					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: PII07					Titlul documentului: **Politica privind evaluarea riscurilor privind confidențialitatea și DPIA**							
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 6.1.1	Both	Primary	Riscuri și oportunități PIMS
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 legătura cu SoA
ISO/IEC 27701:2025	Clause 6.3	Both	Supporting	Modificări PIMS planificate și reevaluarea riscurilor
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Informații documentate privind riscurile de confidențialitate și DPIA
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	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	Supporting	Monitorizarea și măsurarea riscurilor privind confidențialitatea
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Revizuirea de management a riscurilor privind confidențialitatea
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Neconformitate și acțiune corectivă legate de risc
ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Primary	Evaluarea impactului asupra confidențialității

ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Evidențe de prelucrare care susțin evaluarea riscurilor
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Acordul clientului cu persoana împuternicită și asistență pentru DPIA
ISO/IEC 27701:2025	Annex A.2.2.6	Processor	Supporting	Informații ale persoanei împuternicite care susțin conformitatea clientului
GDPR	Article 5(2)	Controller	Supporting	Dovezi privind responsabilitatea
GDPR	Article 24	Controller	Supporting	Responsabilitatea operatorului și măsuri
GDPR	Article 25	Controller	Supporting	Protecția datelor încă din faza de proiectare și protecția datelor în mod implicit
GDPR	Article 28	Both	Supporting	Asistență și instrucțiuni pentru persoana împuternicită
GDPR	Article 30	Both	Supporting	Evidențe de prelucrare care susțin DPIA
GDPR	Article 32	Both	Supporting	Risc de securitate și măsuri de protecție
GDPR	Article 35	Controller	Primary	Evaluarea impactului asupra protecției datelor
GDPR	Article 36	Controller	Primary	Consultare prealabilă
GDPR	Article 39	Conditional	Supporting	Consiliere și monitorizare DPO, acolo unde este aplicabil
ISO/IEC 29100:2020	Clause 4.7; Clause 5.11; Clause 5.12	Both	Supporting	Controale de confidențialitate,

				securitatea informației și conformitatea privind confidențialitatea
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Primary	Domeniul de aplicare, beneficiile, declanșatorul și pregătirea PIA
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2	Both	Supporting	Programul de protecție PII și identificarea cerințelor
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7	Both	Supporting	Integrarea managementului organizațional al riscurilor privind confidențialitatea

1. Domeniu de aplicare

1.1 Această politică definește cerințele pentru evaluarea riscurilor privind confidențialitatea, evaluarea preliminară DPIA, efectuarea DPIA complete, tratamentul riscului, acceptarea riscului rezidual, consultare, revizuire și gestionarea dovezilor pentru prelucrarea PII în domeniul de aplicare al PIMS.

1.2 Această politică se aplică:

1.2.1 activităților noi și modificate semnificativ de prelucrare PII;

1.2.2 contextelor de prelucrare în calitate de operator, operator asociat, persoană împuternicită și persoană subîmputernicită;

1.2.3 sistemelor, aplicațiilor, serviciilor, proceselor de afaceri, furnizorilor, persoanelor împuternicite, persoanelor subîmputernicite, transferurilor internaționale și aranjamentelor de partajare a datelor care afectează prelucrarea PII;

1.2.4 dovezilor privind riscurile de confidențialitate și DPIA păstrate în REG04 și dovezilor suport păstrate în REG02, REG03, REG08, REG09, REG10, REG11 și REG12.

1.3 Această politică nu înlocuiește controalele privind inventarul de prelucrare, controalele privind notele de informare privind confidențialitatea, controalele privind consimțământul, controalele privind drepturile persoanelor vizate, controalele de protecție a datelor încă din faza de proiectare, controalele furnizorilor, controalele transferurilor internaționale, controalele de securitate PII, controalele incidentelor, controalele informațiilor documentate sau controalele de monitorizare/audit/îmbunătățire. Aceste cerințe sunt definite în politicile conexe enumerate în Secțiunea 12.

