenta politică revine tuturor Angajaților, Operatorul va asigura măsurile organizatorice necesare implementării prevederilor Regulamentului și Politicii privind confidențialitate datelor, astfel încât prelucrările datelor cu caracter personal să fie efectuate în conformitate cu Regulamentul (UE) 2016/679;
- ✓ Persoana responsabilă cu protecția datelor va instrui angajații **Asociația Brahma** astfel încât aceștia să respecte confidențialitatea datelor personale prelucrate, mecanismele de asigurare a confidențialității;
- ✓ fără prejudicierea celor de mai sus, Operatorul poate – la alegerea sa, sau dacă este prevăzut de legea în vigoare - să desemneze un **Responsabil cu protecția datelor** care va supraveghea toate activitățile de prelucrare a datelor personale. Indiferent de numirea Responsabilului cu protecția datelor datelor, desemnarea responsabilităților trebuie să reflecte cerințele Operatorului menționate mai sus. În toate cazurile, se va desemna un responsabil cu protecția datelor atunci când aceasta este obligatorie potrivit Regulamentului *(prezența unor operațiuni de prelucrare care necesită o **monitorizare periodică, sistematică a persoanelor vizate pe scară largă** sau **prelucrarea pe scară largă vizează categorii speciale de date**);*
- ✓ Angajații **Asociația Brahma** sunt obligați să respecte Politica de confidențialitate precum și măsurile de prelucrare a datelor cu caracter personal, asigurând-se un nivel adecvat de protecție a datelor astfel prelucrate.

3.2. Prevederi generale

Desfășurarea activității curente a **Asociația Brahma** presupune efectuarea de către angajații **Asociația** Brahma a unor prelucrări de date care se supun următoarelor principii:

- ✓ datele trebuie prelucrate în mod **legal, echitabil și transparent**;
- ✓ datele trebuie colectate în scopuri determinate, **explicite și legitime** și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile inițiale;
- ✓ datele trebuie să fie **adecvate, relevante și limitate la ceea ce este necesar în raport** cu scopurile în care sunt prelucrate;
- ✓ datele trebuie să fie exacte și, în cazul în care este necesar, **să fie actualizate**; trebuie să se 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 șterse sau rectificate fără întârziere;
- ✓ datele trebuie păstrate într-o formă care permite identificarea persoanelor vizate pe o **perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt** prelucrate datele; datele cu caracter personal vor fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice;
- ✓ datele trebuie prelucrate într-un mod care asigură **securitatea adecvată, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare**.

Prin măsurile adoptate, operatorul se angajează să implementeze măsurile tehnice și organizatorice necesare asigurării gradului de confidențialitate necesar și securității prelucrării datelor cu caracter personal.

Datele personale vor putea fi colectate, folosite, reținute, transmise și șterse, respectându-se **confidențialitatea conținutului acestora,** precum și celelalte reguli stabilite în prezenta Politică precum și obligațiile prevăzute în cadrul Regulamentului.

3.3. Securitatea prelucrării

Asigurarea securității prelucrării datelor cu caracter personal implică respectarea unui nivel adecvat al confidențialității datelor și se va face cu respectarea de către Operator a măsurilor tehnice și organizatorice precum:

- ✓ **pseudonomizarea și criptarea datelor cu caracter personal**;
- ✓ **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**;
- ✓ **implementarea unor procese pentru testarea, evaluarea și aprecierea periodică a eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării**.

Operatorul va asigura că principiile de mai sus sunt respectate. De asemenea, acesta trebuie să poată dovedi respectarea principiilor și îndeplinirea obligațiilor ce decurg din acestea.

Accesul angajaților la datele personale deținute va fi acordat în baza unei **autorizații corespunzătoare**, în funcție de **grupul din care fac parte aceștia și de nivelul de securitate la care este arondat.** Orice

Angajat/Parte terță autorizată/Destinatar care va avea acces la datele personale deținute de Operator doar ca urmare a necesității de a utiliza informațiile respective și va avea obligația de a respecta confidențialitatea acestora și de a respecta măsurile tehnice și organizatorice astfel încât datele prelucrate să fie protejate. În acest sens, activitatea angajaților **Asociația Brahma** va putea fi monitorizată pentru a se verifica respectarea conformității cu legile sau normele în vigoare de protecție a datelor personale și cu Politicile de protectie a datelor implementate.
În cazul în care există suspiciunea încălcării prezentei Politici de confidențialitate, incidentul trebuie raportat cel puțin uneia dintre persoanele următoare:

- ✓ Managerul de departament;
- ✓ Ofițerul responsabil de protecția datelor.

Aceștia din urmă sunt obligați să ia măsurile necesare conform regulilor legale sau celor stabilite în procedurile **Asociației Brahma.**

4. OBLIGAȚII GENERALE

Operatorul este obligat ca, în desfășurarea activităților sale comerciale, să procedeze cu prudență, să respecte legislația României, să-și protejeze clienții și Celelalte Persoane Vizate, precum și propriile drepturi și interese.

Operatorul colaborează strâns cu orice alte entități aparținând acestuia, cu entități afiliate, prezente și viitoare ale Operatorului.

Angajații **Asociației Brahma** sunt obligați să asigure confidențialitatea datelor cu caracter personal în baza Contractului de muncă încheiat și a prezentei Politici de confidențialitate. Nerespectarea Politicii de confidențialitate sau a Contractului de muncă încheiat poate conduce către **demararea unor acțiuni** disciplinare, inclusiv la **desființarea contractului de muncă**.

Operatorul își rezervă toate drepturile de a proceda la recuperarea sumelor de bani acordate cu titlu de despăgubire unei persoane vizate, ca urmare a nerespectării de către angajați a Politicii de confidențialitate. Nerespectarea confidențialității datelor cu caracter personal prelucrate poate fi sancționată penal potrivit reglementărilor legale din materie.
Fiecare departament din cadrul **Asociației Brahma** are obligația păstrării unei **evidențe (întocmire și** actualizare) a persoanelor desemnate să prelucreze datele cu caracter personal, dacă prin natura activităților desfășurate în cadrul Departamentului este necesară prelucrarea de date cu caracter personal.

Este obligația departamentului de specialitate să solicite informații tuturor departamentelor în scopul actualizării datelor cu caracter personal la nivelul **Asociației Brahma**

Prin prezenta Politică se stabilește faptul că managementul **Asociației Brahma** are atribuția să supravegheze prelucrarea datelor, inclusiv la buna funcționare a sistemelor informatice utilizate în activitatea de prelucrare și transmitere a datelor cu caracter personal. În exercitarea acestei atribuții, se poate solicita oricărui Angajat informații cu privire la prelucrarea datelor și poate stabili prin instrucțiuni de lucru reguli obligatorii în domeniul prelucrării datelor.

Orice contract încheiat între **Asociația Brahma** în calitate de Operator de date cu caracter personal, și o terță parte, în calitate de Persoană Împuternicită, va trebui să cuprindă **clauzele de confidențialitate și prelucrare a datelor cu caracter personal** în conformitate cu Regulamentul.

4.1. Verificarea corectitudinii datelor cu caracter personal

Toți angajații au obligația să verifice datele personale păstrate de **Asociației Brahma** din perspectiva **acurateței și integralității informațiilor relevante** și trebuie să le modifice corespunzător. Ca regulă generală, accesul este limitat la datele utilizate pentru identificarea unei persoane și nu include toate informațiile pe care **Asociația Brahma** le păstrează despre angajat. De exemplu, **Asociația Brahma** poate permite accesul la formularul de evaluare a performanței și la rezultatele individuale în cadrul planului de dezvoltare, însă informațiile generale ale planului de avansare vizând mai multe persoane nu pot fi împărtășite.

4.2. Activități personale

Angajamentul **Asociației Brahma** de a respecta drepturile de confidențialitate ale Angajaților nu **reprezintă permisiunea de a desfășura activități personale necorespunzătoare în timpul serviciului** (ex. **calculatoarele trebuie să fie utilizate doar în interes de serviciu**). În plus, pentru a asigura securitatea și protecția sistemelor sale IT, **Asociația Brahma** a are dreptul de acces în toate sediile și, dacă este necesar, de a revizui comunicările și informațiile create de angajați în timpul activității, în limitele permise de legislația în vigoare.

4.3. Refuzul de prelucrare a datelor cu caracter personal

Orice angajat are dreptul de a transmite departamentului Resurse Umane obiecțiuni în legătură cu colectarea, utilizarea și divulgarea datelor sale personale. **Asociația Brahma** va evalua obiecțiunile Angajatului, va lua o decizie în conformitate cu legislația în vigoare și va comunica decizia sa Angajatului.

4.4. Transmiterea de informații

Asociația Brahma va transmite datele legate de angajații și clienții săi entităților care aparțin de aceasta doar dacă este necesar sau, dacă este posibil, în conformitate cu legea aplicabilă. Aceste entități vor adopta orice măsuri de precauție menite să asigure legalitatea comunicării și respectării „secretului profesional".

Transmiterea entităților afiliate Operatorului a datelor referitoare la clienții **Asociației Brahma** este permisă, cu titlu de exemplu, în următoarele cazuri:

- ✓ Atunci când interesele în joc sunt echilibrate: transmiterea este permisă, în scopul respectării prevederilor legate de combaterea spălării banilor, în ceea ce privește datele referitoare la „raportarea tranzacțiilor suspecte". Pe cale de consecință, numai Angajații numiți pentru executarea măsurilor împotriva spălării banilor au dreptul de a transmite și a primi asemenea date personale.
- ✓ Date anonime (de ex. în scopuri statistice sau în scopul analizei pieței).

Transmiterea datelor referitoare atât la clienți, cât și la angajați este permisă, cu titlu de exemplu, în următoarele cazuri:

- ✓ **Când există consimțământul expres al persoanelor vizate**: consimțământul trebuie să fie specific și astfel, strict legat de obiectul pentru care respectiva transmitere este efectuată (ex. marketing). Pe cale de consecință, pentru ca **Asociația Brahma** să se asigure că acceptul a fost acordat legitim de către client, este necesară verificarea conținutului notificării de informare trimise clientului și formularul de consimțământ aferent.
- ✓ **Cazurile care sunt echivalente consimțământului**: (ex. încheierea unui contract, obligație legală, interes legitim al Operatorului).

5. OBLIGAȚII SPECIFICE

Prelucrarea datelor cu caracter personal se face doar de către angajații Operatorului ce dețin competența necesară efectuări unei astfel de prelucrări. În situația în care angajatul nu cunoaște gradul său de acces la date confidențiale, se va putea adresa managerului de departament din care acesta face parte.

În vederea menținerii confidențialității adecvate a datelor cu caracter personal, Angajații sunt obligați să respecte restricțiile de procesare a datelor impuse de Operator prin Politica de securitate implementată, în funcție de categoria datelor și nivelul de acces.

Asociația Brahma utilizează măsuri corespunzătoare din punct de vedere administrativ, tehnic, fizic și de securitate, menite:

(i) să respecte cerințele legale și acordurile de muncă;

(ii) să protejeze datele cu caracter personal împotriva pierderilor, furtului, accesului neautorizat, utilizării sau modificării.

Asociația Brahma utilizează toate mijloacele necesare pentru a păstra datele personale corecte, complete și actualizate.

5.1. Drepturile persoanelor vizate

GDPR conferă persoanelor fizice, în principal, următoarele drepturi:

- ✓ Dreptul de a fi informat;
- ✓ Dreptul de acces;
- ✓ Dreptul la rectificare;
- ✓ Dreptul de ștergere;
- ✓ Dreptul de a restricționa prelucrarea;
- ✓ Dreptul la portabilitatea datelor;
- ✓ Dreptul de a se opune;
- ✓ Dreptul legate de luarea de decizii automatizate și de profilare.

5.2. Transferul

Modalitatea prin care **Asociația Brahma** transferă date cu caracter personal, în conformitate cu Regulamentul, respectiv toate operațiunile de transfer se vor face respectându-se Procedura respectivă.

5.3. Reținerea și ștergerea datelor personale

Reținerea/stocarea și ștergerea datelor cu caracter personal, în vederea asigurării confidenţialităţii datelor şi informaţiilor, precum şi pentru păstrarea în siguranţă a acestora, în cadrul activităţii curente executate de către angajaţi se va face cu respectarea dispozițiilor cuprinse în Procedura respectivă.

5.4. Raportare și tratare incidente de securitate

În situația în care un angajat intră în contact cu o informație ce nu este destinată grupului de acces din care acesta face parte, informația parvenită acestuia având un nivel de securitate mai ridicat sau diferit față de cel la care angajatul este îndreptățit conform celor stabilite în Politica de confidențialitate, angajatul este obligat să procedeze de îndată la informarea:

- ✓ Managerului de departament;
- ✓ Ofițerului responsabil de protecția datelor.

Angajații nu vor da curs niciunei solicitări de transmitere/diseminare a unor date cu caracter personal unor

persoane care nu sunt angajate în cadrul **Asociației Brahma**. În situația în care solicitarea este efectuată de către o persoană vizată, angajatul va înainta această solicitare către persoanele competente din cadrul de specialitate pentru a proceda la verificarea cererii transmise și la elaborarea răspunsului în conformitate cu normele Regulamentului.
Angajații nu vor da curs niciunei solicitări de transmitere/diseminare a datelor cu caracter personal către un alt / alți angajați, mai înainte de a se asigura că acesta face parte dintr-un grup cu un nivel de acces adecvat sau solicitarea acestuia este avizată de către Managerul departamentului din care face parte.

Modalitatea concretă de notificare a Autorității de Supraveghere privind Protecția Datelor cu Caracter Personal și de informare a persoanei vizate în cazul în care se produce o încălcare a securității datelor cu caracter personal, inclusiv activitățile ce trebuie desfășurate atunci când se produce un incident de securitate, respectiv, înregistrarea încălcărilor de securitate, întocmirea notificărilor și informărilor impuse de GDPR, stabilirea fluxului de parcurs în redactarea și difuzarea controlată a acestora către Autoritatea de supraveghere și persoanele vizate sunt prevăzute în **Procedura de raportare și tratare incidente de** securitate.

6. REGULI „CLEAN DESK”

Pentru a îmbunătăți securitatea și confidențialitatea informațiilor **Asociația Brahma** a adoptat reguli „Clean Desk” pentru stațiile de lucru pentru computere și imprimante. Acest lucru asigură că toate **informațiile sensibile și confidențiale**, fie că sunt pe hârtie, un dispozitiv de stocare sau un dispozitiv hardware, sunt **blocate sau eliminate în mod corespunzător când o stație de lucru nu este utilizată.** Aceste reguli vor reduce *riscul accesului neautorizat, pierderii și deteriorării informațiilor în timpul și în afara orelor normale de funcționare sau atunci când stațiile de lucru sunt lăsate nesupravegheate.* Regulile reprezintă un control important al securității și confidențialității și sunt necesare pentru respectarea GDPR.

Aceaste reguli se aplică tuturor personalului permanent, temporar și contractat care lucrează în cadrul **Asociației Brahma.**

6.1. Reguli. Ori de câte ori un birou nu este ocupat pentru o perioadă lungă de timp, se vor aplica următoarele reguli:

1. Toate documentele sensibile și confidențiale trebuie să fie scoase de pe birou și blocate într-un sertar sau dulap de depozitare. Acestea includ dispozitive de stocare în masă, cum ar fi CD-uri, DVD-uri și unități USB.
2. Toată hârtia de deșeuri care conține informații sensibile sau confidențiale trebuie plasate în cutiile confidențiale dedicate.
3. Stațiile de lucru pentru calculatoare trebuie să fie blocate atunci când biroul este neocupat și închis complet la sfârșitul zilei de lucru.
4. Laptopurile, tabletele și alte dispozitive hardware trebuie să fie scoase de pe birou și blocate într-un sertar sau dulap de depozitare.
5. Cheile pentru accesarea sertarelor sau a dulapurilor de depozitare nu trebuie lăsate nesupravegheate la un birou.
6. Imprimantele și faxurile trebuie tratate cu aceeași atenție, respectiv:

a. Orice lucrare de imprimare care conține documente sensibile și confidențiale trebuie recuperată imediat. Când este posibil, ar trebui să se utilizeze funcția "Imprimare blocată".
b. Toate documentele rămase la sfârșitul zilei de lucru vor fi eliminate corespunzător.

6.2. Conformitate. Această politică va fi monitorizată oficial de către **Asociația Brahma** și poate include

inspecții aleatorii și planificate.

6.3. Neconformitate. Orice angajat sau contractant care a constatat că a încălcat aceste reguli poate face obiectul unor măsuri disciplinare, până la încetarea contractului de muncă.

7. REGULI „BRING YOUR OWN DEVICE" (BYOD)

Asociația Brahma acordă angajaților dreptul de a utiliza smartphone-uri și tablete personale la locul de muncă. **Asociația Brahma** își rezervă dreptul de a revoca acest privilegiu dacă utilizatorii nu respectă politicile și procedurile **Asociației Brahma.**

Aceste reguli au rolul de a proteja securitatea și integritatea infrastructurii de date și tehnologii a **Asociației Brahma**. Excepții limitate de la aceste reguli pot apărea prin prisma variațiilor de dispozitive și de platforme.

Angajații trebuie să accepte termenii și condițiile stabilite în această politică pentru a putea conecta dispozitivele lor la rețeaua **Asociației Brahma**

7.1. Utilizare acceptabilă

Asociația Brahma definește utilizarea acceptabilă a afacerii ca activități care susțin direct sau indirect activitatea Operatorului. **Asociația Brahma** definește folosirea personală acceptabilă în timpul Operatorului ca o comunicare personală rezonabilă și limitată, cum ar fi citirea.

Angajații sunt blocați de la accesarea anumitor site-uri în timpul orelor de lucru / în timp ce sunt conectați la rețeaua **Asociației Brahma** la discreția sa.
Dispozitivele nu pot fi utilizate în niciun moment pentru:

- ✓ stocarea sau transmiterea unor materiale ilicite;
- ✓ stocarea sau transmiterea unor informații privind proprietatea intelectuală aparținând altor companii;
- ✓ acțiuni de hărțuire a altor persoane;
- ✓ alte acțiuni asemănătoare.

Următoarele aplicații sunt permise: vremea, aplicațiile de productivitate, Facebook etc. Angajații pot utiliza dispozitivul mobil pentru a accesa următoarele resurse deținute de **Asociația Brahma**: e-mail, calendare, contacte, documente etc.

Asociația Brahma are o politică de toleranță la zero pentru trimiterea mesajelor prin SMS sau trimitere prin e-mail în timp ce conduce și este permisă doar vorbirea fără mâini în timpul conducerii.

7.2. Dispozitive și suport

Sunt permise telefoanele inteligente, inclusiv telefoanele iPhone, Android și Windows.
Sunt permise tablete, inclusiv iPad și Android.
Problemele de conectivitate sunt soluționate de Departamentul IT; angajații ar trebui să contacteze producătorul dispozitivului pentru probleme legate de sistemul de operare sau hardware.

Dispozitivele trebuie să fie prezentate IT pentru asigurarea corespunzătoare a locurilor de muncă și configurarea aplicațiilor standard, cum ar fi browserele, software-ul de productivitate a biroului și instrumentele de securitate, înainte de a putea accesa rețeaua.

7.3. Securitate

Pentru a preveni accesul neautorizat, dispozitivele trebuie să fie protejate prin parolă utilizând caracteristicile dispozitivului și este necesară o parolă puternică pentru a accesa rețeaua **Asociația** Brahma.

Politica puternică a parolei Operatorului este: parolele trebuie să aibă cel puțin șase caractere și o combinație de litere mari, mici și cifre și simboluri. Parolele vor fi schimbate la fiecare 90 de zile, iar noua parolă nu poate fi una din cele 15 parole anterioare.

Dispozitivul trebuie să se blocheze cu o parolă sau un cod PIN dacă este inactiv timp de cinci minute.

După cinci încercări de conectare eșuate, dispozitivul se va bloca. Se va contacta Departamentul IT pentru a se redobândi accesul.

Este strict interzisă accesarea rețelelor rădăcină (Android) sau jailbroken (iOS).

Angajații sunt în mod automat împiedicați să descarce, să instaleze și să utilizeze orice aplicație care nu apare în lista de aplicații aprobate a **Asociației Brahma**.

Telefoanele inteligente și tabletele care nu se află pe lista de dispozitive acceptate ale **Asociației Brahma** nu au voie să se conecteze la rețea.

Smartphone-urile și tabletele aparținând angajaților care sunt numai pentru uz personal nu au voie să se conecteze la rețea.

Accesul angajaților la datele **Asociației Brahma** este limitat pe baza profilurilor utilizatorilor definite de IT și aplicate automat.

Dispozitivul angajatului poate fi șters de la distanță dacă:
1. dispozitivul este pierdut;
2. angajatul își încetează raporturile de muncă;
3. departamentul IT detectează o încălcare a datelor sau a politicii, un virus sau o amenințare similară la adresa securității infrastructurii de date și tehnologii a **Asociației Brahma**.

7.4. Riscuri. Disclaimere

În timp ce Departamentul IT va lua toate măsurile de precauție pentru a preveni pierderea datelor personale ale angajatului în cazul în care trebuie să șteargă de la distanță un dispozitiv, este responsabilitatea angajatului de a lua măsuri de precauție suplimentare, cum ar fi copierea de rezervă a e-mail-urilor, a contactelor etc.

