POLITICA DE PROTECTIE A DATELOR CU CARACTER PERSONAL

Cod: GDPR-DOC-03-2.2

Editia: I Revizia: 2 Data 16.06.2022

	Elaborat	Avizat	Aprobat
Numele	Tiberiu Rubnicu	Ion Tufa	Dragos Maracine
Funcţia	Resp Date Personale/DPO	Legal & HR Manager	Director General
Semnătura			
Data	16.06.2022	16.06.2022	17.06.2022

1.INTRODUCERE

Securitas Services Romania SRL, denumită în cele ce urmează și "Securitas", are ca prioritate respectarea legilor aplicabile și regulamentelor în materie de protecție a Datelor cu Caracter Personal în desfasurarea activitatilor sale, respectiv furnizarea serviciilor de securitate.
În conformitate cu prevederile Regulamentului Uniunii Europene 679 din 27 aprilie 2016 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date (GDPR), Securitas Services Romania SRL prelucrează date cu caracter personal, cu respectarea principiilor menţionate în continuare, în scopuri legitime. Prelucrarea datelor cu caracter personal se realizează prin mijloace mixte (manuale şi automate), cu respectarea cerinţelor legale şi în condiţii care să asigure securitatea, confidenţialitatea şi respectarea drepturilor persoanelor vizate.

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

- Regulamentul General de Protecţia Datelor (GDPR/RGPD) 679/2016, adoptat de Parlamentul European şi de Consiliul European la 27 Aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date
- LEGE nr. 190/2018 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016

2. SCOP

Prezenta Politică reglementează principiile esențiale care stau la baza procesării de către Securitas a datelor cu caracter personal ale clienților, furnizorilor, partenerilor de afaceri, angajaților și altor persoane și stabilește responsabilitățile departamentelor interne și ale angajaților în legătura cu prelucrarea datelor cu caracter personal.
Această politică stabilește angajamentul Securitas de a se asigura că orice date cu caracter personal, inclusiv categorii speciale de date personale, procesate de Securitas, sunt realizate în conformitate cu reglementarile si legislatia privind protecția datelor.

Prezenta Politică se aplică Societatii Securitas și subsidiarelor acesteia, deținute parțial sau integral de către Societate, care dezvoltă afaceri în Spațiul Economic European ("SEE") sau care procesează date cu caracter personal ale persoanelor vizate din SEE.

3. DEFINITII

Definițiile termenilor folosiți în prezenta Politică au înțelesul redat în art. 4 din Regulament, după cum urmează:
"date cu caracter personal" înseamnă orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată"); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

„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

„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;

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

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

„operator” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern

„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;

„date genetice” înseamnă datele cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care oferă informații unice privind fiziologia sau

sănătatea persoanei respective și care rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză
„date biometrice” înseamnă o date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice;
„date privind sănătatea” înseamnă date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia
„întreprindere” înseamnă o persoană fizică sau juridică ce desfășoară o activitate economică, indiferent de forma juridică a acesteia, inclusiv parteneriate sau asociații care desfășoară în mod regulat o activitate economică;
„grup de întreprinderi” înseamnă o întreprindere care exercită controlul și întreprinderile controlate de aceasta;
„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 în temeiul articolului 51; In Romania, acest rol este asumat de catre Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal (ANSPDCP).

4. PRINCIPIILE DE BAZĂ PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL.
Principiile relative protecției datelor cu caracter personal reflectă responsabilitățile de bază ale Securitas Services Romania (‘Securitas) care prelucrează asemenea date. Potrivit art. 5 (2) din Regulament, Securitas in calitate de Operator de date, este responsabila pentru și va trebui să poată demonstra conformitatea cu aceste principii

a) Legalitate, echitate şi transparenţă

Datele cu caracter personal trebuie să fie prelucrate *”în mod legal, echitabil şi transparent faţă de persoana vizată.”*

b) Limitări legate de scop

Datele personale trebuie să fie colectate în scopuri bine determinate, explicite şi legitime, iar prelucrările ulterioare nu trebuie să se abată de la aceste scopuri.

c) Reducerea la minimum a datelor

Orice colectare de date personale trebuie foarte bine analizată înainte de obținerea efectivă a datelor, care trebuie să fie cele mai relevante și strict limitate la ceea ce este absolut necesar pentru scopurile în care sunt prelucrate.

d) Exactitatea informațiilor

Trebuie să se ia toate măsurile pentru a asigura validitatea datelor, iar cele dovedite inexacte trebuie actualizate rapid sau șterse.

e) Limitarea stocării

Datele trebuie păstrate fix atâta timp cât sunt necesare pentru pelucrarea asumată. Perioadele mai lungi de stocare sunt excepții.

f) Integritate și confidențialitate

Prelucrarea datelor personale trebuie făcută în cele mai proprii condiții de siguranță, care să includă *"protecţia împotriva prelucrării neautorizate sau ilegale şi împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare"*.