1.4 În sensul acestei politici, evaluarea riscurilor privind confidențialitatea înseamnă identificarea, analiza, evaluarea, tratarea, revizuirea și monitorizarea documentată a potențialelor impacturi adverse asupra confidențialității care decurg din prelucrarea PII.

1.5 În sensul acestei politici, DPIA înseamnă o evaluare documentată utilizată pentru prelucrarea în calitate de operator care este susceptibilă să genereze un risc ridicat pentru persoanele vizate și care evaluează necesitatea prelucrării, proporționalitatea, riscurile, măsurile de protecție, riscul rezidual, necesitatea consultării și condițiile de aprobare.

1.6 În sensul acestei politici, risc rezidual ridicat privind confidențialitatea înseamnă un risc de confidențialitate care rămâne peste pragul de acceptare aprobat după tratamentul riscului propus sau implementat.

1.7 În sensul acestei politici, o modificare semnificativă înseamnă orice schimbare care afectează domeniul de aplicare al PIMS, scopul prelucrării, temeiul juridic, categoriile PII, categoriile de persoane vizate, amploarea prelucrării, tehnologia de prelucrare, monitorizarea sau profilarea, procesul decizional automatizat, persoanele vizate vulnerabile, destinatarii, persoanele împuternicite, persoanele subîmputernicite, transferurile internaționale, retenția, controalele de securitate, profilul de risc, instrucțiunile clientului sau domeniul de certificare.

2. Scop

2.1 Scopul acestei politici este de a asigura că riscurile de confidențialitate și obligațiile DPIA sunt identificate, evaluate, tratate, aprobate, revizuite și documentate prin dovezi înainte ca prelucrarea PII să creeze un risc inacceptabil pentru persoanele vizate sau pentru PIMS.

2.2 Această politică permite organizației să demonstreze guvernanță a confidențialității bazată pe risc, responsabilitatea operatorului privind DPIA, asistența pentru DPIA acordată de persoana împuternicită, tratamentul documentat al riscurilor, aprobarea riscului rezidual, proces decizional privind consultarea prealabilă și îmbunătățirea continuă a controalelor de confidențialitate.

3. Obiective

3.1 Obiectivele acestei politici sunt:

3.1.1 să definească declanșatorii obligatorii pentru evaluarea preliminară a riscurilor privind confidențialitatea;

3.1.2 să definească situațiile în care este necesară o DPIA completă;

3.1.3 să asigure că deciziile operatorului privind DPIA sunt documentate și pot fi revizuite;

3.1.4 să asigure că asistența pentru DPIA acordată de persoanele împuternicite și persoanele subîmputernicite este documentată atunci când este cerută prin instrucțiunea sau acordul clientului;

3.1.5 să asigure că riscurile privind confidențialitatea sunt evaluate înainte ca prelucrarea PII nouă sau modificată semnificativ să continue;

3.1.6 să asigure că tratamentele riscurilor privind confidențialitatea sunt atribuite, implementate și verificate;

3.1.7 să asigure că riscurile reziduale ridicate privind confidențialitatea sunt escaladate și aprobate înainte ca prelucrarea să înceapă sau să continue;

3.1.8 să asigure că deciziile privind consultarea prealabilă sunt documentate atunci când rămâne un risc rezidual ridicat;

3.1.9 să asigure că dovezile privind riscurile de confidențialitate și DPIA sunt păstrate în REG04 și legate de obiectele de dovezi aferente;

3.1.10 să evite crearea unor registre DPIA, de risc sau de consultare separate în afara REG04.

4. Declarații de politică

4.1 Evaluarea preliminară a riscurilor privind confidențialitatea

4.1.1 [Both] The Process Owner / Business Owner MUST iniția evaluarea preliminară a riscurilor privind confidențialitatea în REG04 înainte de începerea prelucrării PII noi sau modificate semnificativ înregistrate în REG02.

