

APROB
DIRECTOR GENERAL
ANDREI FEClORU



PROCEDURA DE SISTEM PRIVIND
PRELUCRAREA DATELOR CU CARACTER PERSONAL

COD: P.S. - 43

Ediția I
Revizia 0

AVIZAT
Comp. Juridic
Canbolant Singrid

Intocmit
Insp. Mediu Jurist
Camelia Teodorescu

A handwritten signature in blue ink, likely belonging to Camelia Teodorescu, positioned below her name.

1. Cuprins:

Numărul componentei în cadrul procedurii documentate	Denumirea componentei din cadrul procedurii documentate	Pagina
1	Cuprins	2
2	Scopul procedurii	2
3.	Domeniu de aplicare	3
4.	Documente de referință	3
5.	Definiții și abrevieri	7
6.	Descrierea procedurii	8
7.	Responsabilități	18
8	Formular evidență modificări	19
9.	Formular analiză procedură	20
10	Anexe	20

2. Scopul procedurii

2.1. Prezenta procedură stabilește aplicarea **Regulamentului nr. 679/2018** 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) - (General Data Protection Regulation - GDPR).

2.2. Orice prelucrare a datelor cu caracter personal în cadrul activităților unui sediu al unui operator sau al unei persoane împuternicite de operator din Uniunea Europeană ar trebui efectuată în conformitate cu regulamentul, indiferent dacă procesul de prelucrare în sine are loc sau nu în cadrul Uniunii Europene. Sediul implică exercitarea efectivă și reală a unei activități în cadrul unor înțelegeri stabile.

2.3. Dă asigurări cu privire la existența documentației adecvate derulării activității.

3. Domeniul de aplicare

Procedura se aplică de către toate compartimentele Salubrizare Sector 5 S.A. în vederea derulării următoarelor activități:

- prelucrarea datelor cu caracter personal;
- respectarea principiilor de protecție a datelor cu caracter personal în activitățile operaționale ale companiei;
- transparența în legătură cu categoriile de date cu caracter personal prelucrate în cadrul Salubrizare Sector 5 S.A, precum și în legătură cu scopurile prelucrărilor și destinatarii datelor cu caracter personal;
- drepturile persoanelor vizate: dreptul la informare, dreptul de acces, dreptul la rectificare, dreptul la ștergerea datelor, dreptul la restricționarea prelucrării, dreptul la portabilitatea datelor, dreptul la opoziție, dreptul de a nu face obiectul unei decizii individuale bazate exclusiv pe prelucrare automată, dreptul de a depune plângere la o autoritate de supraveghere și dreptul de a se adresa justiției;
- efectuarea evaluării de impact;
- efectuarea unei centralizări a tuturor datelor care se prelucrează în companie;
- păstrarea unei evidențe a operațiunilor de prelucrare de către compartimentele companiei;
- completarea Codului de conduită cu norme adecvate pentru protecția drepturilor persoanelor ale căror date cu caracter personal pot fi prelucrate de către companie;
- elaborarea procedurii de notificare a încălcării securității datelor personale.

Organizațiile cu personalitate juridică distinctă care încheie contracte cu Salubrizare Sector 5 S.A și care prin obiectul lor presupun accesul și/sau prelucrarea datelor cu caracter personal vor avea obligativitatea semnării unei anexe distincte la contract (Anexa 7) în care se va specifica tipul de date cu caracter personal prelucrat, scopul și durata prelucrării, cât și angajamentul ca aceste date vor fi folosite strict în scopul în care au fost încredințate.

4. Documente de referință

4.1. Reglementari internaționale

❖ Regulamentul nr. 679/2016 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) - (General Data Protection Regulation - GDPR);

❖ Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului din 09.07.2008 de stabilire a cerințelor de acreditare și de supraveghere a pieței în ceea ce privește comercializarea produselor și de abrogare a Regulamentului (CEE) nr. 339/1993.

4.2. Legislație primară

❖ Legea 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date;

❖ Legea nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal;

❖ O.G. 2/2001 privind regimul juridic al contravențiilor, aprobată cu modificări și completări prin Legea 180/2002, cu modificările și completările ulterioare.

❖ Legea Arhivelor Naționale nr. 16/1996 cu modificările și completările ulterioare.

4.3. Legislație secundară

• Ordinul Secretariatului General al Guvernului nr. 600/2018 privind aprobarea Codului controlului intern managerial al entităților publice;

• Ordinul Secretariatului General al Guvernului nr. 201/2016 pentru aprobarea Normelor metodologice privind coordonarea, îndrumarea metodologică și supravegherea stadiului implementării și dezvoltării sistemului de control intern managerial la entitățile publice.

4.4. Alte documente, inclusiv reglementări interne ale societății

- Regulamentul de organizare și funcționare a Salubrizare Sector 5 S.A;
- Regulamentul intern al Salubrizare Sector 5 S.A;
- Codul de conduită al Salubrizare Sector 5 S.A

5. Definiții, abrevieri și termeni utilizați

5.1. Definiții

Nr. crt.	Termenul	Definiția și/sau, dacă este cazul, actul care definește termenul
1	Date cu caracter personal	Reprezintă 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-prenume, un număr de identificare, date de localizare, un identificator online, unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.
2	Prelucrarea datelor cu caracter personal	Reprezintă 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.
3	Operator	Înseamnă persoana fizică sau juridică, autoritatea publică, 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.

4	Destinatar	Înseamnă persoana fizică sau juridică, autoritatea publică sau alt organism 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.
5	Persoană împuternicită de operator/instituție	Înseamnă persoana fizică sau juridică, autoritatea publică sau alt organism care prelucrează datele cu caracter personal în numele operatorului/instituției.
6	DPO	Data Protection Officer - reprezintă persoana desemnată de operator/instituție, responsabilă cu prelucrarea datelor cu caracter personal.
7	Sistem de evidență a datelor cu caracter personal	Orice structură organizată de date cu caracter personal, accesibilă potrivit unor criterii determinate, indiferent dacă această structură este organizată în mod centralizat ori descentralizat sau este repartizată după criterii funcționale ori geografice.
8	Consimțământul 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. <i>Salariații instituției, petiționari, colaboratori</i>
9	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.
10	Date biometrice	Înseamnă 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.
11	Autoritate de supraveghere	Înseamnă o autoritate publică independentă instituită de un stat membru în temeiul articolului 51 din RGPD.

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	Activitate	Totalitatea atribuțiilor de o anumită natură care determină procese de muncă cu un grad de omogenitate și similaritate ridicat; cunoștințele necesare realizării activității sunt din domenii limitate, personalul utilizat putând avea astfel o pregătire profesională sensibil unitară; activitatea cuprinde atribuții omogene ce revin compartimentelor entității publice.
14	Activitatea procedurabila	Totalitatea atribuțiilor de o anumită natură care determină procese de muncă cu un grad de complexitate și omogenitate ridicat, pentru care se pot stabili reguli și modalități de lucru, general valabile, în vederea îndeplinirii, în condiții de regularitate, eficacitate, economicitate și eficiență, a obiectivelor compartimentului/entității publice
15	Atribuție	Un ansamblu de sarcini de același tip, necesare pentru realizarea unei anumite activități sau unei părți a acesteia, care se execută periodic sau continuu și care implică cunoștințe specializate pentru realizarea unui obiectiv specific.
16	Ediție a unei proceduri..de sistem	Forma inițială sau actualizată, după caz, a unei proceduri documentate aprobată și difuzată.
17	Proces	Un flux de activități sau o succesiune de activități logic structurate, organizate în scopul atingerii unor obiective definite, care utilizează resurse, adaugându-le valoare.
18	Gestionarea documentelor	Procesul de administrare a documentelor unei entități publice, pentru a servi intereselor acesteia, pe parcursul întregii lor durate de viață, de la început, prin procesul de creare, revizuire, organizare, stocare, utilizare, partajare, identificare, arhivare, și până la distrugerea lor.
19	Consultarea prealabilă	Operatorul consultă autoritatea de supraveghere înainte de prelucrare atunci când evaluarea impactului asupra protecției datelor prevăzută la art. 35, din GDPR, indică faptul că prelucrarea ar genera un risc ridicat în absența unor măsuri luate de operator pentru atenuarea riscului.

20	Cookie	<p>Cookie-ul http sau un modul cookie este un text special, deseori codificat, trimis de un server unui navigator web și apoi trimis înapoi (nemodificat) de către navigator, de fiecare dată când accesează acel server. Cookie-urile sunt folosite pentru autentificare precum și pentru urmărirea comportamentului utilizatorilor; aplicații tipice sunt reținerea preferințelor utilizatorilor. În realitate ele sunt doar texte, și nu pot să execute nicio operație. Ele nu sunt nici spyware și nici viruși informatici.</p>
----	---------------	---

5.2. Abrevieri

Nr. crt.	Abrevierea	Termenul abreviat
1.	S 5 S.A.	Salubritate Sector 5 S.A.
2.	DG	Director General
3.	PS	Procedura de sistem
4.	PO	Procedură operațională
5.	CM	Comisia de monitorizare
6.	DCP	Date cu caracter personal
7.	E	Elaborare
8.	V	Verificare
9.	A	Aprobare
10.	Ap	Aplicare
11.	Ah	Arhivare
12.	GDPR	General Data Protection Regulation - Regulamentul (UE) nr. 679/2016
13.	RGPD	Regulamentul General privind Protecția Datelor cu caracter personal
14.	DPO	Data Protection Officer - Responsabil cu protecția datelor
15.	O.U.G.	Ordonanța de Urgență a Guvernului
16.	O.G.	Ordonanță a Guvernului
17.	S.C.I.M.	Sistemul de control intern managerial
18.	ANSPDCP	Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal

6. Descrierea procedurii

Procedura se aplică în cadrul Salubritate Sector 5 S.A și face referire la prelucrarea datelor cu caracter personal efectuate, în tot sau în parte, prin mijloace automate, precum și prelucrarea prin alte mijloace decât cele automate a datelor cu caracter personal, care fac parte dintr-un sistem de evidență sau care sunt destinate să fie incluse într-un asemenea sistem.

Prelucrarea datelor cu caracter personal se va face ținând cont de următoarele:

- prelucrare cu bună-credință și în conformitate cu dispozițiile legale în vigoare;
- colectarea în scopuri determinate, explicite și legitime; prelucrarea ulterioară a datelor cu caracter personal în scopuri statistice, de cercetare istorică sau științifică nu va fi considerată incompatibilă cu scopul colectării dacă se efectuează cu respectarea dispozițiilor prezentei legi, inclusiv a celor care privesc efectuarea notificării către autoritatea de supraveghere, precum și cu respectarea garanțiilor privind prelucrarea datelor cu caracter personal, prevăzute de normele care reglementează activitatea statistică ori cercetarea istorică sau științifică;
- datele trebuie să fie adecvate, pertinente și neexcesive prin raportare la scopul în care sunt colectate și ulterior prelucrate;
- să fie exacte și, dacă este cazul, actualizate; în acest scop se vor lua măsurile necesare pentru ca datele inexacte sau incomplete din punct de vedere al scopului pentru care sunt colectate și pentru care vor fi ulterior prelucrate, să fie șterse sau rectificate;
- stocarea datelor într-o formă în care să se permită identificarea persoanelor vizate (personalul salariat, petiționarii, colaboratorii, după caz) strict pe durata necesară realizării scopurilor în care datele sunt colectate și în care vor fi ulterior prelucrate; stocarea datelor pe o durată mai mare de timp decât cea menționată, în scopuri statistice, de cercetare istorică sau științifică, se va face cu respectarea garanțiilor privind prelucrarea datelor cu caracter personal, prevăzute în normele care reglementează aceste domenii, și numai pentru perioada necesară realizării acestor scopuri.

6.1. Responsabilul cu protecția datelor (DPO - "Data Protection Officer")

Numirea responsabilului cu protecția datelor cu caracter personal trebuie să respecte următoarele cerințe:

- *Criteriul competenței profesionale*, conform art. 37 alin 5 din Regulament. În mod special se va ține cont de cunoștințele sale de specialitate, de practică în domeniul protecției datelor personale, precum și de capacitatea de a îndeplini sarcinile care îi revin. Considerentul 97, precizează că nivelul necesar al cunoștințelor de specialitate va fi apreciat, în mod particular, în funcție de operațiunile de prelucrare a datelor efectuate și de nivelul de protecție impus pentru datele cu caracter personal prelucrate de **operator** sau de persoana împuternicită de operator/împuternicită de DG. Acești responsabili cu protecția datelor, indiferent dacă sunt sau nu salariați ai operatorului, trebuie să fie în măsură să își îndeplinească atribuțiile și sarcinile în mod independent.

- *Capacitatea de a îndeplini sarcinile* este o cerință care se referă la calitățile personale (integritatea profesională, respectarea regulilor de etică) și poziția responsabilului cu protecția datelor în cadrul companiei.

Funcția responsabilului cu protecția datelor

În conformitate cu dispozițiile art. 37-39 din GDPR, desemnarea unui responsabil cu protecția datelor, în cadrul Salubrizare Sector 5 S.A., este o cerință obligatorie.

