Politica GDPR de Protecție a Datelor cu Caracter Personal

Securitas Services România S.R.L.

Cod: **POL-GDPR-01**
Ediţia: **2.0**
Data aplicării: **01.07.2026**

1. Introducere

Securitas Services România S.R.L., denumită în continuare**„Securitas România”** sau **„Securitas”**, are ca prioritate respectarea legislației aplicabile în materia protecției datelor cu caracter personal, a confidențialității și a securității informațiilor, în desfășurarea activităților sale și în furnizarea serviciilor de securitate.

În conformitate cu Regulamentul (UE) 2016/679, denumit în continuare **GDPR**, Securitas prelucrează date cu caracter personal în scopuri determinate, explicite și legitime, cu respectarea principiilor aplicabile privind protecția datelor. Prelucrarea datelor cu caracter personal poate fi realizată prin mijloace manuale, electronice sau mixte, cu aplicarea măsurilor tehnice și organizatorice necesare pentru protejarea datelor, asigurarea confidențialității și respectarea drepturilor persoanelor vizate.

În România, rolul de autoritate națională de supraveghere este asumat de către **Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)**.

2. Scop

Prezenta politică stabilește cadrul general local privind protecția datelor cu caracter personal în cadrul Securitas România. Politica reglementează principiile esențiale care stau la baza prelucrării datelor cu caracter personal ale angajaților, candidaților, foștilor angajați, clienților, furnizorilor, partenerilor de afaceri, vizitatorilor și altor persoane vizate ale căror date sunt prelucrate de către companie.

Politica stabilește responsabilitățile generale ale departamentelor interne, managerilor, angajaților și altor persoane care acționează pentru sau în numele Securitas în legătură cu prelucrarea datelor cu caracter personal. Aceasta exprimă angajamentul Securitas de a se asigura că orice prelucrare de date cu caracter personal, inclusiv categorii speciale de date, se realizează în conformitate cu legislația aplicabilă, politicile Grupului Securitas și documentele interne relevante.

Prezenta politică se aplică tuturor activităților de prelucrare desfășurate de Securitas, indiferent dacă datele sunt prelucrate în format fizic, electronic sau mixt și indiferent dacă Securitas acționează în calitate de operator, operator asociat sau persoană împuternicită de operator.

Politica se aplică Securitas Services România S.R.L. și, după caz, altor entități locale ale Grupului Securitas care aplică prezentul cadru local, în măsura în care acestea desfășoară activități în Spațiul Economic European sau prelucrează date cu caracter personal ale persoanelor vizate din Spațiul Economic European.

3. Definiții

Definitile termenilor folositi în prezenta Politica au întelesul redat în art. 4 din Regulament, dupa cum urmeaza:

1. „**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;

2. „**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, înregis trarea, 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;

3. „**restricționarea prelucrării**” înseamnă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;

4. „**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;

5. „**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;

6. „**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;

7. „**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;

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

9. „**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;

10. „**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;

11. „**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;

12. „**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;

13. „**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;

14. „**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;

15. „**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;

16. „**sediu principal**” înseamnă:

    a. în cazul unui operator cu sedii în cel puțin două state membre, locul în care se află administrația centrală a acestuia în Uniune, cu excepția cazului în care deciziile privind scopurile și mijloacele de prelucrare a datelor cu caracter personal se iau într-un alt sediu al operatorului din Uniune, sediu care are competența de a dispune punerea în aplicare a acestor decizii, caz în care sediul care a luat deciziile respective este considerat a fi sediul principal;

    b. în cazul unei persoane împuternicite de operator cu sedii în cel puțin două state membre, locul în care se află administrația centrală a acesteia în Uniune, sau, în cazul în care persoana împuternicită de operator nu are o administrație centrală în Uniune, sediul din Uniune al persoanei împuternicite de operator în care au loc activitățile principale de prelucrare, în contextul activităților unui sediu al persoanei împuternicite de operator, în măsura în care aceasta este supusă unor obligații specifice în temeiul

prezentului regulament;

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

18. „**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;

19. „**grup de întreprinderi**” înseamnă o întreprindere care exercită controlul și întreprinderile controlate de aceasta;

20. „**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;

21. „**autoritate de supraveghere**” înseamnă o autoritate publică independentă instituită de un stat membru în temeiul articolului 51; În România, acest rol este asumat de către **Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)**.