Principiul Raspunderii

Securitas Services Romania in calitate de Operator de date cu caracter personal este responsabila de respectarea principiilor sus menționate și va demonstra conformitatea cu principiile de protecția datelor prin implementarea prezentei politici de protecția datelor, respectarea codurilor de conduită, implementarea unor măsuri tehnice și organizatorice, precum și adoptarea unor tehnici precum protecția datelor prin design, efectuarea evaluarii impactului prelucrarii (cand este cazul), procedura de notificare a încălcării și planuri de răspuns la incidente.

5. DREPTURILE PERSOANEI VIZATE

Sub rezerva anumitor condiții legale, Persoanele Vizate au următoarele drepturi în legătură cu prelucrarea datelor cu caracter personal:

- Dreptul de a fi informat – să obţină de la Securitas următoarele informaţii:

i. identitatea şi datele de contact ale Securitas , ale reprezentanţilor, şi ale responsabilului cu protecţia datelor;
ii. scopurile şi temeiul juridic al prelucrării datelor cu caracter personal, interesele legitime ale Securitas ;
iii. categoriile de date cu caracter personal;
iv. destinatarii datelor cu caracter personal, inclusiv destinatarii din ţări terţe sau organizaţii internaţionale (dacă există) şi referirea la garanţiile şi mijloacele corespunzătoare;
v. perioada de stocare a datelor cu caracter personal şi criteriile folosite pentru a determina acea perioadă, sub rezerva că Securiats Romania păstrează şi prelucrează datele cu caracter personal atâta timp cât legile şi reglementările legale impun acest lucru. Prelucrarea datelor cu caracter personal încetează imediat daca nu mai există niciun motiv pentru o astfel de prelucrare;
vi. din ce sursă provin datele cu caracter personal (în cazul în care datele cu caracter personal nu au fost obţinute de la persoana vizată);

- *Dreptul de acces la datele cu caracter personal* - să obţină de la Securitas Romania confirmarea dacă datele cu caracter personal sunt prelucrate sau şi dreptul de a primi o copie a oricărei înregistrări care conţine datele sale cu caracter personal;
- *Dreptul la rectificare* - să obţină de la Securitas Romania fără întârzieri nejustificate rectificarea unor date cu caracter personal inexacte cu privire la el/ea, completarea datelor cu caracter personal incomplete, inclusiv prin furnizarea unei declaraţii suplimentare;
- *Dreptul la ştergerea datelor ("dreptul de a fi uitat")* - să obţină de la Securitas ştergerea datelor cu caracter personal fără întârzieri nejustificate (dacă datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate; persoana vizată îşi retrage consimţământul; datele cu caracter personal au fost prelucrare ilegal etc.);
- *Dreptul la restricţionarea prelucrării* - dacă datele cu caracter personal sunt inexacte; prelucrarea este ilegală şi persoana vizată solicită restricţionarea utilizării datelor cu caracter personal în locul ştergerii lor; datele cu caracter personal nu mai sunt necesare în scopul prelucrării, dar ele sunt solicitate pentru constatarea, exercitarea sau apărarea unui drept în instanţă; persoana vizată s-a opus prelucrării pentru intervalul de timp când se verifică dacă drepturile legitime ale operatorului prevalează asupra celor ale persoanei vizate;
- *Dreptul la portabilitatea datelor* – să primească datele cu caracter personal într-un format structurat, utilizat în mod curent şi care poate fi citit automat şi are dreptul de a transmite aceste date cu caracter personal unui alt operator fără obstacole din partea Securitas (dacă

prelucrarea se bazează pe consimţământ sau pe un contract, iar prelucrarea este efectuată prin mijloace automate);