DPO poate fi salariat sau colaborator extern, în directă subordine a conducătorului companiei. Conform prevederilor din GDPR, funcția de DPO poate fi de asemenea exercitată în baza unui contract de prestări servicii încheiat cu o persoană fizică sau o organizație din afara companiei/operatorului, cu îndeplinirea tuturor cerințelor aplicabile din Secțiunea 4 (Desemnarea DPO) din RGPD privitoare, printre altele, la conflictul de interese (evitarea conflictului de interese presupune faptul că DPO să nu dețină funcții de conducere în cadrul instituției (de ex: director executiv, director operațional, director financiar, șeful serviciului resurse umane), dar în același timp, și alte funcții inferioare, dacă acestea conduc la posibilitatea de a stabili scopurile și mijloacele de prelucrare.

Atribuțiile responsabilului cu protecția datelor (DPO-ului):

- să informeze și să consilieze Directorul General și șefii de compartimente, precum și angajații acestora, cu privire la obligațiile existente în domeniul protecției datelor cu caracter personal;
- să monitorizeze respectarea GDPR și a legislației naționale în domeniul protecției datelor. Șefii de servicii trebuie să trimită la sfârșitul fiecărei luni sau de fiecare dată când au nevoie de consilierea DPO-ului, o situație centralizată privind implementarea și respectarea prezentei proceduri, în vederea realizării studiului de impact privind protecția datelor;
- să coopereze cu autoritatea pentru protecția datelor și să reprezinte punctul de contact în relația cu aceasta.
- să își asume rolul de punct de contact pentru ANSPDCP privind aspectele legale de prelucrare a datelor, inclusiv consultarea prealabilă menționată la art. 36 din GDPR precum și, dacă este cazul, consultarea cu privire la orice altă chestiune.
- să informeze, de îndată, conducerea instituției despre vulnerabilitățile și riscurile semnalate în sistemul de securitate a prelucrării datelor cu caracter personal al companiei și propune măsuri pentru înlăturarea acestora; Informarea se va face în scris și va cuprinde evidențierea dovezilor care au condus la nerespectarea prevederilor legale privind prelucrare a datelor, cât și indicarea serviciilor vizate.
- să informeze, imediat, conducerea companiei în legătură cu orice încălcare a normelor de protecție a datelor cu caracter personal de natură a prejudicia drepturile persoanei vizate (personalul salariat, petiționarii, colaboratorii, după caz), cu privire la măsurile dispuse pentru identificarea persoanei responsabile și limitarea efectelor unei diseminări neautorizate a datelor, precum și cu privire la situațiile în care au fost emise recomandări sau aplicate sancțiuni de către autoritatea națională de supraveghere sau când aceasta a dispus efectuarea unui control prealabil ori a unor investigații.

Derularea operațiunilor și acțiunilor activității.

Înainte de începerea activităților de prelucrare a datelor cu caracter personal, persoana vizată (personalul salariat, petiționarii, colaboratorii, după caz) trebuie să își dea consimțământul expres și

neechivoc pentru prelucrarea datelor (consimțământul se va exprima sub forma declarației prevăzute la Anexa 1), S 5 S.A. având obligația de a înștiința persoana vizată (personalul salariat, petiționarii, colaboratorii, după caz) cu privire la politica de confidențialitate privind prelucrarea datelor cu caracter personal, cât și scopul pentru care acestea au fost colectate.

Persoana vizată (personalul salariat, petiționarii, colaboratorii, după caz) are dreptul de a se opune sau să își retragă în orice moment consimțământul, în mod gratuit și fără nicio justificare .

Excepții de la consimțământ:

- când prelucrarea este necesară în vederea executării unui contract sau antecontract la care persoana vizată (personalul salariat, petiționarii, colaboratorii, după caz) este parte, ori în vederea luării unor măsuri, la cererea acesteia, înaintea încheierii unui contract sau antecontract;
- când prelucrarea este necesară în vederea protejării vieții, integrității fizice sau sănătății persoanei vizate (personalul salariat, petiționarii, colaboratorii, după caz) ori a unei alte persoane amenințate;
- când prelucrarea este necesară în vederea îndeplinirii unei obligații legale a DG;
- când prelucrarea este necesară în vederea aducerii la îndeplinire a unor măsuri de interes public sau care vizează exercitarea prerogativelor de autoritate publică cu care este investit D.G. sau terțul căruia îi sunt dezvăluite datele;
- când prelucrarea este necesară în vederea realizării unui interes legitim al D.G. sau al terțului căruia îi sunt dezvăluite datele, cu condiția ca acest interes să nu prejudicieze interesul sau drepturile și libertățile fundamentale ale persoanei vizate (personalul salariat, petiționarii, colaboratorii, după caz);
- când prelucrarea privește date obținute din documente accesibile publicului, conform legii;
- când prelucrarea este făcută exclusiv în scopuri statistice, de cercetare istorică sau științifică.

Conform art. 13 din GDPR operatorul (Directorului General), în momentul obținerii de date cu caracter personal, este obligat să furnizeze persoanei vizate (personalul salariat, petiționarilor, colaboratorilor, după caz) informațiile cuprinse la lit. a)-f), din GDPR.

Notificarea către persoana vizată (personalul salariat, petiționarii, colaboratorii, după caz) va cuprinde cel puțin următoarele informații:

- a) identitatea, datele de contact și adresa sediului S 5 S.A.;
- b) scopul și temeiul legal în baza căruia se efectuează prelucrarea, raportat la art. 6 din GDPR (ex. consimțământul persoanelor vizate, contract, obligația legală);
- c) o descriere a categoriei sau a categoriilor de persoane vizate (personalul salariat, petiționarii, colaboratorii, după caz) și a datelor ori a categoriilor de date ce vor fi prelucrate;
- d) destinatarii sau categoriile de destinatari cărora se intenționează să li se dezvăluie datele;
- e) garanțiile care însoțesc dezvăluirea datelor către terți;
- f) modul în care persoanele vizate (personalul salariat, petiționarii, colaboratorii, după caz) sunt informate asupra drepturilor lor; data estimată pentru încheierea operațiunilor de prelucrare, precum și destinația ulterioară a datelor;
- g) transferuri de date care se intenționează să fie făcute către alte state; (nu se aplică această cerință pentru S 5 S.A.).
- h) o descriere generală care să permită aprecierea preliminară a măsurilor luate pentru

asigurarea securității prelucrării;

i) specificarea oricărui sistem de evidență a datelor cu caracter personal, care are legătură cu prelucrarea, precum și a eventualelor legături cu alte prelucrări de date sau cu alte sisteme de evidență a datelor cu caracter personal, indiferent dacă se efectuează, respectiv dacă sunt sau nu situate pe teritoriul României;

j) în cazul în care operatorul intenționează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost colectate, operatorul furnizează persoanei vizate, înainte de această prelucrare ulterioară, informații privind scopul secundar respectiv și orice informații suplimentare relevante, conform alin. (2) a art.13 din regulament și *anume asigurarea unei prelucrări echitabile și transparente.*

6.2. Descrierea activității și impactul procedurii în cadrul S 5 S.A. pe compartimente

Cartografierea datelor - întocmirea unei evidențe de către șefii compartimentelor care prelucrează datele cu caracter personal în cadrul S 5 S.A..

Fiecare șef de compartiment trebuie să pună la dizpoziția DPO-ului, cât mai curând posibil, în format Word, următoarele:

- datele cu caracter personal (în sensul definit de GDPR) pe care le prelucrează;
- scopul și temeiul legal în baza căruia se efectuează prelucrarea, raportat la art. 6 din regulament (ex. consimțământul persoanelor vizate, contract, obligație legală);
- o descriere a categoriilor de persoane vizate (personalul salariat, petiționarii, colaboratorii, după caz) și a categoriilor de date cu caracter personal (S 5 S.A. prelucrează date cu caracter personal în scopurile de organizare, gestiune economică-financiară-administrativă, privind proprii angajați în cadrul activității de resurse umane; prelucrează, de asemenea, date cu caracter personal cu ocazia organizării de concursuri, examene prin care se stabilesc condiții concrete de asigurare a securității prelucrării datelor, precum și de informare a persoanelor vizate-personalul salariat, petiționarii, colaboratorii, după caz - privind drepturile acestora, cât și a altor situații privitoare la prelucrare datele cu caracter personal); datele cu caracter personal astfel prelucrate se arhivează conform legii după realizarea scopului în care au fost prelucrate. Stocarea acestor date pentru o perioadă mai mare decât cea necesară realizării scopului se poate efectua numai pentru interes statistic, după ce au fost transformate în date anonime.
- categorii de destinatari (personalul salariat, instituții, bănci, ITM, instanțe, executori judecătorești, case de avocatură, secții de poliție, ministere, cabinete medicale, spitale etc.) cărora le-au fost sau le vor fi divulgate datele cu caracter personal.

Întocmirea acestei evidențe are un dublu scop:

- facilitarea punerii în aplicare în mod concret potrivit specificului instituției a Regulamentului UE;
- centralizarea datelor de către DPO, pentru a fi furnizate, la cerere, Agenției Naționale de Supraveghere a Datelor cu Caracter Personal, pentru situațiile în care Agenția efectuează controlul aplicării Regulamentului de către S 5 SA., în calitate de operator de prelucrare a datelor cu caracter personal.

O altă măsură impusă este limitarea accesului în încăperile în care se află documente ce conțin date cu caracter personal și/sau echipamente care prelucrează date cu caracter personal, la utilizatorii desemnați pentru îndeplinirea atribuțiilor de serviciu.

În cazul în care nu se poate restricționa accesul în aceste încăperi, documentele se securizează în dulapuri prevăzute cu încuietori.

În cazul încălcării, la un moment dat, a procedurii prelucrării datelor cu caracter personal,

DPO-ul va informa, în scris, în maxim 72 de ore, persoanele care ar putea fi vizate cât și Directorul General și va soluționa împreună cu șefii de compartimente problema.

Datele colectate trebuie să fie corecte, iar în cazul în care persoana vizată (personalul salariat, petiționarii, colaboratorii, după caz) va cere actualizarea sau ștergerea datelor operatorul trebuie să se conformeze. Actualizarea sau ștergerea datelor se va face prin cerere scrisă la sediul C.M.P.C.V.B. SA, la secretariat sau prin email la adresa office@salubrizare5.ro - Anexa 9.

DPO-ul va redirecționa solicitarea către departamentul vizat și va informa utilizatorul care a dorit ștergerea datelor, prin răspuns scris sau prin email, cu privire la soluționarea cererii.

Este interzisă prelucrarea datelor care conțin informații privind: etnia sau originea rasială, opiniile politice, confesiunea religioasă, apartenența la sindicate, orientarea sexuală.

Serviciul RU are obligația ca la semnarea fiecărui contract individual de muncă să întocmească Anexa 1 și Anexa 3 a prezentei proceduri.

În cazul contractelor încheiate înainte de intrarea în vigoare a GDPR, cât și în cazul personalului salariat prin transfer sau detașare, se va semna Anexa 1 cu fiecare persoană în parte în termen de cel mult 30 de zile de la primirea prezentei. Serviciul RU va efectua o evidență a tuturor salariaților care au luat la cunoștința și au semnat, iar aceasta se va transmite DPO - ului, Evaluarea impactului asupra protecției datelor cu caracter personal.

S 5 S.A., prin serviciile sale este obligată, potrivit art. 35 din GDPR, să întocmească o evaluare a impactului asupra protecției datelor cu caracter personal.

Această evaluare va evidenția riscurile ce pot apărea în procesul de prelucrare a datelor persoanelor vizate. Vor fi avute în vedere: natura datelor, domeniul de aplicare, contextul și scopurile prelucrării, precum și utilizarea noilor tehnologii.

Evaluarea impactului asupra protecției datelor presupune:

(a) o descriere sistematică a operațiunilor de prelucrare preconizate și a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de S 5 S.A.;

(b) o evaluare a necesității și proporționalității operațiunilor de prelucrare în legătură cu aceste scopuri;

(c) o evaluare a riscurilor pentru drepturile și libertățile persoanelor vizate;

(d) măsurile preconizate în vederea abordării riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze conformitatea cu dispozițiile prezentului regulament, luând în considerare drepturile și interesele legitime ale persoanelor vizate și ale altor persoane interesate.

Scopul întocmirii evaluării impactului asupra protecției datelor cu caracter personal urmărește:

- realizarea unei prelucrări de date cu caracter personal sau a unui produs care respectă viața privată;
- estimarea impactului asupra vieții private a persoanelor vizate;
- demonstrarea faptului că principiile fundamentale ale GDPR sunt respectate;
- obligativitatea întocmirii evaluării impactului rezultă din art. 35 din GDPR, articol care detaliază conținutul și scopurile acestuia, potrivit celor mai sus arătate.
- GDPR impune realizarea unei evaluări sistematice și cuprinzătoare a aspectelor referitoare

la persoanele fizice care se bazează pe *prelucrarea automată*, inclusiv crearea de profiluri și care, stă la baza unor decizii care produc efecte juridice privind persoanele fizice sau care o afectează într-o măsură semnificativă.

- Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, potrivit art. 35, alin (4), va întocmi și va publica o listă a tipurilor de operațiuni de prelucrare care fac obiectul cerinței de efectuare a unei evaluări a impactului asupra protecției datelor. Aceste liste vor fi comunicate de ANSPDCP, Comitetului European pentru protecția datelor.

- Art. 35 alin. (11) mai prevede că acolo unde este necesar, **instituția, prin DPO-ul desemnat**, efectuează o analiză pentru a evalua dacă prelucrarea are loc în conformitate cu evaluarea impactului asupra protecției datelor cel puțin atunci când are loc o modificare a riscului reprezentat de prelucrare.