22. „**autoritate de supraveghere vizată**” înseamnă o autoritate de supraveghere care este vizată de procesul de prelucrare a datelor cu caracter personal deoarece:

    a. operatorul sau persoana împuternicită de operator este stabilită pe teritoriul statului membru al autorității de supraveghere respective;

    b. persoanele vizate care își au reședința în statul membru în care se află autoritatea de supraveghere respectivă sunt afectate în mod semnificativ sau sunt susceptibile de a fi afectate în mod semnificativ de prelucrare; sau

    c. la autoritatea de supraveghere respectivă a fost depusă o plângere;

23. „**prelucrare transfrontalieră**” înseamnă:

    a. fie prelucrarea datelor cu caracter personal care are loc în contextul activităților sediilor din mai multe state membre ale unui operator sau ale unei persoane împuternicite de operator pe teritoriul Uniunii, dacă operatorul sau persoana împuternicită de operator are sedii în cel puțin două state membre; sau

    b. fie prelucrarea datelor cu caracter personal care are loc în contextul activităților unui singur sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, dar care afectează în mod semnificativ sau este susceptibilă de a afecta în mod semnificativ persoane vizate din cel puțin două state membre;

24. „**obiecție relevantă și motivată**” înseamnă o obiecție la un proiect de decizie în scopul de a stabili dacă există o încălcare a prezentului regulament sau dacă măsurile preconizate în ceea ce privește operatorul sau persoana împuternicită de operator respectă prezentul regulament, care demonstrează în mod clar importanța riscurilor pe care le prezintă proiectul de decizie în ceea ce privește drepturile și libertățile fundamentale ale persoanelor vizate și, după caz, libera circulație a datelor cu caracter personal în cadrul Uniunii;

25. **„serviciile societății informaționale”** înseamnă un serviciu astfel cum este definit la articolul 1 alineatul (1) litera (b) din Directiva 98/34/CE a Parlamentului European și a Consiliului (1);

26. **„organizație internațională”** înseamnă o organizație și organismele sale subordonate reglementate de dreptul interna țional public sau orice alt organism care este instituit printr-un acord încheiat între două sau mai multe țări sau în temeiul unui astfel de acord.

4. Principiile de bază privind prelucrarea datelor cu caracter personal

Principiile privind protecția datelor cu caracter personal reflectă responsabilitățile de bază ale Securitas Services România S.R.L. în legătură cu prelucrarea acestor date. Potrivit art. 5 alin. (2) din GDPR, Securitas, în calitate de operator de date, este responsabilă de respectarea acestor principii și trebuie să poată demonstra conformitatea cu acestea.

a) Legalitate, echitate și transparență
Datele cu caracter personal trebuie prelucrate în mod legal, echitabil și transparent față de persoana vizată.

b) Limitări legate de scop
Datele cu caracter personal trebuie colectate în scopuri determinate, explicite și legitime, iar prelucrările ulterioare nu trebuie să fie incompatibile cu aceste scopuri.

c) Reducerea la minimum a datelor
Orice colectare de date cu caracter personal trebuie analizată înainte de obținerea efectivă a datelor. Datele colectate trebuie să fie adecvate, relevante și strict limitate la ceea ce este necesar pentru scopurile în care sunt prelucrate.
d) Exactitatea informațiilor
Trebuie luate măsuri rezonabile pentru a asigura exactitatea și actualitatea datelor cu caracter personal. Datele care se dovedesc a fi inexacte trebuie actualizate sau șterse fără întârzieri nejustificate.

e) Limitarea stocării
Datele cu caracter personal trebuie păstrate numai pe durata necesară îndeplinirii scopurilor pentru care sunt prelucrate sau pe durata impusă de cerințele legale, contractuale, arhivistice ori de apărare a drepturilor companiei. Păstrarea datelor pentru perioade mai lungi trebuie justificată printr-un temei aplicabil.

f) Integritate și confidențialitate
Datele cu caracter personal trebuie prelucrate în condiții care asigură securitatea adecvată a acestora, inclusiv protecția împotriva prelucrării neautorizate sau ilegale, împotriva pierderii, distrugerii ori deteriorării accidentale, prin aplicarea unor măsuri tehnice și organizatorice corespunzătoare.

Responsabilitate
Securitas Services România S.R.L., în calitate de operator de date cu caracter personal, este responsabilă de respectarea principiilor menționate mai sus și trebuie să poată demonstra conformitatea cu acestea. Conformitatea se realizează prin implementarea prezentei politici, respectarea politicilor și procedurilor interne aplicabile, aplicarea unor măsuri tehnice și organizatorice adecvate, protecția datelor prin design și implicit, efectuarea evaluărilor de impact atunci când este cazul, gestionarea incidentelor de securitate și aplicarea procedurilor privind notificarea încălcărilor de date cu caracter personal.