Asociația Brahma își rezervă dreptul de a deconecta dispozitivele sau de a dezactiva serviciile fără notificare.

Dispozitivele pierdute sau furate trebuie să fie raportate **Asociației Brahma** în termen de 24 de ore. Angajații sunt responsabili pentru notificarea imediată după pierderea unui dispozitiv.
Angajații trebuie să-și folosească dispozitivele în mod etic în orice moment și să respecte politica de utilizare acceptabilă a **Asociației Brahma**.

Angajații sunt responsabili personal pentru toate costurile asociate cu dispozitivul său.
Angajatul își asumă răspunderea deplină pentru riscuri, inclusiv, dar fără a se limita la pierderea parțială sau completă a datelor **Asociației Brahma** și a datelor personale din cauza unei erori de sistem de operare, erori, viruși, malware și/sau alte defecțiuni software sau hardware sau programare erorile care fac dispozitivul inutilizabil.

Asociația Brahma își rezervă dreptul de a lua măsuri disciplinare corespunzătoare până la încetarea contractului individual de muncă pentru nerespectarea acestor reguli.

8. SUPRAVEGHERE VIDEO ȘI ÎNREGISTRARE TELEFONICĂ

Pentru protejarea securității clienților, a Celorlalte Persoane Vizate și a oricăror alți vizitatori, cât și pentru asigurarea pazei și protecției bunurilor acestora, ale Operatorului și/sau ale angajaților acestuia, sediul Operatorului este protejat prin *supraveghere video/înregistrarea imaginilor* obținute prin mijloace de supraveghere video.

Pentru aceste scopuri, persoanele vizate anterior menționate, precum și bunurile utilizate de acestea când sosesc la, accesează sau vizitează sediul Operatorului și/sau spațiile exterioare adiacente, sunt filmate cu mijloace de supraveghere video instalate în locuri vizibile și utilizate în conformitate cu reglementările legale în vigoare.

Supravegherea video are loc doar în **spațiile destinate publicului**, inclusiv pe căile de acces situate în interiorul sau exteriorul imobilului unde este situat sediul Operatorului, locul amplasării mijloacelor de supraveghere video fiind semnalat prin intermediul unei pictograme care conține o imagine reprezentativă și are vizibilitate suficientă, poziționată în apropierea locului de amplasare.

Imaginile înregistrate prin utilizarea mijloacelor de supraveghere video vor fi transmise de către Operator către organele de poliție și alte autorități cu atribuții privind apărarea drepturilor și libertăților fundamentale ale persoanei, a proprietății private și publice, prevenirea, descoperirea și sancționarea infracțiunilor, respectarea ordinii și liniștii publice, în condițiile legii. Imaginile astfel obținute nu vor fi transmise în străinătate.

Informarea persoanelor vizate cu privire la prelucrarea Datelor Personale prin mijloace de supraveghere video are loc într-o formă concisă, transparentă, inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu, în special pentru orice informaţii adresate în mod specific unui copil. Informaţiile se furnizează în scris sau prin alte mijloace, inclusiv, atunci când este oportun, în format electronic. La solicitarea persoanei vizate, informaţiile pot fi furnizate verbal, cu condiţia ca identitatea persoanei vizate să fie dovedită prin alte mijloace.

Operatorul poate înregistra apelurile telefonice către/de la Operator, purtate de Operator/Împuterniciții Operatorului cu clienții/potențialii clienți și/sau Celelalte Persoane Vizate, indiferent de persoana care a inițiat apelul, și poate păstra aceste înregistrări, în baza Consimțământului obținut în acest sens și cu respectarea prevederilor legale aplicabile. Înregistrările astfel obținute vor fi utilizate de Operator în scopul încheierii și executării în condiții optime a contractelor cu clienții, al investigării anumitor situații apărute în derularea sau în legătură cu acestea, precum și în instanță, ca probe, în cazul unor litigii rezultate din/sau în legătură cu contractele respective/finanțarea acordata. De asemenea, înregistrările telefonice vor putea fi transmise, în condițiile legii, autorităților cu atribuții privind apărarea persoanelor, proprietății private și publice, prevenirea, descoperirea și sancționarea infracțiunilor.

9. PERSOANE ÎMPUTERNICITE DE OPERATOR

Parteneri contractuali/colaboratori ai Operatorului și ai entităților afiliate sau alte societăți ce oferă servicii complementare serviciilor Operatorului, precum:

- ✓ entități care participă la negocierea, încheierea sau la aducerea la îndeplinire a contractelor (furnizori de servicii, operatori IT, avocați și alți consultanți etc.);
- ✓ entități care asigură **buna funcționare a serviciilor Operatorului** și a tuturor tranzacțiilor legate de produsele și serviciile acestuia;
- ✓ entități care asigură **securitatea și alte tipuri de protecție sistemelor informatice** ale Operatorului și ale entităților afiliate care funcționează în România;
- ✓ entități care cercetează nivelul calitativ pentru satisfacerea **cerințelor clienților sau care asigură sau mijlocesc oferta de produse și servicii ale Operatorului;**
- ✓ societăți care **imprimă, administrează și/sau transmit facturi/deconturi/notificări**;
- ✓ curieri;
- ✓ furnizori de servicii de contact/call-center;
- ✓ **societăți de arhivare**-stocare documente;
- ✓ **consultanți, contabili, auditori**;
- ✓ persoane către care au fost transferate **drepturile și/sau obligațiile Operatorului**;
- ✓ entități care asigură **colectarea creanțelor și/sau recuperarea bunurilor**.

Datele transmise Destinatarilor vor fi **adecvate, pertinente și neexcesive** prin raportare la scopurile în care au fost colectate.

Pentru îndeplinirea obligațiilor și angajamentelor ce îi revin din contractele încheiate cu clienții săi, precum și pentru a asigura o prelucrare eficientă și profesionistă, Operatorul poate prelucra Datele cu caracter personal inclusiv prin terțe persoane, împuternicite în acest sens de către Operator, cu care va încheia contracte scrise în condițiile Regulamentului („**Împuterniciții**").

Împuterniciții sunt obligați să respecte **cerințele Operatorului** pentru siguranța prelucrării și să ia măsurile tehnice și organizatorice necesare pentru asigurarea protecției Datelor cu caracter personal.

Cu titlu exemplificativ, pot fi desemnate drept împuterniciți următoarele categorii de persoane:

- ✓ **societăți de arhivare**-stocare documente;
- ✓ **societăți care imprimă, administrează și/sau transmit facturi/deconturi/notificări;**
- ✓ curieri;
- ✓ furnizori de servicii de contact/call center.

10. MĂSURI PREVENTIVE

Angajații înțeleg pericolul reprezentat de atacurile cibernetice sau cele de tip social (social engineering), precum și repercusiunile pe care aceste atacuri le pot avea asupra Operatorului, asupra angajaților acestuia sau a persoanelor vizate.

Pentru a se asigura un standard ridicat de securitate, Operatorul organizează cursuri de instruire cu privire la vulnerabilitățile datelor personale și măsurile preventive de securitate ce se adoptă în cazul atacurilor cibernetice.

Angajatul va fi informat cu privire la atacurile precum:
- Phishing: prin care atacatorii utilizează e-mail-urile de tip spam pentru a direcționa victimele către site-uri web create de atacatori astfel încât datele personale să fie introduse pe acel site web;
- Social engineering: manipularea rău-intenționată a anumitor persone prin care angajații sunt convinși să disemineze date cu caracter confidențial;
- DNS poisoning: Otrăvirea cache este un atac în care datele corupte sunt inserate în baza de date cache a serverului de nume DNS (Domain Name System). Atacatorul intenționează să trimită răspunsuri duplicate de la un DNS impostor pentru a redirecționa un nume de domeniu la o nouă adresă IP. Noua adresă IP este cel mai probabil controlată de atacator și este utilizată pentru a răspândi viermii de calculator și alte programe malware.

POLITICĂ PRIVIND GESTIONAREA DATELOR CU CARACTER PERSONAL

1. DEFINIȚII

„GDPR", „Regulamentul" - Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor, în limba engleză General Data Protection Regulation);
„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;
„prelucrare" - înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;
„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;
„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 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" - 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;

*„**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;

„reprezentant” - înseamnă o persoană fizică sau juridică stabilită în Uniune, desemnată în scris de către operator sau persoana împuternicită de operator, care reprezintă operatorul sau persoana împuternicită în ceea ce privește obligațiile lor respective care le revin în temeiul GDPR;
„reguli corporatiste obligatorii” - înseamnă politicile în materie de protecție a datelor cu caracter personal care trebuie respectate de un operator sau de o persoană împuternicită de operator stabilită pe teritoriul unui stat membru, în ceea ce privește transferurile sau seturile de transferuri de date cu caracter personal către un operator sau o persoană împuternicită de operator în una sau mai multe țări terțe în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună;
„autoritate de supraveghere” - înseamnă o autoritate publică independentă instituită de un stat membru;
„DPIA” - evaluarea impactului asupra protecției datelor (în limba engleză, data-protection impact assessment, DPIA);
„Autoritate de Supraveghere” - Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP).

2. SCOPUL ȘI DOMENIUL DE APLICARE

2.1. SCOPUL

Prezenta politică documentează cerințele GDPR privind gestionarea datelor cu caracter personal ale persoanelor vizate.

Prezenta politică are în vedere reguli generale și măsuri pentru a asigura faptul că orice persoană fizică care acționează sub autoritatea și care **gestionează** date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepția cazului în care această obligație îi revine în temeiul dreptului Uniunii sau al dreptului intern.

Angajații **Asociației Brahma** înțeleg și au reprezentarea deplină a faptului că încălcarea regulilor privind **gestionarea greșită a datelor cu caracter personal** poate conduce la prejudicii fizice, materiale sau morale persoanelor fizice, cum ar fi pierderea controlului asupra datelor lor cu caracter personal sau limitarea drepturilor lor, discriminare, furt sau fraudă de identitate, pierdere financiară, inversarea neautorizată a pseudonimizării, compromiterea reputației, pierderea confidențialității datelor cu caracter personal protejate prin secret profesional sau orice alt dezavantaj semnificativ de natură economică sau socială adus persoanei fizice în cauză.

2.2. DOMENIUL DE APLICARE

Prezenta politică se aplică tuturor structurilor organizatorice ale Operatorului. Prezenta politică va fi considerată ca având caracter general și se va aplica tuturor prelucrărilor efectuate de Operator. În cazul în care se constată existența anumitor aspecte legate de gestionarea datelor cu caracter general pentru care prezenta politică nu oferă directive corespunzătoare, angajații trebuie să solicite imediat consiliere din partea responsabilului cu protecția datelor, dacă a fost numit, sau reprezentantului legal al Operatorului.

2.3. DOCUMENTE DE REFERINȚĂ

- GDPR;
- Regulament intern;
- Proceduri interne.

3. REGULI GENERALE

3.1. Principii privind prelucrarea. Desfășurarea activității curente a **Asociației Brahma** presupune efectuarea de către angajații acesteia a unor prelucrări de date care se supun următoarelor principii:

- datele sunt prelucrate în mod legal, echitabil și transparent;
- datele sunt colectate în **scopuri determinate, explicite și legitime** și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile inițiale;
- datele sunt **adecvate, relevante și limitate** la ceea ce este necesar în raport cu scopurile în care sunt prelucrate;
- datele sunt exacte și, în cazul în care este necesar, să fie actualizate; se vor lua toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere;
- datele sunt păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal sunt stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice;

- datele sunt prelucrate într-un mod care asigură securitatea adecvată, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare.

3.2. Informații referitoare la datele personale reținute

A. Reducerea la minimum a datelor

Asociația Brahma respectă principiul reducerii la minimum a datelor potrivit GDPR, respectiv reține și stochează numai datele relevante și necesare îndeplinirii scopului prelucrării datelor cu caracter personal.

B. Exactitate

Datele personale prelucrate de **Asociația Brahma** sunt exacte și actualizate la momentul stocării, efectuând verificări pentru a asigura acest aspect în cazul în care este necesar.

3.6. Termenele de stocare

Asociația Brahma ia măsuri adecvate privind eliminarea datelor cu caracter personal atunci când acestea nu mai sunt necesare atingerii scopului prelucrării. Acest lucru reduce riscul stocării unor date inexacte, inutile sau irelevante. Această obligație se aplică volumului de date colectate, gradului de prelucrare a acestora, perioadei lor de stocare și accesibilității lor.

La împlinirea termenelor prevăzute de lege și în normele interne, Operatorul va asigura ștergerea/distrugerea datelor personale, cu excepția cazului în care legislația EU sau cea națională prevăd obligația păstrării acestora pe o perioadă mai îndelungată, în scopuri statistice, de arhivare în interes public, de cercetare științifică sau istorică și cu asigurarea măsurilor tehnice și organizatorice adecvate în vederea garantării drepturilor și libertăților persoanei vizate. În aceste cazuri, datele prelucrate al căror timp de stocare s-a împlinit vor putea fi arhivate cu respectarea măsurilor tehnice și organizatorice stabilite în politicile și procedurile interne.

4. REGULI SPECIFICE PRIVIND GESTIONAREA DATELOR
4.1. Sfera datelor personale
Datele clienților

Asociația Brahma prelucrează următoarele date cu caracter personal aparținând clientului și/sau celorlalte Persoane Vizate, astfel cum acestea sunt comunicate:

(i) prin intermediul formularelor de cerere privind acordarea produsului/serviciului solicitat și a anexelor acestora;
(ii) prin intermediul propunerii pentru încheierea contractului și a anexelor acesteia;
(iii) prin intermediul **comunicărilor transmise Operatorului** după data încheierii contractului *(în formă scrisă, în formă electronică, completate la întrebările formulate telefonic de angajații Operatorului/Împuterniciți și prin alte procedee acceptate de persoana vizata)*, precum: prenume, nume, numele anterior, pseudonimul, sexul, adresa de domiciliu și de reședință, data, locul și țara nașterii, codul numeric personal, seria și numărul actului de identitate/pașaportului, alte date ale actului de identitate, alte date din actele de stare civilă, cetățenia, semnătura, datele din permisul de conducere/certificatul de înmatriculare, date de contact *(adrese, numere de telefon, fax, adrese electronice și nr. de telefon mobil),* profesia, locul de muncă, numărul dosarului de pensie, situație militară, situație economică și financiară ale clientului sau, după caz, ale Celorlalte Persoane Vizate.

Asociația Brahma poate colecta și utiliza datele personale ale clienților și potențialilor clienți (de ex. nume, vârsta, data nașterii, adresa, rezidența, e-mail etc.), pentru realizarea scopurilor de afaceri.

Datele angajaților
Asociația Brahma colectează și utilizează datele personale ale angajaților și foștilor angajați în cadrul desfășurării raporturilor de muncă inclusiv a obligațiilor care decurg din acestea, în temeiul legii și numai în scopuri relevante, corespunzătoare și uzuale.

Asociația Brahma recunoaște și respectă drepturile de confidențialitate ale angajaților săi, limitând colectarea, accesul și utilizarea datelor personale aferente angajării. **Asociația Brahma** ia măsuri preventive suplimentare înainte de divulgarea către părțile terțe legitime a informațiilor oricărui angajat. Respectivele divulgări pot avea loc numai în condițiile în care există înțelegerea deplină a faptului că accesul și utilizarea datelor sunt limitate, și că datele trebuie să fie protejate.

4.2. Soluții de organizare
Asociația Brahma în calitate de Operator, a adoptat următoarele soluții de organizare în ceea ce privește gestionarea datelor cu caracter personal:

- ✓ aspectele tehnice de securitate a datelor intră în responsabilitatea Departamentului IT și trebuie gestionate atât în baza liniilor directoare definite, a proceselor și procedurilor, cât și prin controale efectuate la nivelul sistemelor informatice;
- ✓ responsabilitatea privind prelucrarea datelor în acord cu prezenta politică revine tuturor angajaților, Operatorul va asigura măsurile organizatorice necesare implementării prevederilor GDPR, astfel încât prelucrările datelor cu caracter personal să fie efectuate în conformitate cu legislația europeană și națională;
- ✓ Responsabilul cu protecția datelor, respectiv persoana desemnată va instrui angajații astfel încât aceștia să respecte gestionarea corectă a datelor personale;
- ✓ Operatorul poate – la alegerea sa, sau dacă este prevăzut de legea în vigoare - să desemneze un **Responsabil cu protecția datelor** care va superviza toate activitățile de prelucrare a datelor personale. Indiferent de numirea Responsabilului cu protecția datelor, desemnarea responsabilităților trebuie sa reflecte cerințele Operatorului menționate mai sus. În toate cazurile, se va desemna un responsabil cu protecția datelor atunci când aceasta este obligatorie potrivit Regulamentului *(prezența unor operațiuni de prelucrare care necesită o monitorizare periodică, sistematică a persoanelor vizate pe scară largă, prelucrarea pe scară largă vizează categorii speciale de date);*
- ✓ Angajații **Asociației Brahma** sunt obligați să respecte măsurile de prelucrare a datelor cu caracter personal, asigurând-se un nivel adecvat de protecție a datelor astfel prelucrate.

4.3. Verificarea corectitudinii datelor cu caracter personal
Toți angajații au obligația să verifice datele personale păstrate de **Asociația Brahma** din perspectiva **acurateței și integralității informațiilor relevante** și trebuie să le modifice corespunzător. Ca regulă generală, gestionarea datelor este limitată la datele utilizate pentru identificarea unei persoane vizate.

4.4. Activități personale
Angajamentul Operatorului **Asociația Brahma** de a respecta cerințele în materie de protecția datelor cu caracter personal nu reprezintă permisiunea de a desfășura activități personale necorespunzătoare în timpul serviciului (ex. calculatoarele trebuie să fie utilizate doar în interes de serviciu). În plus, pentru a asigura securitatea și protecția sistemelor sale IT, **Asociația Brahma** are dreptul de acces în toate sediile și, dacă este necesar, de a revizui comunicările și informațiile create de angajați în timpul activității, în limitele permise de legislația în vigoare.

4.5. Refuzul de prelucrare a datelor cu caracter personal
Orice angajat are dreptul de a transmite conducerii Operatorului **obiecțiuni** în legătură cu gestionarea datelor cu caracter personal, respectiv colectarea, utilizarea și divulgarea datelor personale. **Asociația Brahma** va evalua obiecțiunile angajatului, va lua o decizie în conformitate cu legislația în vigoare și va comunica decizia sa angajatului.

Politica de reținere și ștergere a datelor cu caracter personal

1. DEFINIȚII

„GDPR", „Regulamentul" - Regulamentul (UE) 2016/679 al Parlamentului Eurpean și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor, în limba engleză General Data Protection Regulation);

„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;

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

„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;
„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 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" - 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;

*„**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;

„reprezentant” - înseamnă o persoană fizică sau juridică stabilită în Uniune, desemnată în scris de către operator sau persoana împuternicită de operator, care reprezintă operatorul sau persoana împuternicită în ceea ce privește obligațiile lor respective care le revin în temeiul GDPR;

„reguli corporatiste obligatorii” - înseamnă politicile în materie de protecție a datelor cu caracter personal care trebuie respectate de un operator sau de o persoană împuternicită de operator stabilită pe teritoriul unui stat membru, în ceea ce privește transferurile sau seturile de transferuri de date cu caracter personal către un operator sau o persoană împuternicită de operator în una sau mai multe țări terțe în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună;

„autoritate de supraveghere” - înseamnă o autoritate publică independentă instituită de un stat membru;

„DPIA” - evaluarea impactului asupra protecției datelor (în limba engleză, data-protection impact assessment, DPIA);

*„**Stocarea / Reținerea datelor cu caracter personal**”* - înseamnă păstrarea pe orice fel de suport a datelor cu caracter personal culese;

„***Ș**tergerea datelor cu caracter personal*” - înseamnă eliminarea/distrugerea efectivă a datelor personale;

„Arhivarea datelor cu caracter personal” - înseamnă păstrarea datelor personale, după criterii prestabilite într-un mediu securizat, acestea putând fi accesate la un moment dat;

„Scoaterea datelor cu caracter personal din uz” - înseamnă plasarea datelor personale într-un mediu securizat, fără nicio intenței din partea Operatorului de a le reaccesa, urmând ca acestea să fie șterse de îndată ce este posibil.

2. SCOPUL ȘI DOMENIUL DE APLICARE

2.1. SCOPUL

2.1.1. Prezenta politică documentează cerințele GDPR privind reținerea/stocarea și ștergerea datelor cu caracter personal, în vederea asigurării confidenţialităţii datelor şi informaţiilor precum şi pentru păstrarea în siguranţă a acestora, în cadrul activităţii curente executate de către angajaţii **Asociației Brahma.**

2.1.2. Politica descrie activitățile desfășurate cu privire la operațiunile de stocare și de ștergere a datelor cu caracter personal, respectiv stabilește cazurile în care datele personale trebuie reținute sau șterse.

2.1.3. Prin prezenta politică se urmărește asigurarea unui cadru legal și eficient de prelucrare a datelor cu caracter personal, în ceea ce privește stocarea și ștergerea datelor cu caracter personal cu respectarea drepturilor persoanelor vizate, în acord cu reglementările Regulamentului și legislației conexe.

