

POLITICA DE CONFIDENTIALITATE A OPERATORULUI BEST TRAVEL SOLUTIONS S.R.L.

1. INTRODUCERE

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;

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

„**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 performanța la locul de muncă, situația economică, sănătatea, preferințele 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 Angajații operatorului cu scopul de a se asigura confidențialitatea datelor personale în operațiunile de prelucrare a **datelor personale** efectuate de BEST TRAVEL SOLUTIONS S.R.L., 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/ colaboratori ai BEST TRAVEL SOLUTIONS S.R.L., precum și pentru orice alte persoane care, deși nu sunt salariații BEST TRAVEL SOLUTIONS S.R.L., pot fi asimilați unui personal dedicat BEST TRAVEL SOLUTIONS S.R.L., *(toate aceste persoane fiind denumite în acest document în mod generic „Angajați” sau “Colaboratori”)*.

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 Responsabilului cu protecția datelor (DPO), dacă a fost desemnat sau a reprezentantului legal al Operatorului.

2.3. Sfera datelor personale

Datele clienților

Operatorul prelucrează următoarele date cu caracter personal aparținând clientului/beneficiarului 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 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.

Compania BEST TRAVEL SOLUTIONS S.R.L., 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

BEST TRAVEL SOLUTIONS S.R.L., 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.

BEST TRAVEL SOLUTIONS S.R.L., recunoaște și respectă drepturile de confidențialitate ale angajaților săi, limitând colectarea, accesul și utilizarea datelor personale aferente angajării. BEST TRAVEL SOLUTIONS S.R.L., 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

BEST TRAVEL SOLUTIONS S.R.L., 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;
- ✓ Responsabilul pentru protecția datelor (DPO-ul) va instrui angajații BEST TRAVEL SOLUTIONS S.R.L. 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 superviza toate activitățile de prelucrare a datelor personale. Indiferent de numirea Responsabilului cu protecția 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, prelucrarea pe scară largă vizează categorii speciale de date*);
- ✓ Angajații BEST TRAVEL SOLUTIONS S.R.L. 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 BEST TRAVEL SOLUTIONS S.R.L. presupune efectuarea de către Angajații BEST TRAVEL SOLUTIONS S.R.L. 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:

- ✓ pseudonimizarea 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 BEST TRAVEL SOLUTIONS S.R.L. 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 protecție 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;
- ✓ Responsabilul pentru protecția datelor.

Aceștia din urmă sunt obligați să ia măsurile necesare conform regulilor legale sau celor stabilite în procedurile BEST TRAVEL SOLUTIONS S.R.L.

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 BEST TRAVEL SOLUTIONS S.R.L. 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 BEST TRAVEL SOLUTIONS S.R.L. are obligația păstrării unei **evidențe (întocmire și actualizare)** a persoanelor desemnate de BEST TRAVEL SOLUTIONS S.R.L. să prelucreze datele cu caracter personal, dacă prin natura activităților desfășurate în cadrul Departamentului este necesară prelucrarea de date cu caracter personal.

Este obligația Responsabilului pentru protecția datelor personale să solicite informații tuturor departamentelor în scopul actualizării datelor cu caracter personal la nivelul BEST TRAVEL SOLUTIONS S.R.L..

Prin prezenta Politică se stabilește faptul că managementul BEST TRAVEL SOLUTIONS S.R.L. 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 BEST TRAVEL SOLUTIONS S.R.L. 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 BEST TRAVEL SOLUTIONS S.R.L. 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 BEST TRAVEL SOLUTIONS S.R.L. le păstrează despre Angajat. De exemplu, BEST TRAVEL SOLUTIONS S.R.L. 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 BEST TRAVEL SOLUTIONS S.R.L. de a respecta drepturile de confidențialitate ale Angajaților nu reprezintă permisiunea de a desfășura activități personale necorespunzătoare în timpul serviciului (ex. calculatoarele BEST TRAVEL SOLUTIONS S.R.L. trebuie să fie utilizate doar în interes de serviciu). În plus, pentru a asigura securitatea și protecția sistemelor sale IT, Compania are dreptul de acces în toate sediile/punctele de lucru 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. BEST TRAVEL SOLUTIONS S.R.L. 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

Compania 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 BEST TRAVEL SOLUTIONS S.R.L. 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, BEST TRAVEL SOLUTIONS S.R.L. 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.