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 obțină de la Securitas următoarele informații:

i. identitatea și datele de contact ale Securitas / ale reprezentanților și ale responsabilului cu
protecția datelor;

ii. scopurile și 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 țări terțe sau organizații
internaționale, dacă există, și referirea la garanțiile și mijloacele corespunzătoare;

v. perioada de stocare a datelor cu caracter personal și criteriile folosite pentru a determina acea perioadă, sub rezerva că Securiats România păstrează și prelucrează datele cu caracter personal atâta timp cât legile și reglementările legale impun acest lucru. Prelucrarea datelor cu caracter personal încetează imediat dacă 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 obținute de la persoana vizată;

- **Dreptul de acces la datele cu caracter personal** să obțină de la Securitas România confirmarea dacă datele cu caracter personal sunt prelucrate sau și dreptul de a primi o copie a oricărei înregistrări care conține datele sale cu caracter personal;

- **Dreptul la rectificare** să obțină de la Securitas România 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 declarații suplimentare;

- **Dreptul la ștergerea datelor** ("dreptul de a fi uitat") să obțină de la Securitas ștergerea 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 își retrage consimțământul; datele cu caracter personal au fost prelucrate ilegal etc.;

- **Dreptul la restricționarea prelucrării** - dacă datele cu caracter personal sunt inexacte; prelucrarea este ilegală și persoana vizată solicită restricționarea utilizării datelor cu caracter personal în locul ștergerii lor; datele cu caracter personal nu mai sunt necesare în scopul prelucrării, dar ele sunt solicitate pentru constatarea, exercitarea sau apărarea unui drept în instanță; 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 și care poate fi citit automat și are dreptul de a transmite aceste date cu caracter personal unui alt operator fără obstacole din partea Securitas, dacă prelucrarea se bazează pe consimțământ 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 dispoziții și au fost date cu caracter personal prelucrate în scopuri de marketing direct;

- **Dreptul la retragerea consimțământului** - în orice moment fără a afecta legalitatea prelucrării bazate pe consimțământ, înainte de retragerea sa. Astfel persoana vizată înțelege și este de acord că, în cazul retragerii, nu se poate ajunge la scopul prelucrării datelor cu caracter personal și 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, Autorității Naționale 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 legislație în domeniu și 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 în scris folosind următoarele date de contact:

SECURITAS SERVICES ROMÂNIA S.R.L. - în atenția Responsabil Protecția Datelor/DPO
Bulevardul Expoziției, Clădirea B2, Etaj 7, Sector 1, București, Cod Poștal 012101.
Tel: +40 743 162 007
E-mail: dpo@securitas.com.ro

6. Prelucrarea Justă și Transparentă 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 inițial și doar la autorizarea 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 înainte de colectarea datelor cu caracter personal pentru orice tip de procesare, incluzând, dar fără a se limita la vânzarea 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 transferului internațional 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. Persoane Vizate

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

- angajații, membrii familiilor angajaților, foști angajați;
- 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;
- reprezentanți ai autorităților, instituțiilor publice și mass-media;
- persoane ce accesează 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 marcă, ID card acces;
- date de identificare informatice: adresă IP, nume de utilizator, parolă;
- date privind persoana: data și locul nașterii, sex, cetățenie, stare civilă, semnătură;
- date de contact: adresa de domiciliu/reședință, adresa de e-mail, număr de telefon fix/mobil;
- date de recrutare și angajare: date conținute în CV-uri, recomandări, carnet muncă sau echivalent, cazier judiciar, date privind starea de sănătate;
- date financiare: număr cont bancar și alte informații financiare;
- date biometrice: voce, imagine;
- date colectate cu ocazia înregistrării și participării la evenimentele organizate sau sprijinite de către Securitas, fotografii, video, citate, postări pe rețele sociale etc.