- *Dreptul la opoziție* - în orice moment al prelucrării datelor cu caracter personal (inclusiv crearea de profiluri pe baza respectivelor dispoziţii şi au fost date cu caracter personal prelucrate în scopuri de marketing direct);
- *Dreptul la retragerea consimţământului* - în orice moment fără a afecta legalitatea prelucrării bazate pe consimţământ, înainte de retragerea sa. Astfel persoana vizată înţelege şi este de acord că, în cazul retragerii, nu se poate ajunge la scopul prelucrării datelor cu caracter personal si Securitas nu va mai prelucra datele cu caracter personal și va lua măsurile corespunzătoare pentru ștergerea datelor personale ale persoanei vizate
- *Dreptul de a depune o plângere* - la o autoritate de supraveghere, Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), în cazul în care persoana vizată decide că drepturile sale sunt încălcate;
- *Dreptul de a vă adresa justiției* - pentru apărarea oricăror drepturi garantate de prezenta legislatie in domeniu si care au fost încălcate;

Securitas se asigură că există măsuri și proceduri adecvate pentru a răspunde drepturilor persoanelor vizate într-un mod conform și în timp util

Pentru exercitarea drepturilor menționate mai sus, Persoanele Vizate pot adresa o cerere in scris folosind următoarele date de contact:

SECURITAS SERVICES ROMANIA S.R.L – in atentia Responsabil Protectia Datelor/DPO
Sos Bucurest-Ploiesti 42-44, Cladirea A, Aripa A1, etaj 2, sector 1, Bucuresti
Tel: 0743 057 052; E-mail: dpo@securitas.com.ro

6. PRELUCRAREA JUSTA SI TRANSPARENTA A DATELOR

Securitas va depune toate eforturile pentru a colecta cât mai puține date cu caracter personal. În situația în care datele cu caracter personal sunt colectate de la o parte terță, Securitas se va asigura asupra faptului că datele cu caracter personal sunt colectate în conformitate cu dispozițiile legale aplicabile privind protecția datelor cu caracter personal
Datele cu Caracter Personal vor fi procesate doar în scopul pentru care au fost colectate initial si doar la autorizarea a Responsabilului cu Protecția Datelor.
Securitas va decide dacă este necesar să se efectueze o evaluare de impact a datelor cu caracter personal
La momentul colectării sau inainte de colectarea datelor cu caracter personal pentru orice tip de procesare, incluzând dar fără a se limita la vînzarea de produse, servicii sau activități de marketing, Responsabilul cu Protecția Datelor se va asigura asupra faptului că persoanele vizate sunt informate corespunzător cu privire la: categoriile de date cu caracter personal colectate, scopurile procesării, metodele procesării, drepturile Persoanelor Vizate cu privire la datele lor cu caracter personal, perioada de retenție, posibilitatea tranferului international de date cu caracter personal, dacă datele cu caracter personal vor fi transmise și unor părți terțe precum și cu privire la măsurile de securitate privind protecția datelor cu caracter personal ale Societății. Această informație este asigurată prin Notificarea de Prelucrare a Datelor cu Caracter Personal

În cazul în care Securitas va dori să proceseze datele cu caracter personal colectate pentru alte scopuri, va solicita consimțământul Persoanelor Vizate, consimțământ care trebuie să fie explicit și scris.

7. PERSONANE VIZATE

Categoriile de persoane vizate de prelucrarea datelor cu caracter personal sunt următoarele:

- angajatii, membrii familiilor angatilor, fosti angajati;
- candidații la posturile vacante din cadrul Securitas;
- părți semnatare ale contractelor și persoanele implicate în încheierea și executarea contractelor;
- participanții la evenimentele organizate sau susținute de către Securitas;
- participanți la cursurile de formare și specializare din cadrul Securitas;
- reprezentanti ai autoritatilor, institutiilor publice si mass-media;;
- persoane ce acceseaza paginile web.

