					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: PII10					Titlul documentului: **Politica privind păstrarea, ștergerea și eliminarea 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	Aplicabilitate	Tip de acoperire	Comentariu
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Dovezi documentate privind păstrarea și control operațional
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorizare, neconformitate și acțiune corectivă
ISO/IEC 27701:2025	Annex A.1.2.8; Annex A.1.2.9	Controller / Joint Controller	Supporting	Responsabilitate comună și evidențe de prelucrare
ISO/IEC 27701:2025	Annex A.1.3.7; Annex A.1.3.8	Controller	Supporting	Sprijin pentru executarea ștergerii
ISO/IEC 27701:2025	Annex A.1.4.6; Annex A.1.4.7; Annex A.1.4.8; Annex A.1.4.9	Controller	Primary	Păstrare, ștergere și eliminare
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Supporting	Instrucțiuni ale clientului și evidențe ale persoanei împuternicite
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.4.2; Annex A.2.4.3	Processor	Primary	Sprijin pentru ștergere și capacitate de eliminare
ISO/IEC 27701:2025	Annex A.3.20; Annex A.3.21; Annex A.3.24	Both	Supporting	Eliminarea mediilor și gestionarea backup-urilor
GDPR	Article 5(1)(e); Article 5(2)	Controller	Primary	Limitarea stocării și responsabilitate
GDPR	Article 17	Controller	Supporting	Sprijin pentru executarea ștergerii
GDPR	Article 24	Controller	Supporting	Măsuri ale operatorului
GDPR	Article 26	Joint Controller	Supporting	Alocarea responsabilității comune

GDPR	Article 28	Processor	Supporting	Ștergerea și returnarea de către persoana împuternicită
GDPR	Article 30	Both	Supporting	Evidențe de prelucrare
GDPR	Article 32	Both	Supporting	Prelucrare securizată și sprijin pentru eliminare
ISO/IEC 29100:2020	Clause 5.5; Clause 5.6; Clause 5.10	Both	Supporting	Minimizare, limitarea păstrării și responsabilitate
ISO/IEC 29151:2022	Annex A.7; Annex A.7.2	Both	Supporting	Controale privind păstrarea și ștergerea fișierelor temporare
ISO/IEC 27555:2025	Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8	Both	Primary	Cadru de ștergere și documentație
ISO/IEC 27555:2025	Clause 7.2; Clause 7.3; Clause 8.3	Controller	Primary	Perioade de ștergere și reguli de ștergere
ISO/IEC 27555:2025	Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7	Both	Primary	Implementare și excepții
ISO/IEC 27555:2025	Clause 10.1; Clause 10.2; Clause 10.3	Both	Primary	Responsabilități și guvernanța implementării
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1	Both	Supporting	Integrarea riscurilor privind confidențialitatea
ISO/IEC 27002:2022	Control 7.14; Control 8.10	Both	Supporting	Eliminare securizată și ștergerea informațiilor

1. Domeniu de aplicare

1.1 Această politică stabilește cerințele organizației pentru definirea, revizuirea, executarea și documentarea prin dovezi a păstrării, ștergerii, anonimizării, dezidentificării, returnării, transferului și eliminării PII.

1.2 Această politică se aplică PII prelucrate în contexte de operator, operator asociat, persoană împuternicită și persoană subîmputernicită, inclusiv PII deținute în sisteme active, arhive, copii de backup, replici, jurnale, medii de staging, fișiere temporare, înregistrări pe suport hârtie și medii de stocare.

1.3 Această politică se aplică obligațiilor de păstrare și ștergere care decurg din scopuri de prelucrare aprobate, evidențe ale temeiului juridic, instrucțiuni ale operatorului, cerințe contractuale, rezultate ale ștergerii pentru persoana vizată, ieșirea din serviciu, eliminarea mediilor de stocare și constatări ale monitorizării PIMS.

1.4 Această politică nu definește selectarea temeiului juridic, conținutul notelor de informare privind confidențialitatea, gestionarea completă a drepturilor persoanei vizate, guvernanța ciclului de viață al persoanei împuternicite, mecanismele de transfer internațional, arhitectura controalelor de securitate, fluxul de răspuns la incidente sau metodologia de audit PIMS. Aceste controale sunt abordate în politicile conexe.

1.5 În sensul acestei politici, o modificare semnificativă înseamnă orice schimbare a scopului prelucrării, categoriei de PII, categoriei de persoană vizată, locației de stocare a sistemului, legii sau contractului privind păstrarea, instrucțiunii clientului, arhitecturii de backup, abordării de arhivare, metodei de eliminare, aranjamentului cu persoana împuternicită sau persoana subîmputernicită, fluxului de ștergere ori domeniului de certificare PIMS care afectează păstrarea, ștergerea sau eliminarea.

2. Scop

2.1 Scopul acestei politici este să asigure că PII sunt păstrate numai pentru scopuri și perioade aprobate, sunt șterse sau eliminate în alt mod atunci când nu mai sunt necesare și sunt susținute de dovezi pregătite pentru audit.

2.2 Această politică permite organizației să demonstreze limitarea stocării, guvernanța responsabilă a păstrării, executarea controlată a ștergerii, eliminarea securizată, alinierea la instrucțiunile persoanei împuternicite, controlul excepțiilor și îmbunătățirea continuă fără a crea un registru separat al ștergerilor.

3. Obiective

3.1 Obiectivele acestei politici sunt să:

3.1.1 definească deținerea regulilor de păstrare și metadatele obligatorii privind păstrarea;

3.1.2 asigure înregistrarea regulilor de păstrare în Inventarul prelucrărilor PII / ROPA;

3.1.3 asigure că acțiunile de ștergere ale persoanelor împuternicite și ale persoanelor subîmputernicite se bazează pe instrucțiunea clientului sau pe contract;

3.1.4 asigure că PII expirate sunt șterse, returnate, transferate, anonimizate, dezidentificate sau eliminate prin metode aprobate;

3.1.5 distingă între sisteme active, arhive, backup-uri, replici, jurnale, zone de staging și fișiere temporare;

3.1.6 asigure păstrarea dovezilor privind ștergerea și eliminarea în obiectele canonice de dovezi PIMS;

3.1.7 asigure că excepțiile de la păstrare sunt limitate în timp, aprobate și revizuite;

3.1.8 integreze monitorizarea păstrării și ștergerii cu neconformitatea, acțiunea corectivă și îmbunătățirea.

4. Declarații de politică

4.1 Atribuirea regulilor de păstrare

4.1.1 [Controller] Process Owner / Business Owner TREBUIE SĂ atribuie o regulă de păstrare documentată fiecărei activități de prelucrare desfășurate în calitate de operator în REG02 înainte de începerea activității de prelucrare.

4.1.2 [Joint Controller] Process Owner / Business Owner TREBUIE SĂ înregistreze alocarea responsabilităților de păstrare și ștergere pentru operatorii asociați în REG02 și REG08 înainte de începerea sau modificarea prelucrării comune.

4.1.3 [Processor] Vendor / Procurement Owner TREBUIE SĂ înregistreze instrucțiunile clientului privind păstrarea, returnarea, transferul sau ștergerea pentru activitățile persoanei împuternicite în REG08 înainte de începerea sau modificarea prelucrării de către persoana împuternicită.

4.1.4 [Subprocessor] Vendor / Procurement Owner TREBUIE SĂ înregistreze cerințele transferate către persoana subîmputernicită privind păstrarea, returnarea, transferul sau ștergerea în REG08 înainte de integrarea persoanei subîmputernicite sau de modificarea instrucțiunilor.

4.1.5 [Both] Privacy Lead / PIMS Manager TREBUIE SĂ verifice faptul că fiecare regulă de păstrare aprobată în REG02 include perioada de păstrare, declanșatorul de început, proprietarul, justificarea, dispunerea finală și data următoarei revizuiri înainte ca regula să fie aprobată.

4.1.6 [Both] Data Protection Officer / Privacy Advisor TREBUIE SĂ înregistreze recomandarea în REG02 sau REG12 înainte de aprobarea oricărei reguli de păstrare care implică un conflict juridic, prelucrare cu risc ridicat, PII din categorii speciale sau păstrare dincolo de scopul inițial al prelucrării.

4.2 Revizuirea și limitarea păstrării

4.2.1 [Both] Process Owner / Business Owner TREBUIE SĂ revizuiască regulile de păstrare atribuite în REG02 cel puțin anual și în termen de 30 de zile de la o modificare semnificativă.

4.2.2 [Both] Privacy Lead / PIMS Manager TREBUIE SĂ aprobe sau să respingă regulile de păstrare noi sau modificate în REG02 în termen de 10 zile lucrătoare de la transmitere.

4.2.3 [Both] System Owner / Application Owner TREBUIE SĂ confirme metoda tehnică sau manuală de aplicare pentru fiecare regulă de păstrare în REG02 înainte de intrarea în producție și în cadrul fiecărei revizuiri anuale a păstrării.

4.2.4 [Controller] Process Owner / Business Owner TREBUIE SĂ restricționeze utilizarea activă a PII păstrate numai din motive juridice, contractuale, de audit sau de dispută în REG02 în termen de cinci zile lucrătoare de la identificarea condiției de restricționare.

4.2.5 [Both] Privacy Lead / PIMS Manager TREBUIE SĂ înregistreze riscul nerezolvat de păstrare excesivă sau revizuirea restantă a păstrării în REG12 în termen de cinci zile lucrătoare de la identificare.

[... 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 transmită orice solicitare de păstrare a PII dincolo de regula de păstrare aprobată în REG02 în REG12 înainte ca excepția să devină activă.

9.1.2 [All] Privacy Lead / PIMS Manager TREBUIE SĂ aprobe sau să respingă solicitările de excepție de la păstrare în REG12 înainte ca excepția să devină activă.

9.1.3 [All] Data Protection Officer / Privacy Advisor TREBUIE SĂ înregistreze recomandarea în REG12 înainte de aprobarea oricărei excepții care implică un conflict juridic, refuzul ștergerii, PII cu risc ridicat, partajare externă sau impact asupra certificării.

9.1.4 [All] Top Management TREBUIE SĂ aprobe excepțiile de la păstrare care depășesc 90 de zile, afectează prelucrarea cu risc ridicat sau afectează asigurarea externă în REG12 înainte ca excepția să devină activă.

9.1.5 [All] Privacy Lead / PIMS Manager TREBUIE SĂ atribuie un proprietar, o dată de expirare, un control compensatoriu și o frecvență de revizuire în REG12 pentru fiecare excepție aprobată privind păstrarea, ștergerea sau eliminarea.

9.1.6 [All] Privacy Lead / PIMS Manager TREBUIE SĂ revizuiască fiecare excepție deschisă în REG12 cel puțin lunar până la închidere.

9.1.7 [All] Process Owner / Business Owner TREBUIE SĂ închidă sau să reînnoiască fiecare excepție în REG12 înainte de data expirării excepției.

10. Aplicare

10.1.1 [All] Privacy Lead / PIMS Manager TREBUIE SĂ înregistreze o neconformitate în REG12 în termen de cinci zile lucrătoare de la identificarea metadatelor lipsă privind păstrarea, a revizuirii restante a păstrării, a păstrării nesusținute, a acțiunii de dispunere finală neefectuate sau a dovezilor lipsă.

10.1.2 [All] System Owner / Application Owner TREBUIE SĂ suspende utilizarea nouă în producție a unei activități de prelucrare în REG12 atunci când controalele tehnice obligatorii privind păstrarea lipsesc înainte de intrarea în producție.

10.1.3 [All] Process Owner / Business Owner TREBUIE SĂ oprească utilizarea activă neaprobată a PII păstrate numai din motive juridice, contractuale, de audit sau de dispută în termen de cinci zile lucrătoare și să înregistreze acțiunea în REG02 sau REG12.

10.1.4 [Processor] Vendor / Procurement Owner TREBUIE SĂ escaladeze acțiunile restante de dispunere finală dispuse de client în REG08 și REG12 în termen de cinci zile lucrătoare de la depășirea termenului contractual.

10.1.5 [Subprocessor] Vendor / Procurement Owner TREBUIE SĂ escaladeze dovezile lipsă privind dispunerea finală de către persoana subîmputernicită în REG08 și REG12 în termen de cinci zile lucrătoare de la depășirea termenului contractual pentru furnizarea dovezilor.

10.1.6 [All] Internal Audit / Compliance Reviewer TREBUIE SĂ verifice eficacitatea acțiunilor corective pentru neconformitățile privind păstrarea, ștergerea și eliminarea în REG12 la următorul audit programat sau în termen de 60 de zile de la închidere, oricare survine mai întâi.

10.1.7 [Conditional] Incident Response Coordinator TREBUIE SĂ inițieze tratarea în REG10 atunci când o neconformitate privind păstrarea, ștergerea sau eliminarea indică un incident PII suspectat.

11. Revizuire și întreținere

11.1.1 [All] Privacy Lead / PIMS Manager TREBUIE SĂ revizuiască această politică anual și să înregistreze rezultatul revizuirii în REG12.

11.1.2 [All] Privacy Lead / PIMS Manager TREBUIE SĂ revizuiască această politică în termen de 30 de zile de la o modificare semnificativă a legii privind păstrarea, a scopului prelucrării, a instrucțiunii persoanei împuternicite, a arhitecturii sistemului, a arhitecturii de backup, a abordării de arhivare, a fluxului de ștergere, a procesului de eliminare sau a cerințelor de certificare PIMS.

11.1.3 [All] Data Protection Officer / Privacy Advisor TREBUIE SĂ revizuiască modificările semnificative din perspectiva confidențialității aduse acestei politici în REG12 înainte de aprobare.

11.1.4 [All] Top Management TREBUIE SĂ aprobe modificările semnificative ale acestei politici în REG12 înainte de publicare.

11.1.5 [All] Privacy Lead / PIMS Manager TREBUIE SĂ 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 PII01 - Politica sistemului 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 nota de informare și transparența

12.6 PII06 - Politica de gestionare a drepturilor persoanei vizate

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

12.8 PII09 - Politica privind colectarea, utilizarea, divulgarea și partajarea PII

12.9 PII12 - Politica de management al confidențialității pentru persoanele împuternicite, persoanele subîmputernicite și terțe părți

12.10 PII14 - Politica privind securitatea PII și controlul accesului

12.11 PII15 - Politica de gestionare a incidentelor și încălcărilor privind PII

12.12 PII17 - Politica de gestionare a informațiilor documentate și a dovezilor PIMS

12.13 PII18 - Politica de monitorizare, audit și îmbunătățire 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 7.5; Clause 8.1** - Mapate la dovezi documentate privind păstrarea, planificare operațională, metadate privind păstrarea, dovezi de implementare și înregistrări privind executarea ciclului de viață. Addressed by clauses [4.1.5; 4.2.3; 4.3.5; 4.4.1; 7.1.1; 7.1.3; 7.1.4; 7.1.5; 7.1.6].

13.2.2 **Clause 9.1; Clause 10.2** - Mapate la monitorizare, metrici, revizuirea acțiunilor restante, neconformitate și acțiune corectivă pentru controalele privind păstrarea, ștergerea și eliminarea. Addressed by clauses [4.2.5; 6.1.1; 6.1.2; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 10.1.1; 10.1.6].

13.2.3 **Annex A.1.2.8; Annex A.1.2.9** - Mapate la dovezile privind responsabilitatea operatorilor asociați și la evidențele de prelucrare ale operatorului care conțin metadate privind păstrarea și dispunerea finală. Addressed by clauses [4.1.1; 4.1.2; 4.1.5; 4.2.1; 6.1.4; 7.1.2].

13.2.4 **Annex A.1.3.7; Annex A.1.3.8** - Mapate la sprijinul pentru executarea ștergerii, rutarea evaluării ștergerii și corelarea dovezilor terților atunci când rezultatele ștergerii necesită acțiune. Addressed by clauses [4.3.2; 4.3.5; 7.1.8; 10.1.7].

13.2.5 **Annex A.1.4.6; Annex A.1.4.7; Annex A.1.4.8; Annex A.1.4.9** - Mapate la ștergerea sau dezidentificarea la sfârșitul prelucrării, gestionarea fișierelor temporare, limitarea păstrării și

controalele documentate privind dispunerea finală. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.3; 4.2.4; 4.3.1; 4.3.5; 4.3.6; 4.4.2; 4.4.5; 4.5.1; 4.5.2; 4.5.3].

13.2.6 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Mapate la acordurile cu clienții ale persoanelor împuternicite, scopurile documentate ale clientului și evidențele de prelucrare ale persoanei împuternicite. Addressed by clauses [4.1.3; 4.1.4; 4.3.3; 4.3.4; 6.1.5; 6.1.6; 7.1.7].

13.2.7 **Annex A.2.3.2; Annex A.2.4.2; Annex A.2.4.3** - Mapate la sprijinul persoanei împuternicite pentru obligațiile clientului, gestionarea fișierelor temporare și capacitatea de returnare, transfer sau dispunere finală. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 4.4.4; 4.4.5; 6.1.5; 7.1.7; 10.1.4; 10.1.5].

13.2.8 **Annex A.3.20; Annex A.3.21; Annex A.3.24** - Mapate la gestionarea ciclului de viață al mediilor de stocare, verificările înainte de reutilizarea sau eliberarea echipamentelor și gestionarea backup-urilor pentru PII. Addressed by clauses [4.3.6; 4.3.7; 4.4.1; 4.4.3; 4.4.4; 4.4.6; 5.1.4].

13.3 GDPR

13.3.1 **Article 5(1)(e); Article 5(2)** - Mapate la limitarea stocării, responsabilitatea privind păstrarea, metadatele aprobate privind păstrarea, dovezi și revizuire. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.2; 4.2.4; 4.3.1; 4.3.5; 6.1.1; 8.1.1; 8.1.2; 10.1.1].

13.3.2 **Article 17** - Mapat la rutarea rezultatului aprobat al ștergerii, dovezi de executare și escaladarea incidentelor atunci când eșecurile controalelor de ștergere indică un incident PII suspectat. Addressed by clauses [4.3.2; 4.3.5; 7.1.8; 10.1.7].

13.3.3 **Article 24** - Mapat la guvernanța operatorului, măsuri de responsabilitate, revizuiri, excepții, acțiune corectivă și întreținerea politicii. Addressed by clauses [4.1.6; 6.1.2; 6.1.3; 9.1.2; 9.1.3; 9.1.4; 11.1.1; 11.1.2; 11.1.4].

13.3.4 **Article 26** - Mapat la alocarea responsabilităților de păstrare și ștergere ale operatorilor asociați. Addressed by clauses [4.1.2; 6.1.4].

13.3.5 **Article 28** - Mapat la alinierea instrucțiunilor pentru persoanele împuternicite și persoanele subîmputernicite, returnare, transfer, dispunere finală, dovezi și escaladare. Addressed by clauses [4.1.3; 4.1.4; 4.3.3; 4.3.4; 6.1.5; 6.1.6; 7.1.7; 10.1.4; 10.1.5].

13.3.6 **Article 30** - Mapat la metadatele privind păstrarea și dispunerea finală din evidențele de prelucrare pentru activitățile operatorului și ale persoanei împuternicite. Addressed by clauses [4.1.1; 4.1.3; 4.1.5; 4.2.1; 4.4.1; 7.1.2].

13.3.7 **Article 32** - Mapat la gestionarea operațională securizată a PII păstrate, aplicare tehnică, controlul mediilor de stocare, gestionarea backup-urilor și escaladarea incidentelor. Addressed by clauses [4.2.3; 4.3.6; 4.4.3; 4.4.4; 4.4.6; 7.1.3; 7.1.4; 7.1.8].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.5; Clause 5.6; Clause 5.10** - Mapate la minimizarea datelor, limitarea utilizării și păstrării, dispunerea finală atunci când nu mai sunt necesare, restricționarea PII păstrate și dovezi de responsabilitate. Addressed by clauses [4.1.5; 4.2.1; 4.2.4; 4.3.1; 4.4.2; 4.5.1; 4.5.2; 6.1.1; 8.1.1; 10.1.1].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.7; Annex A.7.2** - Mapate la păstrarea limitată în timp, dispunerea finală, aplicarea automată sau manuală și gestionarea fișierelor temporare. Addressed by clauses [4.2.3; 4.3.1; 4.4.5; 7.1.3; 7.1.4; 7.1.5; 7.1.6].

13.6 ISO/IEC 27555:2025

13.6.1 **Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8** - Mapate la guvernanța cadrului de ștergere, gruparea PII, perioadele de păstrare și ștergere,

distincția între arhive și backup-uri, structura regulilor de ștergere și cerințele privind procedurile documentate. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.3; 4.4.1; 4.4.2; 4.4.3; 7.1.1; 7.1.2].

13.6.2 **Clause 7.2; Clause 7.3; Clause 8.3** - Mapate la specificarea perioadei regulate de ștergere, identificarea perioadei standard de ștergere și alocarea regulilor de ștergere activităților de prelucrare PII. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.2; 7.1.1; 7.1.2].

13.6.3 **Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7** - Mapate la cerințele de implementare pentru sisteme, procese manuale, aspecte la nivelul organizației, persoane împuternicite, gestionarea recuperării și gestionarea excepțiilor. Addressed by clauses [4.3.1; 4.3.3; 4.3.4; 4.4.1; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 7.1.3; 7.1.4; 7.1.5; 7.1.6; 9.1.1; 9.1.5; 9.1.6].

13.6.4 **Clause 10.1; Clause 10.2; Clause 10.3** - Mapate la atribuirea rolurilor, documentare, integrare operațională, audit și guvernanța implementării pentru păstrare, ștergere și eliminare. Addressed by clauses [5.1.2; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.9; 6.1.7; 7.1.3; 7.1.4; 11.1.1; 11.1.2].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1** - Mapate la guvernanța confidențialității bazată pe risc, conștientizarea conducerii, integrarea riscurilor privind confidențialitatea în PIMS și contextul riscurilor legate de păstrare. Addressed by clauses [4.1.6; 4.2.5; 4.5.4; 6.1.2; 6.1.3; 9.1.3; 9.1.4].

13.8 ISO/IEC 27002:2022

13.8.1 Control 7.14; Control 8.10 - Mapate la ștergerea informațiilor, finalizarea controlată a ciclului de viață, eliberarea mediilor de stocare și dovezile privind dispunerea finală. Addressed by clauses [4.3.1; 4.3.5; 4.3.6; 4.3.7; 4.4.4; 4.4.5; 7.1.3; 7.1.4; 10.1.2].