9. Scopul Prelucrării Datelor cu Caracter Personal

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

- pentru furnizarea produselor și serviciilor noastre de protecție, în baza contractelor încheiate cu clienții;
- pentru îmbunătățirea serviciilor și produselor noastre;
- pentru administrarea furnizorilor și subcontractorilor;
- pentru administrarea și conducerea personalului;

- pentru administrarea clienților, de exemplu pentru a răspunde la solicitări sau întrebări din partea clienților, la anchete privind satisfacția clienților sau pentru a gestiona reclamațiile privind un anumit produs sau serviciu;
- pentru gestionarea relațiilor comerciale cu terțe părți;
- pentru monitorizarea / securitatea persoanelor, spațiilor și / sau bunurilor publice / private, în vederea asigurării pazei și protecției în locațiile Securitas;
- în scopuri administrative în cadrul Grupului Securitas;
- pentru backup sau arhivare;
- pentru gestionarea disputelor / litigiilor;
- pentru îndeplinirea obligațiilor legale.

10. Temei Juridic pentru Prelucrarea Datelor Personale

Securitas prelucrează datele cu caracter personal în conformitate cu prevederile Regulamentului (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestora.

Prelucrarea datelor cu caracter personal intervine în următoarele situații:

Respectarea unei obligații legale - prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi 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 în legătură cu 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 și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal. În această categorie pot intra îndeplinirea obiectivelor de comunicare și diseminare, procesul de recrutare și resurse umane, precum și asigurarea securității persoanelor, bunurilor și operațiunilor Securitas.

Consimțământ - 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, fie printr-o acțiune 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 vizată și / sau reprezentanții săi legali, angajații Securitas, parteneri contractuali și împuterniciți ai Securitas, autorități judecătorești și alte autorități publice, companii ale Grupului Securitas, societăți de asigurare, organizații profesionale naționale sau internaționale, organizații de cercetare a pieței.

12. Durata Prelucrării Datelor

Securitas se angajează să respecte principiul limitării păstrării datelor personale. În această perspectivă, nu vom păstra / reține datele personale mai mult decât este necesar pentru

îndeplinirea contractelor noastre și / sau pentru realizarea unuia dintre celelalte scopuri menționate anterior.

Securitas poate, de asemenea, să fie obligată din punct de vedere legal să păstreze datele personale pentru o perioadă minimă de timp, pentru a se conforma cerințelor legale.

Vom păstra datele personale în baza Nomenclatorului Arhivistic propriu, întocmit conform Legii Arhivelor Naționale nr. 16/1996, cu modificările și completările ulterioare, precum și a instrucțiunilor 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 anonimiza.

13. Securitatea Datelor

Securitas acordă o importanță deosebită protecției datelor dumneavoastră cu caracter personal și, în consecință, a implementat măsuri tehnice și organizatorice adecvate, care sunt revizuite și adaptate periodic pentru protejarea acestora împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii ori accesului ilicit sau neautorizat.
Printre aceste măsuri se numără:

- implementarea și revizuirea periodică a politicilor, procedurilor și instrucțiunilor de lucru destinate securizării prelucrării datelor cu caracter personal;
- instruirea periodică și sistematică a tuturor angajaților care prelucrează date cu caracter personal;
- limitarea accesului la datele cu caracter personal în conformitate cu principiile din politica generală de securitate, precum „nevoia de a ști” și „nevoia de a vedea”;
- accesul securizat la aplicațiile și fișierele care conțin date cu caracter personal;
- implementarea unor soluții tehnice pentru securizarea comunicațiilor care includ date cu caracter personal;
- monitorizarea proceselor de transfer al datelor cu caracter personal, prin serviciul de e-mail, copiere pe suport extern, tipărire, scanare etc., și blocarea tentativelor de transfer neautorizate;
- implementarea unor soluții tehnice pentru asigurarea disponibilității datelor cu caracter personal în sistemele informatice utilizate;
- criptarea comunicărilor ce conțin date cu caracter personal.

14. Confidențialitatea Prelucrării

Datele personale sunt considerate informații confidențiale și 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 confidențială și va fi efectuată numai de persoanele care acționează sub autoritatea Securitas și numai pe baza instrucțiunilor acesteia.

Orice prelucrare de date efectuată de un angajat, care nu a fost autorizată să fie desfășurată ca parte a îndatoririlor sale legitime de serviciu, este considerată ca fiind neautorizată. Întotdeauna se aplică principiul „necesitatea de a cunoaște”. Angajații pot avea acces la informații personale în funcție de adecvarea acestui acces la tipurile de date și de scopul determinat. Acest lucru se bazează pe stabilirea și separarea atentă a atribuțiilor angajaților 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. În cazul utilizării neautorizate a datelor personale, angajații pot fi sancționați în conformitate cu legislația aplicabilă și cu reglementările în vigoare în 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 și Împuternicit

Responsabilitate

Atunci când Securitas prelucrează date cu caracter personal, aceasta acționează fie ca operator de date, fie ca împuternicit. 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 împuternicit în legătură cu prelucrarea de date respectivă.