8. CATEGORII DE DATE CU CARACTER PERSONAL

Securitas prelucrează datele cu caracter personal pe care persoanele vizate le furnizează în mod direct, date care sunt generate pe baza acestora, precum și date din surse publice.
Categoriile de date cu caracter personal prelucrate sunt:

- date de identificare: nume, prenume, titlul academic, funcția, departamentul, codul numeric personal, număr și serie BI/CI/pașaport/permis de conducere, număr marca, ID card acces;
- date de identificare informatice: adresa IP, nume de utilizator, parola;
- date privind persoana: data și locul nasterii, sex, cetățenie, stare civila, semnătura; date de contact: adresa de domiciliu/reședinta, adresa de e-mail, număr de telefon fix/mobil;
- date de recrutare si angajare: date conținute în CV-uri, recomandări, carnet muncă sau echivalent, cazier judiciar, date privind starea de sănătate;
- date financiare: număr cont bancar si alte informații financiare;
- date biometrice: voce, imagine;
- date colectate cu ocazia înregistrarii și participarii la evenimentele organizate sau sprijinite de către Securitas (fotografii, video, citate, postări pe rețele sociale etc.)

9. SCOPUL PRECLUCRĂRII DATELOR CU CARACTER PERSONAL

Colectarea și prelucrarea tipurilor de date personale enumerate mai sus este necesară pentru a indeplini scopuri legitime specifice în desfășurarea activităților noastre comerciale În special, prelucram datele dvs. personale în următoarele scopuri:

- pentru furnizarea produselor si serviciilor noastre de protectie in baza contractelor incheiate cu Clientii
- pentru a îmbunătăți serviciile și produsele noastre;
- pentru administrarea furnizorilor si subcontractorilor;
- pentru administrarea și conducerea personalului
- pentru administrarea clienților, de exemplu, pentru a răspunde la solicitări sau întrebări din partea clienților, a anchetelor privind satisfacția clienților sau pentru a gestiona reclamatiile privind un anumit produs sau serviciu;
- pentru gestionarea relațiilor comerciale cu terțe părți;

- monitorizarea/securitatea persoanelor, spaţiilor şi/sau bunurilor publice/private in vederea asigurarii pazei si protectiei in locatiile Securitas
- în scopuri administrative în cadrul Grupului Securitas:
- pentru backup sau arhivare;
- pentru gestionarea disputelor/litigiilor;
- pentru indeplinirea obligatiilor legale

10. TEMEI JURIDIC PENTRU PRELUCRAREA DATELOR PERSONALE

Securitas prelucrează datele cu caracter personal, în conformitate cu prevederile Regulamentului nr. 679/2016 privind protecția datelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestora.
Prelucrarea datelor cu caracter personal intervine în următoarele situații:

- *Respectare obligație legală* - prelucrarea este necesară în vederea indeplinirii unei obligatii legale care ii revine Securitas ca Operator de date.
- *Executarea unui contract* - 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, inclusiv legate de realizarea obiectului de activitate.
- *Interes legitim* - prelucrarea este necesară în scopul intereselor legitime urmărite de Securitas sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile si libertatile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal. În aceasta categorie pot intra îndeplinirea obiectivelor de comunicare și diseminare, procesul de recrutare și resurse umane si pentru a asigura securitatea persoanelor, bunurilor si operatiunilor Securitas
- *Consimțamant* - persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice. Conform Regulamentului consimțământul este considerat acordat fie prin intermediul unui document scris sau printr-o actiune afirmativă fără echivoc. Consimțământul astfel acordat poate fi retras potrivit prevederilor Regulamentului.

11. DESTINATARII DATELOR CU CARACTER PERSONAL

Pentru îndeplinirea scopurilor de prelucrare, Securitas poate să dezvăluie anumite categorii de date cu caracter personal către următoarele categorii de destinatari: persoana vizata și/sau reprezentanții săi legali, angajatii Securitas, parteneri contractuali si imputerniciti ai Securitas. autoritati judecătorești si alte autorități publice, companii ale Grupului Securitas, societăți de asigurare, organizații profesionale nationale sau internationale, organizații de cercetare a pieței.

12. DURATA PRELUCRARII DATELOR

Securitas se angajează să respecte principiul limitării pastrarii datelor personale. În această perspectivă, nu vom pastra/retine datele personale mai mult decât este necesar pentru îndeplinirea contractelor nostre și / sau pentru realizarea unuia dintre celelalte scopuri menționate anterior. Securitas poate, de asemenea, să fie obligata din punct de vedere legal să păstreze datele personale pentru o perioadă minimă de timp pentru a se conforma cerințelor legale.