2.2. DOMENIUL DE APLICARE

Prezenta politică se aplică tuturor structurilor organizatorice ale Operatorului. Politica este întocmită în scopul prezentării circuitului intern de prelucrare a datelor personale în ceea ce privește reținerea și ștergerea datelor cu caracter personal. La politică participă toate structurile organizatorice conform cu atribuțiile care le revin în ceea ce privește activitatea de prelucrare a datelor personale.

2.3. DOCUMENTE DE REFERINȚĂ

- GDPR
- Regulament intern
- Proceduri interne

3. REGULI PRIVIND POLITICA DE REȚINERE A DATELOR CU CARACTER PERSONAL

Reținerea datelor cu caracter personal reprezintă o prelucrare a datelor cu caracter personal în sensul Regulamentului. Reținerea datelor cu caracter personal se va efectua doar în situația în care operatorul a identificat unul dintre temeiurile legale prevăzute de Regulament pentru o anumită categorie de date personale, în conformitate cu Politica de prelucrare a datelor personale.

3.1. Clasificarea datelor cu caracter personal. Conform Politicii de confidențialitate, **Asociația Brahma** prelucrează în mod legal următoarele categorii de date cu caracter personal:

A.	**Date confidențiale**
Originea etnica Conturi IBAN	Categoria datelor confidențiale va cuprinde datele definite de Regulament ca aparținând categoriei speciale de date cu caracter personal (date care dezvăluie originea rasială sau etnică, opiniile politice, datele genetice, biometrice, date privind sănătatea unei persoane etc.) precum și acele date a căror divulgare neautorizată, alterare sau distrugere ar cauza un risc semnificativ la adresa Operatorului sau a persoanelor vizate. Exemple: Date referitoare la securtatea IT, conturi IBAN, număr carte credit.
B.	Date private
Detalii de contact	Categoria datelor private privește acele date a căror divulgare neautorizată, alterare sau distrugere ar cauza un risc moderat la adresa Operatorului sau a persoanelor vizate. Exemple: comportamentul sau performanța angajaților, salariul angajaților, date media, detalii de contact.
C.	Date publice

Nu este cazul	Datele publice reprezintă acele date a căror divulgare neautorizată, alterare sau distrugere ar cauza un risc scăzut la adresa Operatorului sau a persoanelor vizate. Exemple: Informații din presă, date publicitare, website-uri publice, informații din mediul public.

3.2. Forma datelor reținute

A. Format electronic

Datele personale vor fi reținute în format electronic, cu respectarea măsurilor tehnice și organizatorice prevăzute în Politica de confidențialitate. Datele cu caracter personal vor fi păstrate într-o formă care să permită identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele. În cazul în care scopul prelucrării datelor nu necesită sau nu mai necesită identificarea unei persoane vizate de către operator, operatorul nu va păstra informații suplimentare necesare identificării persoanei vizate în scopul unic al respectării drepturilor persoanelor vizate.

B. Format fizic

Datele prelucrate în format fizic vor reprezenta date personale în acord cu prevederile Regulamentului, în măsura în care acestea fac parte dintr-un sistem de evidență a datelor sau care sunt destinate să facă parte dintr-un sistem de evidență a datelor. Datele vor fi reținute cu respectarea măsurilor tehnice și organizatorice prevăzute în Politica de confidențialitate. Datele cu caracter personal vor fi păstrate într-o formă care să permită identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele. În cazul în care scopul prelucrării datelor nu necesită sau nu mai necesită identificarea unei persoane vizate de către operator, operatorul nu va păstra informații suplimentare necesare identificării persoanei vizate în scopul unic al respectării drepturilor persoanelor vizate.

3.3. Personal competent

În funcție de clasificarea datelor de la pct. 3.1, stocarea datelor personale se face doar de către personalul autorizat să prelucreze anumite categorii de date cu caracter personal. Fiecare membru angajat al **Asociației Brahma** este arondat unui Grup ce deține anumit nivel de acces la datele procesate de către Operator, după cum urmează:

A.	Grup nivel de acces I
Grup implementare proiect (operatori grup țintă și responsabil proiect) Departamentul financiar-contabil	Date publice – Stocarea datelor publice poate fi efectuată de către membrii acestui grup.
B.	Grup nivel de acces II
Grup implementare proiect (operatori grup țintă și responsabil proiect) Departamentul financiar-contabil	Date private – Stocarea datelor private și a celor publice poate fi efectuată de către membrii acestui grup.
C.	Grup nivel de acces III
Nu este cazul	Date confidențiale – Stocarea datelor confidențiale, a celor private precum și a celor publice poate fi efectuată de către membrii acestui grup.

3.4. Stocarea datelor. În cadrul **Asociației Brahma**, datele prelucrate vor fi stocate în funcție de departamentul în care salariații își desfășoară activitatea și de categoria din care acestea fac parte, pe baza următorelor tabele:

A. Format electronic

A.1. Departamentul implementare proiecte

A.	**Date confidențiale**
Originea etnică Conturi IBAN	Stocarea datelor confidențiale se face pe un hard-disk criptat, asigurându-se nivelul adecvat de confidențialitate, integritate, disponibilitate și rezistență continuă a sistemului informatic necesar datelor confidențiale în conformitate cu măsurile tehnice stabilite în Politica de confidențialitate.
B.	Date private
Detalii contact	Datele private sunt stocate pe un hard-disk criptat, asigurându-se nivelul adecvat de confidențialitate, integritate, disponibilitate și rezistență continuă a sistemului informatic necesar datelor private în conformitate cu măsurile tehnice stabilite în Politica de confidențialitate.
C.	Date publice
Nu este cazul	Datele publice sunt stocate pe un hard-disk criptat sau necriptat, asigurându-se nivelul adecvat de confidențialitate, integritate, disponibilitate și rezistență continuă a sistemului informatic necesar datelor publice în conformitate cu măsurile tehnice stabilite în Politica de confidențialitate.

A.2. Departamentul financiar-contabil

A.	**Date confidențiale**
Originea etnică Conturi IBAN	Sunt stocate pe un hard-disk criptat, asigurându-se nivelul adecvat de confidențialitate, integritate, disponibilitate și rezistență continuă a sistemului informatic necesar prelucrării datelor confidențiale în conformitate cu măsurile tehnice stabilite în Politica de confidențialitate.
B.	Date private
Detalii contact	Sunt stocate pe un hard-disk criptat, asigurându-se nivelul adecvat de confidențialitate, integritate, disponibilitate și rezistență continuă a sistemului informatic necesar prelucrării datelor private în conformitate cu măsurile tehnice stabilite în Politica de confidențialitate.
C.	Date publice
Nu este cazul	Sunt stocate pe un hard-disk criptat sau necriptat, asigurându-se nivelul adecvat de confidențialitate,

	integritate, disponibilitate și rezistență continuă a sistemului informatic necesar prelucrării datelor publice în conformitate cu măsurile tehnice stabilite în Politica de confidențialitate.

B. Format fizic

B.1. Departamentul implementare proiecte

A.	**Date confidențiale**
Originea etnică Conturi IBAN	Sunt păstrate într-un spațiu închis, securizat, asigurându-se nivelul adecvat de confidențialitate, integritate și disponibilitate a serviciului de prelucrare corespunzător datelor confidențiale în conformitate cu măsurile tehnice stabilite în Politica de confidențialitate.
B.	Date private
Detalii contact	Sunt păstrate într-un spațiu închis, asigurându-se nivelul adecvat de confidențialitate, integritate și disponibilitate a serviciului de prelucrare corespunzător datelor confidențiale în conformitate cu măsurile tehnice stabilite în Politica de confidențialitate.
C.	Date publice
Nu este cazul	Sunt păstrate într-un spațiu accesibil angajaților și/sau publicului, asigurându-se nivelul adecvat de confidențialitate, integritate și disponibilitate a serviciului de prelucrare corespunzător datelor confidențiale în conformitate cu măsurile tehnice stabilite în Politica de confidențialitate.

B.2. Departamentul financiar contabilitate

A.	**Date confidențiale**
Originea etnică Conturi IBAN	Sunt păstrate într-un spațiu închis, securizat, asigurându-se nivelul adecvat de confidențialitate, integritate și disponibilitate a serviciului de prelucrare corespunzător datelor confidențiale în conformitate cu măsurile tehnice stabilite în Politica de confidențialitate.
B.	Date private
Detalii contact	Sunt păstrate într-un spațiu închis, asigurându-se nivelul adecvat de confidențialitate, integritate și disponibilitate a serviciului de prelucrare corespunzător datelor confidențiale în conformitate cu măsurile tehnice stabilite în Politica de confidențialitate.
C.	Date publice
Nu este cazul	Sunt păstrate într-un spațiu accesibil angajaților și/sau publicului, asigurându-se nivelul adecvat de confidențialitate, integritate și disponibilitate a serviciului de prelucrare corespunzător datelor confidențiale în conformitate cu măsurile tehnice stabilite în Politica de confidențialitate.

3.5. Informații referitoare la datele personale reținute

C. Reducerea la minimum a datelor

Asociația Brahma respectă principiul reducerii la minimum a datelor potrivit Regulamentului, respectiv reține și stochează numai datele relevante și necesare îndeplinirii scopului prelucrării conform Politicii de confidențialitate.

D. Exactitate

Datele personale prelucrate de **Asociația Brahma** sunt exacte și actualizate la momentul stocării, efectuând verificări pentru a asigura acest aspect în cazul în care este necesar.

3.6. Termenele de stocare

Asociația Brahma ia măsuri adecvate privind eliminarea datelor cu caracter personal atunci când acestea nu mai sunt necesare atingerii scopului prelucrării. Acest lucru reduce riscul stocării unor date inexacte, inutile sau irelevante. Această obligație se aplică volumului de date colectate, gradului de prelucrare a acestora, perioadei lor de stocare și accesibilității lor.

La împlinirea termenelor prevăzute în Nomenclatorul Arhivistic se va asigura ștergerea/distrugerea datelor personale, cu excepția cazului în care legislația EU sau cea națională prevăd obligația păstrării acestora pe o perioadă mai îndelungată, în scopuri statistice, de arhivare în interes public, de cercetare științifică sau istorică și cu asigurarea măsurilor tehnice și organizatorice adecvate în vederea garantării drepturilor și libertăților persoanei vizate.

În aceste cazuri, datele prelucrate al cărui timp de stocare s-a împlinit vor putea fi arhivate cu respectarea măsurilor tehnice și organizatorice stabilite în Politica de confidențialitate.

4. REGULI PRIVIND POLITICA DE ȘTERGERE A DATELOR CU CARACTER PERSONAL

La sfârşitul perioadei de reţinere, datele stocate trebuie să fie revizuite şi eliminate. Sistemele automate pot semnala momentul la care datele personale ar trebui revizuite sau şterse după o perioadă de timp determinată.

4.1. Distincție **ștergere**-arhivare

Există o diferență semnificativă între **ștergerea definitivă** și arhivarea datelor cu caracter personal. Dacă datele personale sunt arhivate, acest lucru ar trebui să le reducă disponibilitatea și riscul de pierdere, distrugere accidentală, alterare etc.

Datele personale vor fi arhivate atunci când există obligația de a fi păstrate în continuare.

Persoanelor vizate li se vor permite exercitarea dreptului de acces la datele cu caracter personal și li se vor respecta principiile privind protecția datelor cu caracter personal, având în vedere faptul că arhivarea datelor reprezintă o prelucrare în conformitate cu dispozițiile Regulamentului.
Atunci când este necesar să fie şterse anumite date cu caracter personal, prelucrate în activitatea curentă a organizației, vor fi eliminate orice copii efectuate de pe acestea.

Ștergerea datelor personale presupune eliminarea/distrugerea acestora, precum și a oricăror copii existente.

Ștergerea datelor personale se efectua la momentul împlinirii termenelor stabilite în Nomenclatorul Arhivistic, precum și ori de câte ori datele stocate sunt inexacte și nu pot fi rectificate, persoana vizată și-a retras consimțământul prelucrării datelor cu caracter personal - cu excepțiile prevăzute de lege, sau stocarea acestora nu mai este necesară îndeplinirii scopului/scopurilor în care au fost prelucrate, cu respectarea procedurilor aferente acestor situații.

4.2. Operațiunea de ștergere a datelor cu caracter personal

Ștergerea datelor cu caracter personal este una efectivă și reală, astfel încât conținutul lor să nu mai poată fi recuperat în niciun fel.

A. Date în format electronic

Asociația Brahma va lua următoarele **măsuri de ștergere a datelor cu caracter personal** prin oricare din modalitățile prezentate mai jos:

- printr-un program software de distrugere a datelor de pe hard-disk ;
- prin contractarea unui furnizor de servicii IT specializat în operațiunile de ștergere a datelor;
- prin distrugerea hard disk-ului;
- prin alte metode legale.

Asociația Brahma va lua următoarele măsuri de scoatere din uz a datelor cu caracter personal:

- păstrarea datelor personale într-un folder criptat și restricționat accesului, cu instituirea unor măsuri de securitate tehnice și organizatorice corespunzătoare;
- operatorul nu este în măsură și nu va utiliza datele cu caracter personal;
- operatorul se angajează să șteargă definitiv datele personale de îndată ce acest lucru devine posibil/este fezabil.

Aceste măsuri se vor lua numai în situația în care datele nu pot fi șterse fără a elimina alte informații necesare activității Operatorului ce se regăsesc în aceeași partiție a Hard Disk-ului.

B. Date în format fizic

Asociația Brahma va lua următoarele **măsuri de ștergere a datelor cu caracter personal**:

- prin utilizarea distrugătoarelor de hârtie;
- prin oricare alte metode legale.

4.3. Măsuri organizatorice și tehnice în situația în care datele șterse sunt publice

În cazul în care datele șterse/care urmează să fie șterse sunt publice, Operatorul va lua măsuri rezonabile pentru a informa ceilalți operatori care prelucrează date cu caracter personal că persoana vizată a solicitat ștergerea a oricăror linkuri către datele respective sau a oricăror copii sau reproduceri ale datelor cu caracter personal.

Operatorul va contacta ceilalți operatori care prelucrează datele personale, enumerând și identificând datele personale a căror ștergere se solicită de către persoana vizată, prin următoarele metode:

- prin intermediul e-mail-ului;
- prin intermediul fax-ului;
- prin intermediul serviciilor de curierat rapid;

- prin orice altă metodă care asigură transmiterea confidențială a mesajului și confirmarea primirii;
- prin orice alte metode legale

Procedura de arhivare

1. DEFINIȚII

„GDPR", „Regulamentul" - Regulamentul (UE) 2016/679 al Parlamentului Eurpean și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor, în limba engleză General Data Protection Regulation);

„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;

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

„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;

*„**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 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**"* - 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;

*„**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;

„reprezentant” - înseamnă o persoană fizică sau juridică stabilită în Uniune, desemnată în scris de către operator sau persoana împuternicită de operator, care reprezintă operatorul sau persoana împuternicită în ceea ce privește obligațiile lor respective care le revin în temeiul GDPR;

„reguli corporatiste obligatorii” - înseamnă politicile în materie de protecție a datelor cu caracter personal care trebuie respectate de un operator sau de o persoană împuternicită de operator stabilită pe teritoriul unui stat membru, în ceea ce privește transferurile sau seturile de transferuri de date cu caracter personal către un operator sau o persoană împuternicită de operator în una sau mai multe țări terțe în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună;

„autoritate de supraveghere” - înseamnă o autoritate publică independentă instituită de un stat membru;

„DPIA” - evaluarea impactului asupra protecției datelor (în limba engleză, data-protection impact assessment, DPIA);

*„**Stocarea/Reținerea datelor cu caracter personal**”* - înseamnă păstrarea pe orice fel de suport a datelor cu caracter personal culese;

„***Ș**tergerea datelor cu caracter personal*” - înseamnă eliminarea/distrugerea efectivă a datelor personale;

„Arhivarea datelor cu caracter personal” - înseamnă păstrarea datelor personale, după criterii prestabilite într-un mediu securizat, acestea putând fi accesate la un moment dat;

„Scoaterea datelor cu caracter personal din uz” - înseamnă plasarea datelor personale într-un mediu securizat, fără nicio intenței din partea Operatorului de a le reaccesa, urmând ca acestea să fie șterse de îndată ce este posibil.

2. SCOPUL ȘI DOMENIUL DE APLICARE

2.1. SCOPUL

2.1.1. Prezenta procedură documentează cerințele GDPR privind activitatea de arhivare și păstrare a documentelor în cadrul **Asociației Brahma**, în vederea asigurării protecției datelor cu caracter personal, asigurarea confidențialității datelor şi informațiilor, precum şi păstrarea în siguranță a acestora, în cadrul activității curente executate de către angajații **Asociației Brahma**.

2.1.2. Procedura descrie activitățile desfășurate cu privire la operațiunile de arhivare a documentelor care conțin date cu caracter personal, respectiv stabilește persoanele și/sau compartimentele implicate și responsabilitățile acestora.

2.1.3. Prin prezenta procedură se urmărește asigurarea unui cadru legal și eficient de prelucrare a datelor cu caracter personal, în ceea ce privește arhivarea documentelor care conțin date cu caracter personal cu respectarea drepturilor persoanelor vizate, în acord cu reglementările Regulamentului și legislației conexe.

2.2. DOMENIUL DE APLICARE

Prezenta procedură se aplică tuturor structurilor organizatorice ale Operatorului. Politica este întocmită în scopul prezentării circuitului intern de prelucrare a datelor personale în ceea ce privește arhivarea documentelor care conțin date cu caracter personal. La procedură participă toate structurile organizatorice conform cu atribuțiile care le revin în ceea ce privește activitatea de prelucrare a datelor personale.

2.3. DOCUMENTE DE REFERINȚĂ

- GDPR
- Legea Arhivelor Natționale nr. 16/1996, republicată
- Regulament intern
- Proceduri interne

3. REGULI GENERALE

3.1. Evidența documentelor

La nivelul Operatorului, toate compartimentele sunt obligate să înregistreze şi să țină evidența tuturor documentelor intrate, a celor întocmite pentru uz intern şi a celor ieşite, conform procedurilor activităților respective.

Documentele/înregistrările se păstrează de către inițiatori şi utilizatori la locul de muncă (arhivă activă), pe durata specificată de normele legale. După expirarea perioadei de păstrare operativă, şefii/responsabilii compartimentelor întocmesc propuneri pentru arhivare în arhiva Operatorului.

Anual, persoana responsabilă cu îndosarierea documentelor la fiecare compartiment grupează documentele în unități arhivistice potrivit problematicii şi a termenelor de păstrare stabilite în nomenclatorul arhivistic. Nomenclatorul arhivistic este întocmit de către responsabilul cu arhiva din cadrul Operatorului, pe baza propunerilor transmise de şefii/responsabilii compartimentelor din cadrul Operatorului și este aprobat prin decizia organelor de conducere.

În fiecare dosar se introduce o pagină de gardă, care se completează de către persoana responsabilă cu îndosarierea documentelor la fiecare compartiment. Se numerotează fiecare pagină din dosar şi totalul de pagini se înscrie pe pagina de gardă. Documentele astfel grupate se depun de către persoana responsabilă cu îndosarierea acestora, în al doilea an de la constituire, la depozitul arhivei Operatorului, pe bază de inventar de documente si proces-verbal de predare-primire.

Evidența tuturor intrărilor şi ieşirilor de unități arhivistice în/din depozitul arhivei se ține de către arhivarul Operatorului (persoana desemnată prin decizie internă cu atribuții de arhivar) într-un registru de evidență.

Scoaterea documentelor din evidența arhivei se face numai cu aprobarea conducerii Operatorului, în urma selecționării sau transferului în alt depozit de arhivă.

3.2. Selecționarea documentelor

În cadrul Operatorului funcționează o comisie de selecționare, numită de conducerea Operatorului, compusă din 3 persoane: un preşedinte, un secretar și un membru. Comisia de selecționare se întruneşte anual sau ori

de câte ori este necesar, la propunerea arhivarului Operatorului, pentru a analiza fiecare unitate arhivistică în parte și pentru a aproba lista cu documentele care urmează a fi eliminate ca fiind nefolositoare, expirându-le termenul de păstrare; hotărârea luată se consemnează într-un Proces-Verbal al Comisiei de selecționare.

Procesul-verbal de selecționare, însoțit de inventarele documentelor propuse spre eliminare, precum şi de inventarele documentelor ce se păstrează permanent.
Documentele se scot din evidența arhivei şi se pot elimina numai în baza Proceselor-Verbale ale comisiei menționate mai sus.

3.3. Păstrarea documentelor

Operatorul este obligat să păstreze documentele create sau deținute în condiții corespunzătoare, în spații special amenajate pentru arhivă asigurându-le împotriva distrugerii, degradării, sustragerii ori comercializării în alte condiții decât cele legale.