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 Protecția 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 împuternicit, conform art. 28 GDPR.

Securitas, atunci când acționează ca operator, se va asigura că împuterniciții săi 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, când acționează ca împuternicit, 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 prelucrează datele cu caracter personal în numele Securitas, Responsabilul cu Protecția Datelor trebuie să se asigure că împuternicitul 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 prelucrează 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 România trebuie să țină o evidență / registru al activităților sale de prelucrare a datelor cu caracter personal. Conținutul unei astfel de înregistrări / evidențe trebuie să respecte prevederile Regulamentului General de Protecția 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 România 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 luată 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 în Afara Spațiului Economic European

Securitas va încerca mereu să proceseze datele personale în cadrul Spațiului Economic European (SEE). Totuși, 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). Înainte de a transfera datele dumneavoastră cu caracter personal în afara SEE, vom lua măsuri pentru a ne asigura că respectivele date vor beneficia de același nivel de protecție ca cel prevăzut de legile aplicabile privind protecția datelor din SEE.

Pentru transferurile de date în afara SEE:

- folosim, dacă este cazul, garanțiile aplicabile, inclusiv clauzele contractuale standard adoptate de Comisia Europeană, pentru a ne asigura că această terță parte oferă garanții adecvate cu privire la nivelul de protecție a datelor personale;
- informăm în mod corespunzător persoana vizată;
- asigurăm punerea în executare a drepturilor persoanelor vizate;
- vă oferim remedii legale efective;
- furnizăm o copie a datelor transferate acestor terțe părți, la cererea persoanei vizate.

17. Organizare și Responsabilități

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 România va avea 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 de date cu caracter personal - responsabilități conform Regulamentului (UE) 2016/679 GDPR;
- Persoană împuternicită de operator, Împuternicit - responsabilități conform Regulamentului (UE) 2016/679 GDPR.

Responsabilul cu Protecția Datelor / DPO este responsabil pentru:

- dezvoltarea și promovarea politicilor relative protecției datelor cu caracter personal;
- monitorizarea respectării Regulamentului (UE) 2016/679 GDPR, a altor dispoziții legale și 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;
- monitorizarea și analizarea, împreună cu Consilierul Juridic, a legilor relative protecției datelor cu caracter personal, precum și a oricăror modificări ale acestora, dezvoltarea planurilor de conformitate și asistarea departamentelor 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 Națională de Supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă, precum și, dacă este cazul, consultarea cu privire la orice altă chestiune.

Responsabilul Securitatea Informației / Managerul IT este responsabil pentru:

- implementarea cerințelor Politicii de securitate a informației;
- asigurarea faptului că măsurile de securitate sunt implementate și documentate;
- asigurarea faptului că toate sistemele, serviciile și echipamentele folosite pentru stocarea datelor cu caracter personal sunt conforme cu standardele adecvate aferente;
- efectuarea de 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 tip e-mail sau scrisori;
- abordarea oricărei cereri privind protecția datelor cu caracter personal primite de la jurnaliști / ziariști, acolo unde este cazul;
- colaborarea 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 Managerii au următoarele responsabilități:

- stabilesc regulile pentru utilizarea adecvată și protecția datelor;
- furnizează informații proprietarilor de sistem cu privire la cerințele și măsurile de securitate pentru sistemul / sistemele de informații în care se află informațiile;
- decid cine are acces la date și ce tipuri de privilegii sau drepturi de acces vor fi acordate;
- asistă la identificarea și evaluarea măsurilor de securitate pentru locul în care se află informațiile;
- asigură că datele cu caracter personal sunt prelucrate din motive legale și în conformitate cu principiile GDPR;
- definesc perioadele adecvate de păstrare a datelor împreună cu proprietarul sistemului;
- informează DPO despre activitățile de prelucrare și solicită consultări atunci când este necesar.

Angajații

Un angajat are următoarele responsabilități principale:

- să fie conștient de importanța protecției datelor și să respecte toate politicile relevante pentru rolul său privind confidențialitatea și securitatea datelor companiei;
- să raporteze orice incidente de securitate ori scurgeri de informații reale sau potențiale;
- să contribuie la evaluarea impactului datelor, acolo unde este necesar.