Vom pastra datele personale in baza nomenclatorului arhivistic propriu, întocmit conform Legii Arhivelor Nationale nr. 16/1996, cu modificările și completările ulterioare precum si a Instructiunilor grupului Securitas**.** De asemenea vom efectua verificări periodice pentru a identifica datele personale care nu mai servesc scopului pentru care au fost colectate, pentru a le șterge sau a le anonima.

13. SECURITATEA DATELOR

Securitas acorda o importanta deosebita protectiei datelor dumneavoastra cu caracter personal si in consecinta a implementat masuri tehnice si organizatorice adecvate care sunt revizuite si adaptate periodic pentru protejarea acestora impotriva distrugerii accidentale sau ilegale, pierderii, modificarii, dezvaluirii sau accesului ilicit sau neautorizat. Printre aceste masuri se numara:

- Implementarea si revizuirea periodica a politicilor, procedurilor si instructiunilor de lucru destinate securizarii prelucrarii datelor cu caracter personal
- Instruirea periodica si sistematica a tuturor angajatilor care prelucreaza date cu caracter personal
- Limitarea accesului la datele cu caracter personal in conformitate cu principiile din politica generala de securitate („nevoia de a sti", „nevoia de a vedea" etc.)
- Accesul securizat la aplicatiile si fisierele care contin date cu caracter personal
- Implementarea unor solutii tehnice pentru securizarea comunicatiilor care includ date cu caracter personal
- Monitorizarea proceselor de transfer a datelor cu caracter personal (prin serviciul de email, copiere pe suport extern, tiparire, scanare etc.) si blocarea tentativelor de transfer neautorizate
- Implementarea unor solutii tehnice pentru asigurarea disponibilitatii datelor cu caracter personal in sistemele informatice utilizate
- Criptarea comunicarilor ce contin date cu caracter personal

14. CONFIDENȚIALITATEA PRELUCRARII

Datele personale sunt considerate informatii confidentiale si vor fi tratate ca atare. Orice colectare, prelucrare sau utilizare neautorizată a acestor date de către angajații Securitas este interzisă. Prelucrarea datelor cu caracter personal este confidenţială si va fi efectuată numai de persoanele care acţionează sub autoritatea Securitas şi numai pe baza instrucţiunilor acesteia

Orice prelucrare de date efectuată de un angajat, care nu a fost autorizată să fie desfasurata ca parte a îndatoririlor sale legitime de serviciu, este considerata ca fiind neautorizată. Intotdeauna se aplică principiul "*necesitatea de a cunoaște".* Angajații pot avea acces la informații personale in functie de adecvare a acestui acces la tipurile de date si de scopul determinat. Acest lucru se bazeaza pe stabilirea și separarea atentă a atributiilor angajatilor Securitas și presupune punerea în aplicare a rolurilor și responsabilităților pentru fiecare angajat

Angajaților li se interzice să utilizeze date cu caracter personal în scopuri private sau comerciale, să le dezvăluie persoanelor neautorizate sau să le pună la dispoziție în orice alt mod.

Superiorii ierarhici își informează angajații la începutul relației de muncă cu privire la obligația de a proteja secretul datelor. In cazul utilizarii neautorizate a datelor personale, angajatii pot fi sanctionati in conformitate legislatia aplicabila si cu reglementarile in vigoare in cadrul Securitas

Confidențialitate prin design și implicit
Considerațiile privind protecția datelor trebuie să fie integrate în produse, operațiuni de prelucrare și sisteme încă din primele etape de dezvoltare și pe tot parcursul ciclului de viață al procesării. Scopul confidențialității prin design este de a permite confidențialității să urmeze întregul ciclu de viață al sistemului utilizat pentru prelucrarea datelor cu caracter personal. Măsura și standardele la care se aplică acest lucru vor depinde de legile de confidențialitate aplicabile în care va avea loc prelucrarea.

15. OPERATOR DE DATE SI IMPUTERNICIT

Responsabilitate
Atunci când Securitas prelucrează date cu caracter personal, aceasta acționează fie ca Operator de date, fie ca Imputernicit. În fiecare relație în care Securitas prelucrează date cu caracter personal, este important ca o evaluare să fie efectuată pentru a determina dacă Securitas acționează ca Operator de date sau Imputernicit în legătură cu prelucrarea de date respectiva.
Ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor vizate, Securitas pune în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prevederile Regulamentului General de Protecţia Datelor (GDPR/RGPD) 679/2016. Respectivele măsuri se revizuiesc și se actualizează dacă este necesar.