Depozitele de arhivă vor fi dotate, în funcție de formatul şi de suportul documentelor, cu mijloace adecvate de păstrare şi de protejare a acestora, precum şi cu mijloace, instalații şi sisteme de prevenire şi stingere a incendiilor.
După caz și în funcție de nevoile sale, Operatorul poate numi o persoană care să exercite atribuțiile de arhivar, care are obligația să păstreze documentele deținute în arhivă în condiții corespunzătoare. Conducerea Operatorului, la propunerea arhivarului, alocă spațiul necesar și corespunzător pentru arhivă (din punct de vedere al temperaturii, umidității, luminozității, condițiilor de siguranță).
Arhivarul urmăreşte întoarcerea documentelor ieşite spre consultare, la solicitarea șefilor/responsabililor de compartimente şi sesizează șeful ierarhic superior în cazul întârzierii acestora sau a altor probleme apărute în arhivă.
Păstrarea documentelor în arhivă se face pe durata prevăzută în nomenclatorul arhivistic.

4. Responsabilități

4.1. Conducerea Operatorului:
- ✓ Alocă spațiul necesar arhivării.
- ✓ Asigură resursele umane şi materiale pentru crearea condițiilor de funcționare normală a arhivei.
- ✓ Numeşte componența Comisiei de selecționare.
- ✓ Numeşte persoana care să exercite funcția de arhivar.
- ✓ Aprobă scoaterea documentelor din evidența arhivei, în urma selecționării sau mutării în alt depozit.

4.2. Șefii/responsabilii de compartimente:
- ✓ Asigură păstrarea la locul de muncă a documentelor întocmite în cadrul activității procedurate (arhiva operativă), legarea, cartonarea și constituirea unităților arhivistice, conform Nomenclatorului arhivistic al Operatorului, precum și depunerea la arhivă a documentelor după expirarea perioadei de păstrare operativă.
- ✓ Propun predarea documentelor la arhiva Operatorului.
- ✓ Coordonează îndosarierea documentelor pe unități arhivistice la nivelul compartimentului.
- ✓ Propune persoana responsabilă cu îndosarierea documentelor la nivelul compartimentului.
- ✓ Fac propuneri pentru întocmirea, modificarea şi completarea Nomenclatorului arhivistic al Operatorului, pentru documentele create/păstrate de către compartimentul pe care îl conduc/coordonează.

4.3. Persoana responsabilă cu arhivarea (arhivarul)

- ✓ Inițiază și organizează activitatea de întocmire a nomenclatorului arhivistic al Operatorului.
- ✓ Asigură legătura cu Arhivele Naționale, în vederea verificării şi confirmării nomenclatorului, urmăreşte modul de aplicare a nomenclatorului la constituirea dosarelor.
- ✓ Verifică și preia de la compartimente, pe bază de inventare, documentele grupate în unități arhivistice, pentru păstrarea în arhivă.
- ✓ Întocmeşte inventare pentru documentele fără evidență aflate în depozit.
- ✓ Ține evidenta tuturor documentelor intrate şi ieşite din depozitul de arhivă, pe baza registrului de evidență curentă.
- ✓ Asigură păstrarea documentelor deținute în arhivă în condiții corespunzătoare; verifică modul de păstrare în timp a documentelor.
- ✓ Pune la dispoziție, în anumite situații și conform prezentei proceduri, pe bază de semnătură şi ține evidența documentelor împrumutate compartimentelor creatoare, pe baza registrului de evidență a intrărilor-ieşirilor unităților arhivistice; la restituire verifică integritatea documentelor împrumutate.
- ✓ Este secretarul comisiei de selecționare și, în această calitate, convoacă comisia în vederea analizării dosarelor cu termenele de păstrare expirate şi care, în principiu, pot fi propuse pentru eliminare ca fiind nefolositoare.
- ✓ Întocmește Nomenclatorul arhivistic al Operatorului, pe baza propunerilor șefiilor/responsabililor de compartimente, urmărește avizarea și aprobarea acestuia, potrivit prezentei proceduri.
- ✓ Asigură difuzarea Nomenclatorului arhivistic tuturor compartimentelor din cadrul Operatorului.

4.4. Comisia de selecționare

Analizează şi aprobă lista cu documentele având termenele de păstrare depăşite, propuse spre a fi distruse.

Anexa 1

Aprobat Operator
.....

NOMENCLATORUL ARHIVISTIC
aprobat prin Decizia nr. ..... din .....

Compartimentul	Denumirea dosarului **(conținutul pe scurt al problemelor la care se referă)**	**Termenul de păstrare**	Obs.
A. Serviciul	1.		
	2.		
	3.		
B. Compartimentul	1.		
	2.		
	3.		
C. Compartimentul	1.		
	2.		
	3.		
D. Compartimentul	1.		
	2.		
	3.		

Data: zz.ll.aaaa

Întocmit
Nume Prenume

Anexa 2

Pagina de gardă

Denumire dosar .....
(conținutul pe scurt al problemelor la care se referă)
de la data ..... până la data de ..... (pentru documentele conținute)

Indicativ dosar ..... (ex: II. B 3) .....
(conform nomenclatorului arhivistic)

Nr. de pagini .....

Termen de păstrare .....
(conform nomenclatorului arhivistic)

Anexa 3

Inventarul de documente pentru arhivare
pe anul .....
pentru documentele care se păstrează permanent sau temporar

Nr. crt.	**Indicativul dosarului (după** nomenclator)	**Conținutul pe scurt al dosarului,** registrului	Datele extreme	Nr. filelor	Obs.

Prezentul inventar format din ..... file conține ..... dosare, registre, condici etc. Dosarele de la nr. crt. ..... au fost lăsate la ....., nefiind încheiate.
La preluare au lipsit dosarele de la nr. crt. .....

Astăzi, ..., s-au preluat ..... dosare.

Am predat,
Nume Prenume

Am primit,
Nume Prenume

Anexa 4

Proces-verbal de predare – primire
documente pentru arhivare

Astăzi, ..., subsemnații ....., delegați ai compartimentului ....., şi ..... în calitate de arhivar, am procedat primul la predarea şi al doilea la preluarea documentelor create în perioada ..... de către compartimentul ....., în cantitate de ..... dosare.

Predarea – primirea s-a făcut pe baza inventarelor anexate, cuprinzând ..... pagini, conform dispozițiilor legale.

Am predat,
Nume Prenume Semnătura

Am primit,
Nume Prenume Semnătura

Anexa 5

Proces-verbal Nr. ...../.....

Comisia de selecționare, numită prin Decizia n.r..... din ....., în şedințele din ....., a selecționat documentele din anii ..... și avizează ca dosarele din inventarele anexate să fie înlăturate ca nefolositoare, expirându-le termenele de păstrare prevăzute în nomenclatorul arhivistic al instituției.

Comisia de selecționare

Președinte,
Nume Prenume Semnătura

Membru,
Nume Prenume Semnătura

Secretar,
Nume Prenume Semnătura

Procedura de cartografiere a datelor cu caracter personal

1. DEFINIŢII

„GDPR", „Regulamentul" - Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului 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 (Regulamentul general privind protecţia datelor, în limba engleză General Data Protection Regulation);

„date cu caracter personal" - orice informaţii 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 identităţii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

„prelucrare" - 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;

„operator" - înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care, singur sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile şi 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;

*„**persoana împuternicită de operator**"* - înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

„destinatar" - înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terţă. Cu toate acestea, autorităţile 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 autorităţile publice respective respectă normele aplicabile în materie de protecţie a datelor, în conformitate cu scopurile prelucrării;

*„**parte terţă**"* - înseamnă o persoană fizică sau juridică, autoritate publică, agenţie sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator şi persoanele care, sub directă autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;

*„**consimţământ**"* - al persoanei vizate înseamnă orice manifestare de voinţă liberă, specifică, informată şi lipsită de ambiguitate a persoanei vizate prin care această acceptă, printr-o declaraţie sau printr-o acţiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;

*„**încălcarea securităţii datelor cu caracter personal**"* - înseamnă o încălcare a securităţii 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;

„reprezentant” - înseamnă o persoană fizică sau juridică stabilită în Uniune, desemnată în scris de către operator sau persoana împuternicită de operator, care reprezintă operatorul sau persoana împuternicită în ceea ce priveşte obligaţiile lor respective care le revin în temeiul GDPR;

„reguli corporatiste obligatorii” - înseamnă politicile în materie de protecţie a datelor cu caracter personal care trebuie respectate de un operator sau de o persoană împuternicită de operator stabilită pe teritoriul unui stat membru, în ceea ce priveşte transferurile sau seturile de transferuri de date cu caracter personal către un operator sau o persoană împuternicită de operator în una sau mai multe ţări terţe în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună;

„autoritate de supraveghere” - înseamnă o autoritate publică independentă instituită de un stat membru;

„DPIA” - evaluarea impactului asupra protecţiei datelor (în limba engleză, data-protection impact assessment, DPIA);

„Autoritate de Supraveghere” - Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP).

2. SCOPUL ŞI DOMENIUL DE APLICARE

2.1. SCOPUL

Prezenta procedură documentează cerinţele privind întocmirea documentului numit „Cartografierea datelor cu caracter personal”.

2.2. DOMENIUL DE APLICARE

Prezenta procedură se aplică tuturor structurilor organizatorice ale Operatorului **Asociației Brahma**. Prezenta procedură va fi considerată ca având caracter general şi se va aplica tuturor prelucrărilor efectuate de Operator.

În cazul în care se constată existenţa anumitor aspecte pentru care prezenta procedură nu oferă directive corespunzătoare, Angajaţii trebuie să solicite imediat consiliere din partea persoanei responsabile cu protecţia datelor, dacă a fost numit sau reprezentantului legal al Operatorului.

2.3. DOCUMENTE DE REFERINȚĂ

- GDPR;
- Regulament intern;
- Proceduri interne.

3. REGULI GENERALE

3.1. GENERAL. Operatorul **Asociația Brahma** va întocmi un tabel (de preferat în format excel), în care va enumera fiecare linie de business (de ex. "activitate" desfăşurată în cadrul fiecărui proces de business) împreună cu informaţiile legate de colectare, stocare, utilizare, transfer şi distrugere a conţinutului datelor critice pentru fiecare departament.

IMPORTANT: Operatorul va trece prin puncte de mai jos fiecare tip de document care conţine date cu caracter

personal.

3.2. TIPUL/NUMELE DOCUMENTELOR PENTRU COLECTAREA DATELOR CU CARACTER PERSONAL

Operatorul **Asociația Brahma** va identifica tipul/numele documentelor pentru colectarea datelor cu caracter personal se vor selecta categoriile de date din Schema de Clasificare a datelor (Anexa 1).

3.3. CATEGORIILE DE DATE

Operatorul **Asociația Brahma** va selecta categoriile de date cu caracter personal. În vederea identificării categoriilor de date cu caracter personal colectate se va avea în vedere Schema de Clasificare a datelor (Anexa 1).

3.4. TIPUL DATELOR

Operatorul **Asociația Brahma** va selecta tipul de date cu caracter personal. În vederea identificării tipului de date cu caracter personal colectate se va avea în vedere Schema de Clasificare a datelor (Anexa 1).

3.5. SURSA DATELOR

Operatorul **Asociația Brahma** va selecta de unde provin datele personale (ex. sursa de intrare)? Bifaţi cu "X" sursa de intrare a datelor (sunt posibile mai multe opţiuni).

☐ Clienţi (PF sau PJ)
☐ Angajaţi
☐ Părţi terţe (furnizori, parteneri, prestatori de servicii)

3.6. METODA DE COLECTARE A DATELOR
Operatorul **Asociația Brahma** va selecta metoda de colectare a datelor cu caracter personal. Bifaţi cu "X" tipul suport al colectării datelor (sunt posibile mai multe opţiuni).

☐ Fizic (Suport Hârtie)
☐ Poștă/Curier
☐ Fax
☐ E-mail
☐ Portal Web
☐ Formular Online
☐ USB Drive
☐ Hard Drive
☐ CDs/DVDs
☐ Server FTP
☐ Social Media
☐ Call Center

3.7. LOCAŢIA DE TRANSFER URMĂTOARE
Operatorul **Asociația Brahma** va selecta locaţia de transfer a datelor cu caracter personal. Bifaţi cu "X" locaţia de transfer a datelor (sunt posibile mai multe opţiuni).

☐ Birouri (Dosare)

☐ E-mail Server
☐ Aplicaţii IT (numele aplicaţiilor utilizate)
☐ Baze de Date
☐ Fişiere Electronice
☐ Telefoane Mobile

3.8. LOCAŢIA DE STOCARE

Operatorul **Asociația Brahma** va selecta locaţia de stocare a datelor cu caracter personal. Bifaţi cu "X" locaţia de stocare a datelor (sunt posibile mai multe opţiuni).

☐ Birouri (Dosare)
☐ E-mail Server
☐ Aplicaţii IT (numele aplicaţiilor utilizate)
☐ Sistem Generic/Server
☐ Fişiere Electronice
☐ Baze de Date
☐ Server Web
☐ Arhiva Electronică (back-up)
☐ Cloud

3.9. UTILIZAREA DATELOR (Intern)

Operatorul **Asociația Brahma** va selecta modalitatea de utilizare a datelor cu caracter personal. Bifaţi cu "X" modalitatea de utilizare (sunt posibile mai multe opţiuni).

☐ Departament
☐ Transfer intern către alt departament
☐ Câţi angajaţi au acces la datele cu caracter personal?

3.10. TRANSFERUL DATELOR (Extern)

Operatorul **Asociația Brahma** va selecta modalitatea de transfer a datelor cu caracter personal. Bifaţi cu "X" modalitatea de transfer (sunt posibile mai multe opţiuni).

☐ Autorităţi
☐ Părţi terţe (furnizori, parteneri, prestatori servicii)
☐ Transfrontalier (în UE/ SEE sau în afara UE/SEE)

3.11. REŢINEREA ŞI ARHIVAREA DATELOR

Operatorul **Asociația Brahma** va selecta locaţia de reţinere/stocare a datelor. Bifaţi cu "X" locaţia de reţinere/stocare a datelor (sunt posibile mai multe opţiuni).

☐ Birouri (Arhivă)
☐ E-mail Server
☐ Aplicaţii IT (numele aplicaţiilor utilizate)
☐ Sistem Generic/Server
☐ Fişiere Electronice
☐ Baze de date
☐ Server Web
☐ Arhivare Electronică (back-up)
☐ Cloud

3.12. **TERMEN DE STOCARE/REŢINERE**
Operatorul **Asociația Brahma** va completa termenul de stocare/reţinere pentru fiecare temei de prelucrare a datelor cu caracter personal.

- ☐ Consimţământ
- ☐ Obligaţie legală
- ☐ Obligaţie contractuală
- ☐ Interes public
- ☐ Autorităţi publice
- ☐ Protejarea intereselor vitale
- ☐ Interes legitim

3.13. DISTRUGERE/ŞTERGERE
Operatorul **Asociația Brahma** va completa modalitatea de distrugere/ştergere a datelor cu caracter personal. Bifaţi cu "X" modalitatea de ştergere/distrugere a datelor (sunt posibile mai multe opţiuni).

- ☐ Coş gunoi
- ☐ Distrugător de hârtie
- ☐ Ştergere sisteme informatice .

Anexa 1: Schema de clasificare a datelor

Atenţie!	Se au în vedere DOAR atributele (datele) unei persoane fizice
Mai jos sunt furnizate o serie de categorii ce conţin date cu caracter personal (D.C.P.). Lista de mai jos nu este limitativă, în măsura în care consideraţi că sunt colectate/procesate şi alte D.C.P. vă rugăm să le marcaţi în tabel în dreptul unei categorii sau la final (alte date).	

CATEGORIA	DESCRIERE	DA/NU
A	**Date de identificare şi caracteristici personale**	
A.1	Nume şi prenume	
A.2	Data naşterii	
A.3	CNP	
A.4	Cetăţenie	
A.5	Serie şi număr buletin/carte de identitate/paşaport/alt act de identitate (e.g. permis de şedere, de muncă, permis de conducere etc.)	
A.6	Adresa de domiciliu (inclusiv cele anterioare, dacă există)	
A.7	Data emiterii a actelor de identitate	
A.8	Data expirării a actelor de identitate	
A.9	Fotografie (CV, acte de identitate, diplome etc.)	
A.10	Reşedinţa (dacă există)	
A.11	Stare Civilă	

A.12	Număr de telefon (personal şi/sau de serviciu)	
A.13	E-mail (personal şi/sau de serviciu)	
A.14	Pseudonim	
A.15	Semnătura	
A.16	Vârsta	
A.17	Religie	
A.18	Sex	
A.19	Locul naşterii	
A.20	Naţionalitate	
A.21	Nume şi prenume tată	
A.22	Nume şi prenume mamă	
A.23	Numărul plăcuţei de înmatriculare a autoturismului (personal şi/sau de serviciu)	
A.24	Numărul permisului de conducere	
A.25	Numărul de asigurare socială sau de sănătate	
A.26	Limbi vorbite	
A.27	Origine rasială sau etnică	
A.28	Credinţe religioase sau filizofice	
CATEGORIA	DESCRIERE	DA/NU
B.	Detalii despre membrii familiei	
B.1	Nume şi prenume soţ/soţie	
B.2	Data naştere soţ/soţie	
B.3	Numele dinainte de căsătorie al soţului/soţiei	
B.4	Numele după căsătorie soţ/soţie	
B.5	Nume şi prenume copii	
B.6	Dată naştere copil	
B.7	CNP copii	
B.8	Seria şi numărul certificatului de căsătorie, divorţ, deces etc.	
B.9	CNP soţ/soţie	
B.10	Nume şi prenume parinti ,soţi	
B.11	Istoricul stării civile: căsătorii anterioare, divorţuri etc.	
B.12	Informaţii despre alţi membri ai familei: numărul copiilor, persoane aflate în întreţinere, părinţi etc.	
B.13	Informaţii despre copii în întreţinere (pensii alimentare)	
B.14	Informatii legate de starea materiala și veniturile din gospodărie	
CATEGORIA	DESCRIERE	DA/NU
C.	**Identificare electronică**	
C.1	“Cookies”	
C.2	Loguri de acces ale angajaţilor	

C.3	Adresele IP ale angajaţilor	
C.4	Coordonate GPS, locaţie	
C.5	Seria şi numărul cardului de acces al unui angajat sau vizitator	
C.6	Numărul de marcă al angajatului	
C.7	Dispozitive de sănătate şi de fitness	
CATEGORIA	DESCRIERE	DA/NU
D.	**Elemente Financiare (bancare, financiare şi de avere)**	
D.1	Date identificare bancă al unei persoane fizice (e.g. număr cont bancar al angajatului).	
D.2	Numărul unui card bancar al unei persoane fizice	
D.3	Coduri secrete (ex. coduri de acces în anumite spaţii)	
D.4	Orice tranzacţii financiare in care sunt implicate PF (e.g. persoane fizice beneficiari/plătitori în cadrul unei operaţiuni de plată)	
D.5	Contracte comerciale, alte documente de natură financiară încheiate de PJ cu PF, sau de către PF din PJ cu un terţ (PF sau PJ)	
D.6	Venit şi avere	
D.7	Datorii şi Cheltuieli	
D.8	Împrumuturi şi ipoteci	
D.9	Solvență, restanţe, incidente	
D.10	Tranzacţii financiare	
D.11	Compensări	
D.12	Acorduri şi angajamente	
D.13	Materiale şi echipamente	
D.14	Proprietăţi locuinţe, terenuri etc.	
D.15	Certificări, Training Dezvoltare Personală, Activităţi profesionale (tipuri de activităţi, relaţii de afaceri) ale PF din cadrul PJ	
CATEGORIA	DESCRIERE	DA/NU
E.	Alte caracteristici personale	
E.1	Informaţii despre stagiul militar	
E.2	Informaţii despre străin: detalii viză, permis de muncă, condiţii speciale	
E.3	Numere de identificare emise de guvern	
CATEGORIA	DESCRIERE	DA/NU
F.	Caracteristici fizice	
F.1	Înălţime	
F.2	Greutate	
F.3	Culoarea părului	
F.4	Culoarea ochilor	
F.5	Semne distinctive	

CATEGORIA	DESCRIERE	DA/NU
G.	**Informaţii privind stilul de viaţă şi comportamentul**	
G.1	Consum de tutun, alcool	
G.2	Consum de bunuri	
G.3	Detalii privind călătoriile: vize, permise de muncă	
G.4	Contacte pe medii sociale: prieteni, asociaţi, relaţii altele decât familia	
G.5	Funcţii publice deţinute	
G.6	Informaţii privind accidentele suferite, persoane implicate, natură accidentului	
G.7	Profil psihologic	
G.8	Distincţii civile	

CATEGORIA	DESCRIERE	DA/NU
H.	Hobby-**uri şi interese**	
H.1	Activităţi de tip hobby, sporturi practicate	
CATEGORIA	DESCRIERE	DA/NU
I.	Afilieri	
I.1	Membru în diferite organizaţii (mai puţin politice): caritabile, voluntari, cluburi, asociaţii etc.	
I.2	Apartenenţă la sindicate, uniuni profesionale	
CATEGORIA	DESCRIERE	DA/NU
J.	**Informaţii de natură juridică**	
J.1	Condamnări penale	
J.2	Amenzi administrative	
J.3	Suspiciuni, punere sub acuzare, investigaţii (civile, penale)	
J.4	Măsuri judiciare: punere sub tutelă, sechestru judiciar etc.	
J.5	Sancţiuni administrative: administrativ-disciplinara, administrativ-contraventionala, administrativ-patrimoniala	
J.6	Sancţiuni sub legislaţia muncii: administrativ-disciplinara - advertismente, cercetare disciplinară, reţinere salariu	
J.7	Sancţiuni administrative: administrativ-patrimoniala - reţineri din salariu/poprire conturi bancare	
J.8	Certificat de cazier judiciar, fiscal, auto	
CATEGORIA	DESCRIERE	DA/NU
K.	**Date privind starea de sănătate (categorii speciale)**	
K.1	Număr asigurare socială	
K.2	Informaţii privind starea de sănătate a persoanei vizate: certificate medicale,	

	rapoarte medicale, fişe medicale, tratamente, rezultate ale analizelor, diagnostice, certificate concediu medical etc.	
K.3	Grupa de sânge	
K.4	Statut Dizabilităţi	
K.5	Informaţii privind starea de sănătate a persoanei vizate din punctul de vedere al vieţii sexuale: boli sexuale cu transmitere	
CATEGORIA	DESCRIERE	DA/NU
L.	**Informaţii privind studiile şi cursurile**	
L.1	Informaţii privind studiile persoanei vizate: instituţii de învăţământ absolvite, cursuri urmate, diplome, rezultate ale examenelor etc.	
L.2	Calificări profesionale: patente, licenţe, calificări, certificări etc.	
L.3	Publicaţii: reviste, cărţi, articole, rapoarte etc.	