18. Controlul Protecției 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 România este informat despre rezultatele principale ca parte a sarcinilor de raportare ale Responsabilului cu Protecția 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.
În completarea celor expuse mai sus, Securitas Services România deține o certificare a Sistemului de Management al Securității Informației conform standardului ISO/IEC 27001:2013 și este auditată periodic.

19. Răspuns la Incidente de Securitate A Datelor

Toți angajații sunt obligați să informeze fără întârziere superiorul direct sau Responsabilul cu Protecția Datelor (DPO) cu privire la cazurile de încălcare a securității datelor sau alte situații privind protecția datelor cu caracter personal, denumite în continuare incidente de protecție a datelor, indiferent dacă este vorba despre o încălcare a confidențialității, a integrității datelor sau a disponibilității acestora.

În cazul în care Securitas are rolul de persoană împuternicită de operator, Responsabilul cu Protecția Datelor (DPO), după ce a luat cunoștință despre producerea unui incident de securitate referitor la datele operatorului, va informa în maximum 24 de ore reprezentantul desemnat al operatorului cu privire la incidentul de securitate produs privind protecția datelor.

Atunci când Securitas află despre o încălcare a securității datelor cu caracter personal sau are suspiciuni rezonabile cu privire la o asemenea încălcare, 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 Națională 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 România este stabilit în București. În consecință, indiferent dacă Securitas acționează în calitate de operator sau în calitate de persoană împuternicită de operator, Autoritatea de Supraveghere competentă este Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal.

Datele de contact ale ANSPDCP sunt:

Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal
B-dul G-ral. Gheorghe Magheru nr. 28-30
Sector 1, cod poștal 010336
București, România
E-mail: anspdcp@dataprotection.ro

Responsabilul cu Protecția Datelor/DPO pentru Securitas poate fi contactat la:

Securitas Services România S.R.L. - În atenția Responsabilului cu Protecția Datelor/DPO
Bulevardul Expoziției, Clădirea B2, Etaj 7, Sector 1, cod poștal 012101, București, România
Telefon: +40 743 162 007
E-mail: dpo@securitas.com.ro

20. Implementare, monitorizare, instruire și responsabilitate

Prezenta Politică de Protecție a Datelor se aplică tuturor angajaților, directorilor și persoanelor care acționează pentru sau în numele Securitas, în măsura în care aceștia au acces la date cu caracter personal sau sunt implicați în activități de prelucrare. Politica va fi comunicată și pusă în aplicare, în măsura aplicabilă, și în relațiile cu partenerii de afaceri, clienții, furnizorii, subcontractorii, consultanții și alte terțe părți care prelucrează date cu caracter personal în legătură cu activitățile Securitas.

Respectarea prezentei Politici, a procedurilor interne aplicabile și a legislației privind protecția datelor este monitorizată prin mecanismele interne de control, audituri, autoevaluări, verificări periodice și alte activități de monitorizare desfășurate în cadrul companiei sau al Grupului Securitas, inclusiv prin procesul Securitas Enterprise Risk Management (ERM), acolo unde este aplicabil.

Responsabilul cu Protecția Datelor/DPO contribuie la monitorizarea gradului de implementare a prezentei Politici, la evaluarea conformității proceselor de prelucrare și la formularea

recomandărilor necesare pentru îmbunătățirea cadrului de protecție a datelor. Rezultatele relevante ale controalelor sau auditurilor pot fi raportate managementului Securitas, conform responsabilităților interne aplicabile.

Securitas se asigură că angajații care gestionează date cu caracter personal beneficiază de instruire adecvată, în funcție de rolul lor, nivelul de acces la date și riscurile asociate activității desfășurate. Responsabilul cu Protecția Datelor/DPO poate contribui la dezvoltarea, actualizarea și implementarea instruirilor privind protecția datelor cu caracter personal.

Orice încălcare a prezentei Politici, a procedurilor interne aplicabile sau a legislației privind protecția datelor poate atrage măsuri disciplinare, contractuale sau alte măsuri legale corespunzătoare. Angajații pot răspunde pentru prejudiciile de natură civilă, administrativă sau penală, în măsura în care conduita acestora determină încălcarea legislației privind protecția datelor cu caracter personal sau a Regulamentului (UE) 2016/679 GDPR.

Prezenta Politică va fi revizuită periodic, anual sau ori de câte ori apar modificări semnificative privind legislația aplicabilă, politicile Grupului Securitas, structura organizațională, sistemele utilizate, procesele de prelucrare sau riscurile relevante privind protecția datelor.