Acord/Contract de prelucrare a datelor
Securitas va încheia un Acord/Contract de prelucrare a datelor („APD") atât atunci când Securitas acționează ca Operator de date, cât și atunci când acționează ca Imputernicit (art.28.GDPR)
Securitas atunci când acționează ca Operator, se va asigura că Imputernicitii sai pentru prelucrarea datelor personale oferă suficiente garanții pentru a implementa măsurile tehnice și organizaționale adecvate pentru a fi conforme și pentru a proteja datele cu caracter personal aflate sub responsabilitatea sa.
Responsabilitatea Securitas cand acționează ca Imputernicit este de a se asigura că se angajează doar la măsuri tehnice și organizatorice pe care le va putea respecta.
De fiecare dată când Securitas utilizează terțe părți în calitate de furnizori sau parteneri de afaceri care prelucreaza datele cu caracter personal în numele Securitas, Responsabilul cu Protecția Datelor trebuie să se asigure că Imputernicitul respectiv, (furnizor sau partener de afaceri), va oferi măsuri de securitate adecvate riscurilor aferente astfel încât să asigure protecția datelor cu caracter personal.
Atunci când Securitas prelucreaza date cu caracter personal în asociere cu o terță persoană independentă, Securitas va specifica în mod explicit prin contract sau orice alt act încheiat, responsabilitățile sale precum și ale terței părți.

Evidența activităților de prelucrare

Securitas Services Romania trebuie să țină o evidență / registru al activităților sale de prelucrare a datelor cu character personal. Conținutul unei astfel de înregistrări/evidente trebuie să respecte prevederile Regulamentului General de Protecţia Datelor (GDPR/RGPD) 679/2016. Dacă este furnizat un proces sau un sistem la nivel de Securitas Grup pentru menținerea unei evidențe a activităților de prelucrare, Securitas Services Romania va fi responsabilă să urmeze procesul sau sistemul respectiv

Servicii bazate pe cloud

Atunci când externalizați servicii către terți, cum ar fi furnizorii de servicii IT sau când utilizați furnizori de servicii cloud pentru prelucrarea datelor cu caracter personal, trebuie luate în considerare protecția datelor, iar Securitas trebuie să asigure cerințele de securitate a informațiilor ca parte a implementării sau externalizării.

16. TRANSFERUL DATELOR DVS PERSONALE IN AFARA SPATIULUI ECONOMIC EUROPEAN

Securitas va incerca mereu să proceseze datele personale în cadrul Spatiului Economic European (SEE). Dar, pentru a atinge unul dintre scopurile menționate mai sus, este posibil ca datele dvs. personale să fie transferate în țări din afara Spațiului Economic European (SEE).
Inainte de a transfera Datele dumneavoastra cu Caracter Personal in afara SEE, vom lua masuri pentru a ne asigura ca respectivele date vor beneficia de acelasi nivel de protectie ca cel prevazut de legile aplicabile privind protectia datelor din SEE.
Pentru transferurile de date in afara SEE:

- folosim, daca este cazul, garantiile aplicabile, inclusiv clauzele contractuale standard adoptate de Comisia Europeana pentru a se asigura că această terță parte oferă garanții adecvate cu privire la nivelul de protecție a datelor personale;
- informam în mod corespunzător persoana vizată
- asigurăm punerea în executare a drepturilor persoanelor vizate;
- și vă oferă remedii legale efective
- furnizam o copie a datelor transferate acestor terțe părți, la cererea persoanei vizate

17. ORGANIZARE SI RESPONSABILITATI

Responsabilitatea privind asigurarea unei prelucrări adecvate a datelor cu caracter personal este obligația oricărei persoane care lucrează pentru sau cu Securitas și care are acces la datele cu caracter personal prelucrate de companie.