CATEGORIA	DESCRIERE	DA/NU
M.	**Informaţii privind istoricul profesional şi viaţa profesională**	
M.1	Informaţii despre angajatorul curent: angajator, funcţia, data angajării, măsuri disciplinare etc.	
M.2	Informaţii despre terminarea contractului de muncă: data plecării, preavize etc.	
M.3	Carieră: istoric profesional, poziţie, informaţii despre angajatorii precedenţi	
M.4	Informaţii financiare: salarii, beneficii, bonusuri, pensii, taxe etc.	
M.5	Detalii de contact angajare (adresă email loc de muncă, telefon loc de muncă, adresă loc de muncă)	
M.6	Bunuri deţinute de angajat: obiecte de inventar, maşini, utilizaje etc.	
M.7	Afilieri organizaţii profesionale	
M.8	Poziţii publice deţinute	
M 9	Situație actuală pe piața muncii	
CATEGORI	DESCRIERE	DA/NU
A.	**Informaţii privind opiniile politice, filozofice şi sindicate. Opinii** religioase	
N.1	Opinii şi preferinţe politice	
N.2	Calitatea de membru într-un partid politic	
N.3	Activităţi de lobby	
N.4	Apartenenţa la un sindicat	
N.5	Opinii religioase	
CATEGORIA	DESCRIERE	DA/NU
O.	**Informaţii privind procesarea de imagini**	
O.1	Fotografii, înregistrări video etc.	

O.2	Date biometrice: amprente digitale, modelele retiniene, structura facială, vocile, dar şi geometria mâinilor, modelul venelor, sau chiar unele abilităţi adânc înrădăcinate sau alte caracteristici comportamentale (e.g. semnătura)	
CATEGORIA	DESCRIERE	DA/NU
P.	**Informaţii privind procesarea de sunete**	
P.1	Înregistrarea de apeluri telefonice	

CATEGORIA	DESCRIERE	DA/NU
R.	**Informaţii privind viaţa sexuală**	
R.1	Informaţii privind orientare sexuală	
R.2	Informaţii privind viaţa sexuală	
CATEGORIA	DESCRIERE	DA/NU
S.	Alte date cu caracter personal	DA/NU

POLITICA PRIVIND ACCESUL LA DATE CU CARACTER PERSONAL

1. DEFINIȚII

„GDPR", „Regulamentul" - Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor, în limba engleză General Data Protection Regulation);

„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;

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

„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;

*„**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 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**"* - 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;

*„**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;

„reprezentant” - înseamnă o persoană fizică sau juridică stabilită în Uniune, desemnată în scris de către operator sau persoana împuternicită de operator, care reprezintă operatorul sau persoana împuternicită în ceea ce privește obligațiile lor respective care le revin în temeiul GDPR;

„reguli corporatiste obligatorii” - înseamnă politicile în materie de protecție a datelor cu caracter personal care trebuie respectate de un operator sau de o persoană împuternicită de operator stabilită pe teritoriul unui stat membru, în ceea ce privește transferurile sau seturile de transferuri de date cu caracter personal către un operator sau o persoană împuternicită de operator în una sau mai multe țări terțe în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună;

„autoritate de supraveghere” - înseamnă o autoritate publică independentă instituită de un stat membru;
„DPIA” - evaluarea impactului asupra protecției datelor (în limba engleză, data-protection impact assessment, DPIA);

„Autoritate de Supraveghere” - Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP).

2. SCOPUL ȘI DOMENIUL DE APLICARE

2.1. SCOPUL

Prezenta politică documentează cerințele GDPR privind menținerea unui nivel adecvat de securitate și de protecție a datelor cu caracter personal al persoanelor vizate, ținând seama de riscurile prezentate de prelucrare, 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.

Prezenta politică are în vedere reguli generale și măsuri pentru a asigura faptul că orice persoană fizică care acționează sub autoritatea **Asociației Brahma** și care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepția cazului în care această obligație îi revine în temeiul dreptului Uniunii sau al dreptului intern.

Angajații **Asociației Brahma** înțeleg și au reprezentarea deplină a faptului că încălcarea regulilor privind accesul la datele cu caracter personal poate conduce la prejudicii fizice, materiale sau morale persoanelor fizice, cum ar fi pierderea controlului asupra datelor lor cu caracter personal sau limitarea drepturilor lor, discriminare, furt sau fraudă de identitate, pierdere financiară, inversarea neautorizată a pseudonimizării, compromiterea reputației, pierderea confidențialității datelor cu caracter personal protejate prin secret profesional sau orice alt dezavantaj semnificativ de natură economică sau socială adus persoanei fizice în cauză.

Printre măsurile principale luate în considerare de **Asociația Brahma** în vederea asigurării unui nivel de securitate corespunzător se numără:
a) **pseudonimizarea și criptarea datelor** cu caracter personal;

b) capacitatea de a asigura **confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare**;
c) 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;
d) un **proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării**.

2.2. DOMENIUL DE APLICARE

Prezenta politică se aplică tuturor structurilor organizatorice ale Operatorului [și, respectiv, tuturor computerelor, dispozitivelor de calcul, aplicațiilor, platformelor, sistemelor informatice și sistemelor de operare, deținute sau operate de **Asociația Brahma.**

Prezenta politică va fi considerată ca având caracter general și se va aplica tuturor prelucrărilor efectuate de Operator. Acest document stabilește modul în care vor fi protejate datele personale pe care Operatorul le deține și le prelucrează în îndeplinirea activităților sale comerciale.

În cazul în care se constată existența anumitor aspecte legate de accesul la date pentru care prezenta politică nu oferă directive corespunzătoare, Angajații trebuie să solicite imediat consiliere din partea Ofițerului responsabil cu protecția datelor (DPO), dacă a fost numit, sau reprezentantului legal al Operatorului.

2.3. DOCUMENTE DE REFERINȚĂ

- GDPR;
- Regulament intern;
- Proceduri interne;

3. REGULI GENERALE

3.1. Principii privind prelucrarea. Desfășurarea activității curente a [denumire societate] presupune efectuarea de către angajații [denumire societate] a unor prelucrări de date care se supun următoarelor principii:

- datele trebuie prelucrate în mod legal, echitabil și transparent;
- datele trebuie colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile inițiale;
- datele trebuie să fie adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate;
- datele trebuie să fie exacte și, în cazul în care este necesar, să fie actualizate; trebuie să se 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 șterse sau rectificate fără întârziere;
- datele trebuie păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal vor fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice;

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

3.2. Securitatea prelucrării. Asigurarea securității prelucrării datelor cu caracter personal, implică respectarea unui nivel adecvat al accesibilității datelor și se va face cu respectarea de către Operator a măsurilor tehnice și organizatorice.

În cazul în care există suspiciunea încălcării prezentei Politici de confidențialitate, incidentul trebuie raportat cel puțin uneia dintre persoanele următoare:
- Managerul de departament;
- Persoana responsabilă de protecția datelor.

3.3. Obligații specifice. Prelucrarea datelor cu caracter personal se face doar de către angajații Operatorului ce dețin competența necesară efectuării unei astfel de prelucrări. În situația în care angajatul nu cunoaște gradul său de acces, se va putea adresa managerului de departament din care acesta face parte.
În vederea menținerii unui acces adecvat asupra datelor cu caracter personal, Angajații sunt obligați să respecte restricțiile de procesare a datelor impuse de Operator prin Politica de securitate implementată, în funcție de categoria datelor și nivelul de acces.

3.4. Transmiterea de informații
Asociația Brahma va transmite datele legate de angajații și clienții săi entităților care aparțin de aceasta doar dacă este necesar sau, dacă este posibil, în conformitate cu legea aplicabilă.
Transmiterea entităților afiliate Operatorului a datelor referitoare la clienții **Asociației Brahma** este permisă, cu titlu de exemplu, în următoarele cazuri:
- ✓ Atunci când interesele în joc sunt echilibrate: transmiterea este permisă, în scopul respectării prevederilor legate de combaterea spălării banilor, în ceea ce privește datele referitoare la „raportarea tranzacțiilor suspecte". Pe cale de consecință, numai Angajații numiți pentru executarea măsurilor împotriva spălării banilor au dreptul de a transmite și a primi asemenea date personale;
- ✓ Date anonime (de ex. în scopuri statistice sau în scopul analizei pieței).

Transmiterea datelor referitoare atât la clienți, cât și la angajați este permisă, cu titlu de exemplu, în următoarele cazuri:
- ✓ **Când există consimțământul expres al persoanelor vizate**: consimțământul trebuie să fie specific și, astfel, strict legat de obiectul pentru care respectiva transmitere este efectuată (ex. marketing). Pe cale de consecință, pentru ca, **Asociația Brahma** să se asigure că acceptul a fost acordat legitim de către client, este necesară verificarea conținutului notificării de informare trimise clientului și formularul de consimțământ aferent.
- ✓ **Cazurile care sunt echivalente consimțământului**: (ex. încheierea unui contract, obligație legală, interes legitim al Operatorului).

4. REGULI SPECIFICE PRIVIND ACCESUL

4.1. Dispozitive și suport

Sunt permise telefoanele inteligente, inclusiv telefoanele iPhone, Android și Windows.

Sunt permise tablete, inclusiv iPad și Android.

Problemele de conectivitate sunt soluționate de Departamentul IT; angajații ar trebui să contacteze producătorul dispozitivului pentru probleme legate de sistemul de operare sau hardware.
Dispozitivele trebuie să fie prezentate departamentului IT pentru asigurarea corespunzătoare a locurilor de muncă și configurarea aplicațiilor standard, cum ar fi browserele, software-ul de productivitate a biroului și instrumentele de securitate, înainte de a putea accesa rețeaua.

4.2. Securitate

Pentru a preveni accesul neautorizat, dispozitivele trebuie să fie protejate prin parolă utilizând caracteristicile dispozitivului și este necesară o parolă puternică pentru a accesa rețeaua **Asociația Brahma.**

Politica puternică a parolei Companiei este: parolele trebuie să aibă cel puțin șase caractere și o combinație de litere mari, mici și cifre și simboluri. Parolele vor fi schimbate la fiecare 90 de zile, iar noua parolă nu poate fi una din cele 15 parole anterioare.

Dispozitivul trebuie să se blocheze cu o parolă sau un cod PIN dacă este inactiv timp de cinci minute.

După cinci încercări de conectare eșuate, dispozitivul se va bloca. Se va contacta Departamentul IT pentru a se redobândi accesul.

Este strict interzisă accesarea rețelelor rădăcină (Android) sau jailbroken (iOS).

Angajații sunt în mod automat împiedicați să descarce, să instaleze și să utilizeze orice aplicație care nu apare în lista de aplicații aprobate a **Asociația Brahma.**

Telefoanele inteligente și tabletele care nu se află pe lista de dispozitive acceptate ale **Asociația Brahma** nu au voie să se conecteze la rețea.

Smartphone-urile și tabletele aparținând angajaților care sunt numai pentru uz personal nu au voie să se conecteze la rețea.

Accesul angajaților la datele **Asociației Brahma** este limitat pe baza profilurilor utilizatorilor definite de IT și aplicate automat.

Dispozitivul angajatului poate fi șters de la distanță dacă:

1. dispozitivul este pierdut;
2. angajatul își încetează raporturile de muncă;
3. departamentul IT detectează o încălcare a datelor sau a politicii, un virus sau o amenințare similară la adresa securității infrastructurii de date și tehnologii a **Asociației Brahma**.

4.3. Riscuri

În timp ce Departamentul IT va lua toate măsurile de precauție pentru a preveni pierderea datelor personale ale angajatului în cazul în care trebuie să șterge de la distanță un dispozitiv, este responsabilitatea angajatului de a lua măsuri de precauție suplimentare, cum ar fi copierea de rezervă a e-mail-urilor, a contactelor etc.

Asociația Brahma își rezervă dreptul de a deconecta dispozitivele sau de a dezactiva serviciile fără notificare.
Dispozitivele pierdute sau furate trebuie să fie raportate **Asociației Brahma** în termen de 24 de ore.
Angajații sunt responsabili pentru notificarea imediată după pierderea unui dispozitiv.
Angajații trebuie să-și folosească dispozitivele în mod etic în orice moment și să respecte politica de utilizare acceptabilă a **Asociației Brahma.**

Angajații sunt responsabili personal pentru toate costurile asociate cu dispozitivul său.
Angajatul își asumă răspunderea deplină pentru riscuri, inclusiv, dar fără a se limita la pierderea parțială sau completă a datelor **Asociației Brahma** și a datelor personale din cauza unei erori de sistem de operare, erori, viruși, malware și/sau alte defecțiuni software sau hardware sau programarea erorilor care fac dispozitivul inutilizabil.

Asociația Brahma își rezervă dreptul de a lua măsuri disciplinare corespunzătoare până la încetarea contractului individual de muncă pentru nerespectarea regulilor din prezenta politică.

Procedura de răspuns la drepturile persoanelor vizate

1. DEFINIȚII

„GDPR", „Regulamentul" - Regulamentul (UE) 2016/679 al Parlamentului Eurpean și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor, în limba engleză General Data Protection Regulation);

„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;

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

„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;

*„**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 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**”* - 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;

*„**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;

„reprezentant” - înseamnă o persoană fizică sau juridică stabilită în Uniune, desemnată în scris de către operator sau persoana împuternicită de operator, care reprezintă operatorul sau persoana împuternicită în ceea ce privește obligațiile lor respective care le revin în temeiul GDPR;

„reguli corporatiste obligatorii” - înseamnă politicile în materie de protecție a datelor cu caracter personal care trebuie respectate de un operator sau de o persoană împuternicită de operator stabilită pe teritoriul unui stat membru, în ceea ce privește transferurile sau seturile de transferuri de date cu caracter personal către un operator sau o persoană împuternicită de operator în una sau mai multe țări terțe în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună;

„autoritate de supraveghere” - înseamnă o autoritate publică independentă instituită de un stat membru;

„DPIA” - evaluarea impactului asupra protecției datelor (în limba engleză, data-protection impact assessment, DPIA).

2. SCOPUL ȘI DOMENIUL DE APLICARE

2.1. SCOPUL

2.1.1. Prezenta procedură documentează cerințele GDPR privind drepturile persoanelor vizate și are rolul de a prezenta modalitatea concretă de răspuns în cazul în care persoana vizată exercită unul dintre drepturi.

2.1.2. Prezenta procedură descrie activitățile desfășurate cu privire la drepturile persoanelor vizate, respectiv stabilește fluxul de parcurs în primirea și difuzarea controlată a răspunsurilor către persoanele vizate.

2.1.3. Prin procedură se urmărește asigurarea unui flux corect, eficient și legal al solicitărilor venite din partea persoanelor vizate cu privire la unul sau mai multe drepturi exercitate în temeiul GDPR și al legislației conexe.

2.2. DOMENIUL DE APLICARE

2.2.1. GDPR conferă persoanelor fizice, în principal, următoarele drepturi:

- ✓ Dreptul de a fi informat

- ✓ Dreptul de acces
- ✓ Dreptul la rectificare
- ✓ Dreptul de ștergere
- ✓ Dreptul de a restricționa prelucrarea
- ✓ Dreptul la portabilitatea datelor
- ✓ Dreptul de a se opune
- ✓ Dreptul legate de luarea de decizii automatizate și de profilare.

2.2.2. Prezenta procedură se aplică tuturor structurilor organizatorice ale Operatorului. Procedura este întocmită în scopul prezentării circuitului solicitărilor din partea persoanelor vizate venite din exterior, precum și a atribuțiilor persoanelor implicate în procesul de răspuns. La procedură participă toate structurile organizatorice conform cu atribuțiile care le revin în ceea ce privește exercitarea drepturilor persoanelor vizate.

2.3. DOCUMENTE DE REFERINȚĂ
- GDPR
- Regulament intern
- Proceduri interne

3. DREPTURILE PERSOANELOR VIZATE
3.1. DREPTUL DE A FI INFORMAT [art. 12-14 GDPR]

Descriere. Dreptul de a fi informat se referă la obligația operatorului de a lua toate măsurile adecvate pentru a furniza persoanei vizate orice informații referitoare la prelucrarea datelor cu caracter personal. Informațiile pot fi comunicate în scris sau verbal, cu condiția ca identitatea persoanei vizate să fie dovedită prin alte mijloace.

Prin dreptul de a fi informat, GDPR stabilește informațiile care trebuie furnizate și când trebuie subiecții prelucrării datelor cu caracter personal să fie informați. Principalul atribut al datelor ce trebuie furnizate este transparența.

3.2. DREPTUL DE ACCES [art. 15 GDPR]

Descriere. Dreptul de acces înseamnă că persoana vizată are dreptul de a obține din partea operatorului o confirmare că se prelucrează sau nu date cu caracter personal care o privesc. În caz afirmativ, persoana vizată trebuie să aibă acces la datele respective și la o serie de informații.

3.3. DREPTUL LA RECTIFICAREA ȘI/SAU COMPLETAREA DATELOR [art. 16 GDPR]

Descriere. Dreptul la rectificarea datelor se referă la faptul că persoana vizată are dreptul de a obține de la operator, fără întârzieri nejustificate, actualizarea datelor care o privesc, în special în ceea ce privește datele cu caracte personal inexacte. Dreptul la completarea datelor se referă la ipoteza în care, având în vedere scopurile în care au fost prelucrate datele, persoana vizată dorește să modifice datele cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declarații suplimentare.

3.4. DREPTUL LA ȘTERGEREA DATELOR [art. 17 GDPR]

Descriere. Dreptul la ștergerea datelor cu caracter personal („*dreptul de a fi uitat*“) se bazează pe principiul de a garanta oricărui individ libertatea de a dispune cum dorește de datele sale personale, inclusiv de a le șterge, dacă nu există un motiv convingător sau special pentru continuarea procesării și stocării acestora.

Obligaţia de a şterge datele cu caracter personal se aplică în cazul în care sunt incidente unul dintre următoarele motive:

- ✓ datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;
- ✓ persoana vizată îşi retrage consimţământul pe baza căruia are loc prelucrarea, în conformitate cu articolul 6 alineatul (1) litera (a) sau cu articolul 9 alineatul (2) litera (a), din Regulament şi nu există niciun alt temei juridic pentru prelucrare;
- ✓ persoana vizată se opune prelucrării în temeiul articolului 21 alineatul (1) din Regulament şi nu există motive legitime care să prevaleze în ceea ce priveşte prelucrarea sau persoana vizată se opune prelucrării în temeiul articolului 21 alineatul (2) din Regulament;
- ✓ există neclarități legate de legalitatea prelucrării datelor cu caracter personal;
- ✓ datele cu caracter personal trebuie şterse pentru respectarea unei obligaţii legale care vă revine, în calitate de operator;
- ✓ datele cu caracter personal aparțin unor copii, cu vârsta sub 16 ani.

Situațiile în care este permis refuzul de a da curs unei cereri de ștergere a datelor cu caracter personal, sunt prevăzute ca situații de excepție, respectiv, cele în care prelucrarea este necesară pentru:

- ✓ exercitarea dreptului la liberă exprimare şi la informare;
- ✓ respectarea unei obligaţii legale;
- ✓ motive de interes public în domeniul sănătăţii publice *(Articolul 9 alin. (2) lit. h) şi i) și art. 9 alin. (3) din Regulament)*;
- ✓ scopuri de arhivare în interes public, cercetare ştiinţifică sau istorică ori în scopuri statistice (art. 89 alin. (1) din Regulament);
- ✓ constatarea, exercitarea sau apărarea unui drept în instanţă.

3.5. **DREPTUL LA RESTRICȚIONAREA PRELUCRĂRII [art. 18 GDPR]**

Descriere. Dreptul la restricționarea prelucrării se referă la posibilitatea oferită persoanei vizate de la limita operatorului posibilitatea de a prelucra anumite date cu caracter personal.