Având în vedere serviciile care colectează și prelucrează date cu caracter personal, se impune ca aceste compartimente să întocmească punctual, pe sectorul coordonat, evaluarea în discuție.

6.4 Comunicarea datelor cu caracter personal

Datele cu caracter personal se pot comunica operatorului și împuterniciților acestora ori organismelor publice/entităților de drept public sau privat, în una din următoarele situații:

- dacă persoana vizată (personalul salariat, petiționarii, colaboratorii, după caz) și-a dat consimțământul expres și neechivoc pentru comunicarea datelor sale;
- fără consimțământul persoanei vizate în cazurile prevăzute de lege.

Comunicarea datelor cu caracter personal se va efectua doar după semnarea Anexei 7 a procedurii și se va considera anexă la contractul de prestări servicii semnat cu persoana vizată (colaboratorii, după caz) care trebuie să conțină cel puțin: numărul de înregistrare a notificării, temeiul legal al prelucrării și scopul acesteia, termenul maxim de prelucrare, drepturile și obligațiile părților, modalitățile de asigurare a securității prelucrării și de respectarea datelor persoanei vizate, precum și mențiunea că datele pot fi utilizate doar de structura beneficiară și numai în scopul pentru care au fost solicitate; în cazul contractelor semnate înaintea intrării legii în vigoare, acestea se vor semna la data aprobării procedurii cu fiecare colaborator în parte, Anexa 7, responsabilitatea revenindu-i Serviciului Urmărire Contracte. Șeful de serviciu are obligația de a informa, prin email la adresa office@salubrizare5.ro centralizarea documentelor semnate, în maxim 7 zile de la primirea prezentei proceduri.

6.5. Organizarea procedurilor interne.

Pentru a asigura permanent un nivel ridicat de protecție a datelor cu caracter personal, Directorul General, prin prin șefii de compartimentei, trebuie să elaboreze proceduri interne care să garanteze respectarea protecției datelor în orice moment, luând în considerare toate evenimentele care pot apărea pe parcursul efectuării prelucrărilor de date, precum:

- breșe de securitate;
- solicitări privind exercitarea drepturilor persoanelor vizate;
- modificarea datelor cu caracter personal colectate;
- schimbarea prestatorului/furnizorului - se vor respecta prevederile din Anexa 8 a prezentei proceduri.

Organizarea procedurilor interne implică, în special:

- ❖ *luarea în considerare a protecției datelor cu caracter personal încă de la momentul*

conceperii (privacy by design) unei aplicații sau a unei prelucrări : minimizarea colectării datelor în funcție de scop, cookie-uri, perioada de stocare, informațiile furnizate persoanelor vizate, obținerea consimțământului persoanelor vizate (personalul salariat, petiționarii, colaboratorii, după caz), securitatea și confidențialitatea datelor cu caracter personal, garantarea rolului și responsabilităților părților implicate în efectuarea prelucrării datelor;

❖ *aplicarea de măsuri tehnice și organizatorice, de către șefii de compartimente, adecvate pentru a se asigura că, în mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării (privacy by default)* având în vedere: volumul de date colectate, gradul de prelucrare al acestora, perioada de stocare și accesibilitatea lor, astfel încât datele cu caracter personal să nu fie accesate, fără intervenția persoanei, de un număr nelimitat de persoane;

❖ *sensibilizarea și organizarea diseminării informației*, în special prin stabilirea unui plan de pregătire și de comunicare cu persoanele care prelucrează date cu caracter personal; această procedură revine în sarcina șefilor de serviciu dar și a personalului salariat angajat direct în prelucrarea datelor cu caracter personal;

❖ *soluționarea plângerilor și cererilor adresate de persoanele vizate* (personalul salariat, petiționarii, colaboratorii, după caz) *în exercitarea drepturilor lor*, stabilind părțile implicate și modalitățile de exercitare a acestora; exercitarea drepturilor trebuie să se poată realiza inclusiv pe cale electronică, la adresa de email office@salubrizare5.ro, în cazul în care datele au fost colectate prin astfel de mijloace. Această procedură revine în sarcina șefilor de compartimente, prin consilierea acestora de către DPO;

❖ *anticiparea unei posibile încălcări a securității datelor* specificând, pentru anumite cazuri, obligativitatea notificării ANSPDCP în termen de 72 de ore și a persoanelor vizate în cel mai scurt timp. Această procedură revine în sarcina șefilor de compartimente, prin consilierea acestora de către DPO;

❖ *asigurarea confidențialității și securității prelucrării*, de către șefii de compartimente, prin consilierea acestora de către DPO și prin adoptarea de măsuri tehnice și organizatorice adecvate, incluzând printre altele, după caz:

a) pseudonimizarea și criptarea datelor cu caracter personal;

b) capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continuă a sistemelor și serviciilor de prelucrare;

c) capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util, în cazul în care are loc un incident de natură fizică sau tehnică (Anxa 5);

d) un proces pentru testarea, evaluarea și aprecierea periodică a eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

Implementarea acestora va avea loc prin întocmirea unei situații centralizatoare privind implementarea și respectarea prezentei proceduri, în vederea realizării studiului de impact privind protecția datelor, ce se va transmite pe adresa de mail office@salubrizare5.ro, la comunicarea DPO.

6.6 Condiții de legitimitate ale prelucrării datelor.

Orice prelucrare de date cu caracter personal, cu excepția prelucrărilor care vizează date legate de originea rasială sau etnică, de convingerile politice, religioase etc., a prelucrării codului numeric personal sau a altor date cu caracter personal având o funcție de identificare de aplicabilitate generală ori a prelucrării datelor privind starea de sănătate, poate fi efectuată numai dacă persoana vizată (personalul salariat, petiționarii, colaboratorii, după caz) și-a dat consimțământul, în mod

expres și neechivoc pentru acea prelucrare.

Evidența păstrată de S 5 S.A. va cuprinde:

- numele și datele de contact ale Directorul General și, după caz, ale șefilor de servicii și ale DPO-ului,
- scopurile prelucrării;
- descrierea categoriilor de persoane vizate și a categoriilor de date cu caracter personal;
- categoriile de destinatari cărora le vor fi divulgate datele cu caracter personal;
- acolo unde este posibil, termenele limită preconizate pentru ștergerea diferitelor categorii de date;
- o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la art. 32 alin. (1) din GDPR ;

Evidențele menționate anterior se formulează în scris, inclusiv în format electronic și se pun la dispoziția ANSDCP, la cererea acesteia.

6.7. Notificarea autorității de supraveghere în cazul încălcării securității datelor cu caracter personal.

Conform art. 32 din regulament, în cazul în care se constată că a avut loc o încălcare a securității datelor cu caracter personal, Directorul General va notifica acest lucru autorității de supraveghere competente, în temeiul art. 55, fără întârzieri nejustificate și, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta, cu excepția cazului în care încălcarea este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice.

Șefii de serviciu înștiințează Directorul General și DPO-ul, fără întârzieri nejustificate, după ce iau cunoștință de o încălcare a securității datelor cu caracter personal.

Notificarea către ANSPDCP se întocmește de către DPO și trebuie să cuprindă următoarele elemente:

a) descrierea caracterului încălcării securității datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile și numărul aproximativ al persoanelor vizate în cauză, precum și categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;

(b) comunicarea numelui și a datelor de contact ale DPO-ului sau un alt punct de contact de unde se pot obține mai multe informații;

(c) descrierea consecințelor probabile ale încălcării securității datelor cu caracter personal;

(d) descrierea măsurilor luate sau propuse spre a fi luate de Directorul General pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

Atunci când și în măsura în care, nu este posibil să se furnizeze informațiile în același timp, acestea pot fi furnizate în mai multe etape, fără întârzieri nejustificate.

Directorul General păstrează documentele referitoare la toate cazurile de încălcare a securității datelor cu caracter personal, care cuprind o descriere a situației de fapt în care a avut loc încălcarea securității datelor cu caracter personal, a efectelor acesteia și a măsurilor de remediere întreprinse. Această documentație permite ANSPDCP să verifice conformitatea aplicării regulamentului.

6.7.1. Informarea persoanei vizate (personalul salariat, petiționarii, colaboratorii, după caz) cu privire la încălcarea securității datelor cu caracter personal.

Potrivit art. 34 din GDPR, atunci când încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, șefii de

serviciu informează persoana vizată (personalul salariat, petiționarii, colaboratorii, după caz), cât și DPO-ul și DG, fără întârzieri nejustificate cu privire la această încălcare. Informarea va fi transmisă în format scris sau electronic.

În informarea transmisă persoanei vizate (personalul salariat, petiționarii, colaboratorii, după caz) se include o descriere, într-un limbaj clar și simplu, a caracterului încălcării securității datelor cu caracter personal, precum și informațiile și măsurile menționate la art.33 alin. (3) lit. b)-d), din GDPR (cele menționate la pct. 6.7. lit.b)-d) de mai sus).

Informarea persoanei vizate (personalul salariat, petiționarii, colaboratorii, după caz) *nu este necesară* în cazul în care oricare dintre următoarele condiții este îndeplinită:

(a) Directorul General a implementat măsuri de protecție tehnice și organizatorice adecvate, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securității datelor cu caracter personal, în special, măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze (cum ar fi criptarea);

(b) Directorul General a luat măsuri ulterioare, prin care se asigură că riscul ridicat pentru drepturile și libertățile persoanelor vizate nu mai este susceptibil să se materializeze;

(c) Informarea ar necesita un efort disproporționat. În această situație, se efectuează pe loc o informare publică sau se ia o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficace.

În ipoteza în care Directorul General nu a comunicat deja încălcarea securității datelor cu caracter personal către persoana vizată (personalul salariat, petiționarii, colaboratorii, după caz), autoritatea de supraveghere, după ce a luat în considerare probabilitatea ca încălcarea securității datelor cu caracter personal să genereze un risc ridicat, poate să îi solicite acestuia să facă acest lucru sau poate decide că oricare dintre condițiile menționate la alineatul (3) sunt îndeplinite.

6.8. Sancțiuni

Potrivit art. 83 din GDPR, nerespectarea dispozițiilor Regulamentului atrage aplicarea de sancțiuni pentru impunerea amenzilor administrative.

Fiecare autoritate de supraveghere asigură faptul că impunerea unor amenzi administrative în conformitate cu articolul 83, pentru încălcările prevederilor GDPR menționate la alin. (4)-(6), este, în fiecare caz, eficace, proporțională și disuasivă.

Pentru încălcările dispozițiilor următoare, în conformitate cu art. 83 alin. (2), se aplică amenzi administrative de până la 10.000.000 EURO:

- obligațiile operatorului/insituției și ale persoanei împuternicite de operator/insituție în conformitate cu art.8, 11, 25-39, 42 și 43 din RGPD;
- obligațiile organismului de certificare în conformitate cu art. 42 și 43;
- obligațiile organismului de monitorizare în conformitate cu art. 41 alin. (4).

Pentru încălcările dispozițiilor următoare, în conformitate cu alin. (2), se aplică amenzi administrative de până la 20 000 000 EUR:

- ✧ principiile de bază pentru prelucrare, inclusiv condițiile privind consimțământul, în conformitate cu articolele 5, 6, 7 și 9;
- ✧ drepturile persoanelor vizate în conformitate cu art. 12-22;
- ✧ transferurile de date cu caracter personal către un destinatar dintr-o țară terță sau o organizație internațională, în conformitate cu art. 44-49;
- ✧ orice obligații în temeiul legislației naționale adoptate în temeiul capitolului IX;

✧ nerespectarea unui ordin sau a unei limitări temporare sau definitive asupra prelucrării, sau a suspendării fluxurilor de date, emisă de către autoritatea de supraveghere în temeiul articolului 58 alineatul (2) sau neacordarea accesului, încălcând art. 58 alin. (1).

Pentru încălcarea unui ordin emis de autoritatea de supraveghere în conformitate cu art. 58 alin. (2) se aplică amenzi administrative de până la 20.000.000 EUR.

6.9. Descrierea procedurii și impactul asupra departamentului IT.

Cu ocazia proiectării, întreținerii, actualizării aplicațiilor de gestiune a bazelor de date, se interzice accesul programatorilor/personalului de întreținere a sistemelor informatice în orice fel de date cu caracter personal deținute/create/accesate de personalul din structura respectivă. În aceste situații, se vor pune la dispoziția programatorilor/personalului de întreținere, numai date anonime.

Pentru cazuri excepționale, numai pe durata intervenției și circumstanțiat limitative la datele strict necesare, persoanele care asigură suportul tehnic pot avea acces la datele cu caracter personal, numai în prezența unui utilizator desemnat de Directorul General în sau a DPO, în această situație, răspunderea pentru păstrarea confidențialității datelor aparține celui în cauză, sens în care trebuie să semneze un *angajament de confidențialitate* (Anexa 3).

Operațiunile de colectare, introducere, modificare și actualizare a datelor cu caracter personal, se fac numai cu personalul anume desemnat de către Directorul General.

Directorul General dispune măsurile necesare care să permită identificarea utilizatorului care a introdus, modificat sau actualizat datele.

Prin urmare, baza de date (care conține datele cu caracter personal) deținută, creată și programele folosite de instituție sunt salvate prin copii de siguranță, la un interval de timp stabilit de DPO împreună cu seful de compartiment, în departamentul căruia se prelucrează date cu caracter personal, în funcție de mărimea, volumul și importanța acestora și care nu poate depăși 6 luni.

Directorul General va desemna utilizatorii (personalul IT sau altă persoană desemnată de D.G.) care trebuie să aibe ca atribuții de serviciu și executarea copiilor de siguranță ale bazelor de date deținute, create și ale programelor folosite.

Ținând cont de impactul mediului online asupra prelucrării și protecției datelor cu caracter personal se impune implementarea pe website a următoarelor:

a) website-ul va avea detaliată *politica cookies* (Anexa 6), unde se va specifică module sunt folosite, ce date se colectează, pentru cât timp și în ce scopuri sunt folosite cookie-urile. În acest sens măsura se va implementa cu ajutorul unui pop-up în care utilizatorul/persoana vizată (personalul salariat, petiționarii, colaboratorii, după caz) are opțiunea să își dea acordul sau să respingă acest lucru printr-un link către o pagină în care sunt detaliate toate informațiile precizate mai sus;

b) *Politica de Confidențialitate* - scopul ei este de a informa utilizatorul final despre colectarea, stocarea și folosirea datelor cu caracter personal (Anexa 2), pagina trebuie să apară în website, astfel încât să poată fi accesată în orice moment al navigării pe website-ul www.cmpevb.ro;

Informațiile esențiale care trebuie cuprinse în politica de confidențialitate:

- datele de identificare ale S 5 S.A.;
- datele colectate de către S 5 S.A. în mediul online (nume, număr de telefon, email, adresa, ip, etc);
- motivele pentru care au fost colectate datele (facturare, ofertare, comunicare email, marketing etc).

- modul de descărcare a datelor (în mod automat, manual, prin personal responsabil pentru protecția datelor);
 - dacă un utilizator dorește să își steargă datele personale din baza de date, acesta va trimite un mail de informare cu privire la aceasta cerință pe adresa de mail office@salubrizare5.ro
 - respectarea art. 13 și 14 din GDPR.
- c) crearea unei adrese de mail destinată atribuțiilor DPO-ului ”**dataprotection@cmpevb.ro**”;
- d) formularul de contact al paginii de web trebuie să conțină bifă și link către pagina de confidențialitate prin care utilizatorul să își poată da acordul asupra prelucrării datelor. Datele furnizate în acest formular se vor folosi strict în scopul în care au fost furnizate;
- e) în cazul în care există utilizatori cu vârste sub 16 ani, trebuie implementat un alt câmp în care minorului i se cere să completeze adresa de mail a unui părinte, pentru a i se cere acordul asupra prelucrării datelor;
- f) instalarea certificatelor SSL - certificatele criptează informațiile înainte ca acestea să circule prin Internet. Informațiile criptate să nu poată fi decriptate decât de serverul căruia îi sunt adresate, acest lucru garantând că informațiile trimise către un website nu pot fi modificate sau furate;
- g) schimbarea parolelor de acces și setarea unor parole puternice;
- h) Reducerea cantității datelor stocate;
- i) setarea unui mesaj prestabilit pe pagina de web a GDPR prin care persoanele vizate sunt înștiințate cu privire la politica de confidențialitate a datelor cu caracter personal, împreună cu un link pe pagina www.cmpevb.ro/politicadeconfidențialitate și li se va cere acordul privind continuarea discuției și prelucrarea datelor cu caracter personal, dacă este cazul. Implementarea va fi comunicată către Biroul Comunicare și Relații Publice.
- j) Detalierea unei politici, în cazul încălcării la un moment dat a procedurii prelucrării datelor cu caracter personal, care să cupindă persoanele care ar putea fi implicate, cele care trebuie informate în maxim 72 de ore și modul în care se va rezolva problema.

7. Responsabilități.

7.1. Persoanele cu funcții de conducere.

Persoanele cu funcții de conducere din cadrul fiecărui compartiment al S 5 S.A. sunt responsabile cu protecția datelor cu caracter personal la nivelul companiei și au următoarele atribuții:

- informează și instruesc personalul contractual de execuție privind importanța respectării și implementării prezentei proceduri privind protecția datelor cu caracter personal;
- întocmesc o situație centralizată privind persoanele instruite, situația va fi semnată de către aceștia și va fi predată DPO-ului.
- în cazul apariției unor posibile probleme sau legat de orice problemă cu privire la protecția datelor cu caracter personal, aceștia au obligația de a se consulta cu DPO-ul instituției;
- stabilesc scopul și mijloacele de prelucrare a datelor cu caracter personal atunci când acestea sunt necesare pentru exercitarea unor competențe legale;
- asigură elaborarea procedurilor proprii și după aprobarea acestora le pun în aplicare, le transmit DPO-ului;
- coordonează și monitorizează activitatea personalului din subordine, pe linia protecției datelor cu caracter personal, la nivelul compartimentului;
- asigură instruirea utilizatorilor în acest domeniu;

- dispun măsuri de completare sau, după caz, de modificare a fișei de post a utilizatorilor;
- analizează și dispun în ceea ce privește suspendarea sau revocarea dreptului de acces al utilizatorilor la sisteme de evidență a datelor cu caracter personal, în condițiile legii;
- dispun măsuri pentru exercitarea drepturilor de către persoana vizată (personalul salariat, petiționarii, colaboratorii, după caz);
- coordonează soluționarea cererilor persoanelor vizate (personalul salariat, petiționarii, colaboratorii, după caz) prin centralizarea acestora și transmiterea acestora către DPO;
- țin evidența cererilor persoanelor vizate (personalul salariat, petiționarii, colaboratorii, după caz);
- analizează periodic activitatea utilizatorilor;
- transmit lunar o situație centralizată privind punerea în practică și respectarea prezentei proceduri, în vederea realizării studiului de impact privind protecția datelor, ce se va transmite pe adresa de mail office@salubrizare5.ro, cel târziu până la data de 5 ale lunii următoare.

7.2. Funcțiile implicate în elaborarea, verificarea și aprobarea procedurii

Nr. crt.	Structura funcțională (postul)/acțiunea (operațiunea)	Responsabilul cu protecția datelor cu caracter personal	Comisia de Monitorizare	Director General	Compartimentele din cadrul S 5 S.A.
0	1	2	3	4	5
1.	a. Elaborarea procedurii	E			
2.	b. Verificarea procedurii		V		
3.	c. Aplicarea procedurii	Ap	Ap		Ap
4.	d. Aprobarea procedurii			A	
5.	e. Arhivarea procedurii	Ah			

8. Formular evidență modificări

Nr. crt.	Ediția sau, după caz, revizia în cadrul ediției	Componenta revizuită	Modalitatea reviziei	Data de aplicare
0	1	2	3	4
8.1.	Ediția I	X	X	
8.2.	Revizia 0	X	X	
8.3.	Ediția II			
8.4.	Revizia 0			

9. Formular de analiză procedură

În acest sens, pentru evitarea situațiilor în care procedura poate deveni neaplicabilă, pentru eliminarea confuziei responsabilităților sau pentru eliminarea unor potențiale erori în procesul de implementare a procedurii, este utilă consultarea compartimentelor implicate în aplicarea (implementarea) procedurii.

Pentru aceasta, anterior intrării în vigoare a procedurii și difuzării acesteia, procedura se transmite spre analiză compartimentelor implicate, în vederea exprimării unui punct de vedere.

Ulterior, procedura se transmite secretariatului tehnic al Comisiei de monitorizare care analizează conformitatea structurii procedurii cu prevederile Ordinului secretarului general al Guvernului pentru aprobarea Codului controlului intern managerial al entităților publice sau cu reglementările interne.

10. Anexe

Nr. crt.	Denumirea anexei	Elaborat	Aprobă	Nr. Exemplare	Difuzare	Arhivare		Pagina
						Loc	Perioadă	
0	1	2	3	4	5	6	7	8
1.	Declarație de consimțământ privind prelucrarea DCP	DPO	Director General	1	Compartimente din S 5 S.A.			P. 21
2.	Angajament confidențialitate	DPO	Director General	1	Compartimente din S 5 S.A			p. 23
3.	Completări ale Codului de Conduită	DPO	Director General	1	Compartimente din S 5 S.A			p. 24
4.	Procedura Backup	DPO	Director General	1	Compartimente din S 5 S.A			p. 29
5.	Politica Cookie-uri	DPO IT	Director General	1	Compartimente din S 5 S.A			p. 31
6.	Acord prelucrare DCP-persoană împuternicită	DPO	Director General	1	Compartimente din S 5 S.A			p. 34
7.	Acord prelucrare DCP -clienți	DPO	Director General	1	Compartimente din S 5 S.A			p. 40
8	Formular cerere persoană vizată	DPO	Director General	1	Compartimente din S 5 S.A			p. 44

DECLARAȚIE
privind consimțământul pentru colectarea și procesarea datelor cu caracter personal

I. Între

Subsemnatul/subsemnata, legitimat/ă cu CI seria....., nr, eliberat de către SPCLEP/SPCEP..... la data de, denumit în continuare, subiectul și

Salubrizare Sector 5 S.A., cu sediul în România, Municipiul București, sector 5, str....., telefon:, e-mail: office@salubrizare5.ro, înregistrată la Oficiul Registrul Comerțului sub numărul, CUI, reprezentată prin Director General, ANDREI FECIORU, în calitate de angajator, a intervenit următoarea declarație de consimțământ:

II. Obiectul consimțământului

Prezentul consimțământ aprobă colectarea, procesarea și utilizarea de către companie a datelor mele cu caracter personal.

III. Datele colectate

Datele colectate de la subiect sunt, în principal, următoarele:

cod numeric personal
carte identitate/pașaport – copie, serie și număr, fotografie
certificat de naștere/căsătorie, stare civilă
marca (număr intern de angajat)
curriculum vitae, studii
permis auto
naționalitatea, sexul
nume și prenume, adresa, număr de telefon, e-mail
locuri de muncă anterioare (foști angajatori)
cont IBAN
cazier judiciar și/sau fiscal
adeverința apt de muncă/medicina muncii
fișe SSM și PSI, date privind mărimile echipamentelor de protecție
monitorizare adresa IP la calculatorul de serviciu
contract de muncă/act adițional/decizie încetare activitate
baza REVISAL
date privind evaluarea performanțelor
informații privind training-urile și instruirile desfășurate în cadrul companiei
date privind persoana/persoanele din familie aflate în întreținere

IV. Scopul în care va fi utilizat consimțământul

Datele cu caracter personal, care fac obiectul prezentei, vor fi utilizate strict în următoarele scopuri:

- întocmirea dosarului de personal;
- înscrierea în Registrul de evidență a salariaților (REVISAL);
- întocmirea fișelor de SSM și PSI;
- întocmirea borderourilor/ordinelor de plată/dispozițiilor de plată/alte documente impuse de bănci/casierie.

V. Drepturile subiectului

Subiectul este protejat de **Regulamentul UE nr. 679 din 27 aprilie 2016** privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date, poate interveni când dorește și poate solicita:

- informarea și consultarea informațiilor vizate;
- actualizarea informațiilor vizate;
- ștergerea informațiilor vizate;
- restricționarea și opunerea în prelucrarea informațiilor vizate.

VI. Valabilitate

Prezentul consimțământ este valabil pe întreaga perioadă a contractului individual de muncă sau până la retragerea acestuia, cu excepția datelor conținute de statele de plată, care se păstrează 50 ani, conform Legii 82/1991 - Legea contabilității – republicată și actualizată, Art. 25 (1).

VII. Declarație:

Îmi exprim consimțământul cu privire la utilizarea datelor mele cu caracter personal în scopurile descrise mai sus. Utilizarea datelor mele cu caracter personal în alte scopuri decât cele descrise mai sus sau transmiterea acestora către terți, fără acordul meu, este strict interzisă.

Locație

Data

Numele în clar și semnătura subiectului

Notă:

Prezentul consimțământ a fost dat în conformitate cu **Regulamentul UE nr. 679 din 27 aprilie 2016** privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date, cu aplicabilitate obligatorie începând cu data de 25.05.2018, art. 4, pct.11 și art. 7.

ANGAJAMENT DE CONFIDENȚIALITATE

Subsemnatul/a _____ născut/ă în localitatea _____ la data de _____, fiul (fiica) lui _____ și a _____ angajat/ă al/a Salubrizare Sector 5 S.A. în funcția de _____, cu domiciliul în localitatea _____ strada _____, nr. _____, bl. _____, sc. _____, et. _____, ap. _____, județul/sectorul _____, declar că am luat cunoștință de dispozițiile legale cu privire la protecția informațiilor, a datelor cu caracter personal și a altor date, altele decât cele destinate publicității, cu care intru în contact pe timpul desfășurării activității.

Mă angajez să păstrez cu strictețe secretul acestora, atât pe timpul desfășurării activității cât și după încetarea contractului de muncă, pentru o perioadă de doi ani de zile.

Sunt conștient că, în cazul în care voi încălca prevederile prezentului contract de confidențialitate, voi răspunde, potrivit legii, administrativ, disciplinar, material, civil ori penal, în raport cu gravitatea faptei.

Data

Semnătura

.....

DAT ÎN PREZENȚA

(funcția, numele și prenumele)
Semnătura

Notă: Prezentul angajament de confidențialitate a fost încheiat în conformitate cu Legea 53/2003 actualizată în 2018 – Codul Muncii Art. 26 (1) „Prin clauza de confidențialitate părțile convin ca, pe toată durata contractului individual de muncă și după încetarea acestuia, să nu transmită date sau informații de care au luat cunoștință în timpul executării contractului, în condițiile stabilite în regulamentele interne, în contractele colective de muncă sau în contractele individuale de muncă.”

COMPLETAREA CODULUI DE CONDUITĂ AL SALUBRIZARE SECTOR 5 S.A.

CONFIDENȚIALITATEA INFORMAȚIILOR ȘI A DATELOR

- Salariații trebuie să păstreze confidențialitatea informațiilor și înregistrărilor nepublice carele sunt încredințate de S 5 S.A. și a tuturor celorlalte informații care le sunt comunicate, indiferent de sursă, în timpul îndeplinirii responsabilităților lor, cu excepția cazurilor în care divulgarea acestora este autorizată sau este impusă de legile, regulile, reglementările sau procedura legală.
- Informații cum ar fi rezultatele financiare, estimări ale câștigurilor sau pierderilor viitoare, știri despre achiziția sau cedarea de bunuri materiale sau entități de afaceri, probleme legate de lichiditățile financiare, câștigarea sau pierderea unui client sau a unui furnizor important, anunțuri importante despre produse noi, oferte noi privind capitalul sau datoriile etc. trebuie să fie considerate întotdeauna ca materiale.
- Manipularea responsabilă a datelor personale reprezintă o componentă în păstrarea încrederii în S 5 S.A. și asigurarea persoanelor că li se respectă dreptul la confidențialitate.

- **Principiile care guvernează prelucrarea datelor cu caracter personal, de către membrii companiei, sunt:**

❖ *Legalitatea prelucrării*

Prelucrarea este legală numai dacă și în măsura în care se aplică cel puțin una dintre următoarele **condiții**:

- a) persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;
- b) 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;
- c) prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;
- d) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;
- e) prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul.

❖ *Consimțământul persoanei vizate*

(1) În cazul în care prelucrarea se bazează pe consimțământ, compania trebuie să fie în măsură să demonstreze că persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal.

(2) În cazul în care consimțământul persoanei vizate este dat în contextul unei declarații scrise, cererea privind consimțământul trebuie să fie prezentată într-o formă inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu. Nicio parte a respectivei declarații care constituie o încălcare a prezentului regulament nu este obligatorie.

(3) Persoana vizată are dreptul să își retragă în orice moment consimțământul.

(4) Atunci când se evaluează dacă consimțământul este dat în mod liber, se ține seama cât mai mult de faptul că, printre altele, executarea unui contract, inclusiv prestarea unui serviciu, este condiționată sau nu de consimțământul cu privire la prelucrarea datelor cu caracter personal.

5) **Se interzice prelucrarea de date** cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice.

❖ **Transparența**

Compania ia măsuri adecvate pentru a furniza persoanei vizate orice informații și orice comunicări referitoare la prelucrare, 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.

❖ **Informare și acces la date cu caracter personal**

În cazul în care datele cu caracter personal referitoare la o persoană vizată sunt colectate de la aceasta, compania, în momentul obținerii acestor date cu caracter personal, furnizează persoanei vizate toate informațiile următoare:

- a) identitatea și datele de contact ale companiei și, după caz, ale reprezentantului acesteia;
- b) datele de contact ale responsabilului cu protecția datelor;
- c) scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării;
- d) interesele legitime urmărite de operator sau de o parte terță;
- e) destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
- f) dacă este cazul, intenția operatorului de a transfera date cu caracter personal către o țară terță sau o organizație internațională;
- g) perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;

❖ **Dreptul de acces al persoanei vizate**

Persoana vizată are dreptul de a obține din partea companiei o confirmare că se prelucrează sau nu date cu caracter personal care o privesc și, în caz afirmativ, acces la datele respective și la următoarele informații:

- a) scopurile prelucrării;
- b) categoriile de date cu caracter personal vizate;
- c) destinatarii sau categoriile de destinatari cărora datele cu caracter personal le-au fost sau urmează să le fie divulgate, în special destinatari din țări terțe sau organizații internaționale;
- d) acolo unde este posibil, perioada pentru care se preconizează că vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
- e) existența dreptului de a solicita operatorului rectificarea sau ștergerea datelor cu caracter personal ori restricționarea prelucrării datelor cu caracter personal referitoare la persoana vizată sau a dreptului de a se opune prelucrării;
- f) dreptul de a depune o plângere în fața unei autorități de supraveghere;
- g) în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, orice informații disponibile privind sursa acestora.

3.2. **Informațiile referitoare la datele personale ale angajaților, aflate în posesia Companiei, trebuie să fie protejate după cum urmează:**

- datele personale sunt colectate, procesate, stocate și transferate cu măsurile de precauție adecvate pentru a asigura confidențialitatea și pot fi accesate numai de un număr strict limitat de persoane, desemnate de Directorul General, care au semnat un angajament de confidențialitate înainte de a procesa datele respective, respectându – se principiul „nevoia de a cunoaște”;
- personalul desemnat pentru a colecta, procesa, stoca și gestiona datele personale ale angajaților își va desfășura activitatea în încăperi separate, prevăzute cu încuietori, acesta

- având obligativitatea de a securiza încăperea ori de câte ori o părăsește;
- dosarele conținând date cu caracter personal vor fi păstrate în dulapuri încuiate, dispuse în încăperea în care își desfășoară activitatea personalul desemnat;
 - persoanele desemnate, care operează datele personale ale angajaților pe sisteme informatice, au obligația de a pseudonimiza aceste date, de a stoca și procesa aceste date într-un fișier parolat, astfel încât accesul la acestea să fie restricționat și controlat;
 - fișierul care conține datele personale ale angajaților va fi stocat și pe un mediu de stocare portabil securizat, astfel încât, capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea să se efectueze timp util, în cazul în care are loc un incident de natură fizică sau tehnică;
 - eficacitatea măsurilor tehnice și organizatorice pentru garantarea securității prelucrării datelor cu caracter personal va fi supusă unui proces de testare, evaluare și apreciere periodică;
 - personalul desemnat pentru a colecta, procesa, stoca și gestiona datele personale ale angajaților are obligația notificării autorităților de supraveghere cu privire la încălcările securității datelor cu caracter personal și informarea persoanelor vizate cu privire la aceste încălcări;
 - ori de câte ori va fi necesar, salariaților și altor persoane li se vor cere consimțământul în vederea colectării, procesării, transferului și stocării datelor personale;
 - salariații pot să revizuiască datele personale privind eventualele erori;
 - salariații au obligația comunicării schimbărilor provenite în datele personale;
 - la plecarea din S 5 S.A., foștii angajați au dreptul de a obține din partea societății ștergerea datelor cu caracter personal care îi privesc, iar operatorul desemnat are obligația de a șterge datele cu caracter personal fără întârzieri, în cazul în care se aplică unul dintre următoarele motive:
 - datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;
 - persoana vizată își retrage consimțământul pe baza căruia are loc prelucrarea, și nu există niciun alt temei juridic pentru prelucrarea acestora.

3.3. **Raportarea și comunicarea informațiilor de interes public**

Salariații sunt responsabili, pe zona de activitate, pentru raportări, rapoarte și documente pe care societatea le depune la autorități și alte comunicate publice - trebuie să conțină informații financiare sau de altă natură complete, corecte, exacte, actuale și logice. Accesul la informații, înregistrări sau facilități ale S 5 S.A. se permite cu dispoziția/aprobarea unui reprezentant abilitat din societate.

3.4. **Relația cu autorități și instituții publice**

Salariații au obligația să aprobe în mod loial prestigiul companiei și să se abțină de la orice act ori fapt care poate produce prejudicii imaginii sau intereselor legale ale acesteia.

3.5. **Salariaților le este interzis:**

- să exprime în public aprecieri neconforme cu realitatea în legătură cu activitatea societății, cu politicile și strategiile acesteia;
- să dezvăluie informațiile la care au acces în exercitarea funcției, dacă aceasta dezvăluire este de natură să atragă avantaje necuvenite ori să prejudicieze societatea; această prevedere se aplică și după încetarea raportului de serviciu, pentru o perioadă de 2 ani;
- să dezvăluie informațiile care nu au caracter public sau să remită documente care conțin asemenea informații, fără acordul Directorului General;
- să folosească telefonul sau oricare alte mijloace tehnice pentru a înregistra, atât video

cât și audio, ședințele la care participă, alți angajați sau persoanele de conducere ale companiei.

3.6. Legile antitrust și legile referitoare la concurență

Se interzice salariaților, contractorilor, consultantilor, agenților și altor persoane care reprezintă compania să încheie acorduri oficiale/neoficiale/scrise/verbale care încalcă politica societății:

- acorduri sau înțelegeri cu competitorii în privința prețurilor sau în privința „împărțirii” clienților, produselor, serviciilor sau a teritoriilor;
- participarea la „licitații cu oferte trucate” ex. acorduri sau înțelegeri cu competitorii pentru impunerea comportamentului în licitare sau pentru a nu licita, în scopul dezavantajării altor competitori.

3.7. Oportunități corporaționale; conflicte de interese

Salariaților le este interzis să obțină avantaje personale din oportunități în care pot anticipa în mod rezonabil un interes al S 5 S.A. pentru o afacere în care este în relație directă, este în legătură cu aceasta sau a anunțat intenția sa de a se angaja.

Salariații S.5.S.A., indiferent de funcție, nu trebuie:

- să întreprindă acțiuni sau să aibă interese care i-ar putea împiedică să își desfășoare obiectiv și eficient activitatea în favoarea societății;
- să aibă un interes direct sau indirect într-o tranzacție în care societatea este sau poate deveni parte ex. relații de afaceri, achiziții etc.;
- să aibă un membru al familiei care primește beneficii personale necorespunzătoare ca urmare a poziției sale ca salariat al societății;
- să lucreze pentru sau să reprezinte un client sau un furnizor în negocierile cu societatea.

Al doilea job trebuie să fie separat de angajamentul în societate, nu trebuie să genereze sau să pară că generează un conflict de interese cu responsabilitățile în societate; nu trebuie să discrediteze societatea sau să afecteze independența și obiectivitatea salariatului.

Orice salariat care lucrează în afara S 5 S.A. este obligat să respecte în continuare contractele de confidențialitate pe care le-a încheiat cu societatea.

3.8. Interdicția privind practicile de corupere

Prevederile anticorupție interzic plata (mita) către un salariat al unei autorități în scopul obținerii, păstrării, direcționării de afaceri precum și intenția de a asigura un avantaj necuvenit în afaceri.

Societatea prin salariați, agenți, reprezentanți, consultanți sau terțe părți nu trebuie să încerce direct sau indirect să influențeze afacerile prin plăți ilegale, mită, sau alte mijloace imorale sau ilegale.

Politica S 5 S.A. incriminează și interzice oferirea sau acordarea de obiecte de valoare/bani/divertisment/favoruri etc. funcționarilor autorităților, partidelor politice sau candidaților pentru o funcție politică în vederea obținerii, păstrării, direcționării afacerilor sau în scopul obținerii unui avantaj necuvenit în afaceri.

Prevederile contabile ale societății impun să păstreze registre și înregistrări contabile care să reflecte exact și corect tranzacțiile, precum și să planifice și să întrețină un sistem adecvat de controale contabile interne pentru a asigura acuratețea registrelor și înregistrărilor contabile.

3.12 **Standarde de conformitate, raportare și acțiuni disciplinare**

S 5 S.A. se angajează să își desfășoare activitatea conform cu standardele de conduită în raporturile de muncă impuse angajaților și în afaceri.

Salariații trebuie să raporteze cu bună credință încălcările reale sau posibile ale legilor în vigoare sau neconformitatea cu acest cod de etică – adresate ierarhic, către structuri abilitate sau direct Directorului General.

Compartimentul Juridic este responsabil în general pentru aplicarea Codului de Etică în ceea ce privește salariații.

Informațiile furnizate vor fi păstrate confidențial și se va impune o politică antirepresivă pentru protejarea celor care, de bună credință, raportează posibile încălcări ale politicilor societății sau legilor în vigoare.

Orice derogare de la acest cod se analizează punctual, după dezvăluirea tuturor faptelor de către persoana care solicită derogarea și va fi solutionată, conform legii și reglementărilor aplicabile.

3.13. **Interzicerea acțiunilor represive**

S 5 S.A. interzice acțiunile represive împotriva unei persoane pentru raportarea unei activități pe care aceasta, de bună credință, o consideră a fi o încălcare a unei legi, politici, reglementări sau prevederi ale acestui cod.

Orice salariat care consideră că este victimă a unei acțiuni represive de orice natură trebuie să raporteze situația ierarhic sau unui reprezentant Compartimentul Juridic.

PROCEDURA DE BACKUP

POLITICA DE REALIZAREA COPIERII DATELOR

1. Scop

Politica de copiere a datelor furnizează o documentație cuprinzătoare a reglementărilor aplicabile în companie și măsurile luate pentru back-upul datelor. Aceasta servește ca dovadă terțelor părți, faptul că, controlul disponibilității legale necesare este efectuat corect.

2. Responsabilități în cadrul companiei

S 5 S.A. trebuie să asigure securitatea IT și backup-ul datelor.

Conducerea S 5 S.A. este direct responsabilă pentru acest lucru și este responsabilă personal atunci când este aplicabilă.

3. Condiții legale generale

Legea impune anumite controale prin măsuri tehnice și organizatorice, atât cu prelucrarea datelor în scopuri proprii, cât și cu prelucrarea datelor comandate; în acest context, se aplică, în special, un control al disponibilității.

Verificarea controalelor sau a măsurilor tehnice și organizatorice trebuie, printre altele, să fie oferită clienților în cadrul prelucrării datelor comandate.

4. Riscuri

- ✓ eroare umană: funcționare incorectă / accident, sabotaj, atac;
- ✓ întreruperi tehnice: defecțiuni tehnice, defecțiuni hardware, tulburări de linie;
- ✓ forță majoră, accidente, catastrofe: apă, incendiu etc.;
- ✓ posibile efecte existente amenințătoare asupra companiei.

5. Proceduri de backup de date, opțiuni

- suport complet;
- backup incremental;
- backup diferențial.

6. Reglementări tehnice și organizatorice minime

6.1 Reglementări generale:

- suportul de date trebuie să fie efectuat în mod responsabil și competent;
- fără ocolirea accidentală a modelelor de autorizare prin măsuri de salvare a datelor;
- confidențialitatea și obligația de protecție a datelor;
- nominalizarea persoanelor responsabile pentru fiecare domeniu de activitate;
- determinarea nevoii de confidențialitate, integritate și disponibilitate.

6.1 Implementarea tehnică:

- crearea planului de salvare a datelor;
- determinarea perioadei de păstrare și numărul de generații;
- coordonarea cu politica de prevenire a situațiilor de urgență;

- întocmirea procedurii de recuperare;
- crearea directorului de inventar;
- evaluarea folderelor;
- teste privind reconstrucția/restaurarea datelor și exercițiile de urgență;
- configurarea comenzilor necesare, în special pentru controlul accesului;
- implementarea cerințelor de protecție pentru confidențialitate, integritate și disponibilitate
- specificarea și asigurarea căile de transport;
- alocarea capacităților: capacitatea de transfer, volumul, cantitatea de dispozitive de stocare a datelor;
- implementarea cerințelor de copiere de rezervă (calculatoare mobile, PDA/ MDA, baze de date, fișiere deschise, date de sistem, date din jurnal etc.)

IT: Se va asigura, în special, controlul accesului, controlul permisiunilor de acces, controlul transmisiei, controlul de intrare și controlul separării, inclusiv în ceea ce privește seturile de backup de date.

POLITICA COOKIE-URILOR

Politica de utilizare Cookie-uri

Această politică se referă la cookie-urile și paginile web operate de SALUBRIZARE SECTOR 5 S.A. pe websit

Ce sunt Cookie-urile?

Cookie-urile sunt fișiere de mici dimensiuni, format din litere și numere, care vor fi stocat pe computerul, telefonul mobil sau alte echipamente ale unui utilizator de pe care acesta accesează internetul. Cookie-ul este instalat prin solicitarea emisă de către un web-server unui browser (ex: Internet Explorer, Chrome, Firefox) și este complet "pasiv" (nu conține programe software, viruși sau spyware și nu poate accesa informațiile de pe hard driverul utilizatorului).

La ce sunt folosite Cookie-urile?

Aceste fișiere fac posibilă recunoașterea terminalului utilizatorului și prezentarea conținutului într-un mod relevant, adaptat preferințelor utilizatorului. Cookie-urile asigura utilizatorilor o experiență plăcută de navigare și susțin eforturile S 5 S.A. pentru a oferi servicii confortabile utilizatorilor: ex: – preferințele în materie de confidențialitate online, coșul de cumpărături sau publicitate relevanta. De asemenea, sunt utilizate în pregătirea unor statistici anonime agregate care ne ajută să înțelegem cum un utilizator beneficiază de paginile noastre web, permițându-ne îmbunătățirea structurii și conținutului lor, excluzând indentificarea personală a utilizatorului.

Ce Cookie-uri folosim?

Folosim două tipuri de Cookie-uri: per sesiune și fixe. Cele din urmă sunt fișiere temporare ce rămân în terminalul utilizatorului până la terminarea sesiunii sau închiderea aplicației (browser-ului web). Fișierele fixe rămân pe terminalul utilizatorului pe o perioadă în parametrii Cookie-ului sau până sunt șterse manual de utilizator.

Cum sunt folosite cookie-urile de către acest site?

O vizită pe acest site poate plasa cookie-uri în scopuri de:

- Cookie-uri de performanță a site-ului;
- Cookie-uri de analiză a vizitatorilor;
- Cookie-uri pentru geotargetting;
- Cookie-uri de înregistrare;
- Cookie-uri pentru publicitate;
- Cookie-uri ale furnizorilor de publicitate.

Conțin Cookie-urile date personale?

Cookie-urile în sine nu solicită informații cu caracter personal pentru a putea fi utilizate și, în cele mai multe cazuri, nu identifica personal utilizatorii de internet. Datele personale colectate prin utilizarea Cookie-urilor pot fi colectate doar pentru a facilita anumite funcționalități pentru utilizator. Atare date sunt criptate într-un mod care face imposibil accesul persoanelor neautorizate la ele.

Ștergerea..Cookie-urilor

În general, o aplicație folosită pentru accesarea paginilor web permite salvarea Cookie-urilor pe terminal în mod implicit. Aceste setări pot fi schimbate în așa fel încât administrarea automată a Cookie-urilor să fie blocată de browser-ul web sau utilizatorul să fie informat de fiecare dată când Cookie-uri sunt trimise către terminalul sau. Informații detaliate despre posibilitățile și modurile de administrare a Cookie-urilor pot fi găsite în zona de setări a aplicației (browser-ului web). Limitarea folosirii Cookie-urilor poate afecta anumite funcționalități ale paginii web.

De ce sunt cookie-urile importante pentru Internet?

Cookie-urile reprezintă punctul central al funcționării eficiente a Internetului, ajutând la generarea unei experiențe de navigare prietenoase și adaptată preferințelor și intereselor fiecărui utilizator. Refuzarea sau dezactivarea cookie-urilor poate face unele site-uri imposibil de folosit.

Refuzarea sau dezactivarea cookie-urilor nu înseamnă că nu veți mai primi publicitate online – ci doar că aceasta nu va mai putea ține cont de preferințele și interesele dvs, evidențiate prin comportamentul de navigare.

Exemple de întrebări importante ale cookie-urilor (care nu necesită autentificarea unui utilizator prin intermediul unui cont):

- conținut și servicii adaptate preferințelor utilizatorului – categorii de produse și servicii;
- oferte adaptate pe interesele utilizatorilor – reținerea parolelor;
- reținerea filtrelor de protecție a copiilor privind conținutul pe Internet (opțiuni family mode, funcții de safe search);
- limitarea frecvenței de difuzare a reclamelor – limitarea numărului de afișări a unei reclame pentru un anumit utilizator pe un site;
- furnizarea de publicitate mai relevantă pentru utilizator;
- măsurarea, optimizarea și caracteristicile de analytics – cum ar fi confirmarea unui anumit nivel de trafic pe un website, ce tip de conținut este vizualizat și modul cum un utilizator ajunge pe un website (ex prin motoare de căutare, direct, din alte website-uri etc). Website-urile derulează aceste analize a utilizării lor pentru a îmbunătăți site-urile în beneficiul ușurilor.

Securitate și probleme legate de confidențialitate

Cookie-urile NU sunt viruși! Ele folosesc formate tip plain text. Nu sunt alcătuite din bucăți de cod așa că nu pot fi executate nici nu pot auto-rula. În consecință, nu se pot duplica sau replica pe alte rețele pentru a se rula sau replica din nou. Deoarece nu pot îndeplini aceste funcții, nu pot fi considerate..viruși.

Cookie-urile pot fi totuși folosite pentru scopuri negative. Deoarece stochează informații despre preferințele și istoricul de navigare al utilizatorilor, atât pe un anumit site cât și pe mai multe alte site-uri, cookie-urile pot fi folosite ca o formă de Spyware. Multe produse anti-spyware sunt conștiente de acest fapt și în mod constant marchează cookie-urile pentru a fi șterse în cadrul procedurilor de ștergere/scanare anti-virus/anti-spyware.

În general browserele au integrate setări de confidențialitate care furnizează diferite nivele de acceptare a cookie-urilor, perioada de valabilitate și ștergere automată după ce utilizatorul a vizitat un anumit site.

Alte aspecte de securitate legate de cookie-uri

Deoarece protecția identității este foarte valoroasă și reprezintă dreptul fiecărui utilizator de internet, este indicat să se știe ce eventuale probleme pot crea cookie-urile.

Prin intermediul lor se transmit în mod constant în ambele sensuri informații între browser și website; dacă un atacator sau persoană neautorizată intervine în parcursul de transmitere a datelor, informațiile conținute de cookie pot fi interceptate.

Deși foarte rar, acest lucru se poate întâmpla dacă browserul se conectează la server folosind o rețea necriptată (ex: o rețea WiFi nesecurizată).

Alte atacuri bazate pe cookie implică setări greșite ale cookieurilor pe servere. Dacă un website nu solicită browserului să folosească doar canale criptate, atacatorii pot folosi această vulnerabilitate pentru a păcăli browserele în a trimite informații prin intermediul canalelor nesecurizate. Atacatorii utilizează apoi informațiile în scopuri de a accesa neautorizat anumite site-uri. Este foarte important să fiți atenți în alegerea metodei celei mai potrivite de protecție a informațiilor personale.

Sfaturi pentru o navigare sigură și responsabilă, bazată pe cookies.

Datorită flexibilității lor și a faptului că majoritatea dintre cele mai vizitate site-uri și cele mai mari folosesc cookieuri, acestea sunt aproape inevitabile. Dezactivarea cookie-urilor nu va permite accesul utilizatorului pe site-urile cele mai răspândite și utilizate printre care Youtube, Gmail, Yahoo.și.altele.

Iată câteva sfaturi care vă pot asigura că navigați fără griji, însă cu ajutorul cookieurilor:

- Particularizați-vă setările browserului în ceea ce privește cookie-urile pentru a reflecta un nivel confortabil pentru voi al securității utilizării cookie-urilor.
- Dacă nu vă deranjează cookie-urile și sunteți singura persoană care utilizează computerul, puteți seta termene lungi de expirare pentru stocarea istoricului de navigare și al datelor personale de acces.
- Dacă împărțiți accesul la calculator, puteți lua în considerare setarea browserului pentru a șterge datele individuale de navigare de fiecare dată când închideți browserul. Aceasta este o variantă de a accesa site-urile care plasează cookieuri și de a șterge orice informație de vizitare la închiderea sesiunii de navigare.
- Instalați-vă și actualizați-vă constant aplicații antispyware.

Multe dintre aplicațiile de detectare și prevenire a spyware-ului includ detectarea atacurilor pe site-uri. Astfel, împiedică browserul de la a accesa website-uri care ar putea să exploateze vulnerabilitățile browserului sau să descarce software periculos.

Asigurați-vă că aveți browserul mereu actualizat.

Multe dintre atacurile bazate pe cookies se realizează exploatând punctele slabe ale versiunilor vechi ale browserelor.

Cookie-urile sunt pretutindeni și nu pot fi evitate dacă doriți să vă bucurați de acces pe cele mai bune și cele mai mari site-uri de pe Internet – locale sau internaționale. Cu o înțelegere clară a modului lor de operare și a beneficiilor pe care le aduc, puteți lua măsurile necesare de securitate astfel încât să puteți naviga cu încredere pe internet.

Dezactivarea și refuzul de a primi cookie-uri pot face anumite site-uri impracticabile sau dificil de vizitat și folosit. De asemenea, refuzul de a accepta cookie-uri nu înseamnă că nu veți mai primi/vedea publicitate online.

Este posibilă setarea din browser pentru ca aceste cookie-uri să nu mai fie acceptate sau poți seta browserul să accepte cookie-uri de la un site anumite. Dar, de exemplu, dacă nu ești înregistrat folosind cookie-urile, nu vei putea lăsa comentarii. Toate browserele moderne oferă posibilitatea de a schimba setările cookie-urilor. Aceste setări se găsesc de regulă în "opțiuni" sau în meniul de "preferințe" al browserului tău.

ACORD DE PRELUCRARE A DATELOR CU CARACTER PERSONAL

Acest acord de prelucrare date personale („**Acordul**”) a fost încheiat între:

SALUBRIZARE SECTOR 5 S.A., având punctul de lucru situat în București, sector 5, B-dul Rahova reprezentată prin ANDREI FECIORU, în calitate de **Director General**, denumită în continuare „**Operatorul**”,
și

....., având sediul în București,, înregistrată la sub nr, Cod Unic de Înregistrare....., reprezentată prin, în calitate de **Director General** denumită în continuare „**Persoana Împuternicită de Operator**”,

denumite în continuare în mod colectiv, „**Părțile**” și individual, „**Partea**”.

1. DEFINIȚII

„**Contract**” înseamnă **Contractul**sub nrși la CMPCVB SA sub nr., încheiat la data de

„**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;

„**Date cu caracter Personal ale Operatorului și ale Persoanei împuternicită de Operator**” sau orice altă exprimare similară, înseamnă Datele Personale pe care Operatorul le pune la dispoziția Persoanei Împuternicite de Operator, în vederea îndeplinirii Contractului, precum și orice alte Date Personale deținute de Operator la care Persoana Împuternicită de Operator are sau dobândește acces în scopul îndeplinirii obligațiilor care îi revin conform Contractului;

„**GDPR**” înseamnă Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului Uniunii Europene 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);

„**Incident de securitate privind Datele Personale**” înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a Datelor Personale transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea;

„Măsuri tehnice și organizatorice” înseamnă acele măsuri destinate protejării Datelor Personale stocate cât și a celor transmise în cadrul rețelei interne sau către persoane terțe, precum criptare, pseudonimizare, firewall, antivirus etc. ;

„Prelucrare” înseamnă orice operațiune sau set de operațiuni efectuate asupra Datelor Personale sau asupra seturilor de Date Personale, 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;

„Servicii” înseamnă serviciile prestate de Persoana Împuternicită de Operator pentru Operator care implică prelucrare de Date Personale, astfel cum sunt acestea prevăzute în Contract;

„DPO” înseamnă persoana desemnată de Operator, responsabilă cu prelucrarea datelor cu caracter personal.

2. PRELUCRAREA DATELOR PERSONALE

2.1. Îndeplinirea obligațiilor asumate prin Contract și furnizarea Serviciilor implică prelucrarea de Date Personale de către Persoana Împuternicită de Operator. În acest sens, Persoana Împuternicită de Operator se obligă să respecte toate dispozițiile legale aplicabile cu privire la protecția datelor cu caracter personal.

2.2. Operatorul declară și garantează prin prezenta că Datele Personale care fac obiectul prelucrării de către Persoana Împuternicită de Operator în baza prezentului Acord au fost colectate cu respectarea tuturor dispozițiilor legale aplicabile și pot fi prelucrate în condițiile descrise în prezentul Acord.

2.3. Persoana Împuternicită de Operator va prelucra Datele Personale ale Operatorului exclusiv în scopul furnizării Serviciilor către Operator. În acest sens, Persoana Împuternicită de Operator va acționa exclusiv în limitele prevăzute de Contract și de prezentul Acord, precum și în limita oricăror instrucțiuni documentate ulterioare ale Operatorului.

2.4. Persoana Împuternicită de Operator informează imediat Operatorul în cazul în care, în opinia sa, o instrucțiune primită din partea Operatorului încalcă legislația aplicabilă privind protecția Datelor Personale.

2.5. Persoana Împuternicită de Operator va da curs tuturor solicitărilor de informații și/sau documente formulate de Operator, în scopul verificării respectării de către Persoana Împuternicită de Operator a obligațiilor legale privind protecția Datelor Personale. De asemenea, Persoana Împuternicită de Operator va permite și va contribui activ la orice inspecție desfășurată de către Operator în acest sens, fără ca aceasta să fie prea împovărătoare sau să necesite eforturi disproporționate sau nerezonabile din partea Persoanei Împuternicite de Operator.

2.6. În temeiul GDPR, Persoana Împuternicită de Operator va crea și menține un registru al activităților de prelucrare desfășurate conform prezentului Acord și va pune la dispoziția Operatorului sau oricărui auditor sau mandatar numit de acesta, la cerere, toate informațiile incluse în registrul menționat necesare pentru a demonstra respectarea prezentului Acord.

2.7. Dacă Operatorul solicită, Persoana Împuternicită de Operator îl va asista pe Operator cu privire la desfășurarea unei evaluări a impactului asupra protecției datelor, ținând cont de natura prelucrării și de informațiile disponibile Persoanei Împuternicite de Operator.

2.8. *Tipurile de date cu caracter personal care fac obiectul prelucrării, în baza contractului:*

- *pentru părțile contractante:* numele și prenumele reprezentanților legali pentru cele două instituții semnatare ale contractului;
- *părțile vizate:* numele și prenumele, codul numeric personal, seria și numărul actului de identitate, adresa poștală, adresa e-mail de contact, telefon, fax, după caz, precum și toate informațiile necesare derulării contractului.

2.9. *Durata prelucrării:* durata contractuală, la care se adaugă încă 5 ani după împlinirea duratei contractuale.

2.10. *Locul unde se prelucrează datele cu caracter personal:* la sediile părților contractante, precum și așa cum sunt acestea definite prin contract;

2.11. *Natura și scopul prelucrării:* Părțile contractante vor prelua datele cu caracter personal, având temei legal, contractual și pe bază de consimțământ scris. Scopul prelucrării este reprezentat de îndeplinirea drepturilor și obligațiilor contractuale și a activităților corelate pentru îndeplinirea respectivelor drepturi și obligații.

2.12. *Dreptul de proprietate asupra datelor cu caracter personal:* titularii datelor cu caracter personal sunt și vor rămâne proprietarii respectivelor date cu caracter personal;

Drepturile și obligațiile părților contractante cu privire la prelucrarea datelor cu caracter personal:

- a) Părțile vor prelucra datele cu caracter personal în mod legal, echitabil și transparent față de persoanele vizate;
- b) Părțile vor colecta datele personale ale persoanelor vizate, pe bază de consimțământ scris, în scopuri determinate, explicite și legitime, ulterior nefiind permisă prelucrarea într-un mod incompatibil scopurilor menționate în prezentul act adițional;
- c) Părțile se vor asigura că datele personale ale persoanelor vizate, care sunt prelucrate sunt adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate;
- d) Datele cu caracter personal vor fi stocate de părți într-o formă care să permită identificarea persoanelor vizate, pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate, respectiv pe toată durata contractuală și încă timp de 1 an după împlinirea duratei contractuale;
- e) Părțile garantează că datele personale sunt prelucrate într-un mod care asigură securitatea adecvată a datelor, inclusiv protecția împotriva prelucrării neautorizate sau ilegale, împotriva pierderii, a distrugerii sau a deteriorării accidentale;
- f) Părțile se obligă reciproc să pună în aplicare măsuri tehnice și organizatorice proprii, adecvate pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu Regulamentul privind protecția datelor cu caracter personal, revizuiind și actualizând în mod efectiv respectivele măsuri;
- g) Măsurile tehnice și organizatorice trebuie să asigure faptul că sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific prelucrării;
- h) Părțile se asigură că persoanele autorizate să prelucreze datele cu caracter personal păstrează confidențialitatea respectivelor date;
- i) Părțile au obligația să se informeze reciproc cu privire la orice date cu caracter personal eronate, rectificate, actualizate sau șterse la adresele de e-mail menționate în cuprinsul contractului.

2.15. Raportarea încălcării securității datelor cu caracter personal:

Părțile se obligă să își notifice reciproc orice violare a datelor cu caracter personal prelucrate, în termen de 24 de ore de la data la care au luat la cunoștință de aceasta și să își transmită reciproc, în scris informații despre încălcarea securității datelor cu caracter personal.

În ceea ce privește fiecare încălcare, fiecare parte va ajuta pe cealaltă, în orice mod, care va include furnizarea de informații suficiente, precum și sprijin în investigațiile efectuate de către autoritatea de supraveghere și reglementare, cu scopul de a remedia și de a investiga încălcarea, de a preveni viitoare incidente, de a limita impactul incidentului asupra părților implicate și/sau limita prejudiciul produs, ca o consecință a încălcării securității datelor.

Partea la care a survenit incidentul cu privire la securitatea datelor, este exonerată față de cealaltă parte, pentru prejudiciul suferit, ca urmare a încălcării securității datelor cu caracter personal prelucrate, dacă dovedește că a luat măsurile adecvate organizatorice și tehnice pentru asigurarea respectivei securități. Orice prejudiciu va fi constatat de instanțele de judecată competente.

2.16. Autoritatea de supraveghere și reglementare.

Părțile agreează că autoritatea de supraveghere și reglementare este Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal.

3. MĂSURI TEHNICE ȘI ORGANIZATORICE

3.1. Persoana Împuternicită de Operator va obține și va menține toate licențele, autorizațiile și avizele, solicitate astfel prin legislația aplicabilă, necesare pentru a prelucra Date Personale, precum și orice alte date și informații derivate din acestea.

3.2. Persoana Împuternicită de Operator se obligă să implementeze și să mențină toate măsurile tehnice și organizatorice prevăzute, pe toată durata Acordului și ulterior, până la ștergerea sau distrugerea Datelor Personale ale Operatorului.

3.3. Persoana Împuternicită de Operator va notifica Operatorul cu privire la orice Incident de Securitate privind Datele Personale, în cel mult 48 de ore din momentul în care a luat la cunoștință despre acesta. De asemenea, Persoana Împuternicită de Operator va comunica Operatorului, dacă este posibil, natura încălcării, volumul de date și numărul aproximativ de persoane afectate, precum și măsurile luate sau propuse spre a fi luate în vederea remedierii sau atenuării efectelor negative ale incidentului.

4. DREPTURILE PERSOANELOR VIZATE

4.1. Persoana Împuternicită de Operator, luând în considerare natura prelucrării și în limita posibilităților, îl va asista pe Operator să dea curs oricăror plângeri sau solicitări formulate de persoanele vizate, cu privire la prelucrarea Datelor Personale, în conformitate cu drepturile persoanelor vizate prevăzute în Capitolul III din GDPR.

4.2. În acest sens, Persoana Împuternicită de Operator îl va informa pe Operator cu privire la orice plângere sau solicitare primită de la persoanele vizate, în termen de 3 zile din momentul recepționării, și va furniza acestuia orice informații sau documente relevante în vederea soluționării acestora.

5. CONFIDENȚIALITATEA DATELOR PERSONALE

5.1. Obligațiile de confidențialitate prevăzute în Contract, se aplică în mod corespunzător și cu privire la Datele Personale ale Operatorului.

5.2. Persoana Împuternicită de Operator este obligată să se asigure că DPO care are datoria de a prelucra Datele Personale ale Operatorului a informat Operatorul cu privire la obligativitatea acestuia de a încheia angajamente de confidențialitate sau au obligații de confidențialitate profesionale sau legale, după caz.

5.3. La încetarea prezentului Acord, din orice motiv, Persoana Împuternicită de Operator, la alegerea Operatorului, va șterge sau va returna toate Datele Personale ale Operatorului, inclusiv orice copii de rezervă a acestora, cu excepția cazului când stocarea acestora pe o perioadă mai lungă este prevăzută de dispozițiile legale aplicabile. Persoana Împuternicită de Operator va transmite Operatorului o declarație scrisă care să confirme îndeplinirea tuturor cerințelor de ștergere și/sau returnare a Datelor Personale ale Operatorului.

6. ÎNCETARE

6.1. Prezentul Acord încetează de drept la momentul încetării Contractului.

6.2. Cu toate acestea, orice obligație a Persoanei Împuternicite de Operator în baza prezentului Acord, care prin natura ei supraviețuiește încetării Acordului, va continua să producă efecte și după încetarea acestuia.

7. DISPOZIȚII FINALE

7.1. În cazul existenței unor neconcordanțe între prevederile acestui Acord și orice alte acorduri încheiate între Părți, inclusiv, dar fără a se limita la Contract, prevederile acestui Acord vor prevala cu privire la obligațiile Părților de protecție a Datelor Personale.

7.2. Acest Acord și disputele care pot apărea ca urmare a încheierii, executării, interpretării sau încetării sale vor fi guvernate de legile României.

7.3. În caz de dispute, pretenții sau alte asemenea decurgând din acest Acord, Părțile vor încerca să ajungă la o soluționare a acestora pe cale amiabilă. Dacă nu se poate ajunge la o soluționare pe cale amiabilă a acestora, disputa va fi supusă și soluționată de instanța judecătorească competentă română.

7.4. Acest Acord nu presupune plata unei remunerații suplimentare de către oricare dintre Părți și nu derogă de la Contract, în ceea ce privește condițiile financiare stabilite de către Părți.

7.5. Dacă orice prevedere a acestui Acord este sau devine nulă sau inaplicabilă, restul Acordului va rămâne valabil și va produce efecte. Dacă orice prevedere a Acordului este sau devine nulă, ilegală sau inaplicabilă, se va considera ca fiind modificată strict cât este necesar pentru a o face validă, legală și aplicabilă, cu condiția ca asta să nu declanșeze o modificare esențială cu privire la înțelegerea comercială inițială a Părților, conform acestui Acord. Altfel, Părțile vor negocia cu bună-credință

înlocuirea clauzei nule, ilegale sau inaplicabile, cu o clauză validă, legală și aplicabilă, păstrând pe cât posibil, efectele comerciale ale clauzei inițiale.

7.6. Prezentul Acord și Contractul, în măsura în care se referă la orice aspect ce vizează prelucrarea Datelor Personale, reprezintă întreaga voință a Părților referitor la prelucrarea Datelor Personale ale Operatorului în vederea furnizării Serviciilor și nu poate fi modificat decât cu acordul scris al ambelor Părți.

7.7. Părțile la acest Acord declară și agreează că acest Acord a fost prezentat fiecăreia dintre Părți, a fost în mod atent și detaliat analizat și evaluat de fiecare Parte, și că au fost asistate pe tot parcursul redactării, negocierii și semnării, de consultanți și experți calificați (cel puțin dintr-o perspectivă legală, tehnică și fiscală).

7.8. Părțile declară și agreează că acest Acord nu reprezintă un contract de adeziune, nu include clauze standard și/sau neuzuale, așa cum sunt acestea definite în legislația românească în mod expres și Acordul a fost negociat „clauză cu clauză” de către Părți. Fiecare Parte agreează și acceptă, în mod irevocabil de la semnarea Acordului de către fiecare Parte, toate clauzele acestuia.

Prezentul Acord a fost redactat și semnat în (2) două exemplare originale, astăzi,.....

OPERATOR
SALUBRIZARE SECTOR 5 S.A.
Director General
ANDREI FECIORU

PERSOANA ÎMPUTERNICITĂ DE OPERATOR
„Firma IT,,
Director General

ACORD DE PRELUCRARE A DATELOR CU CARACTER PERSONAL

SALUBRIZARE SECTOR 5 S.A. (S 5 S.A.)

se află sub autoritatea Consiliului Local al Primăriei Sector 5 al Municipiului București, având ca domeniu principal de activitate „Colectare deseuri nepericuloase”.

Datele de identificare sunt:

- Sediul societății este în România, Municipiul București, sector 5, Cal. Rahova ;
- Număr de înmatriculare la Registrul Comerțului: nr.;
- Cod unic de identificare:
- Capital social integral de stat : lei;
- Telefon:
- E-mail: office@salubrizare5.ro

Vă informăm cu privire la prelucrarea de date cu caracter personal, denumite în continuare Date, pe care o facem în cazul în care datele sunt primite direct de la persoanele vizate în baza derulării raporturilor comerciale/contractuale sau participări la anumite acțiuni și evenimente desfășurate de S 5 S.A. sau vizitați site-ul.

S 5 S.A. prelucrează Datele numai în condițiile prevăzute de Regulamentul General privind Protecția Datelor nr. 679/2016 al Uniunii Europene, denumit în continuare Regulamentul, conform scopurilor și temeiurilor reflectate în secțiunile de următoare.

„*Prelucrare*” înseamnă orice operațiune sau set de operațiuni efectuate asupra Datelor cu caracter personal sau asupra seturilor de Date personale, 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.

Tipurile de date cu caracter personal care fac obiectul prelucrării, în baza contractului:

- *pentru părțile contractante:* numele și prenumele și funcțiile reprezentanților legali pentru cele două instituții/societăți semnatare ale contractului;

- *părțile vizate:* numele și prenumele, codul numeric personal, seria și numărul actului de identitate, adresa poștală, adresa e-mail de contact, telefon, fax, după caz, precum și toate informațiile necesare derulării contractului.

Durata prelucrării: durata contractuală, la care se adaugă încă 5 ani după împlinirea duratei contractuale, conform legilor în vigoare.

Locul unde se prelucrează datele cu caracter personal: la sediile părților contractante, precum și așa cum sunt acestea definite prin contract.

Natura și scopul prelucrării

Părțile contractante vor prelua datele cu caracter personal, având temei legal, contractual și pe bază de consimțământ scris. Scopul prelucrării este reprezentat de îndeplinirea drepturilor și

obligărilor contractuale și a activităților corelate pentru îndeplinirea respectivelor drepturi și obligații, cum ar fi:

- evaluarea eligibilității în vederea furnizării unor produse și servicii;
- derularea oricăror raporturi contractuale (cu clienții, colaboratorii, partenerii sau angajații noștri);
- monitorizarea tuturor obligațiilor asumate față de S 5 S.A. sau față de entități afiliate;
- îndeplinirea obligațiilor în materie fiscală;
- constatarea, exercitarea sau apărarea unor drepturi în instanță ori față de alte autorități;
- gestionarea de solicitări/reclamații/plângeri/petiții/investigații în legătură cu activitatea S 5 S.A. și serviciile ori produsele acesteia;
- asigurarea securității în incintele S 5 S.A.;
- administrarea portofoliului de clienți, furnizori și colaboratori;
- păstrarea/depozitarea/ stocarea și arhivarea documentelor;
- furnizarea de raportări și informații la solicitarea autorităților (de exemplu, instanțe, organe de cercetare, organe de executare silită, notari publici, autorități fiscale);
- punerea în executare a hotărârilor judecătorești și a altor ordine ale autorităților;
- gestionarea auditurilor, a raportărilor, precum și controalelor și investigațiilor din partea autorităților naționale, locale sau europene;
- îmbunătățirea calității serviciilor furnizate prin eficientizarea fluxurilor, optimizarea costurilor, pregătirea angajaților etc;
- diversificarea produselor și serviciilor și adaptarea acestora la nevoile clienților, administrarea afacerii, inclusiv prin fuziuni, achiziții, transferuri de portofolii sau de părți ale afacerii, ori prin alte tranzacții similare;
- marketing simplu și efectuare de sondaje cu privire la serviciile oferite de S 5 S.A. și activitatea acesteia.
- orice alte categorii de date pe care clienții le furnizează către S 5 S.A. sau pe care aceasta le dobândește și le prelucrează cu respectarea legii sau a contractelor aplicabile în relația cu clienții.

Date cu caracter special

- De regulă, nu solicităm și nu prelucrăm Date cu caracter special;
- Totuși, având în vedere specificul activității noastre, protecție civilă și voluntariat, este posibil ca pe parcursul derulării unor evenimente publice, să intrăm în posesia unor Date cu caracter special, cum ar fi cele legate de starea de sănătate. În această situație, Datele respective vor fi prelucrate în strictă conformitate cu Regulamentul.

Dreptul de proprietate

Titularii datelor cu caracter personal sunt și vor rămâne proprietarii respectivelor date cu caracter personal.

Partajarea/dezvăluirea Datelor

S 5 S.A., pentru a putea desfășura activitatea la cele mai înalte standarde, în urmărirea intereselor noastre legitime ori pentru că suntem obligați prin lege, este posibil să dezvăluim sau să transmitem Date către anumite persoane sau entități, cum ar fi:

- reprezentanții legali (membrii AGA, membrii CA, tutore, curator), împuterniciți ai clientului ori ai persoanei vizate;
- consultanți (juridici, fiscali, etc), executori judecătorești, auditori, notari, experți, traducători;
- parteneri contractuali și prestatori de servicii cum ar fi: printare extrase și notificări, curierat, servicii IT și telecomunicații, furnizori, arhivare, de distrugere documente, etc;
- asociații profesionale, autorități de supraveghere locale, autorități de protecție a consumatorilor etc;

- instanțe de judecată și alte entități autorizate de lege să primească informații financiare (organe de executare silită, organe fiscale etc.);
- Agenția Națională de Administrare Fiscală, în scopul transmiterii de informații, în conformitate cu regulile și legile în vigoare.

În unele cazuri, destinatarii Datelor au obligația legală de păstrare a secretului profesional (autoritățile, avocații, experții, alte instituții financiare etc). În celelalte cazuri, vom solicita, contractual, respectarea confidențialității, inclusiv luarea măsurilor tehnice și organizatorice adecvate pentru asigurarea securității Datelor. S 5 S.A. nu va putea condiționa dezvăluirea Datelor de luarea unor astfel de măsuri și de asumarea unei obligații de confidențialitate, când Datele sunt dezvăluite în baza unei obligații legale sau în apărarea unui interes legitim.

Implicațiile refuzului de a furniza Date

Puteți alege să nu furnizați Date către S 5 S.A., însă această opțiune poate determina lipsa conformării cu obligațiile noastre contractuale sau legale. Poate limita serviciile pe care suntem capabili să vi le oferim. Ne poate împiedica să continuăm a vă furniza sau a vă reînnoi produsele și serviciile existente.

În cazul în care nu sunteți de acord cu prelucrarea Datelor, în scop de marketing sau în orice alt scop pentru care v-am solicitat în mod expres acordul, precum și în situația în care vă retrageți acordul dat, relația dumneavoastră contractuală cu S 5 S.A. nu va suferi.

Prelucrarea datelor în afara Spațiului Economic European (SEE)

În prezent, în vederea îndeplinirii scopurilor pe care vi le-am înfățișat în această politică S 5 S.A. nu transferă Date în afara României, în state din cadrul SEE și nici în afara SEE.

Drepturile persoanei vizate

În legătură cu prelucrarea exclusiv a Datelor dumneavoastră, beneficiați de unele drepturi pe care le puteți exercita la cerere și în mod gratuit, în limitele și în măsura îndeplinirii condițiilor legale, după cum urmează:

Dreptul de acces la date - puteți verifica efectuarea prelucrării Datelor dumneavoastră de către S 5 S.A., precum și detalii cu privire la prelucrare;

Dreptul la rectificare - puteți solicita rectificarea Datelor inexacte sau suplimentarea Datelor incomplete;

Dreptul la ștergerea datelor ("dreptul de a fi uitat") - îl puteți exercita în măsura în care sunt îndeplinite condițiile prevăzute de lege (de exemplu, dacă Datele nu mai sunt necesare scopului prelucrării sau au fost prelucrate ilegal);

Dreptul la restricționarea prelucrării - puteți solicita limitarea prelucrării Datelor, de exemplu în caz de contestare a legalității prelucrării;

Dreptul la portabilitatea datelor - ne puteți solicita ca Datele prelucrate prin mijloace automate, pe bază de consimțământ sau în temeiul unui contract, să vi le transmitem dumneavoastră sau către un alt operator de date, dacă acest lucru este tehnic fezabil;

Dreptul la opoziție - vă puteți opune în orice moment, din motive întemeiate și legitime legate de situația dumneavoastră particulară, ca Datele dumneavoastră să facă obiectul unei prelucrări, inclusiv prin crearea de profiluri; de asemenea, vă puteți opune în orice moment, în mod gratuit și fără nicio justificare, ca Datele să fie prelucrate în scop de marketing;

Dreptul de a nu fi supus unei decizii individuale - puteți cere și obține retragerea, anularea sau reevaluarea oricărei decizii bazate exclusiv pe prelucrări efectuate prin mijloace automate

(incluzând crearea de profiluri) care produce efecte juridice cu privire la dumneavoastră sau vă afectează în mod similar, într-o măsură semnificativă;

Dreptul de a depune o plângere în fața unei autorități sau de a vă adresa justiției - aveți dreptul de a vă adresa cu plângere Autorității Naționale de Supraveghere a prelucrării datelor cu caracter personal, respectiv de a vă adresa justiției pentru apărarea oricăror drepturi garantate de legislația aplicabilă în domeniul protecției datelor cu caracter personal, care au fost încălcate, în măsura în care considerați necesar.

Măsuri tehnice și organizatorice

Părțile semnatare se obligă să implementeze și să mențină toate măsurile tehnice și organizatorice prevăzute, pe toată durata Acordului și ulterior, până la ștergerea sau distrugerea datelor cu caracter personal ale acestora.

Părțile se vor notifica cu privire la orice Incident de Securitate privind datele cu caracter personal, în cel mult 48 de ore din momentul în care a luat la cunoștință despre acesta. De asemenea, dacă este posibil, natura încălcării, volumul de date și numărul aproximativ de persoane afectate, precum și măsurile luate sau propuse spre a fi luate în vederea remedierii sau atenuării efectelor negative ale incidentului.

Partea la care a survenit incidentul cu privire la securitatea datelor, este exonerată față de cealaltă parte, pentru prejudiciul suferit, ca urmare a încălcării securității datelor cu caracter personal prelucrate, dacă dovedește că a luat măsurile adecvate organizatorice și tehnice pentru asigurarea respectivei securități. Orice prejudiciu va fi constatat de instanțele de judecată competente.

Responsabilul cu protecția datelor

Vă puteți exercita oricare dintre drepturile legale în legătură cu prelucrarea Datelor printr-o cerere scrisă, datată și semnată olograf (de mână), transmisă în format hârtie la sediul companiei sau electronic prin e-mail, scanat, la office@salubrizare5.ro. De asemenea, vă puteți adresa Responsabilului nostru cu protecția datelor cu caracter personal

Prezentul acord se semnează odată cu încheierea contractului comercial.

Prin semnarea prezentului acord, dumneavoastră confirmați că ați citit, ați fost informat/informată corect și sunteți de acord cu prevederile acestui document, precum și de faptul că, S 5 S.A. nu va prelucra datele dumneavoastră cu caracter personal decât în măsura în care acest demers este necesar scopurilor menționate în acest document, cu respectarea măsurilor legale de securitate și confidențialitate a Datelor.

Totodată, prin semnarea acestui document vă dați consimțământul liber și documentat cu privire la prelucrarea datelor dumneavoastră cu caracter personal.

**Director General
ANREI FECIORU**

Reperzentant client/furnizor

**Compartiment Juridic
Canbolant Singrid**

FORMULAR CERERE PERSOANĂ VIZATĂ
(pentru exercitarea drepturilor prevăzute la art. 7, 12-22 din GDPR)

Detalii privind persoana vizată (titularul cererii):

Modalitate de adresare:	
Nume, prenume:	
Modalitate de contact (adresă de e-mail sau adresă poștală):	
ID client (dacă este cazul):	

Obiectul cererii:

Vă rugăm să selectați care este obiectul cererii:

- Retragere a consimțământului pentru prelucrarea de date cu caracter personal*
- Cerere de acces la datele cu caracter personal prelucrate*
- Cerere de rectificare a datelor cu caracter personal prelucrate*
- Cerere de ștergere a datelor cu caracter personal prelucrate*
- Cerere de restricționare a prelucrării datelor cu caracter personal*
- Cerere de portare a datelor cu caracter personal prelucrate*
- Cerere de opoziție la prelucrarea datelor cu caracter personal*
- Cerere privind prelucrările automate și crearea de profile*

Categoriile de date cu caracter personal care fac obiectul cererii:

--

Detalii privind cererea dumneavoastră:

--

Nume, prenume: poștal):	
Semnătură (în cazul cererilor trimise prin serviciul poștal):	
Data:	