Guvernarea/Administrarea datelor

Securitas Romania va vea o structură solidă și conformă de guvernanță a datelor. O astfel de structură de guvernanță a datelor trebuie să includă cel puțin următoarele roluri;

Operator date cu caracter personal – responsabilitati conform Regulamentul (UE) 2016/679 GDPR

Persoana Imputernicita de Operator (Imputernicit) - responsabilitati conform Regulamentul (UE) 2016/679 GDPR

Responsabilul cu Protectia Datelor/DPO este responsabil pentru

- dezvoltarea și promovarea politicilor relative protecției datelor cu caracter personal.
- monitorizarea respectării Regulamentul (UE) 2016/679 GDPR, a altor dispozitii legale si de reglementare referitoare la protecția datelor și a politicilor operatorului sau ale persoanei împuternicite de operator în ceea ce privește protecția datelor cu caracter personal
- Responsabilul cu Protecția Datelor cu Consilierul Juridic, monitorizează și analizează legile relative protecției datelor cu caracter personal precum și orice modificări ale acestora, dezvoltă planuri de conformitate și asistă departamentele de afaceri în vederea atingerii obiectivelor privind datele cu caracter personal.
- organizarea de traininguri privind protecția datelor cu caracter personal pentru toți angajații care lucrează cu date cu caracter personal,
- asumarea rolului de punct de contact pentru Autoritatea Nationala de Supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă, precum și, dacă este cazul, consultarea cu privire la orice altă chestiune.
- Responsabil Securitatea Informatiei/Managerul IT este responsabil pentru:
- Implementeaza cerințele Politicii de securitate a informatiei
- Se asigura că masurile de securitate sunt implementate și documentate
- asigurarea faptului că toate sistemele, serviciile și echipamentele folosite pentru stocarea datelor cu caracter personal sunt conforme cu standarde adecvate aferente.
- efectuează verificări și scanări periodice pentru a se asigura că securitatea hardware-ului și software-ului funcționează corect.

Directorul General este responsabil pentru:

- aprobarea oricărei declarații privind protecția datelor cu caracter personal atașată comunicărilor de timp e-mail sau scrisori,
- abordarea oricărei cereri privind protecția datelor cu caracter personal primite de la jurnaliști / ziariști, acolo unde este cazul, colaborează cu Responsabilul cu Protecția Datelor pentru a se asigura că inițiativele de marketing respectă principiile privind protecția datelor cu caracter personal,
- îmbunătățirea gradului de conștientizare a importanței datelor cu caracter personal ale Persoanelor Vizate,
- asigurarea protecției datelor cu caracter personal ale angajaților. Se va asigura asupra faptului că datele cu caracter personal ale angajaților sunt prelucrate în conformitate cu necesitățile și interesele legitime rezultate din raporturile contractuale dintre părți.
- transmiterea responsabilităților privind protecția datelor cu caracter personal către furnizori și îmbunătățirea gradului de conștientizare al acestora precum și transmiterea cerințelor relative protecției datelor cu caracter personal către orice terță parte contractată de furnizor.

Managerii de Departamente/Area Manageri au urmatoarele responsabilitati

- Stabilesc regulile pentru utilizarea adecvată și protecția datelor
- Furnizeaza informații proprietarilor de sistem cu privire la cerințele si masurile de securitate pentru sistemul (sistemele) de informații în care se află informațiile
- Decide cine are acces la date și ce tipuri de privilegii sau drepturi de acces vor fi acordate
- Asista la identificarea și evaluarea masurilor de securitate pentru locul în care se află informațiile
- Asigura că datele cu caracter personal sunt prelucrate din motive legale și în conformitate cu principiile GDPR
- Definiste perioadele adecvate de păstrare a datelor împreună cu proprietarul sistemului

- Informeaza DPO despre activitățile de prelucrare și solicita consultări atunci când este necesar

Angajatii
Un angajat are principalele responsabilități;

- Sa fie constient de importanta protectiei datelor și sa respecte toate politicile relevante pentru rolul lor privind confidentialitatea si securitatea datelor companiei,
- Raporteaza orice incidente de securitate ori scurgeri de informatii reale sau potențiale
- Contribuie la evaluarea impactului datelor, acolo unde este necesar

18. CONTROLUL PROTECTIEI DATELOR

Respectarea politicii de protecție a datelor și a legilor aplicabile privind protecția datelor este verificată în mod regulat prin intermediul auditurilor de protecție a datelor precum și al altor controale. Realizarea acestor controale este responsabilitatea responsabilului cu protecția datelor, a coordonatorilor de protecție a datelor și a altor unități ale grupului cu drepturi de audit sau a auditorilor externi angajați.
Rezultatele controalelor privind protecția datelor sunt raportate responsabilului cu protecția datelor. Managementul Securitas Services Romania este informat despre rezultatele primare ca parte a sarcinilor de raportare ale responsabilului cu protectia datelor cu caracter personal. La cerere, rezultatele controalelor privind protecția datelor vor fi puse la dispoziția autorității responsabile de protecția datelor. Autoritatea responsabilă cu protecția datelor poate efectua propriile controale de conformitate cu reglementările din această politică, conform legislației naționale.
In completare a celor expuse mai sus, Securitas Services Romania detine o certificare a Sistemului de Management al Securității Informației conform standardului ISO/IEC 27001:2013 si este auditata periodic