✓ **Când există protocol/acord privind transmiterea și prelucrarea datelor cu caracter personal** (protocolul/acordul este obligatoriu să fie încheiat ori de câte ori sunt transferate sau prelucrate date cu caracter personal de către operator și colaboratorii/partenerii contractuali ai acestuia)

✓ **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 efectuării 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.

BEST TRAVEL SOLUTIONS S.R.L. 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.

BEST TRAVEL SOLUTIONS S.R.L. 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 BEST TRAVEL SOLUTIONS S.R.L. transferă date cu caracter personal, în conformitate cu Regulamentul, respectiv toate operațiunile de transfer se vor face respectându-se **Procedura privind schimbul de date cu caracter personal.**

5.3. Reținerea și ștergerea datelor personale

Reținerea/stocarea și ștergerea datelor cu caracter personal, în vederea asigurării confidențialității datelor și informațiilor, precum și pentru păstrarea în siguranță a acestora, în cadrul activității curente executate de către angajați se va face cu respectarea dispozițiilor cuprinse în **Procedura de reținere și ștergere date cu caracter personal.**

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 BEST TRAVEL SOLUTIONS S.R.L. În situația în care solicitarea este efectuată de către o persoană vizată, angajatul va înainta această solicitare către Responsabilul pentru protecția datelor 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 BEST TRAVEL SOLUTIONS S.R.L., 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.

Aceste reguli se aplică tuturor personalului permanent, temporar și contractat care lucrează în cadrul BEST TRAVEL SOLUTIONS S.R.L.

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 BEST TRAVEL SOLUTIONS S.R.L. 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)

BEST TRAVEL SOLUTIONS S.R.L. **acordă** angajaților dreptul de a utiliza smartphone-uri și tablete personale la locul de muncă. BEST TRAVEL SOLUTIONS S.R.L. își rezervă dreptul de a revoca acest privilegiu dacă utilizatorii nu respectă politicile și procedurile BEST TRAVEL SOLUTIONS S.R.L..

Aceste reguli au rolul de a proteja securitatea și integritatea infrastructurii de date și tehnologii a BEST TRAVEL SOLUTIONS S.R.L. 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 BEST TRAVEL SOLUTIONS S.R.L.

7.1. Utilizare acceptabilă

BEST TRAVEL SOLUTIONS S.R.L. definește utilizarea acceptabilă a afacerii ca activități care susțin direct sau indirect activitatea Companiei. BEST TRAVEL SOLUTIONS S.R.L. definește folosirea personală acceptabilă în timpul Companiei ca o comunicare personală rezonabilă și limitată, cum ar fi citirea.

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;

✓ etc.

Angajații pot utiliza dispozitivul mobil pentru a accesa următoarele resurse deținute de BEST TRAVEL SOLUTIONS S.R.L.: e-mail, calendare, contacte, documente etc.

BEST TRAVEL SOLUTIONS S.R.L. 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. 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 BEST TRAVEL SOLUTIONS S.R.L.

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 BEST TRAVEL SOLUTIONS S.R.L..

Telefoanele inteligente și tabletele care nu se află pe lista de dispozitive acceptate ale BEST TRAVEL SOLUTIONS S.R.L. 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 BEST TRAVEL SOLUTIONS S.R.L. 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 BEST TRAVEL SOLUTIONS S.R.L..

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.

BEST TRAVEL SOLUTIONS S.R.L. își rezervă dreptul de a deconecta dispozitivele sau de a dezactiva serviciile fără notificare.

Dispozitivele pierdute sau furate trebuie să fie raportate BEST TRAVEL SOLUTIONS S.R.L. 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 BEST TRAVEL SOLUTIONS S.R.L..

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 BEST TRAVEL SOLUTIONS S.R.L. 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.

BEST TRAVEL SOLUTIONS S.R.L. 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 și ușor accesibilă, utilizând un limbaj clar și simplu, în special pentru orice informații adresate în mod specific unui copil. Informațiile se furnizează în scris sau prin alte mijloace, inclusiv, atunci când este oportun, în format electronic. La solicitarea persoanei vizate, informațiile pot fi furnizate verbal, cu condiția ca identitatea persoanei vizate să fie dovedită prin alte mijloace.

Operatorul poate înregistra apelurile telefonice către/de la Operator, purtate de Operator/Împuternicirii 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 acordată. 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 produselor și serviciilor Operatorului, precum:

- ✓ entități care participă la negocierea, încheierea sau la aducerea la îndeplinire a contractelor (furnizori de servicii și bunuri, operatori IT, avocați și alți consultanți etc.);
- ✓ entități care asigură buna funcționare a produselor și 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 Destinatariilor 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 persoane 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.