Persoana vizată are dreptul de a obţine din partea operatorului restricţionarea prelucrării în cazul în care se aplică unul dintre următoarele cazuri:

- ✓ se contestă exactitatea datelor, pentru o perioadă care vă permite ca operator să verificați exactitatea datelor în cauză;
- ✓ prelucrarea este nelegală, iar persoana vizată se opune ştergerii datelor cu caracter personal, solicitând în schimb restricţionarea utilizării lor;
- ✓ ca operatori nu mai aveți nevoie de datele cu caracter personal în scopul prelucrării, dar persoana vizată vi le solicită pentru o acțiune în instanţă;
- ✓ persoana vizată s-a opus prelucrării (art. 21 alin. (1)) pentru intervalul de timp în care se verifică dacă drepturile dumneavoastră legitime ca operatori prevalează asupra celor ale persoanei vizate.

Dacă prelucrarea a fost restricţionată, astfel de date cu caracter personal pot, cu excepţia stocării, să fie prelucrate numai cu consimțământul persoanei vizate sau pentru constatarea, exercitarea sau apărarea unui drept în instanţă. În situația datelor cu caracter personal asupra cărora au fost instituite măsuri de restricție acestea pot fi în continuare stocate fără îndeplinirea altor formalități suplimentare.

În situația în care se impune prelucrarea datelor cu caracter personal restricționate, aceasta poate opera cu respectarea următoarelor condiții prevăzute situațiilor ce impun necesitatea obținerii consimțământului, precum și:

- ✓ prelucrarea să fie necesară pentru constatarea, exercitarea sau apărarea unui drept în instanţă;

- ✓ prelucrarea să fie necesară pentru protecţia drepturilor unei alte persoane fizice sau juridice sau din motive de interes public important al Uniunii sau al unui stat membru;
- ✓ în orice alte cazuri care ar necesita prelucrarea datelor în discuție este necesară obținerea consimțământului persoanei vizate.

3.6. DREPTUL LA PORTABILITATEA DATELOR [art. 20 GDPR]

Descriere. Scopul acestui drept de a-i oferi persoanei vizate mai mult control asupra datelor cu caracter personal care o privesc. Dreptul la portabilitatea datelor permite acestora să obțină și să reutilizeze datele lor personale în scopuri proprii în cadrul diferitelor servicii. Acest drept permite mutarea, copierea sau transferul datelor personale cu ușurință de la un mediu informatic la altul, într-un mod sigur.

Dreptul de portabilitate a datelor se aplică numai în cazul în care:
- ✓ datele sunt procesate prin mijloace automate;
- ✓ persoana vizată și-a dat consimțământul pentru prelucrare;
- ✓ prelucrarea este necesară pentru a îndeplini condițiile stipulate printr-un contract.

Portabilitatea datelor constituie un drept al persoanei vizate de a primi un subset de date cu caracter personal prelucrate de către un operator cu privire la aceasta și de a stoca datele respective pentru uz personal în viitor. În acest context, stocarea poate fi realizată pe un dispozitiv privat sau un sistem cloud privat, fără a transmite neapărat datele unui alt operator.

Din punct de vedere tehnic, **Asociația Brahma** are implementate următoarele mecanisme de a pune la dispoziția persoanelor vizate date portabile:
- ➢ transmiterea directă a întregului set de date portabile *(sau mai multe părți extrase din setul de date global)*;
- ➢ un instrument automat care permite obținerea datelor relevante.

Datele cu caracter personal incluse în domeniul de aplicare a acestui drept sunt:
- ✓ date cu caracter personal care privesc persoana vizată *(telefonul, sistemul de mesagerie interpersonală)*, fiind excluse datele anonime sau datele care nu se referă la persoana vizată;
- ✓ datele furnizate de persoana vizată: date furnizate în mod activ și cu bună știință de persoana vizată – adresa poștală, numele de utilizator, vârsta etc. sau date observate furnizate de către persoana vizată prin virtutea utilizării serviciului sau a dispozitivului –
- ✓
- ✓ istoricul de căutare a unei persoane, datele privind traficul și datele de localizare, daca este cazul.

3.7. DREPTUL LA OPOZIȚIE [art. 21 GDPR]

Descriere. În anumite situații expres prevăzute de GDPR, persoana vizată are dreptul, din motive legate de situația particulară în care se află, de a se opune prelucrării. Situațiile când persoana vizată se poate opune prelucrării sunt atunci când:
- ✓ prelucrarea datelor personale în scopuri de marketing direct;
- ✓ prelucrarea datelor pentru realizarea de profiluri;
- ✓ prelucrarea datelor prin mijloace automate;
- ✓ prelucrarea în scopuri științifice sau istorice.

Situațiile de excepție care anulează dreptul la obiecții al persoanelor vizate apar atunci când, se poate demonstra că există motive legitime convingătoare pentru susținerea prelucrării, care depășesc interesele, drepturile și libertățile persoanei vizate. Alte situații de excepție sunt motivate de stabilirea, exercitarea sau

apărarea unor revendicări legale sau în situațiile în care prelucrarea este necesară pentru îndeplinirea unei sarcini de interes public.

3.8. DREPTUL DE A NU FACE OBIECTUL UNEI DECIZII BAZATE EXCLUSIV PE PRELUCRAREA **AUTOMATĂ, INCLUSIV CREAREA DE PROFILURI [art. 22 GDPR]**

Descriere. Persoanele fizice au dreptul de a nu face obiectul unei decizii atunci când aceasta se bazează pe prelucrarea automată și aceasta poate produce un efect juridic sau un efect semnificativ similar asupra individului.

Pentru a asigura conformitatea cu acest drept, se va identifica dacă oricare dintre operațiunile de procesare include un proces automat de luare a deciziilor și, bineînțeles, trebuie să actualizați procedurile, pentru a răspunde cerințelor GDPR.

Acest drept nu se aplică tuturor deciziilor automate. Dreptul nu se aplică în cazul în care decizia:

- ✓ este necesară pentru încheierea sau executarea unui contract între dumneavoastră și persoana fizică;
- ✓ este autorizată prin lege (*de exemplu, în scopuri de fraudă sau prevenirea evaziunii fiscale*);
- ✓ pe baza consimțământului explicit (*art. 9 alin. (2) din Regulament*);
- ✓ atunci când o decizie nu are un efect legal sau similar semnificativ asupra unei persoane.

GDPR definește profilarea ca orice formă de procesare automată destinată să evalueze anumite aspecte personale ale unei persoane, în special pentru a le analiza sau a prezice: performanța la locul de muncă; situația economică; starea de sănătate; preferințele personale; fiabilitatea; comportamentul; locația; deplasările.
La prelucrarea datelor cu caracter personal în scop de realizare a unui profil, **Asociația Brahma** se va asigura că există garanții adecvate cu privire la următoarele aspecte:

- ✓ procesarea este corectă și transparentă prin furnizarea de informații semnificative despre logica implicată, precum și despre semnificația și consecințele avute în vedere;
- ✓ folosește procedurile matematice sau statistice adecvate pentru profilare;
- ✓ are implementate măsurilor tehnice și organizatorice adecvate care să vă permită remedierea erorilor și minimizarea riscului de eroare;
- ✓ asigură securitatea datelor personale într-o manieră proporțională cu riscul pentru interesele și drepturile individului și previne efectele discriminatorii.

4. REGULI PRIVIND PROCEDURA DE RĂSPUNS LA DREPTURILE PERSOANELOR VIZATE

Orice informații care se adresează persoanei vizate trebuie să fie concise, ușor accesibile și ușor de înțeles și să utilizeze un limbaj simplu și clar, precum și elemente grafice acolo unde este cazul.

4.1. PRIMIREA SOLICITĂRII

În cadrul **Asociației Brahma** se primesc solicitări cu privire la drepturile persoanelor vizate prin următoarele mijloace:
- e-mail
- telefonic
- formular online disponibil la adresa
- alte modalități

4.2. ÎNREGISTRAREA SOLICITĂRII

Orice solicitare din partea persoanelor vizate, primită pe canalele descrise la pct. 4.1., se înregistrează la secretariat și se completează în registrul special Registrul] se păstrează de către persoana desemnata cu atributii de secretariat în biroul financiar-contabil. Persoana responsabilă cu înregistrarea solicitărilor din partea persoanelor vizate este Barac Georgiana.

Reguli generale privind înregistrarea solicitării:
a) toate actele care privesc aceeași solicitare se conexează la primul act înregistrat, numărul primului act fiind numărul de bază;
b) solicitările primite se înregistrează cronologic, începând cu data de 1 ianuarie] și terminând cu data de 31 decembrie] a fiecărui an; actele care se primesc prin poștă sau curieri se înregistrează în ordinea sosirii lor;
c) atât documentele care se înregistrează, cât și răspunsurile și actele transmise către persoanele vizate vor purta numărul de înregistrare al documentului, opțional și indicativul dosarului la care se păstrează;
d) este interzisă circulația în cadrul **Asociației Brahma** a solicitărilor primite din partea persoanelor vizate care nu sunt înregistrate;
e) poșta electronică disponibilă la adresa oficiala se descarcă zilnic la orele 10.00 [de către persoana responsabilă cu această activitate și se înregistrază în același mod ca documentele fizice;
f) în cazul în care în solicitare nu se menționează adresa persoanei vizate, se anexează plicul, dacă acesta conține adresa respectivă. Dacă lipsesc anexele menționate în actul înregistrat, persoana responsabilă cu primirea înscrie mențiunea „*lipsă anexe*”, în caz contrar fiind răspunzător de pierderea lor.

4.3. **CONFIRMAREA IDENTITĂȚII**

După primirea solicitării, persoana responsabilă cu această activitate va verifica identitatea persoanei vizate, respectiv:
- date de identificare (nume, prenume, cod client etc.)
- date de contact (număr de telefon, adresa de e-mail etc.)
- motivul formulării solicitării
- alte aspecte.

În vederea confirmării identității persoanei vizate, persoana responsabilă va obține de la următoarele departamente:
- Departament Implementare Proiecte persoană de contact Barac Georgiana
- Departament Financiar-Contabil, persoană de contact Anghel Stamescu

Persoanele din cadrul departamentelor care întocmesc și transmit documente și informații despre persoanele vizate poartă întreaga răspundere asupra datelor și conținutului acestora, iar în cazul transmiterii unor date sau informații eronate, vor răspunde potrivit reglementărilor în vigoare.

Dacă identitatea persoanei vizate este confirmată, se va proceda la analiza solicitării, potrivit pct. 4.5 din prezenta procedură. În măsura în care identitatea persoanei vizate nu se poate confirma, respectiv se poate demonstra că **Asociația Brahma** nu este în măsură să identifice persoana vizată, va trebui informată persoana vizată în mod corespunzător, în cazul în care este posibil.

Persoana responsabilă de transmiterea răspunsului este Barac Georgiana. Termenul de transmitere a răspunsului este 3 zile lucratoare.

Dacă persoana vizată, în scopul exercitării drepturilor sale, oferă informații suplimentare care permit identificarea sa, se va proceda la analiza solicitării, potrivit pct. 4.5 din prezenta procedură. În măsura în care identitatea persoanei vizate nu se poate confirma, se va proceda la respingerea cererii.

Persoana responsabilă de transmiterea informării de respingere a cererii este Barac Georgiana. Termenul de transmitere a răspunsului este 3 zile lucrătoare.

4.4. TAXE

În cadrul **Asociației Brahma** informațiile furnizate persoanei vizate și orice comunicare sunt oferite în mod gratuit. În cazul în care cererile din partea unei persoane vizate sunt în mod vădit nefondate sau excesive (în special din cauza caracterului lor repetitiv) se va proceda la:
a) perceperea unei taxe in lei adecvate având în vedere costurile administrative pentru furnizarea informațiilor sau a comunicării sau pentru luarea măsurilor solicitate.
b) refuzul de a da curs solicitării

4.5. ANALIZA SOLICITĂRII

Persoana responsabilă de analiza solicitării primite din partea persoanelor vizate cu privire la drepturile persoanelor vizate este: Barac Georgiana

Barac Georgiana are următoarele sarcini:
- ✓ primește solicitările din partea persoanelor vizate;
- ✓ organizează preluarea solicitărilor, înregistrează solicitărilor în Registrul;
- ✓ conlucrează cu celelalte departamente în vederea analizării solicitării din partea persoanelor vizate;
- ✓ răspunde de menținerea Registrului;
- ✓ constituie dosarele, inventarierea și predarea lor către Arhiva;

În vederea analizării solicitărilor primite din partea persoanei vizate, persoana responsabilă va obține informații, de la următoarele departamente:
- Departament implementare proiecte
- Departament Financiar-contabil

Persoanele din cadrul departamentelor respective care întocmesc documente și transmit informații despre persoanele vizate poartă întreaga răspundere asupra datelor și conținutului acestora, iar în cazul transmiterii unor date sau informații eronate, vor răspunde potrivit reglementărilor în vigoare.

4.5.1. Dreptul de a fi informat

- ➢ Pentru solicitarea de furnizare de informații în cazul în care datele cu caracter personal au fost **colectate de la persoana vizată** se va putea folosi un model pus la dispoziție de Operator;
- ➢ Pentru solicitarea de furnizare de informații în cazul în care datele cu caracter personal nu au fost **obținute de la persoana vizată** se va putea folosi un model pus la dispoziție de Operator.

4.5.2. Dreptul de acces

- ➢ Pentru confirmare că se prelucrează date cu caracter personal care privesc persoana vizată se va putea folosi modelul pus la dispoziție de Operator.

- Pentru infirmarea că nu se prelucrează date cu caracter personal în legătură cu persoana vizată se va putea folosi modelul pus la dispoziție de Operator.

4.5.3. Dreptul la rectificarea și/sau completarea datelor

- Pentru rectificarea datelor cu caracter personal care privesc persoana vizată se va putea folosi un model pus la dispoziție de Operator.
- Pentru completarea datelor cu caracter personal care privesc persoana vizată se va putea folosi un model pus la dispoziție de Operator.

4.5.4. Dreptul la ștergerea datelor cu caracter personal

Dacă societate a făcut publice datele cu caracter personal ale persoanei vizate și este obligată să le şteargă, în funcție de tehnologia disponibilă şi de costul implementării, trebuie să ia „*măsuri rezonabile*”, inclusiv măsuri tehnice, pentru a informa toți procesatorii care prelucrează datele cu caracter personal că persoana vizată a solicitat ştergerea de către aceşti operatori a oricăror linkuri către datele respective sau a oricăror copii sau reproduceri ale acestor date cu caracter personal. Pentru această ipoteză se va putea folosi un model pus la dispoziție de Operator.

Trebuie comunicat fiecărui destinatar căruia i-au fost divulgate datele cu caracter personal orice ştergere efectuată, cu excepţia cazului în care acest lucru se dovedeşte imposibil sau presupune eforturi disproporţionate. Pentru această ipoteză se va putea folosi un model pus la dispoziție de Operator. De asemenea, trebuie să fie informată persoana vizată cu privire la destinatarii respectivi dacă persoana vizată solicită acest lucru. Pentru această ipoteză se va putea folosi un model pus la dispoziție de Operator.

4.5.5. Dreptul la restricționarea prelucrării

În situația încetării/dispariției împrejurării care a determinat restricționarea prelucrării datelor cu caracter personal, **Asociația Brahma** va notifica persoana vizată, înainte de ridicarea restricției de prelucrare cu privire la acest lucru.

Metodele de restricţionare a prelucrării de date cu caracter personal folosite de **Asociația Brahma** sunt următoarele:
- mutarea temporară a datelor cu caracter personal selectate într-un alt sistem de prelucrare.
- anularea accesului utilizatorilor la datele selectate.
- înlăturarea temporară a datelor publicate de pe site-ul **Asociației Brahma**
- alte metode necesare.

În ceea ce priveşte sistemele automatizate de evidenţă a datelor deținute de **Asociația Brahma**, restricţionarea prelucrării este asigurată prin mijloace tehnice în aşa fel încât datele cu caracter personal să nu facă obiectul unor operaţiuni de prelucrare ulterioară şi să nu mai poată fi schimbate.

4.5.6. Dreptul la portabilitatea datelor

În situația primirii unei solicitări de portabilitate a datelor, se va verifica, în prealabil, acuratețea și corectitudinea datelor.

În cazul exercitării dreptului la portabilitatea datelor de către persoanele vizate, **Asociația Brahma** va lua măsuri de securitate necesare pentru a asigura că datele cu caracter personal sunt transmise în condiții de siguranță la destinația corectă și pentru a proteja în continuare datele cu caracter personal care rămân în

sistemele sale. Ca atare, va evalua riscurile specifice legate de portabilitatea datelor și va lua măsuri adecvate de atenuare a riscurilor.

Portabilitatea datelor garantează dreptul de a primi date cu caracter personal și de a le prelucra conform intențiilor persoanei vizate *(dreptul la portabilitatea datelor nu se limitează la datele cu caracter personal care sunt utile și relevante pentru servicii similare furnizate de concurenții operatorului)*. În consecință, **Asociația** Brahma nu poartă răspunderea pentru prelucrarea gestionată de către persoana vizată sau de către o altă societate care primește date cu caracter personal.

Înainte de închiderea oricărui cont pe care persoana vizată l-ar avea, **Asociația Brahma** va include și informații despre dreptul la portabilitatea datelor. În cazul în care o persoană vizată descoperă că datele cu caracter personal solicitate în temeiul dreptului la portabilitatea datelor nu îi satisfac pe deplin cererea, va trebui să se adreseze cu o nouă cerere în temeiul dreptului de acces, în conformitate cu art. 15 din GDPR.

4.5.7. Dreptul la opoziție

Dacă scopul principal al procesării datelor personale este de natură legală sau în interesul legitim al **Asociația** Brahma, în momentul primirii unei obiecții legate de natura acestor procesări, va fi încetată prelucrarea datelor respective numai dacă nu se va putea demonstra cu claritate că prelucrarea se face pentru stabilirea, exercitarea sau apărarea revendicărilor legale. Toate acestea trebuie explicate clar și concis persoanei vizate care a ridicat vreo obiecție.

Dacă prelucrarea de date personale în scop de marketing direct, în momentul primirii unei obiecții legate de natura acestor procesări, va fi încetată prelucrarea datelor respective. Chiar dacă în anumite circumstanțe a existat un consimțământ inițial pentru prelucrarea datelor, ridicarea unei obiecții explicite pentru interzicerea prelucrării datelor personale în scopuri de marketing direct trebuie acceptată fără întârziere și comunicată persoanei vizate

În situația în care scopul prelucrării datelor este de cercetare științifică sau istorică, sau în scopuri statistice, persoanele fizice trebuie să aibă *„motive legate de situația lor particulară”* pentru a-și exercita dreptul de a se opune prelucrării în scopuri de cercetare. Dacă scopul principal al proiectului de cercetare este legat în mod direct de îndeplinirea unei sarcini de interes public **Asociația Brahma** nu este obligată să se conformeze unei obiecții față de prelucrarea datelor.

4.5.8. Dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri

În urma unei solicitări din partea persoanei vizate cu privire dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, trebuie ca persoana vizată să fie informaă într-o manieră specifică care să includă: existența unor procese decizionale automatizate în privința datelor sale, care se bazează exclusiv pe prelucrarea automată, scopurile acestora, efectele juridice care se pot produce în privința persoanei vizate, existența unor garanții corespunzătoare, măsura în care persoana vizată ar fi afectată, precum şi dreptul acesteia de a obţine intervenţie umană, de a-şi exprima punctul de vedere, de a primi o explicaţie privind decizia luată în urma unei astfel de evaluări, precum şi dreptul de a contesta decizia.

4.6. SEMNARE

Toate documentele întocmite de **Asociația Brahma** cu privire la drepturile persoanelor vizate pentru a fi transmise în exteriorul societății cu privire la drepturile persoanelor vizate vor fi semnate de către Președinte.

4.7. RĂSPUNS

Timpul maxim de răspuns este de 30 de zile. Atunci când este necesar, din motive legate de complexitatea și volumul cererilor primite simultan, această perioadă poate fi prelungită până la maximum trei luni. Chiar și în aceste condiții de prelungire, trebuie ca persoana vizată să fie informată de această prelungire tot în intervalul de o lună de la primirea cererii.

Pentru cererile recepționate în format electronic, răspunsul trebuie să fie furnizat în format electronic – acolo unde este posibil, cu excepția cazului în care persoana vizată solicită informațiile într-un alt format.

Informațiile care urmează să fie furnizate persoanelor vizate pot fi furnizate în combinație cu pictograme standardizate pentru a oferi într-un mod ușor vizibil, inteligibil și clar lizibil o imagine de ansamblu semnificativă asupra prelucrării avute în vedere. În cazul în care pictogramele sunt prezentate în format electronic, acestea trebuie să poată fi citite automat.

4.8. ÎNCHIDEREA SOLICITĂRII

După transmiterea răspunsului către persoana vizată, solicitările, inclusiv dovezile de comunicare a răspunsurilor, se grupează și se predau la arhivă în termen rezonabil. Predarea la arhivă se face pe bază de inventare (opis) întocmite în trei exemplare (un exemplar pentru cel care predă, un exemplar pentru dosarul din arhivă și un exemplar pentru dosarul de evidență a departamentului).

