					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: PII09					Titlul documentului: **Politica privind colectarea, utilizarea, divulgarea și partajarea informațiilor cu caracter personal (PII)**							
Versiunea: 1.0		Data intrării în vigoare: 01.01.2025			Proprietarul documentului:							
X	Politică		Standard		Procedură		Formular		Registru		Altul	

Istoricul reviziilor				
Numărul reviziei	**Data reviziei**	**Modificări**	**Revizuit de**	**Proprietarul procesului**

Aprobări			
Nume	**Funcție**	**Data**	**Semnătură**

Aliniată la standardele și reglementările aplicabile

Standard / reglementare	Clauză / control / articol	Applicability	Coverage Type	Comentariu
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Control operațional documentat
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorizare și acțiune corectivă
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.9	Controller	Primary	Scopuri și înregistrări de prelucrare
ISO/IEC 27701:2025	Annex A.1.2.3	Controller	Referenced	Legătură cu temeiul juridic
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Supporting	Responsabilități de partajare ale operatorilor asociați
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5	Controller	Primary	Limite privind colectarea, prelucrarea și minimizarea
ISO/IEC 27701:2025	Annex A.1.5.2; Annex A.1.5.3	Conditional	Referenced	Legătură privind rutarea transferurilor
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Înregistrări privind transferurile și divulgările
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Primary	Instrucțiuni și înregistrări ale persoanei împuternicite
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Referenced	Legătură privind rutarea transferurilor efectuate de persoana împuternicită
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Înregistrări și solicitări privind divulgările persoanei împuternicite
GDPR	Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Primary	Limitarea scopului, minimizare și responsabilitate
GDPR	Article 6	Controller	Referenced	Legătură cu temeiul juridic

GDPR	Article 24	Controller	Supporting	Responsabilitatea operatorului
GDPR	Article 26	Joint Controller	Supporting	Aranjamente între operatori asociați
GDPR	Article 28	Both	Supporting	Instrucțiuni pentru persoanele împuternicite și limite de divulgare
GDPR	Article 30	Both	Supporting	Înregistrări privind prelucrarea și destinatarii
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Limitarea scopului, colectării, minimizării și divulgării
ISO/IEC 29100:2020	Clause 5.10; Clause 5.12	Both	Supporting	Responsabilitate și conformitate privind confidențialitatea
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7	Both	Supporting	Controale privind scopul, colectarea, minimizarea, utilizarea și divulgarea

1. Domeniu de aplicare

1.1 Prezenta politică definește cerințele pentru colectarea, utilizarea, divulgarea și partajarea PII în cadrul domeniului de aplicare al PIMS.

1.2 Prezenta politică se aplică pentru:

1.2.1 colectarea PII prin canale directe, indirecte, automatizate, manuale, interne, externe și ale terților;

1.2.2 utilizarea internă aprobată a PII de către procesele, sistemele și aplicațiile organizației;

1.2.3 utilizarea secundară a PII pentru un scop nou sau modificat semnificativ;

1.2.4 divulgarea externă a PII către destinatari, parteneri, autorități, persoane împuternicite, persoane subîmputernicite, furnizori și alți terți;

1.2.5 aranjamente recurente de partajare a datelor și divulgări punctuale;

1.2.6 contexte de operator, operator asociat, persoană împuternicită și persoană subîmputernicită;

1.2.7 REG02 - Inventarul prelucrărilor PII / ROPA, REG08 - Registrul persoanelor împuternicite, al persoanelor subîmputernicite și al partajării datelor, REG09 - Registrul transferurilor internaționale și REG12 - Registrul de audit, neconformități, acțiuni corective și îmbunătățiri.

1.3 Prezenta politică nu înlocuiește:

1.3.1 PII03 pentru inventarul prelucrărilor, temeiul juridic și responsabilitatea asupra ROPA;

1.3.2 PII04 pentru conținutul notelor de informare privind confidențialitatea, publicarea și controlul versiunilor;

1.3.3 PII05 pentru operarea consimțământului și a preferințelor;

1.3.4 PII06 pentru gestionarea cererilor de exercitare a drepturilor persoanelor vizate;

1.3.5 PII07 pentru metodologia DPIA și evaluarea riscurilor privind confidențialitatea;

1.3.6 PII08 pentru punctele de control privind protecția datelor încă din faza de proiectare;

1.3.7 PII10 pentru executarea retenției, ștergerii și eliminării;

1.3.8 PII11 pentru managementul acurateței și calității;

1.3.9 PII12 pentru guvernanța ciclului de viață al persoanelor împuternicite, al persoanelor subîmputernicite și al terților;