19. RASPUNS LA INCIDENTE DE SECURITATE A DATELOR

Toți angajații sunt obligati să informeze fara intarziere superiorul sau ori Responsabilul cu Protectia Datelor (DPO) cu privire la cazurile de încălcare a securitatii datelor sau alte reglementări privind protecția datelor cu caracter personal (incidente de protecție a datelor), indiferent dacă este vorba despre o încalcare a confidentialității, a integrității datelor sau a disponibilității acestora.
In cazul in care Securitas are rolul de Imputernicit al Operatorului Responsabilul cu Protectia Datelor (DPO) cand a luat la cunostinta despre producerea unui incident de securitate referitoare la datele Operatorului va informa in maxim 24 ore reprezentantul desemnat al Operatorului cu privire la incidentul de securitate produs privind protectia datelor

Atunci când Securitas află despre o încălcare a securității datelor cu caracter personal sau are suspiciuni rezonabile în privința unei asemenea încălcări, Responsabilul cu Protecția Datelor va efectua o investigație internă și va întreprinde măsuri de remediere adecvate în timp util. Atunci când există riscuri cu privire la drepturile și libertățile Persoanelor Vizate, Securitas va notifica Autoritatea Nationala de Supraveghere fără întârziere și, atunci când este posibil, în termen de maximum 72 de ore.

Aspecte privind stabilirea Autorității de Supraveghere competente

Sediul principal al Securitas Services Romania este stabilit în București. În consecinta, indifferent daca Securitas acționează în calitate de Operator sau în calitate de Împuternicit, Autoritatea de Supraveghere competentă este Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal.
Datele de contact sunt:
Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal
B-dul G-ral. Gheorghe Magheru 28-30
Sector 1, cod postal 010336 Bucuresti, Romania
anspdcp@dataprotection.ro

Responsabil Protectia Datelor/DPO pentru Securitas poate fi contactat la:

Securitas Services Romania SRL - in atentia Responsabilului cu Protectia Datelor/DPO

Sos. Bucuresti-Ploiesti nr.42-44, Cladirea A, Aripa A1, Etaj 2, Sector 1, 013696 Bucuresti
Telefon: 0743 057 052; email: dpo@securitas.com.ro

20. AUDIT și RESPONSABILITATI

Responsabilul cu Protecția Datelor este obligat să auditeze gradul și modul de implementare a prezentei Politici. Orice angajat care încalcă această Politică va fi supus unor măsuri disciplinare precum și va putea fi responsabil pentru orice prejudicii de natură civilă sau penală dacă din conduita acestuia rezultă încălcarea legilor relative protecției datelor cu caracter personal sau Regulamentului (UE) 2016/679 GDPR.

21. APLICABILITATE

Această Politică de Protectie a Datelor se aplică tuturor angajaților și directorilor companiilor din cadrul companiei Securitas, adică companiile în care Securitas AB (public.) deține direct sau indirect controlul. Această Politică de Protectie a datelor va fi comunicată și pusă în aplicare, în cea mai mare măsură posibila, în toate parteneriatele de afaceri (clienti, furnizori, subcontractori) și în relațiile contractuale de consultanță

22. MONITORIZARE

Respectarea acestei Politici de confidențialitate de către companiile (entitățile) și angajații Securitas va fi monitorizată ca parte a procesului de gestionare a riscurilor - Securitas Enterprise Risk Management (ERM), care include autoevaluări, audituri interne și externe și monitorizări de rutină ale tuturor problemelor raportate.

23. TRAINING

Este responsabilitatea Securitas să se asigure că este furnizată o instruire adecvată tuturor angajaților care gestioneaza de date cu caracter personal. Responsabil Protectia Datelor/DPO ar trebui să contribuie la dezvoltarea și, după caz, la implementarea unei astfel de instruiri
========== // ==========