Procedura de obținere/revocare consimțământ persoane

1. DEFINIȚII

„GDPR", „Regulamentul" - Regulamentul (UE) 2016/679 al Parlamentului Eurpean și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor, în limba engleză General Data Protection Regulation);

„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;

„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;

„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**”* - 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;

*„**încălcarea securității datelor cu caracter personal**”* - 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;

„reprezentant” - persoană fizică sau juridică stabilită în Uniune, desemnată în scris de către operator sau persoana împuternicită de operator, care reprezintă operatorul sau persoana împuternicită în ceea ce privește obligațiile lor respective care le revin în temeiul GDPR;

„reguli corporatiste obligatorii” - politicile în materie de protecție a datelor cu caracter personal care trebuie respectate de un operator sau de o persoană împuternicită de operator stabilită pe teritoriul unui stat membru, în ceea ce privește transferurile sau seturile de transferuri de date cu caracter personal către un operator sau o persoană împuternicită de operator în una sau mai multe țări terțe în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună;

„autoritate de supraveghere” - autoritate publică independentă instituită de un stat membru cu atribuții în materia protecției datelor cu caracter personal;

„DPO” - responsabilului cu protecția datelor (în limba engleză, data protection officer);

„DPIA” - evaluarea impactului asupra protecției datelor (în limba engleză, data-protection impact assessment, DPIA).

2. SCOPUL ȘI DOMENIUL DE APLICARE

2.1. SCOPUL

2.1.1. Prezenta procedură documentează cerințele și **modalitatea de obținere/revocare a consimțământului în contextul GDPR**, ca temei de prelucrare a datelor cu caracter personal. În cazul in care, în conformitate cu GDPR, este necesar consimțământul persoanei vizate pentru

prelucrarea datelor sale cu caracter personal, acesta va intra în domeniul de aplicare al prezentei proceduri.

2.1.2. Prezenta procedură descrie activitățile desfășurate cu privire la modalitatea de obținere/revocare a consimțământului din partea persoanelor vizate, respectiv stabilește condițiile ce trebuie respectate privind exprimarea în mod valabil a consimțământului.

2.2. DOMENIUL DE APLICARE

2.2.1. Prezenta procedura se aplică tuturor structurilor organizatorice ale Operatorului. La procedură participă toate structurile organizatorice conform cu atribuțiile care le revin în ceea ce privește modalitatea de obținere/revocare a consimțământului din partea persoanelor vizate.

2.3. DOCUMENTE DE REFERINȚĂ

- GDPR
- Regulament intern
- Proceduri interne

3. ASPECTE GENERALE. CONSIMȚĂMÂNT

3.1. NECESITATEA CONSIMȚĂMÂNTULUI

Descriere. Potrivit dispozițiilor art. 6 alin. (1) lit. a) din GDPR, prelucrarea datelor cu caracter personal este legală dacă persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale pentru unul sau mai multe scopuri specifice.

Prelucrarea datelor cu caracter personal este legală și în cazul în care consimțământul este cuprins într-un contract, caz în care consimțământul este subînțeles (art. 6 alin. (1) lit. B) GDPR). Deopotrivă, prelucrarea poate fi legală și atunci când consimțământul persoanelor nu doar că nu există, dar persoanele vizate chiar se opun prelucrării datelor lor cu caracter personal, atunci când prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului (art. 6 alin. (1) lit. b) GDPR).

3.2. **CONDIȚII PRIVIND CONSIMȚĂMÂNTUL**

Forma. Forma consimțământului trebuie să fie **inteligibilă și ușor accesibilă**, utilizând un **limbaj clar și** simplu.

Momentul. Consimțământul va fi întotdeauna obținut **înainte ca să se înceapă prelucrarea datelor** cu caracter personal pentru care consimțământul este necesar.

Consimțământ separat. În cazul în care consimțământul persoanei vizate este dat în contextul unei **declarații scrise** care se referă și la alte aspecte, cererea privind consimțământul trebuie să fie prezentată într-o formă care **o diferențiază în mod clar de celelalte aspecte**.

Dovada consimțământului. Dacă prelucrarea datelor cu carcacter personal se bazează pe consimțământ, trebuie să se poată demonstra că persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale.

3.3. SITUAȚII ÎN CARE NU ESTE NECESAR CONSIMȚĂMÂNTUL

Nu este necesară obținerea consimțământului de la persoana vizată în următoarele situații:

- ✓ prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;
- ✓ prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;
- ✓ prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;
- ✓ prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul;
- ✓ prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.

3.4. LIPSA CONSIMȚĂMÂNTULUI

Reguli. La încheierea operațiunilor de prelucrare, dacă persoana vizată nu și-a dat în mod expres și neechivoc consimțământul pentru o altă destinație sau pentru o prelucrare ulterioară, datele cu caracter personal vor fi, după caz:

a) distruse;

b) transferate unui alt operator, cu condiția ca operatorul inițial să garanteze faptul că prelucrările ulterioare au scopuri similare celor în care s-a făcut prelucrarea inițială;

c) transformate în date anonime și stocate exclusiv în scopuri statistice, de cercetare istorică sau științifică.

În cazul operațiunilor de prelucrare efectuate în vederea îndeplinirii unei obligații legale sau pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice, datele se vor

putea stoca pe perioada necesară realizării scopurilor concrete urmărite, cu condiția asigurării unor măsuri corespunzătoare de protejare a acestora, după care va proceda la distrugerea lor dacă nu sunt aplicabile prevederile legale privind păstrarea arhivelor.

4. REGULI PRIVIND PROCEDURA DE OBȚINERE/REVOCARE A CONSIMȚĂMÂNTULUI DIN PARTEA PERSOANELOR VIZATE

4.1. OBȚINEREA/SOLICITAREA CONSIMȚĂMÂNTULUI

Descriere. Obținerea consimțământului este un drept recunoscut legislativ și trebuie efectuată doar de către lucrători instruiți în domeniul protecției datelor. Consimțământul poate fi obținut printr-o declarație scrisă sau o declarație orală (înregistrată), inclusiv prin mijloace electronice. Indiferent de modalitatea de obținere a consimțământului, acesta se va acorda printr-o acțiune neechivocă care să constituie o manifestare liber exprimată, specifică, în cunoștință de cauză și clară a acordului persoanei vizate pentru prelucrarea datelor sale cu caracter personal.

În cadrul **Asociației Brahma** obținerea/revocarea consimțământului din partea persoanelor vizate se poate face prin următoarele mijloace:

- ☐ semnarea unei declarații de consimțământ printr-un formular pe hârtie;
- ☐ bifarea unei căsuțe pentru consimțământ explicit, pe hârtie sau în format electronic;
- ☐ executarea unui click pe un buton sau un link online de acordare a consimțământului explicit;
- ☐ selectarea uneia dintre opțiunile da/nu vizibile;
- ☐ alegerea unor setări tehnice sau unor setări ale tabloului de preferințe;
- ☐ răspunsul la un mesaj e-mail prin care se solicită consimțământul;
- ☐ răspunsul „da" la o solicitare verbală clară a consimțământului;
- ☐ oferirea, în mod voluntar, a unor informații opționale pentru un anumit scop - de ex., completarea unor câmpuri opționale într-un formular (combinată cu declarații de confidențialitate tip „just-in-time" - exact la timp) sau depunerea unei cărți de vizită într-o cutie;
- ☐ alte modalități.

4.1.1. Obținerea consimțământului prin declarație scrisă

Reguli. Pentru obținerea consimțământului din partea persoanelor vizate prin declarație scrisă se va folosi un model pus la dispoziție în acest fel.

Registru management consimțământ. Orice declarație de obținere a consimțământului din partea persoanelor vizate, primită printr-o declarație scrisă, se înregistrează și se completează în registrul special denumit Registru management consimțământ.

4.1.2. Obținerea consimțământului în format electronic

Reguli. Obținerea consimțământului în format electronic se va putea face și prin completarea unui formular electronic, prin trimiterea unui e-mail, prin încărcarea unui document scanat care poartă semnătura persoanei vizate.

În cazul în care consimțământul va fi acordat în urma unei cereri transmise în format electronic, solicitarea consimțământului nu va perturba în mod inutil utilizarea serviciului pentru care se acordă consimțământul.

Dovada. Dovada luării consimțământului în format electronic va fi stocată în baza de date și după ce acesta va fi retras, până la respectarea obligațiilor legale, după caz, sau până la respectarea până la dispariția unui potențial litigiu între operator și persoana vizată. Aceste termene pot include termenele de prescripție stabilite de legea civilă, inclusiv termenele de prescripție care, în temeiul unei legi penale sau al altor legi sau regulamente, sunt mai mari decât primele.

Registru management consimțământ. Orice declarație de obținere a consimțământului din partea persoanelor vizate, primită în format electronic, se înregistrează și se completează în Registrul special **denumit Registru management consimțământ.**

4.1.3. Prelucrarea unor categorii speciale de date

Reguli. Sunt considerate date cu caracter special datele cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice.

Pentru prelucrarea unor categorii speciale de date, consimțământul va fi luat printr-**o declarație separată.** Declarația separată se va putea lua și în condițiile obținerii consimțământului în format electronic. Cererile pentru prelucrarea unor categorii speciale de date se înregistrează și se completează în registrul special denumit Registru management consimțământ.

4.1.4. Prelucrarea datelor cu caracter personal ale copiilor

Reguli. Prelucrarea datelor cu caracter personal ale copiilor se va face numai după verificarea dacă aceștia au vârsta de 16 ani împlinită. Dacă copilul are sub vârsta de 16 ani, consimțământul va fi obținut numai de la titularul răspunderii părintești asupra copilului, în condițiile obținerii consimțământului prevăzute în prezenta procedură.

Dacă utilizatorii afirmă că au împlinit vârsta minimă necesară pentru consimțământul obținut în format electronic, se vor efectua verificări pentru a se asigura că această afirmație este adevărată prin introducerea datei nașterii.

În cazul în care există dubii cu privire la vârsta copilului se vor lua măsuri prin verificarea confirmării via e-mail a persoanei care exprimă consimțământul în numele copilului care este titularul răspunderii părintești. În această situație, verificarea nu se va putea face decât după obținerea consimțământului părintelui, în condițiile prevăzute de prezenta procedură.

Consimțământul acordat sau autorizat de titularul răspunderii părintești expiră odată ce minorul a atins vârsta minimă obligatorie pentru exprimarea consimțământului digital. După împlinirea vârstei minime obligatorii, va fi obținut un nou consimțământ, în condițiile prevăzute de prezenta procedură.

4.1.5. Prelucrarea datelor personale ale angajaților

Pentru prelucrările datelor personale din cadrul locului de muncă, baza legală de prelucrare nu este consimțământul angajaților, având în vedere natura relației dintre angajat și angajator.

Asociația Brahma prelucrează datele cu caracter personal ale salariaților în următoarele scopuri prevăzute de dispoziții legale și/sau necesare pentru respectarea dispozițiilor legale:
- respectarea clauzelor contractului de muncă, inclusiv descărcarea de obligațiile stabilite prin lege sau prin acorduri colective;
- gestionarea, planificarea și organizarea muncii;
- asigurarea egalității și diversității la locul de muncă;
- asigurarea sănătății și securității la locul de muncă;
- evaluarea capacității de muncă a salariaților;
- valorificarea drepturilor de asistență socială;
- exercitarea drepturilor legate de ocuparea unui loc de muncă;
- organizării încetării raporturilor de muncă.

4.2. ÎNREGISTRAREA CONSIMȚĂMÂNTULUI

În toate cazurile de prelucrare a datelor cu caracter personal care presupun acordarea consimțământului din partea persoanelor vizate, se va păstra **evidența datei și modului** în care a fost obținut consimțământul.

Registru management consimțământ. Orice declarație de obținere a consimțământului din partea persoanelor vizate, primită printr-o declarație scrisă, se înregistrează și se completează în registrul special

denumit Registru management consimțământ. Registrul se păstrează de către responsabilul delegat în departamentu Resurse Umane, respectiv Proiecte.

4.3. GESTIONAREA CONSIMȚĂMÂNTULUI

Reguli. **Asociația Brahma** se asigură că respectă următoarele principii în ceea ce privește gestionarea consimțământului cu privire la prelucrarea datelor cu caracter personal, acordat de către persoanele vizate:

- ☐ consimțământul este revizuit periodic pentru a verifica dacă relația, prelucrarea și scopurile prelucrării s-au schimbat;
- ☐ are implementate **procese de reînnoire a consimțământului la intervale de timp adecvate**, inclusiv orice acorduri parentale;
- ☐ procesul de **retragere a consimțământului este facil** și se poate exercita în orice mod de către persoanele vizate; acest lucru este cunoscut de persoanele vizate;
- ☐ atunci când o persoana vizată formulează o cerere de retragere a consimțământului, se acționează cât mai repede posibil;
- ☐ nu **sunt penalizate persoanele vizate care doresc să își retragă consimțământul**.

Dacă scopul inițial al prelucrării datelor pentru care s-a obținut consimțământul s-a schimbat, se va obține un consimțământ nou și specific pentru acel scop. Astfel, scopul prelucrării datelor se modifică după ce consimțământul a fost obținut sau dacă un nou scop este avut în vedere. În acest caz, va fi obținut un nou consimțământ, conform dispozițiilor prezentei proceduri si legislației aplicabile.

4.4. RETRAGEREA CONSIMȚĂMÂNTULUI

Reguli. Persoana vizată își poate retrage consimțământul în orice moment, aplicându-se procedura obținerii acestuia. Retragerea consimțământului nu afectează legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia. Înainte de luarea consimțământului, persoana vizată va fi informată **în mod clar și expres despre dreptul de a-și retrage oricând consimțământul**, prin intermediul formularului de consimțământ, prin inserarea unui paragraf la începutul formularului, înainte de orice alt text.

Retragerea consimțământului în ceea ce privește prelucrarea unor categorii speciale de date, nu afectează consimțământul obținut pentru prelucrarea celorlalte date, altele decât cele considerate sensibile.

Retragerea consimțământului care vizează un anumit scop al prelucrării nu afectează prelucrările de date care au un alt scop pentru care a fost obținut un consimțământ valabil.

4.4.1. Cererea de retragere a consimțământului

Persoana responsabilă de analiza solicitării de retragere a consimțământului primite din partea persoanelor vizate are următoarele sarcini:

- ✓ primește solicitările de retragere a consimțământului din partea persoanelor vizate;
- ✓ organizează preluarea solicitărilor, înregistrează solicitările în Registru;
- ✓ conlucrează cu celelalte departamente în vederea analizării solicitării din partea persoanelor vizate;
- ✓ răspunde de menținerea Registrului.

În vederea analizării solicitărilor primite din partea persoanei vizate, persoana responsabilă va obține informații de la următoarele departamente:
- Departament Proiecte,
- Departament Resurse Umane

- Departament Financiar-Contabil
- Departamentul Contractare

Persoanele din cadrul departamentelor respective care întocmesc documente și transmit informații despre persoanele vizate poartă întreaga răspundere asupra datelor și conținutului acestora, iar în cazul transmiterii unor date sau informații eronate, vor răspunde potrivit reglementărilor în vigoare.

Politica de raportare și tratare incidente de securitate

1. DEFINIȚII

„GDPR", „Regulamentul" - Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor, în limba engleză General Data Protection Regulation);

„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;

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

„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;

*„**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 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**"* - 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;

*„**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;

„reprezentant” - înseamnă o persoană fizică sau juridică stabilită în Uniune, desemnată în scris de către operator sau persoana împuternicită de operator, care reprezintă operatorul sau persoana împuternicită în ceea ce privește obligațiile lor respective care le revin în temeiul GDPR;

„reguli corporatiste obligatorii” - înseamnă politicile în materie de protecție a datelor cu caracter personal care trebuie respectate de un operator sau de o persoană împuternicită de operator stabilită pe teritoriul unui stat membru, în ceea ce privește transferurile sau seturile de transferuri de date cu caracter personal către un operator sau o persoană împuternicită de operator în una sau mai multe țări terțe în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună;

„autoritate de supraveghere” - înseamnă o autoritate publică independentă instituită de un stat membru;

„DPIA” - evaluarea impactului asupra protecției datelor (în limba engleză, data-protection impact assessment, DPIA);

„Autoritate de Supraveghere” - Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP).

SCOPUL ȘI DOMENIUL DE APLICARE

2.1. SCOPUL

2.1.1. Prezenta politică documentează cerințele GDPR privind procedura de **raportare și tratare a incidentelor de securitate** și are rolul de a prezenta modalitatea concretă de notificare a Autorității de Supraveghere privind Protecția Datelor cu Caracter Personal și de informare a persoanei vizate în cazul în care se produce o încălcare a securității datelor cu caracter personal.

2.1.2. Prezenta politică descrie activitățile desfășurate atunci când se produce un incident de securitate, respectiv, **înregistrarea încălcărilor de securitate**, **întocmirea notificărilor și informărilor impuse de** GDPR, **stabilirea fluxului de parcurs în redactarea și difuzarea controlată** a acestora către Autoritatea de supraveghere și persoanele vizate.
2.1.3. Prin politică se urmărește asigurarea unui flux corect, eficient și legal al notificărilor transmise către Autoritatea de supraveghere și al informărilor persoanelor vizate în cazul încălcării securității datelor cu caracter personal, în temeiul GDPR și al legislației conexe.

2.1.4. GDPR introduce o obligație pentru toate organizațiile de a **raporta anumite tipuri de încălcare** a securității datelor cu caracter personal către autoritatea de supraveghere – ANSPDCP în termen de 72 de **ore de la constatarea încălcării**. Dacă este depășit acest termen, trebuie furnizate motive temeinice pentru întârziere.

2.1.5. GDPR introduce **obligația informării persoanelor vizate** cu privire la încălcarea securității datelor cu caracter personal dacă încălcarea respectivă este susceptibilă să genereze un risc ridicat de afectare **negativă a drepturilor și libertăților persoanelor vizate**, fără întârzieri nejustificate.

2.2. DOMENIUL DE APLICARE

Prezenta politică se aplică tuturor structurilor organizatorice ale Operatorului. Procedura este întocmită în scopul pregătirii pentru producerea unei încălcări a securității datelor cu caracter personal și planul de reacție la aceasta, precum și a atribuțiilor persoanelor implicate în procesul de notificare a Autorității de supraveghere și de informare a persoanelor vizate afectate. La politică participă toate structurile organizatorice conform cu atribuțiile care le revin în ceea ce privește asigurarea securității datelor cu caracter personal.

2.3. DOCUMENTE DE REFERINȚĂ

- GDPR;
- Regulament intern;
- Proceduri interne;

3. REGULI PRIVIND PROCEDURA DE RAPORTARE ȘI TRATARE INCIDENTE DE SECURITATE

3.1. Aspecte generale. Incidentul de securitate înseamnă o încălcare a securității care duce la distrugerea, **pierderea, modificarea, divulgarea neautorizată sau** accesul neautorizat la datele cu caracter personal, în mod accidental sau ilegal. Aceasta include încălcările cauzate atât în mod accidental, cât și în mod intenționat.

Încălcările de securitate vor fi raportate la ANSPDCP fără întârzieri nejustificate, în cel mult 72 de ore de la constatarea acesteia. În măsura în care nu este posibilă furnizarea tuturor informațiilor în termenul menționat, acestea vor fi transmise etapizat. În orice situație de depășire a termenului de 72 de ore de la constatarea încălcării, vor fi furnizate motive pentru întârziere, precum și termenul preconizat în interiorul căruia vor fi transmise mai multe informații.

În cazul în care încălcarea este susceptibilă să genereze un **risc ridicat pentru drepturile și libertățile** persoanelor vizate, vor fi informate persoanele în cauză în mod direct și fără întârzieri nejustificate, cât mai repede posibil.

În momentul producerii unei încălcări a securității datelor cu caracter personal, orice informații care se furnizează ANSPDCP sau persoanei vizate vor fi concise, ușor accesibile și ușor de înțeles și să utilizeze un limbaj simplu și clar, precum și elemente grafice acolo unde este cazul.

3.2. Descrierea încălcărilor. Încălcarea securității datelor cu caracter personal poate afecta confidențialitatea, integritatea sau disponibilitatea datelor cu caracter personal.

Încălcările securității datelor cu caracter personal pot cuprinde:

- ✓ accesul unui terț neautorizat;
- ✓ acțiunea (sau inacțiunea) intenționată sau accidentală a unui operator sau unei persoane împuternicite de operator;
- ✓ trimiterea unor date cu caracter personal către un destinatar greșit;
- ✓ pierderea sau furtul unor dispozitive informatice care conțin date cu caracter personal;
- ✓ modificarea datelor cu caracter personal fără permisiune;

- ✓ pierderea disponibilității datelor cu caracter personal.

3.3. **Înregistrarea încălcărilor de securitate**. Persoana responsabilă de înregistrarea incidentelor cu privire la încălcarea securității datelor cu caracter personal este: Barac Georgiana are următoarele sarcini:

- ✓ primește informările cu privire la incidentele de securitate;
- ✓ conlucrează cu celelalte departamente în vederea analizării incidentului de securitate;
- ✓ înregistrează incidentele de securitate în Registrul de evidență [**Registrul privind încălcările securității datelor cu caracter personal**];
- ✓ răspunde de menținerea Registrului de evidență.