1.3.10 PII13 pentru selectarea mecanismului de transfer internațional și controalele riscurilor de transfer;

1.3.11 PII14 pentru securitatea PII și controlul accesului;

1.3.12 PII15 pentru gestionarea incidentelor și a încălcărilor;

1.3.13 PII18 pentru guvernanța la nivelul întregului PIMS privind monitorizarea, auditul, neconformitățile, acțiunile corective și îmbunătățirea.

1.4 În sensul prezentei politici:

1.4.1 „utilizare aprobată” înseamnă o utilizare a PII care este înregistrată în REG02 pentru o anumită activitate de prelucrare, un anumit scop, o categorie PII, o categorie de persoane vizate, un proprietar de proces și rolul PIMS aplicabil.

1.4.2 „colectare” înseamnă obținerea PII direct de la o persoană vizată, indirect de la o altă parte, automat dintr-un sistem sau dispozitiv ori printr-o sursă de date internă sau externă.

1.4.3 „utilizare secundară” înseamnă utilizarea PII într-un scop care nu este deja înregistrat ca scop aprobat în REG02 pentru activitatea de prelucrare relevantă.

1.4.4 „verificare a compatibilității” înseamnă o evaluare documentată în REG02 a scopului inițial, a scopului propus, a dependenței de temeiul juridic, a categoriilor PII, a așteptărilor persoanelor

vizate, a justificării minimizării, a impactului divulgării sau transferului și a rutării către alte politici PIMS, atunci când este necesar.

1.4.5 „divulgare externă” înseamnă punerea PII la dispoziția unei părți din afara organizației sau din afara lanțului documentat de instrucțiuni ale clientului.

1.4.6 „partajarea datelor” înseamnă un aranjament recurent sau structurat în temeiul căruia PII sunt divulgate, transferate, accesate, schimbate sau puse la dispoziția unei alte părți.

1.4.7 „partajare recurentă sensibilă” înseamnă partajarea recurentă care implică PII din categorii speciale, PII privind infracțiuni, PII ale copiilor, înregistrări cu impact ridicat, partajare la scară largă sau partajare externă care implică o locație de transfer înregistrată în REG09.

2. Scop

2.1 Scopul prezentei politici este de a asigura că PII sunt colectate, utilizate, divulgate și partajate numai pentru scopuri documentate, aprobate, limitate și supuse responsabilității.

2.2 Prezenta politică permite organizației să demonstreze că activitățile de colectare și utilizare sunt legate de înregistrările de prelucrare din REG02, că divulgările și aranjamentele de partajare a datelor sunt înregistrate în REG08, că rutarea transferurilor internaționale este legată de REG09 și că excepțiile și neconformitățile sunt gestionate prin REG12.

3. Obiective

3.1 Obiectivele prezentei politici sunt:

3.1.1 limitarea colectării la PII necesare pentru scopurile documentate;

3.1.2 asigurarea aprobării utilizării interne a PII înainte de începerea prelucrării;

3.1.3 impunerea verificărilor de compatibilitate înainte de utilizarea secundară;

3.1.4 impunerea aprobării și a dovezilor înainte de divulgarea externă;

3.1.5 menținerea dovezilor privind partajarea datelor în REG08, fără crearea unui registru separat de partajare a datelor;

3.1.6 rutarea dependențelor privind transferurile internaționale către REG09 și PII13, fără duplicarea controalelor privind mecanismul de transfer;

3.1.7 definirea periodicității revizuirii pentru partajarea recurentă;

3.1.8 menținerea dovezilor pregătite pentru audit privind colectarea, utilizarea, divulgarea, partajarea, excepțiile și acțiunile corective.

4. Declarații de politică

4.1 Limitarea colectării

4.1.1 [Controller] Process Owner / Business Owner MUST să înregistreze în REG02 scopul colectării, sursa sau canalul, categoriile PII, categoriile de persoane vizate și elementele minime de date înainte de începerea oricărei activități noi de colectare sau a oricărei modificări semnificative a colectării.

4.1.2 [Controller] Privacy Lead / PIMS Manager MUST să revizuiască înregistrarea colectării din REG02 înainte de începerea colectării atunci când se adaugă o nouă categorie PII, sursă, canal sau scop.

4.1.3 [Controller] Process Owner / Business Owner MUST să înregistreze în REG02 o justificare a necesității pentru fiecare element de date PII înainte ca elementul respectiv să fie colectat.

4.1.4 [Processor] Process Owner / Business Owner MUST să înregistreze în REG02 referința instrucțiunii clientului din REG08 înainte de colectarea PII în numele unui client.

4.1.5 [Joint Controller] Process Owner / Business Owner MUST să înregistreze în REG08 alocarea responsabilităților de colectare ale operatorilor asociați înainte de începerea colectării comune.

4.2 Controale privind utilizarea internă aprobată

4.2.1 [Controller] Process Owner / Business Owner MUST să înregistreze în REG02 regulile de utilizare internă aprobată pentru fiecare activitate de prelucrare înainte de începerea utilizării.

4.2.2 [Controller] System Owner / Application Owner MUST să implementeze numai câmpuri de flux de lucru, rapoarte sau exporturi pentru utilizare internă care au o regulă corespunzătoare de utilizare aprobată în REG02 înainte de lansarea în producție.

4.2.3 [Processor] Process Owner / Business Owner MUST să înregistreze în REG08 alinierea la instrucțiunile clientului înainte de utilizarea PII ale clientului pentru orice activitate de persoană împuternicită sau persoană subîmputernicită.

4.2.4 [Controller] Privacy Lead / PIMS Manager MUST să revizuiască regulile de utilizare aprobată din REG02 cel puțin anual pentru fiecare activitate de prelucrare activă.

4.2.5 [All] Privacy Lead / PIMS Manager MUST să înregistreze o neconformitate în REG12 în termen de cinci zile lucrătoare atunci când este identificată o utilizare internă nedocumentată a PII.

[... Secțiunile 4.3–8 nu sunt incluse în această previzualizare. Achiziționați documentul complet pentru a accesa conținutul integral. ...]

9. Excepții

9.1.1 [All] Process Owner / Business Owner MUST să înregistreze o solicitare de excepție în REG12 înainte de abaterea de la o regulă aprobată de colectare, utilizare, divulgare sau partajare.

9.1.2 [All] Privacy Lead / PIMS Manager MUST să înregistreze o decizie de aprobare sau respingere în REG12 înainte ca o excepție să fie activată.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor MUST să înregistreze recomandări în REG12 înainte de aprobarea unei excepții care implică utilizare secundară incompatibilă, partajare recurentă sensibilă, conflict privind o divulgare obligatorie din punct de vedere juridic sau rutarea transferului.

9.1.4 [All] Top Management MUST să înregistreze aprobarea în REG12 înainte de activarea oricărei excepții cu o durată mai mare de 30 de zile calendaristice sau care afectează mai mult de o activitate de prelucrare.

9.1.5 [All] Process Owner / Business Owner MUST să închidă o excepție în REG12 până la data expirării sau în termen de cinci zile lucrătoare după încetarea condiției care a generat excepția.

10. Aplicare

10.1.1 [All] Privacy Lead / PIMS Manager MUST să înregistreze colectarea, utilizarea, divulgarea sau partajarea neaprobată ca neconformitate în REG12 în termen de cinci zile lucrătoare de la identificare.

10.1.2 [Controller] Process Owner / Business Owner MUST să suspende colectarea, utilizarea, divulgarea sau partajarea în termen de o zi lucrătoare atunci când Privacy Lead / PIMS Manager înregistrează în REG12 absența dovezilor aprobate din REG02 sau REG08.

10.1.3 [Processor] Process Owner / Business Owner MUST să înregistreze o decizie de oprire sau escaladare în REG08 și REG12 în termen de o zi lucrătoare atunci când PII ale clientului sunt utilizate sau divulgate în afara instrucțiunilor documentate.

10.1.4 [All] Top Management MUST să revizuiască în REG12 neconformitățile nerezolvate cu impact ridicat privind colectarea, utilizarea, divulgarea sau partajarea în termen de 30 de zile calendaristice de la escaladare.

10.1.5 [All] Internal Audit / Compliance Reviewer MUST să verifice în REG12 dovezile de închidere a acțiunilor corective în termen de 15 zile lucrătoare după ce Privacy Lead / PIMS Manager marchează închiderea.

11. Revizuire și întreținere

11.1.1 [All] Privacy Lead / PIMS Manager MUST să revizuiască prezenta politică cel puțin anual și să înregistreze decizia în REG12.

11.1.2 [All] Privacy Lead / PIMS Manager MUST să revizuiască prezenta politică în termen de 30 de zile calendaristice de la o modificare semnificativă a domeniului de aplicare al PIMS, a scopurilor prelucrării, a modelului de partajare, a rutării transferurilor sau a obligației aplicabile și să înregistreze rezultatul în REG12.

11.1.3 [All] Process Owner / Business Owner MUST să recertifice înregistrările active REG02 și REG08 cel puțin anual și în termen de 30 de zile calendaristice de la o modificare semnificativă a prelucrării.

11.1.4 [All] Internal Audit / Compliance Reviewer MUST să includă controalele PII09 în eșantionarea anuală de audit și să înregistreze acoperirea în REG12.

11.1.5 [All] Privacy Lead / PIMS Manager MUST să actualizeze referințele la politicile conexe în REG12 în termen de zece zile lucrătoare atunci când PII03, PII08, PII10, PII12, PII13, PII14 sau PII18 modifică limita operațională a prezentei politici.

12. Politici conexe

12.1 Prezenta politică trebuie citită împreună cu:

12.2 PII01 - Politica privind Sistemul de management al informațiilor privind confidențialitatea

12.3 PII02 - Politica privind rolurile, responsabilitățile și răspunderea în materie de confidențialitate

12.4 PII03 - Politica privind inventarul prelucrărilor PII și temeiul juridic

12.5 PII04 - Politica privind notele de informare privind confidențialitatea și transparența

12.6 PII05 - Politica privind gestionarea consimțământului și a preferințelor

12.7 PII06 - Politica privind gestionarea drepturilor persoanelor vizate

12.8 PII07 - Politica privind evaluarea riscurilor privind confidențialitatea și DPIA

12.9 PII08 - Politica privind protecția datelor încă din faza de proiectare și în mod implicit

12.10 PII10 - Politica privind retenția, ștergerea și eliminarea PII

12.11 PII11 - Politica privind acuratețea și calitatea PII

12.12 PII12 - Politica privind managementul confidențialității pentru persoanele împuternicite, persoanele subîmputernicite și terți

12.13 PII13 - Politica privind transferul internațional al PII

12.14 PII14 - Politica privind securitatea PII și controlul accesului

12.15 PII15 - Politica privind gestionarea incidentelor și a încălcărilor referitoare la PII

12.16 PII17 - Politica privind informațiile documentate și managementul dovezilor în cadrul PIMS

12.17 PII18 - Politica privind monitorizarea, auditul și îmbunătățirea PIMS

13. Standarde și cadre de referință

13.1 Prezenta politică este mapată la următoarele standarde și reglementări. Maparea explică modul în care politica susține cerințele citate și identifică clauzele interne care le implementează sau le susțin.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Mapate la înregistrări operaționale documentate și la controlul dovezilor privind colectarea, utilizarea aprobată, utilizarea secundară, divulgarea, partajarea și rutarea transferurilor. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.3; 4.3.5; 4.4.1; 4.4.2; 4.5.1; 7.1.1; 7.1.4].

13.2.2 **Clause 9.1; Clause 10.2** - Mapate la monitorizare, măsurare, revizuire, gestionarea excepțiilor, neconformitate și acțiune corectivă pentru controalele privind colectarea, utilizarea, divulgarea și partajarea. Addressed by clauses [4.2.4; 4.2.5; 6.1.1; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 9.1.1; 10.1.1; 10.1.5; 11.1.4].

13.2.3 **Annex A.1.2.2; Annex A.1.2.9** - Mapate la scopurile documentate ale operatorului, la înregistrările de utilizare aprobată și la dovezile de prelucrare din REG02. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.4; 4.3.1; 4.3.2; 4.3.4; 4.5.5].

13.2.4 **Annex A.1.2.3** - Mapată la legătura cu temeiul juridic pentru colectare, utilizare și rutarea utilizării secundare, fără înlocuirea PII03. Addressed by clauses [4.3.4; 6.1.2; 7.1.1].

13.2.5 **Annex A.1.2.8** - Mapată la dovezile privind responsabilitățile de colectare și partajare ale operatorilor asociați din REG08. Addressed by clauses [4.1.5; 4.4.4; 6.1.4].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5** - Mapate la limitarea colectării, limitarea prelucrării și justificarea minimizării înainte ca PII să fie colectate sau utilizate. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.3.1; 4.3.2; 7.1.2].

13.2.7 **Annex A.1.5.2; Annex A.1.5.3** - Mapate la legătura privind rutarea transferurilor prin REG09, fără înlocuirea controalelor PII13 privind mecanismul de transfer. Addressed by clauses [4.5.1; 4.5.2; 7.1.4].

13.2.8 **Annex A.1.5.4; Annex A.1.5.5** - Mapate la înregistrările transferurilor, divulgărilor și aranjamentelor recurente de partajare a datelor din REG08. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.5.1; 4.5.3; 4.5.4; 4.5.5].

13.2.9 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Mapate la alinierea la instrucțiunile clientului pentru persoana împuternicită și la înregistrările persoanei împuternicite privind limitele de colectare, utilizare și utilizare secundară. Addressed by clauses [4.1.4; 4.2.3; 4.3.6; 7.1.3; 10.1.3].

13.2.10 **Annex A.2.5.2; Annex A.2.5.3** - Mapate la legătura privind rutarea transferurilor efectuate de persoana împuternicită prin REG09, fără înlocuirea controalelor PII13 privind mecanismul de transfer. Addressed by clauses [4.5.1; 4.5.2; 7.1.4].

13.2.11 **Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Mapate la înregistrările divulgărilor persoanei împuternicite, la stadiul notificării cererilor de divulgare și la dovezile de autorizare a divulgării din REG08. Addressed by clauses [4.4.5; 4.4.6; 4.4.7; 10.1.3].

13.3 GDPR

13.3.1 **Article 5(1)(b); Article 5(1)(c); Article 5(2)** - Mapate la dovezile privind limitarea scopului, minimizarea datelor și responsabilitatea pentru colectare, utilizare, utilizare secundară, divulgare și partajare. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.5.3; 8.1.3; 10.1.1].

13.3.2 Article 6 - Mapat la legătura cu temeiul juridic și la rutarea pentru utilizări secundare noi sau incompatibile, fără înlocuirea PII03. Addressed by clauses [4.3.4; 6.1.2; 7.1.1].

13.3.3 **Article 24** - Mapat la guvernanța operatorului, aprobări, revizuire și măsuri de responsabilitate pentru colectare, utilizare, divulgare și partajare. Addressed by clauses [4.1.2; 4.2.4; 4.3.2; 4.3.3; 4.3.5; 4.4.1; 6.1.1; 9.1.2; 10.1.4; 11.1.1].

13.3.4 **Article 26** - Mapat la dovezile privind responsabilitățile de colectare și partajare ale operatorilor asociați. Addressed by clauses [4.1.5; 4.4.4; 6.1.4].

13.3.5 **Article 28** - Mapat la alinierea la instrucțiuni pentru persoanele împuternicite și persoanele subîmputernicite, autorizarea clientului și limitele de divulgare. Addressed by clauses [4.1.4; 4.2.3; 4.3.6; 4.4.5; 4.4.6; 4.4.7; 7.1.3; 10.1.3].

13.3.6 **Article 30** - Mapat la înregistrările privind prelucrarea, destinatarii, divulgarea și partajarea din REG02 și REG08. Addressed by clauses [4.1.1; 4.2.1; 4.4.2; 4.4.3; 4.5.1; 4.5.5; 8.1.1; 8.1.2].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Mapate la specificarea scopului, limitarea colectării, minimizarea datelor, limitarea utilizării și limitarea divulgării. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.5.3].

13.4.2 **Clause 5.10; Clause 5.12** - Mapate la responsabilitate, dovezi de conformitate, revizuire, gestionarea excepțiilor, eșantionare de audit și acțiune corectivă. Addressed by clauses [4.2.4; 4.2.5; 5.1.2; 6.1.1; 8.1.1; 9.1.1; 10.1.1; 11.1.4].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7** - Mapate la scop, limitarea colectării, minimizare, limitarea utilizării, limitarea divulgării și suport pentru înregistrările de divulgare. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.4.6; 4.5.3].