					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: PII17					Titlul documentului: **Politica PIMS privind gestionarea informațiilor documentate și a dovezilor**							
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	Aplicabilitate	Tip acoperire	Comentariu
ISO/IEC 27701:2025	Clause 6.1.3	Both	Supporting	Informații documentate privind SoA
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Informații documentate ale PIMS
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Controlul dovezilor operaționale
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Dovezi de monitorizare
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Dovezi de audit
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Dovezi aferente revizuirii de management
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Dovezi privind neconformitatea și acțiunea corectivă
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Înregistrări de prelucrare ale operatorului
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Dovezi privind acordul cu persoana împuternicită și instrucțiunile
ISO/IEC 27701:2025	Annex A.3.14	Both	Primary	Protecția înregistrărilor
GDPR	Article 5(2)	Controller	Supporting	Dovezi privind responsabilitatea
GDPR	Article 24	Controller	Supporting	Măsuri și dovezi ale operatorului
GDPR	Article 28	Both	Supporting	Documentația persoanei împuternicite
GDPR	Article 30	Both	Supporting	Evidențe ale activităților de prelucrare
GDPR	Article 32	Both	Supporting	Protecția dovezilor
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Dovezi privind conformitatea în

				materie de confidențialitate
ISO/IEC 29151:2022	Clause 18.1.4	Both	Supporting	Protecția înregistrărilor
ISO/IEC 27001:2022	Clause 7.5	Both	Supporting	Controlul informațiilor documentate
ISO/IEC 27002:2022	Control 5.33	Both	Supporting	Protecția înregistrărilor
ISO/IEC 27002:2022	Control 5.34	Both	Supporting	Protecția confidențialității și a PII

1. Domeniu de aplicare

1.1 Prezenta politică definește cerințele obligatorii pentru crearea, aprobarea, versionarea, protejarea, păstrarea, regăsirea, traducerea, retragerea și evidențierea informațiilor documentate ale PIMS.

1.2 Prezenta politică se aplică politicilor PIMS, registrelor, aprobărilor documentate, înregistrărilor de dovezi, dovezilor de audit, înregistrărilor aferente revizuirii de management, dovezilor privind acțiunile corective și traducerilor controlate utilizate pentru a demonstra conformitatea PIMS.

1.3 Prezenta politică se aplică în contexte de operator, operator asociat, persoană împuternicită și persoană subîmputernicită.

1.4 Prezenta politică nu creează un registru separat de control al documentelor. Dovezile privind controlul informațiilor documentate sunt menținute prin obiectele canonice de dovezi PIMS REG01 până la REG12, REG03 și REG12 fiind utilizate pentru aplicabilitatea controalelor, audit, neconformitate, acțiune corectivă și dovezi de îmbunătățire.

2. Scop

2.1 Scopul prezentei politici este de a asigura că informațiile documentate ale PIMS sunt exacte, controlate, accesibile utilizatorilor autorizați, protejate împotriva modificării sau divulgării neautorizate, păstrate pentru auditabilitate și retrase atunci când devin perimate.

2.2 Prezenta politică sprijină pregătirea pentru certificare prin asigurarea faptului că dovezile necesare pentru demonstrarea conformității PIMS pot fi localizate, verificate, regăsite și asociate cu politicile, controalele, activitățile de prelucrare, riscurile, auditurile și acțiunile corective aplicabile.

3. Obiective

3.1 Obiectivele prezentei politici sunt:

3.1.1 definirea cerințelor de control al informațiilor documentate ale PIMS;

3.1.2 menținerea integrității dovezilor la nivelul REG01 până la REG12;

3.1.3 asigurarea trasabilității aprobării politicilor și a dovezilor;

3.1.4 asigurarea documentării istoricului versiunilor și a deciziilor de retragere;

3.1.5 asocierea dovezilor PIMS cu Declarația de aplicabilitate și mapările politicilor;

3.1.6 controlul accesului la documentele PIMS și la înregistrările de dovezi;

3.1.7 sprijinirea controlului versiunilor pentru politici și dovezi multilingve;

3.1.8 facilitarea regăsirii la timp a dovezilor de audit;

3.1.9 prevenirea birocrației inutile privind controlul documentelor;

3.1.10 păstrarea înregistrărilor pregătite pentru audit în scopul certificării, asigurării solicitate de clienți și îmbunătățirii continue.

4. Declarații de politică

4.1 Controlul informațiilor documentate ale PIMS

4.1.1 [All] Privacy Lead / PIMS Manager trebuie să mențină un index al informațiilor documentate ale PIMS în REG12 înainte de publicarea inițială a PIMS și trimestrial ulterior.

4.1.2 [All] Process Owner / Business Owner trebuie să identifice în REG02 informațiile documentate necesare pentru fiecare activitate de prelucrare PII deținută, înainte de începerea activității de prelucrare și anual ulterior.

4.1.3 [All] Privacy Lead / PIMS Manager trebuie să asocieze politicile, controalele și obligațiile privind dovezile PIMS aplicabile cu REG03 înainte de fiecare publicare a politicii și în termen de 15 zile lucrătoare de la orice modificare semnificativă a aplicabilității controalelor.

4.1.4 [All] Privacy Lead / PIMS Manager trebuie să atribuie un nivel de acces și o clasificare a sensibilității dovezilor fiecărei categorii de informații documentate ale PIMS în REG12 înainte ca respectiva categorie să fie utilizată.

4.2 Creare, aprobare, versionare și publicare

4.2.1 [All] Privacy Lead / PIMS Manager trebuie să atribuie un identificator de document, un proprietar, un număr de versiune, statutul aprobării, data intrării în vigoare și data revizuirii în REG12 înainte de publicarea informațiilor documentate ale PIMS.

4.2.2 [All] Top Management trebuie să aprobe politicile PIMS de bază și modificările semnificative ale politicilor în REG12 înainte de publicare.

4.2.3 [All] Privacy Lead / PIMS Manager trebuie să aprobe șabloanele de dovezi PIMS sau secțiunile de registru încorporate în REG12 înainte de utilizarea operațională.

4.2.4 [All] Privacy Lead / PIMS Manager trebuie să consemneze istoricul versiunilor și justificarea modificărilor în REG12 înainte de lansarea informațiilor documentate ale PIMS actualizate.

4.2.5 [All] Privacy Lead / PIMS Manager trebuie să consemneze comunicarea modificărilor aprobate ale informațiilor documentate ale PIMS în REG11 în termen de 30 de zile de la publicare.

[... 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 trebuie să solicite în REG12 excepții privind informațiile documentate sau controlul dovezilor înainte de a se abate de la prezenta politică.

9.1.2 [All] Privacy Lead / PIMS Manager trebuie să evalueze fiecare excepție privind informațiile documentate sau controlul dovezilor în REG12 în termen de 10 zile lucrătoare de la solicitare.

9.1.3 [All] Data Protection Officer / Privacy Advisor trebuie să consemneze recomandările în REG12 înainte de aprobarea oricărei excepții care implică divulgarea dovezilor PII, o discrepanță de traducere, un conflict de păstrare sau o limitare a dovezilor de audit.

9.1.4 [All] Top Management trebuie să aprobe în REG12 excepțiile privind informațiile documentate care depășesc 30 de zile sau afectează certificarea, prelucrările cu risc ridicat ori asigurarea externă, înainte ca excepția să producă efecte.

9.1.5 [All] Privacy Lead / PIMS Manager trebuie să stabilească în REG12 o dată de expirare care să nu depășească 90 de zile pentru fiecare excepție aprobată privind informațiile documentate sau controlul dovezilor.

9.1.6 [All] Privacy Lead / PIMS Manager trebuie să închidă sau să reevalueze fiecare excepție privind informațiile documentate sau controlul dovezilor în REG12 în termen de cinci zile lucrătoare de la expirare.

10. Aplicare

10.1.1 [All] Privacy Lead / PIMS Manager trebuie să consemneze informațiile documentate ale PIMS lipsă, inexacte, necontrolate, perimate sau care nu pot fi regăsite ca neconformitate în REG12 în termen de cinci zile lucrătoare de la identificare.

10.1.2 [All] Privacy Lead / PIMS Manager trebuie să împiedice publicarea informațiilor documentate ale PIMS atunci când din REG12 lipsesc dovezile obligatorii privind aprobarea, versiunea, proprietarul sau data intrării în vigoare.

10.1.3 [All] Process Owner / Business Owner trebuie să împiedice transmiterea pentru audit a dovezilor de prelucrare atunci când din REG02 lipsesc dovezile obligatorii privind proprietarul, data, statutul sau aprobarea.

10.1.4 [All] System Owner / Application Owner trebuie să elimine accesul neautorizat la depozitele de informații documentate ale PIMS și să consemneze eliminarea în REG12 în termen de o zi lucrătoare de la identificare.

10.1.5 [All] Internal Audit / Compliance Reviewer trebuie să verifice eficacitatea acțiunilor corective pentru neconformitățile privind informațiile documentate în REG12 la următorul audit programat sau în termen de 60 de zile de la închidere, oricare dintre acestea survine mai întâi.

11. Revizuire și mentenanță

11.1.1 [All] Privacy Lead / PIMS Manager trebuie să revizuiască prezenta politică anual și în termen de 30 de zile de la o modificare semnificativă a cerințelor privind informațiile documentate ale PIMS.

11.1.2 [All] Privacy Lead / PIMS Manager trebuie să revizuiască prezenta politică în termen de 30 de zile după o constatare majoră de audit, o neconformitate de certificare, o modificare a platformei de depozitare sau o modificare a procesului de publicare multilingvă.

11.1.3 [All] Data Protection Officer / Privacy Advisor trebuie să revizuiască în REG12 modificările prezentei politici cu impact semnificativ asupra confidențialității înainte de aprobare.

11.1.4 [All] Top Management trebuie să aprobe în REG12 modificările semnificative ale prezentei politici înainte de publicare.

11.1.5 [All] Privacy Lead / PIMS Manager trebuie să consemneze comunicarea modificărilor aprobate ale prezentei politici în REG11 în termen de 30 de zile de la publicare.

12. Politici conexe

12.1 Prezenta politică este susținută de următoarele politici conexe:

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

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

12.4 PII03 - Politica privind inventarul prelucrării PII și temeiul juridic

12.5 PII04 - Politica privind notele de informare și transparența

12.6 PII05 - Politica privind consimțământul și gestionarea preferințelor

12.7 PII06 - Politica privind gestionarea drepturilor persoanei 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 PII09 - Politica privind colectarea, utilizarea, divulgarea și partajarea PII

12.11 PII10 - Politica privind păstrarea, ștergerea și eliminarea PII

12.12 PII11 - Politica privind exactitatea și calitatea PII

12.13 PII12 - Politica privind managementul confidențialității pentru persoane împuternicite, persoane subîmputernicite și terți

12.14 PII13 - Politica privind transferul internațional al PII

12.15 PII14 - Politica privind securitatea PII și controlul accesului

12.16 PII15 - Politica privind gestionarea incidentelor și încălcărilor securității PII

12.17 PII16 - Politica privind instruirea, conștientizarea și competența în materie de confidențialitate

12.18 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 sprijină cerințele citate și identifică clauzele interne care le implementează sau le susțin.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.3** - Mapată la menținerea Declarației de aplicabilitate PIMS, a înregistrărilor privind aplicabilitatea controalelor și a legăturii dintre politici și dovezi. Addressed by clauses [4.1.3; 4.3.3; 6.1.3; 7.1.2].

13.2.2 **Clause 7.5** - Mapată la identificarea informațiilor documentate, aprobare, controlul versiunilor, acces, regăsire, conservare, retragere, legătura dintre versiunile traduse și metadatele de păstrare. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.5; 4.4.1; 4.4.2; 4.4.4; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.1; 4.6.2; 4.6.3; 4.6.4].

13.2.3 **Clause 8.1** - Mapată la dovezile privind planificarea și controlul operațional pentru înregistrările de prelucrare, șabloanele de dovezi, calitatea dovezilor operaționale și dovezile furnizate extern. Addressed by clauses [4.1.2; 4.2.3; 4.3.2; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1** - Mapată la menținerea dovezilor documentate privind măsurarea, performanța regăsirii, lacunele de dovezi, neconcordanțele de traducere și finalizarea revizuirii accesului la depozite. Addressed by clauses [8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6].

13.2.5 **Clause 9.2** - Mapată la regăsirea dovezilor de audit, eșantionarea de audit, trasabilitatea dovezilor de audit și constatările de audit legate de controlul informațiilor documentate. Addressed by clauses [4.3.4; 4.4.4; 6.1.3; 8.1.3; 10.1.5].

13.2.6 **Clause 9.3** - Mapată la dovezile aferente revizuirii de management, luarea în considerare în cadrul revizuirii de management a controlului informațiilor documentate și revizuirea de către Top Management a performanței controlului dovezilor. Addressed by clauses [6.1.2; 8.1.1; 8.1.2; 11.1.4].

13.2.7 **Clause 10.2** - Mapată la neconformitățile privind informațiile documentate, acțiunea corectivă, gestionarea excepțiilor, închiderea și verificarea eficacității. Addressed by clauses [4.3.4; 6.1.4; 9.1.1; 9.1.2; 9.1.4; 9.1.5; 9.1.6; 10.1.1; 10.1.5].

13.2.8 **Annex A.1.2.9** - Mapată la înregistrările de prelucrare ale operatorului, înregistrările privind responsabilitatea, calitatea dovezilor de prelucrare și păstrarea dovezilor care susțin obligațiile operatorului. Addressed by clauses [4.1.2; 4.3.2; 4.5.1; 7.1.3].

13.2.9 **Annex A.2.2.2** - Mapată la acordul cu persoana împuternicită, instrucțiunea clientului, dovezile furnizate extern și controlul dovezilor privind relația cu persoana împuternicită. Addressed by clauses [5.1.7; 7.1.4].

13.2.10 **Annex A.3.14** - Mapată la protecția înregistrărilor PIMS împotriva pierderii, modificării neautorizate, accesului neautorizat, furnizării neautorizate și eliminării necorespunzătoare. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.2; 4.5.4; 4.5.5; 10.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapată la dovezile privind responsabilitatea, trasabilitatea dovezilor, regăsirea dovezilor, înregistrările de neconformitate și înregistrările pregătite pentru audit care demonstrează conformitatea. Addressed by clauses [4.1.1; 4.3.2; 4.3.3; 4.4.4; 4.5.4; 6.1.3; 8.1.3; 10.1.1].

13.3.2 **Article 24** - Mapată la dovezile privind guvernanța operatorului, înregistrările de aprobare, controlul politicilor, măsurile de responsabilitate, revizuirea documentată și supravegherea de către Top Management. Addressed by clauses [4.2.2; 4.3.3; 6.1.2; 9.1.4; 11.1.4].

13.3.3 **Article 28** - Mapată la documentația privind persoanele împuternicite și persoanele subîmputernicite, dovezile privind instrucțiunile clientului, dovezile de proces furnizate extern și controlul divulgării dovezilor. Addressed by clauses [4.4.5; 5.1.7; 7.1.4].

13.3.4 **Article 30** - Mapată la dovezile privind înregistrările de prelucrare, cerințele de calitate a dovezilor, referințele activităților de prelucrare și metadatele privind proprietarul/statutul dovezilor de prelucrare. Addressed by clauses [4.1.2; 4.3.2; 7.1.3; 10.1.3].

13.3.5 **Article 32** - Mapată la protecția depozitelor de dovezi, restricțiile de acces, aprobările de acces, revizuirea protecției depozitelor și eliminarea accesului neautorizat. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Mapată la dovezile privind conformitatea în materie de confidențialitate, regăsirea dovezilor de audit, trasabilitatea dovezilor, sprijinirea revizuirii independente și dovezile privind acțiunile corective. Addressed by clauses [4.3.3; 4.4.4; 4.6.3; 6.1.3; 8.1.3; 10.1.5].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.1.4** - Mapată la protecția înregistrărilor legate de PII, păstrarea înregistrărilor și controalele de acces și ștergere pentru depozitele de dovezi. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.5.2; 4.5.5; 10.1.4].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 7.5** - Mapată la identificarea informațiilor documentate, aprobare, disponibilitate, protecție, controlul versiunilor, păstrare, dispunere și controlul informațiilor documentate impuse extern. Addressed by clauses [4.1.1; 4.2.1; 4.2.4; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.6.4].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.33 - Mapată la protejarea înregistrărilor PIMS împotriva pierderii, distrugerii, falsificării, accesului neautorizat, furnizării neautorizate și eliminării necorespunzătoare. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.7.2 Control 5.34 - Mapată la protejarea confidențialității și a PII în informațiile documentate, depozitele de dovezi, divulgări și înregistrări cu acces controlat. Addressed by clauses [4.1.4; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 6.1.5].