Reguli generale privind înregistrarea:

a) toate documentele care privesc aceeași problemă se conexează la primul act înregistrat, numărul primului act fiind numărul de bază;
b) actele transmise se înregistrează cronologic, începând cu 1 ianuarie și terminând cu 31 decembrie al fiecărui an; actele care sunt transmise de către societate prin poștă sau curieri se înregistrează în ordinea transmiterii lor;
c) atât documentele care se înregistrează, cât și răspunsurile și actele transmise către Autoritatea de supraveghere și/sau persoanele vizate vor purta numărul de înregistrare al documentului
d) este interzisă circulația în cadrul societății a documentelor cu privire la încălcarea securității datelor cu caracter personal care nu sunt înregistrate.

3.4. Analiza încălcărilor de securitate. Unele încălcări a securității datelor cu caracter personal nu vor conduce la riscuri ce depășesc posibilele inconveniențe pentru persoanele care au nevoie de datele respective pentru munca lor. Alte încălcări pot afecta în mod semnificativ persoanele ale căror date cu caracter personal au fost compromise.

În analiza incidentelor de securitate se vor avea în vedere următoarele aspecte:

- ✓ prejudicii de natură fizică, materială sau morală persoanelor fizice, cum ar fi: pierderea controlului asupra propriilor date cu caracter personal, limitarea propriilor drepturi, discriminarea, furtul sau frauda identității, pierderea financiară, inversarea neautorizată a pseudonimizării;
- ✓ compromiterea reputației societății;
- ✓ pierderea confidențialității datelor cu caracter personal protejate prin secret profesional;
- ✓ orice alt dezavantaj semnificativ de natură economică sau socială pentru persoana fizică vizată.

În vederea analizării acestora, persoana responsabilă Barac Georgiana va obține informații de la departamente constituite în cadrul organizației, cum ar fi :
- Departament Resurse Umane persoană de contact [.....]
- Departament Financiar-Contabil persoană de contact [.....]
- Departament Proiecte persoană de contact [.....]
- Departamentul Contractare persoană de contact [.....]

Persoanele din cadrul departamentelor care întocmesc documente și transmit informații despre persoanele vizate poartă întreaga răspundere asupra datelor și conținutului acestora, iar în cazul transmiterii unor date sau informații eronate, vor răspunde potrivit reglementărilor în vigoare.

Persoana responsabilă de înregistrarea încălcărilor va consemna următoarele elemente:
- descrierea situației de fapt în care a avut loc încălcarea securității datelor cu caracter personal;
- efectele produse;
- măsurile de remediere întreprinse.

3.5. Evaluarea gravității impactului posibil sau efectiv. În evaluarea riscului pentru drepturile și libertățile persoanelor vizate, se va pune accentul pe posibilele consecințe negative și vor fi indicate elemente din care să rezulte probabilitatea materializării și gravitatea riscului rezultat ca urmare a incidentului produs. Dacă există probabilitatea ca un risc să se materializeze, atunci trebuie notificată ANSPDCP; dacă nu există această probabilitate, atunci nu trebuie raportată încălcarea.

Societatea păstrează documente referitoare la toate incidentele de securitate, chiar dacă nu există obligația de raportare către Autoritate sau nu prezintă un risc ridicat pentru persoanele vizate.

Persoana responsabilă cu evaluarea gravității impactului, este Barac Georgiana, in calitate de reprezentant al Operatorului. În urma evaluării gravității impactului persoana responsabilă, în raport de toți factorii relevanți, va completa un raport care se păstrează de către în biroul Secretariat.

3.6. Notificarea către Autoritatea de supraveghere. În cadrul societății se transmit notificări cu privire la încălcarea securității datelor cu caracter personal prin următoarele mijloace:
- e-mail
- alte modalități

În momentul raportării unei încălcări, trebuie incluse următoarele informații:
- ✓ descrierea caracterului încălcării securității datelor cu caracter personal, inclusiv, acolo unde este posibil: categoriile și numărul aproximativ al persoanelor vizate în cauză; categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;
- ✓ numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;
- ✓ descrierea consecințelor probabile ale încălcării securității datelor cu caracter personal;
- ✓ descrierea măsurilor luate sau propuse spre a fi luate pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile luate pentru atenuarea eventualelor efecte negative.

Pentru transmiterea Notificării către Autoritatea de supraveghere se va folosi modelul pus la dispoziție [**Formular de notificare a încălcării securității datelor către ANSPDCP**].

Persoana responsabilă de transmiterea Notificării către Autoritatea de supraveghere Barac Georgiana. Termenul de transmitere a notificării este 72 de ore. Dacă este depășit acest termen, trebuie furnizate motive temeinice pentru întârziere.

3.7. Informarea persoanei vizate la solicitarea Autorității de supraveghere. Persoana responsabilă de analiza solicitării primite din partea Autorității de supraveghere cu privire la informarea persoanelor vizate este: Barac Georgiana, in calitate de reprezentant al Prestatorului

În cadrul societății se transmit informări cu privire la încălcarea securității datelor cu caracter personal prin următoarele mijloace:
- e-mail
- alte modalități

Persoanele vizate vor fi informate în următoarele situații:
- ✓ în cazul în care încălcarea este susceptibilă să genereze un risc ridicat (pragul pentru informarea persoanelor vizate este mai ridicat decât cel pentru notificarea ANSPDCP) pentru drepturile și libertățile persoanelor vizate, în mod direct și fără întârzieri nejustificate;

- ✓ gravitatea impactului posibil sau efectiv al unei încălcări asupra persoanelor vizate, cât și probabilitatea materializării sale este mare.

În măsura în care decizia este de a nu informa persoanele vizate, trebuie notificată ANSPDCP, dacă nu se poate demonstra că încălcarea nu este susceptibilă să genereze un risc pentru drepturi și libertăți. În orice caz, trebuie păstrate documente cu privire la procesul de luare a deciziei în conformitate cu cerințele principiului responsabilității.

Informarea către persoanele vizate va descrie, într-un limbaj clar și simplu, caracterul încălcării securității datelor cu caracter personal și va cuprinde următoarele informații:

- ✓ numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;
- ✓ descrierea consecințelor probabile ale încălcării securității datelor cu caracter personal;
- ✓ descrierea măsurilor luate sau propuse spre a fi luate pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile luate pentru atenuarea eventualelor efecte negative.

Pentru transmiterea Informării către persoanele vizate se va folosi modelul pus la dispoziție [Informare **persoana vizată privind încălcarea securității datelor**].

Informarea persoanei vizate **nu este necesară** în cazul în care:

a) s-au implementat măsuri de protecție tehnice și organizatorice adecvate în cazul datelor cu caracter personal afectate de încălcarea securității;
b) au fost luate măsuri de natură a conferi siguranța că riscul ridicat pentru drepturile și libertățile persoanelor vizate nu mai este susceptibil să se materializeze;
c) ar necesita un efort disproporționat, caz în care se va efectua o informare publică sau se ia o măsură similară prin care persoanele vizate sunt informate într-un mod eficace.

Persoana responsabilă de transmiterea Informării către persoana vizată este Barac Georgiana. Termenul de transmitere a Informării este de 72 de ore. Dacă este depășit acest termen, trebuie furnizate motive temeinice pentru întârziere.

3.8. Persoanele împuternicite de operator. Dacă societatea utilizează una sau mai multe persoane împuternicite, iar acestea suferă o încălcare de securitate, vor trebui să informeze operatorul fără întârzieri nejustificate, de îndată ce constată încălcarea pentru a lua măsuri în vederea tratării încălcării și a-și îndeplini obligațiile de raportare a încălcărilor conform GDPR. Cerințele privind raportarea încălcărilor trebuie să fie detaliate în contractul încheiat cu persoana împuternicită, conform art. 28 GDPR.

3.9. Taxe. În cadrul Operatorului, informațiile furnizate persoanei vizate și orice comunicare sunt oferite în mod gratuit. În cazul în care cererile din partea unei persoane vizate sunt în mod vădit nefondate sau excesive (în special din cauza caracterului lor repetitiv) se va proceda la:

a) perceperea unei taxe având în vedere costurile administrative pentru furnizarea informațiilor sau a comunicării sau pentru luarea măsurilor solicitate;
b) refuzul de a da curs solicitării.

3.10. Semnare. Toate documentele întocmite cu privire la raportarea și tratarea incidentelor de securitate pentru a fi transmise în exteriorul Operatorului vor fi semnate de către reprezentantul legal al acesteia.

3.11. Închidere. Înainte de închiderea analizei incidentelor de securitate se va investiga dacă încălcarea a fost rezultatul unei erori umane sau al unei probleme sistematice și vor fi analizate măsuri pentru a preveni reapariția - fie prin procese mai bune, fie prin instruire suplimentară, fie prin alte măsuri corective.

După rezolvarea lor, toate actele cu privire la raportarea și tratarea incidentelor de securitate se grupează pe categorii și se predau la arhivă în termenul stabilit de conducere. Predarea la arhivă se face pe bază de inventare (opis) întocmite în trei exemplare (un exemplar pentru cel care predă, un exemplar pentru dosarul din arhivă și un exemplar pentru dosarul de evidență a departamentului).

Politica generală de protecție a datelor cu caracter personal pe website uri

Pentru Asociatia Brahma protecția datelor personale este foarte importantă. Prelucrarea datelor se face în condiții de legalitate, echitate și transparență, cu asigurarea securității adecvate a datelor, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale. Personalul Asociatiei Brahma respectă cu strictețe cerințele legale în privința protecției datelor și are grijă ca toate operațiunile de prelucrare să fie realizate numai în interesul dumneavoastră.

Prezentul angajament de respectare a confidențialității explică toate aspectele cu privire la prelucrarea datelor cu caracter personal și asigură respectarea tuturor principilor referitoare la prelucrare, stabilite de legislația în vigoare, precum și de Regulamentul (UE) 679/2016 (GDPR).

Asociatia Brahma nu răspunde pentru politica de confidențialitate practicată de către oricare alt terț la care se poate ajunge prin legături, indiferent de natura acestora, în afara website-ului asociației.

Pentru orice prelucrare efectuată total sau parțial prin orice mijloace a datelor cu caracter personal care fac parte dintr-un sistem de evidență a datelor sau care sunt destinate să facă parte dintr-un sistem de evidență a datelor, vă vom asigura că datele dumneavoastră sunt:

- ✓ prelucrate în mod legal, echitabil și transparent;
- ✓ colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile inițiale;
- ✓ adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate;
- ✓ exacte și, în cazul în care este necesar, să fie actualizate vom lua toate măsurile necesare pentru a ne asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere;
- ✓ păstrate într-o formă care permite identificarea dumneavoastră pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal vor fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice;
- ✓ prelucrate într-un mod care asigură securitatea adecvată, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare.

Serviciile noastre sunt dinamice și introducem frecvent funcționalități noi, ceea ce poate necesita colectarea de informații noi. În cazul în care colectăm date personale cu diferențe materiale sau aducem modificări materiale modului de utilizare a datelor, vă vom notifica și este posibil să modificăm și această politică de confidențialitate.

Datele dumneavoastră personale vor fi păstrate într-o **formă care permite identificarea dumneavoastră pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele.**

SCOPUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL

Scopul principal pentru care procesăm datele dumneavoastră personale sunt de a asigura că **înțelegerile contractuale dintre noi pot fi implementate în mod corespunzător**, astfel încât relația să poată funcționa fără probleme și să respecte cerințele legale, soluționarea disputelor și implementarea acordurilor noastre.

Asociatia Brahma colectează date cu caracter personal, pe paginile website-lui asociatiei, numai cu consimțământul Clientului, în următoarele scopuri:

- ✓ newsletter în format electronic sau sondaje;
- ✓ promovare – comunicare pe canale media și rețele de socializare;
- ✓ scopuri de cercetare și efectuarea de statistici.

Clientul își poate retrage consimțământul, în orice moment, acest lucru neafectând prelucrarea efectuată pe baza consimțământului înainte de retragerea acestuia. Retragerea consimțământului se poate face simplu prin transmiterea unui email la adresa oficiala de e-mail a **Asociației Brahma**.

În cazul în care intenționăm să prelucrăm ulterior datele dumneavoastră cu caracter personal într-un alt scop decât cel pentru care acestea au fost colectate, vă vom furniza, înainte de această prelucrare ulterioară, informații privind scopul prelucrării și orice informații suplimentare relevante solicitate de dumneavoastră care includ:

- ✓ perioada pentru care vor fi stocate datele cu caracter personal conform criteriilor utilizate pentru a stabili această perioadă;
- ✓ existența dreptului de a ne solicita în ceea ce privește datele cu caracter personal ale dumneavoastră, accesul la acestea, rectificarea sau ștergerea acestora sau restricționarea prelucrării sau a dreptului de a vă opune prelucrării, precum și a dreptului la portabilitatea datelor;
- ✓ atunci când prelucrarea se bazează pe consimțământul dumneavoastră pentru prelucrarea datelor cu caracter personal pentru unul sau mai multe scopuri specifice existența dreptului de a vă retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia;
- ✓ dreptul de a depune o plângere în fața unei autorități de supraveghere;
- ✓ dacă furnizarea de date cu caracter personal reprezintă o obligație legală sau contractuală sau o obligație necesară pentru încheierea unui contract, precum și dacă dumneavoastră sunteți obligat să furnizați aceste date cu caracter personal și care sunt eventualele consecințe ale nerespectării acestei obligații;
- ✓ existența unui proces decizional automatizat incluzând crearea de profiluri, menționat la precum și, cel puțin în cazurile respective, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana dumneavoastră.

CE TIPURI DE DATE COLECTĂM?

Colectăm datele pentru a opera eficient și a vă furniza cele mai bune experiențe legate de serviciile noastre. În cazul în care alegeți să nu furnizați date care sunt necesare pentru a furniza un produs sau o caracteristică, există posibilitatea să nu puteți utiliza produsul sau caracteristica respectivă.

Clientul are dreptul de a se opune colectării datelor sale personale și să solicite ștergerea acestora, revocându-

și astfel acordul dat pentru document, și renunțând astfel la orice drept implicit specificat în acesta și fără nicio obligație ulterioară a vreunei părți față de cealaltă sau fără ca vreo parte să poată pretinde celeilalte daune-interese și în orice moment.

Pentru exercitarea drepturilor conform legislației în vigoare Clientul se va adresa la adresa oficiala de e-mail a **Asociației Brahma** conform datelor de contact disponibile pe website, valabile la acea dată.

Folosindu-se de formularele disponibile pe website, Clientul are dreptul de a modifica datele pe care le-a declarat inițial pentru a reflecta orice modificare survenită, în cazul în care aceasta există.

Asociația Brahma se obligă că datele colectate ale Clientului să fie folosite numai în conformitate cu scopurile declarate și să nu facă publică, să vândă, închirieze, licențieze, transfere, etc. baza de date conținând informații referitoare la datele cu caracter personal sau special ale Clientului vreunui terț neimplicat în îndeplinirea scopurilor declarate.

Asociația Brahma garantează că datele personale ale unui Utilizator, colectate prin intermediul formularului de contact, dacă este cazul, vor fi folosite numai până la soluționarea problemei comunicate de acesta, după care vor deveni date cu caracter exclusiv statistic.

Date furnizate către noi pot include

- numele și prenumele dumneavoastră, adresa de e-mail, adresa poștală, numărul de telefon;
- date despre dispozitivul dumneavoastră și despre modul în care dumneavoastră și dispozitivul interacționați cu noi și cu serviciile noastre.

Informații pe care le obținem atunci când folosiți serviciile noastre

Informații despre dispozitivul folosit. Colectăm informații despre dispozitiv (cum ar fi modelul de hardware, versiunea sistemului de operare, identificatorii unici ai dispozitivului și informații despre rețeaua mobilă, inclusiv numărul de telefon);

Datele dumneavoastră personale pe care le colectăm sau le stocăm, nu vor fi prelucrate mai înainte ca:

- ✓ dumneavostră să vă dați consimțământul pentru prelucrarea datelor cu caracter personal pentru unul sau mai multe scopuri specifice;
- ✓ prelucrarea să fie necesară pentru executarea unui contract la care dumneavostră sunteți parte sau pentru a face demersuri la cererea dumneavostră înainte de încheierea unui contract;
- ✓ prelucrarea să fie necesară în vederea îndeplinirii unei obligații legale care ne revine;
- ✓ prelucrarea să fie necesară în scopul intereselor legitime urmărite de către noi sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale dumneavostră, care necesită protejarea datelor cu caracter personal, în special atunci când este vorba despre datele cu caracter personal ale unui copil sau direct marketing.

Principiile protecției datelor nu se aplică informațiilor anonime, adică informațiilor care nu sunt legate de o persoană fizică identificată sau identificabilă sau datelor cu caracter personal care sunt anonimizate astfel încât dumneavoastră nu sunteți sau nu mai sunteți identificabil. Prin urmare, această politică de confidențialitate nu vizează prelucrarea unor astfel de informații anonime, inclusiv în cazul în care acestea sunt utilizate în scopuri statistice sau de cercetare sau în alte scopuri.

Utilizarea datelor personale

Vom utiliza datele personale numai pentru scopul în care au fost colectate și vom stoca datele numai atât cât este necesar pentru acel scop.

Dacă prelucrarea este necesară pentru executarea unui contract sau pentru a face demersuri înainte de încheierea unui contract, perioada de utilizare a datelor este întreaga perioada contractuală, precum și 3 ani de la data încheierii acesteia.

Dacă prelucrarea se face în baza consimțământului pentru unul sau mai multe scopuri specifice perioada de utilizare a datelor este 5 ani.

STOCAREA DATELOR CU CARACTER PERSONAL.

DURATA

Stocăm datele dumneavoastră cu caracter personal atât timp cât este necesar pentru a presta serviciile pe care le-ați solicitat sau în alte scopuri esențiale, precum respectarea obligațiilor legale, soluționarea disputelor și implementarea acordurilor noastre.

Deoarece aceste necesități pot varia în funcție de tipurile de date diferite din contextul produselor diferite, perioadele reale de retenție pot varia semnificativ. Criteriile utilizate pentru a determina perioadele de retenție cuprind:

- ✓ perioada pentru care dumneavostră v-ați exprimat consimțământul sau până când vă exprimați intenția într-una din modalitățile prevăzute în prezenta politică de a nu mai păstra datele cu caracter personal furnizate;
- ✓ situația în care o lege prevede obligativitatea retenției datelor personale, pentru menținerea datelor relevante pentru o investigație sau date care trebuie să fie păstrate în cazul unui litigiu.

În virtutea dreptului de control al datelor personale pe care le avem despre dumneavostră, în cazul în care prelucrarea este efectuată în baza consimțământului, puteți opta pentru/să:

- ✓ Dreptul de a fi informat se referă la obligația de a vă furniza informații corecte cu privire la prelucrare datelor, în ceea ce privește modul în sunt utilizate datele dumneavoastră cu caracter personal;
- ✓ Dreptul de acces înseamnă că aveți dreptul de a obține din partea noastra o confirmare că vă prelucrăm sau nu date cu caracter personal, iar daca da, vă oferim accesul la aceste date precum și informații despre cum sunt prelucrate;
- ✓ Dreptul la portabilitate se refera la faptul că puteți primi datele cu caracter personal într-un format structurat, utilizat în mod curent și care poate fi citit automat precum și transmiterea acestor date altui operator;
- ✓ **Dreptul la opoziție** vizeaza dreptul de a vă opune prelucrării datelor personale atunci când aceasta deservește un interes public ori un interes legitim al nostru.
- ✓ Dreptul la rectificare se refera la corectarea, fără întârzieri nejustificate, a datelor personale inexacte;
- ✓ **Dreptul la ștergere/dreptul de a fi uitat** înseamnă ca aveți dreptul să vă ștergem datele colectate fără întârzieri nejustificate, în oricare din următoarele situații: nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate, retragerea consimțământului, opunerea la prelucrare,

colectarea ilegală, ștergerea pentru respectarea unei obligații legale sau colectarea făcută cu oferirea de servicii ale societății informaționale;

- ✓ **Dreptul la restricționarea prelucrării** poate fi exercitat dacă se contestă exactitatea datelor pe o anumita perioadă, suficientă pentru verificarea datelor, dacă prelucrarea este ilegala dar nu se dorește ștergerea datelor doar restricționarea, în cazul în care nu mai avem nevoie de datele personale în vederea prelucrării însa ni le solicitați pentru apărarea unui drept în instanță sau dacă v-ați opus prelucrării;
- ✓ Dreptul de a nu face obiectul unei decizii bazate **exclusiv pe prelucrarea automată, inclusiv** crearea de profiluri.

Contact și suport privind prelucrarea datelor cu caracter personal în proiectul cod SMIS 330685:
E-mail: office@asociatia-brahma.ro
Persoană de contact: Barac Georgiana (DPO)

PLÂNGERI
În situația în care considerați că datele dumneavoastră nu sunt prelucrate legal, aveți dreptul de a depune o plângere în fața Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal.