					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: PII01					Titlul documentului: **Politica privind Sistemul de management al informațiilor privind confidențialitatea**							
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 de acoperire	Comentariu
ISO/IEC 27701:2025	Clause 4.1	Both	Primary	Determinarea contextului și a rolului PIMS
ISO/IEC 27701:2025	Clause 4.2	Both	Primary	Părți interesate și cerințe
ISO/IEC 27701:2025	Clause 4.3	Both	Primary	Domeniul de aplicare al PIMS
ISO/IEC 27701:2025	Clause 4.4	Both	Primary	Instituirea și îmbunătățirea PIMS
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Leadership și angajament
ISO/IEC 27701:2025	Clause 5.2	Both	Primary	Politica de confidențialitate
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	Roluri și autorități
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	Riscuri și oportunități
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Evaluarea riscurilor privind confidențialitatea
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Tratamentul riscurilor privind confidențialitatea și SoA
ISO/IEC 27701:2025	Clause 6.2	Both	Primary	Obiective privind confidențialitatea
ISO/IEC 27701:2025	Clause 6.3	Both	Primary	Modificări PIMS planificate
ISO/IEC 27701:2025	Clause 7.1	Both	Primary	Resurse
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Competență
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Conștientizare
ISO/IEC 27701:2025	Clause 7.4	Both	Primary	Comunicări
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Informații documentate

ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Planificare și control operațional
ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Evaluarea operațională a riscurilor privind confidențialitatea
ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Tratamentul operațional al riscurilor privind confidențialitatea
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Monitorizare și evaluare
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Audit intern
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Revizuire de management
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Îmbunătățire continuă
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	Neconformitate și acțiune corectivă
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9	Controller	Primary	Înregistrări de guvernanță ale operatorului
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3	Processor	Primary	Acordul persoanei împuternicite și scopurile
ISO/IEC 27701:2025	Annex A.3.3	Both	Primary	Legătura cu politica de securitate a PII
GDPR	Article 5(2)	Controller	Supporting	Dovezi privind responsabilitatea demonstrabilă
GDPR	Article 24	Controller	Supporting	Măsuri și politică ale operatorului
GDPR	Article 26	Joint Controller	Supporting	Aranjamente între operatori asociați
GDPR	Article 28	Both	Supporting	Guvernanța persoanelor împuternicite
GDPR	Article 30	Both	Supporting	Evidențe ale prelucrării
GDPR	Article 32	Both	Supporting	Securitatea prelucrării

GDPR	Article 35	Controller	Supporting	Guvernanța DPIA
ISO/IEC 29100:2020	Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12	Both	Supporting	Controale și principii privind confidențialitatea
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	Procesul PIA și pregătirea acestuia
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2; Annex A.2	Controller	Supporting	Programul și politica de protecție a PII
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1	Both	Supporting	Integrarea riscurilor organizaționale privind confidențialitatea

1. Domeniu de aplicare

1.1 Această politică instituie Sistemul de management al informațiilor privind confidențialitatea al organizației pentru prelucrarea PII în contexte de operator, operator asociat, persoană împuternicită și persoană subîmputernicită.

1.2 Această politică se aplică următoarelor:

1.2.1 domeniul de aplicare al PIMS, contextului, părților interesate și limitelor organizaționale;

1.2.2 determinării rolului PIMS pentru activitățile de prelucrare a PII;

1.2.3 politicii de confidențialitate, obiectivelor privind confidențialitatea, evaluării riscurilor privind confidențialitatea, tratamentului riscurilor privind confidențialitatea și Declarației de aplicabilitate PIMS;

1.2.4 guvernanței PIMS, monitorizării, auditului intern, revizuirii de management, neconformității, acțiunii corective și îmbunătățirii continue;

1.2.5 informațiilor documentate și dovezilor necesare pentru a demonstra conformitatea PIMS și responsabilitatea demonstrabilă.

1.3 În sensul acestei politici, o modificare semnificativă înseamnă orice modificare care afectează domeniul de aplicare al PIMS, scopurile prelucrării PII, categoriile de PII, categoriile de persoane vizate, locațiile de prelucrare, alocarea rolului de operator sau de persoană împuternicită, arhitectura sistemului, aranjamentele cu furnizorii sau persoanele subîmputernicite, profilul de risc privind confidențialitatea, obligațiile legale sau contractuale aplicabile ori domeniul de certificare.

2. Scop

2.1 Această politică definește cerințele obligatorii de guvernanță pentru instituirea, implementarea, menținerea, monitorizarea și îmbunătățirea continuă a PIMS.

2.2 Scopul acestei politici este de a asigura că organizația poate demonstra managementul responsabil, bazat pe risc și susținut de dovezi al prelucrării PII în toate rolurile PIMS aplicabile.

3. Obiective

3.1 Obiectivele acestei politici sunt:

3.1.1 să definească domeniul de aplicare al PIMS, contextul, limitele și aplicabilitatea rolurilor;

3.1.2 să atribuie responsabilitatea de guvernanță pentru PIMS utilizând rolurile canonice PIMS;

3.1.3 să stabilească obiective privind confidențialitatea și așteptări măsurabile privind performanța PIMS;

3.1.4 să mențină o Declarație de aplicabilitate PIMS pentru controalele selectate și excluse;

3.1.5 să integreze evaluarea riscurilor privind confidențialitatea, tratamentul riscurilor privind confidențialitatea și guvernanța DPIA în operarea PIMS;

3.1.6 să asigure identificarea obligațiilor de operator, operator asociat, persoană împuternicită și persoană subîmputernicită înainte de începerea prelucrării;

3.1.7 să mențină dovezi pregătite pentru audit pentru pregătirea certificării și îmbunătățirea continuă;

3.1.8 să evite rolurile, registrele, formularele și controalele operaționale duplicate care nu sunt necesare.

4. Declarații de politică

4.1 Instituirea, contextul și domeniul de aplicare al PIMS

4.1.1 [Both] Top Management MUST aprobe domeniul de aplicare al PIMS în REG01 înainte de implementarea inițială a PIMS și în termen de 30 de zile de la orice modificare semnificativă.

4.1.2 [Both] Privacy Lead / PIMS Manager MUST documenteze aspectele externe și interne ale contextului privind confidențialitatea în REG01 anual și în termen de 30 de zile de la orice modificare semnificativă.

4.1.3 [Both] Privacy Lead / PIMS Manager MUST documenteze părțile interesate relevante și cerințele lor PIMS în REG01 anual și în termen de 30 de zile de la orice modificare semnificativă.

4.1.4 [Both] Privacy Lead / PIMS Manager MUST menționă sinteza interacțiunilor proceselor PIMS în REG01 înainte de fiecare revizuire de management.

4.2 Determinarea rolului PIMS

4.2.1 [Both] Process Owner / Business Owner MUST clasifice rolul PIMS al organizației pentru fiecare activitate de prelucrare a PII în REG02 înainte de începerea activității de prelucrare.

4.2.2 [Joint Controller] Vendor / Procurement Owner MUST documenteze alocarea responsabilităților între operatorii asociați în REG08 înainte de începerea prelucrării în comun.

4.2.3 [Processor] Vendor / Procurement Owner MUST documenteze instrucțiunile de prelucrare ale clientului pentru activitățile de persoană împuternicită în REG08 înainte de integrarea serviciului.

4.2.4 [Subprocessor] Vendor / Procurement Owner MUST documenteze instrucțiunile clientului din amonte și aranjamentele aprobate de subîmputernicire în REG08 înainte de începerea subprelucrării.

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

9. Excepții

9.1 Solicitarea și aprobarea excepțiilor

9.1.1 [All] Process Owner / Business Owner MUST documenteze orice excepție solicitată de la această politică în REG12 înainte ca abaterea să aibă loc.

9.1.2 [Both] Privacy Lead / PIMS Manager MUST evalueze riscul privind confidențialitatea aferent fiecărei excepții solicitate în REG04 înainte de aprobare.

9.1.3 [Both] Top Management MUST aprobe excepțiile care depășesc pragurile acceptate de risc privind confidențialitatea în REG12 înainte de implementare.

9.1.4 [Both] Privacy Lead / PIMS Manager MUST revizui excepțiile PIMS active în REG12 trimestrial până la închidere.

9.2 Închiderea excepțiilor

9.2.1 [All] Process Owner / Business Owner MUST documenteze dovezile de închidere a excepției în REG12 până la data de expirare aprobată a excepției.

9.2.2 [Both] Internal Audit / Compliance Reviewer MUST verifica dovezile de închidere a excepțiilor expirate în REG12 în cadrul următorului audit intern planificat.

10. Aplicare

10.1 Tratarea neconformităților

10.1.1 [All] Privacy Lead / PIMS Manager MUST înregistreze neconformitățile suspectate față de această politică în REG12 în termen de cinci zile lucrătoare de la identificare.

10.1.2 [All] Process Owner / Business Owner MUST implementeze acțiunile corective aprobate în REG12 până la termenul-limită atribuit, după aprobarea neconformității.

10.1.3 [All] Top Management MUST revizui neconformitățile PIMS majore nerezolvate în REG12 la fiecare revizuire de management.

10.1.4 [All] Internal Audit / Compliance Reviewer MUST verifica eficacitatea acțiunilor corective în REG12 în termen de 30 de zile de la închiderea raportată.

10.2 Escaladare

10.2.1 [All] Privacy Lead / PIMS Manager MUST escaladeze acțiunile corective majore restante către Top Management în REG12 în termen de cinci zile lucrătoare după termenul-limită.

10.2.2 [All] Top Management MUST înregistreze deciziile privind acțiunile corective majore restante în REG12 în termen de 15 zile lucrătoare de la escaladare.

11. Revizuire și menținere

11.1 Revizuirea politicii

11.1.1 [All] Privacy Lead / PIMS Manager MUST revizui această politică în REG12 anual și în termen de 30 de zile de la orice modificare semnificativă juridică, organizațională, de prelucrare, tehnologică sau a domeniului de certificare.

11.1.2 [All] Data Protection Officer / Privacy Advisor MUST furnizeze recomandări documentate în REG12 înainte de aprobarea politicii atunci când se modifică obligații semnificative privind confidențialitatea.

11.1.3 [All] Top Management MUST aprobe modificările semnificative ale acestei politici în REG12 înainte de publicare.

11.1.4 [All] Privacy Lead / PIMS Manager MUST actualizeze REG01 și REG03 în termen de 15 zile lucrătoare după modificările aprobate ale politicii care schimbă domeniul de aplicare al PIMS sau aplicabilitatea controalelor.

11.1.5 [All] Privacy Lead / PIMS Manager MUST înregistreze comunicarea modificărilor aprobate ale politicii în REG11 în termen de 30 de zile de la publicare.

12. Politici conexe

12.1 Această politică este susținută de următoarele politici conexe:

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

12.3 PII03 - Politica privind inventarul prelucrărilor PII și temeiul juridic

12.4 PII07 - Politica privind evaluarea riscurilor privind confidențialitatea și DPIA

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

12.6 PII12 - Politica privind persoanele împuternicite, persoanele subîmputernicite și partajarea datelor

12.7 PII14 - Politica privind securitatea PII și controlul accesului

12.8 PII15 - Politica privind incidentele și încălcările referitoare la PII

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

12.10 PII17 - Politica privind informațiile documentate și managementul dovezilor PIMS

12.11 PII18 - Politica privind monitorizarea, auditul și îmbunătățirea PIMS

13. Standarde și cadre de referință

13.1 Această 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 4.1** - Mapată la determinarea contextului organizațional, a aspectelor contextului privind confidențialitatea și a aplicabilității rolului de operator sau persoană împuternicită pentru activitățile PIMS. Addressed by clauses [4.1.2; 4.2.1; 6.1.3].

13.2.2 **Clause 4.2** - Mapată la identificarea părților interesate, a persoanelor vizate, a clienților, a autorităților de supraveghere, a persoanelor împuternicite, a persoanelor subîmputernicite și a cerințelor lor PIMS relevante. Addressed by clauses [4.1.3; 7.2.1; 11.1.1].

13.2.3 **Clause 4.3** - Mapată la definirea, aprobarea, menținerea și modificarea domeniului de aplicare al PIMS documentat. Addressed by clauses [4.1.1; 6.1.3; 11.1.4].

13.2.4 **Clause 4.4** - Mapată la instituirea, implementarea, menținerea și îmbunătățirea proceselor PIMS și a interacțiunilor acestora. Addressed by clauses [4.1.4; 7.1.1; 7.2.1].

13.2.5 **Clause 5.1** - Mapată la aprobarea de către Top Management, resurse, revizuirea guvernanței și leadershipul privind eficacitatea și îmbunătățirea PIMS. Addressed by clauses [4.3.1; 5.1.1; 6.1.1; 8.1.4; 10.1.3].

13.2.6 **Clause 5.2** - Mapată la menținerea acestei politici de confidențialitate ca informație documentată aprobată și la comunicarea modificărilor politicii. Addressed by clauses [4.3.1; 11.1.1; 11.1.3; 11.1.5].

13.2.7 **Clause 5.3** - Mapată la atribuirea și comunicarea rolurilor, responsabilităților și autorităților PIMS. Addressed by clauses [5.1.1; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.8 **Clause 6.1.1** - Mapată la planificarea acțiunilor pentru riscurile și oportunitățile PIMS utilizând contextul, cerințele părților interesate, obiectivele și elementele de intrare pentru îmbunătățire. Addressed by clauses [4.1.2; 4.1.3; 4.4.1; 6.1.1; 8.1.1].

13.2.9 **Clause 6.1.2** - Mapată la cerința de evaluare a riscurilor privind confidențialitatea înaintea prelucrării noi sau modificate semnificativ și la menținerea dovezilor privind riscurile de confidențialitate. Addressed by clauses [4.4.1; 5.1.3; 8.2.4; 9.1.2].

13.2.10 **Clause 6.1.3** - Mapată la tratamentul riscurilor privind confidențialitatea, selectarea controalelor, legătura cu programul de securitate a informației și menținerea Declarației de aplicabilitate. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.3; 7.1.4; 8.2.2].

13.2.11 **Clause 6.2** - Mapată la stabilirea, măsurarea, monitorizarea, comunicarea și actualizarea obiectivelor PIMS. Addressed by clauses [4.3.1; 4.3.2; 8.1.2; 8.1.4].

13.2.12 **Clause 6.3** - Mapată la modificările PIMS planificate și la controlul modificărilor care afectează domeniul de aplicare, rolurile, controalele și informațiile documentate. Addressed by clauses [4.1.1; 6.1.3; 7.1.1; 11.1.4].

13.2.13 **Clause 7.1** - Mapată la determinarea și asigurarea resurselor pentru instituirea, operarea, menținerea și îmbunătățirea PIMS. Addressed by clauses [5.1.1; 6.1.1; 7.1.1].

13.2.14 **Clause 7.2** - Mapată la așteptările privind competența și dovezile care susțin responsabilitățile PIMS și exercitarea rolurilor. Addressed by clauses [5.1.3; 5.1.8; 11.1.5].

13.2.15 **Clause 7.3** - Mapată la conștientizarea politicii de confidențialitate, contribuția la eficacitatea PIMS și implicațiile neconformității. Addressed by clauses [11.1.5; 10.1.1; 10.2.1].

13.2.16 **Clause 7.4** - Mapată la comunicările interne și externe relevante pentru guvernanța PIMS, modificările politicii și escaladare. Addressed by clauses [6.2.1; 10.2.1; 11.1.5].

13.2.17 **Clause 7.5** - Mapată la crearea, menținerea, controlul, pregătirea dovezilor și păstrarea informațiilor documentate. Addressed by clauses [4.5.1; 4.5.3; 7.1.6; 11.1.4].

13.2.18 **Clause 8.1** - Mapată la planificarea, implementarea și controlul proceselor operaționale PIMS și al proceselor furnizate din exterior. Addressed by clauses [4.4.4; 7.1.3; 7.1.5; 7.2.1].

13.2.19 **Clause 8.2** - Mapată la efectuarea evaluărilor riscurilor privind confidențialitatea la intervale planificate și atunci când sunt propuse sau apar modificări semnificative. Addressed by clauses [4.4.1; 8.2.4; 9.1.2].

13.2.20 **Clause 8.3** - Mapată la implementarea planurilor de tratament al riscurilor privind confidențialitatea și păstrarea dovezilor privind rezultatele tratamentului. Addressed by clauses [4.4.3; 7.1.3; 8.2.2].

13.2.21 **Clause 9.1** - Mapată la monitorizare, măsurare, analiză, evaluare, metrici și raportarea eficacității PIMS. Addressed by clauses [8.1.1; 8.1.2; 8.1.4; 8.2.1; 8.2.2; 8.2.3; 8.2.4].

13.2.22 **Clause 9.2** - Mapată la planificarea auditului intern, eșantionarea dovezilor, rezultatele auditului și revizuirea independentă. Addressed by clauses [5.1.9; 6.2.1; 8.1.3; 9.2.2].

13.2.23 **Clause 9.3** - Mapată la elementele de intrare pentru revizuirea de management, revizuirea performanței, rezultatele revizuirii de management și deciziile de îmbunătățire. Addressed by clauses [6.1.1; 6.1.2; 8.1.4; 10.1.3].

13.2.24 **Clause 10.1** - Mapată la îmbunătățirea continuă prin revizuire de management, metrici, urmărirea acțiunilor corective și menținerea politicii. Addressed by clauses [6.1.1; 6.2.2; 10.1.4; 11.1.1].

13.2.25 **Clause 10.2** - Mapată la tratarea neconformităților, acțiunea corectivă, escaladare, închidere și verificarea eficacității. Addressed by clauses [4.5.2; 6.2.2; 6.2.3; 10.1.1; 10.1.2; 10.1.4; 10.2.1; 10.2.2].

13.2.26 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9** - Mapată la înregistrările de pe partea operatorului privind scopurile prelucrării, legătura cu temeiul juridic, determinarea necesității DPIA, alocarea responsabilităților între operatorii asociați și înregistrările dovezilor privind prelucrarea. Addressed by clauses [4.2.1; 4.2.2; 4.4.2; 4.5.1; 7.1.2; 8.2.1].

13.2.27 **Annex A.2.2.2; Annex A.2.2.3** - Mapată la acordurile cu clienții ale persoanei împuternicite, instrucțiunile documentate ale clientului și limitările scopurilor persoanei împuternicite. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.2.28 **Annex A.3.3** - Mapată la legătura cu politica de securitate PII, deținerea bazei de referință a controalelor de securitate PII și stadiul controalelor de securitate a informației în Declarația de aplicabilitate PIMS. Addressed by clauses [4.3.4; 5.1.4; 7.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapată la dovezile privind responsabilitatea demonstrabilă, aprobarea politicii, clasificarea rolului de prelucrare, aplicabilitatea controalelor, monitorizarea, auditul și înregistrările privind acțiunile corective. Addressed by clauses [4.3.1; 4.5.1; 4.5.2; 6.1.1; 8.1.3].

13.3.2 **Article 24** - Mapată la măsurile de guvernanță ale operatorului, aprobarea politicii, obiectivele PIMS, revizuirea eficacității și dovezile documentate privind responsabilitatea demonstrabilă a operatorului. Addressed by clauses [4.3.1; 4.3.2; 6.1.1; 8.1.4; 11.1.1].

13.3.3 **Article 26** - Mapată la determinarea și documentarea alocării responsabilităților între operatorii asociați înainte de începerea prelucrării în comun. Addressed by clauses [4.2.2; 5.1.7; 7.1.5].

13.3.4 **Article 28** - Mapată la înregistrările de guvernanță privind persoanele împuternicite și persoanele subîmputernicite, instrucțiunile de prelucrare ale clientului și controlul proceselor furnizate din exterior. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.3.5 **Article 30** - Mapată la înregistrările activităților de prelucrare, clasificarea rolurilor, înregistrările privind responsabilitatea pentru prelucrare și dovezile păstrate pentru auditabilitate. Addressed by clauses [4.2.1; 5.1.5; 7.1.2; 8.2.1].

13.3.6 **Article 32** - Mapată la guvernanța bazei de referință de securitate PII, deținerea controalelor de securitate, stadiul implementării securității și confirmarea controlului operațional. Addressed by clauses [4.3.4; 4.4.4; 5.1.4; 7.1.4].

13.3.7 **Article 35** - Mapată la determinarea necesității DPIA și evaluarea riscurilor privind confidențialitatea înainte ca prelucrarea efectuată în calitate de operator, cu risc ridicat sau modificată semnificativ, să continue. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12** - Mapată la identificarea controalelor privind confidențialitatea, principiile de confidențialitate, securitatea informației, conformitatea în materie de confidențialitate, audit, dovezi și guvernanța privind confidențialitatea bazată pe risc. Addressed by clauses [4.3.3; 4.3.4; 4.4.1; 4.5.1; 8.1.3; 10.1.4].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Mapată la guvernanța PIA, determinarea declanșatorului DPIA, pregătirea PIA, criteriile de risc privind confidențialitatea și dovezile documentate ale evaluării riscurilor privind confidențialitatea. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4; 9.1.2].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2; Annex A.2** - Mapată la cerințele programului de protecție PII, identificarea cerințelor de protecție PII, selectarea controalelor bazată pe riscul privind confidențialitatea și direcția politicii de protecție PII. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.4].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1** - Mapată la principiile organizaționale privind riscul de confidențialitate, angajamentul conducerii, integrarea riscului privind confidențialitatea în guvernanța PIMS și înțelegerea rolului organizației în prelucrarea PII. Addressed by clauses [4.1.2; 4.2.1; 4.4.1; 4.4.3; 6.1.1].