4.1.2 [Both] The Privacy Lead / PIMS Manager MUST menține criteriile de evaluare preliminară a riscurilor privind confidențialitatea în REG04 înainte de operarea inițială a PIMS și anual ulterior.

4.1.3 [Controller] The Process Owner / Business Owner MUST finaliza evaluarea preliminară DPIA în REG04 înainte de începerea prelucrării în calitate de operator care îndeplinește criteriile de evaluare preliminară a riscurilor privind confidențialitatea.

4.1.4 [Processor] The Vendor / Procurement Owner MUST înregistra cerințele de asistență pentru DPIA ale clientului în REG08 înainte de începerea prelucrării în calitate de persoană împuternicită, atunci când acordul cu clientul sau instrucțiunea documentată impune suport pentru DPIA.

4.1.5 [Both] The System Owner / Application Owner MUST furniza în REG04 dovezi privind proiectarea sistemului, accesul, securitatea, jurnalizarea și fluxurile de date înainte de aprobarea evaluării riscurilor privind confidențialitatea pentru sistemele noi sau modificate semnificativ care prelucrează PII.

4.1.6 [Both] The Privacy Lead / PIMS Manager MUST înregistra în REG04 rezultatul evaluării preliminare și justificarea deciziei privind DPIA completă înainte ca activitatea de prelucrare să continue.

4.2 Declanșatori DPIA și stabilirea cerinței

4.2.1 [Controller] The Privacy Lead / PIMS Manager MUST solicita o DPIA completă în REG04 înainte de începerea prelucrării în calitate de operator susceptibile să genereze un risc ridicat.

4.2.2 [Controller] The Process Owner / Business Owner MUST transmite către The Privacy Lead / PIMS Manager, în REG04, prelucrările care implică scară largă, monitorizare sistematică, profilare, decizii automate, categorii speciale de PII, date privind condamnări penale sau infracțiuni, persoane vizate vulnerabile, tehnologie inovatoare sau prelucrări modificate semnificativ, înainte de începerea prelucrării.

4.2.3 [Controller] The Data Protection Officer / Privacy Advisor MUST înregistra consilierea în REG04 înainte de aprobarea unei decizii privind cerința de DPIA completă pentru prelucrarea cu risc ridicat în calitate de operator.

4.2.4 [Both] The Process Owner / Business Owner MUST reface evaluarea preliminară a riscurilor privind confidențialitatea în REG04 înainte de utilizarea PII pentru un scop nou, adăugarea unui destinatar nou, introducerea unei persoane împuternicite sau persoane subîmputernicite noi, modificarea arhitecturii sistemului sau inițierea unui nou transfer internațional.

4.2.5 [Processor] The Privacy Lead / PIMS Manager MUST documenta în REG08 dacă este necesar suport DPIA din partea persoanei împuternicite în termen de 10 zile lucrătoare de la primirea unei solicitări de asistență pentru DPIA din partea clientului.

4.2.6 [Subprocessor] The Vendor / Procurement Owner MUST documenta cerințele de asistență pentru DPIA din amonte în REG08 înainte de începerea subprelucrării, atunci când clientul din amonte sau acordul cu persoana împuternicită impune o astfel de asistență.

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

9. Excepții

9.1 Excepții privind riscurile de confidențialitate și DPIA

9.1.1 [All] The Process Owner / Business Owner MUST solicita în REG12 orice excepție de la această politică înainte ca abaterea să se producă.

9.1.2 [All] The Privacy Lead / PIMS Manager MUST evalua impactul asupra confidențialității, juridic, de certificare, operațional și asupra persoanelor vizate al fiecărei excepții solicitate în REG04 sau REG12 în termen de 10 zile lucrătoare de la solicitare.

9.1.3 [All] The Data Protection Officer / Privacy Advisor MUST înregistra consilierea în REG12 înainte de aprobarea oricărei excepții care afectează prelucrarea cu risc ridicat, finalizarea DPIA complete, consultarea prealabilă, riscul rezidual ridicat privind confidențialitatea sau asistența pentru DPIA pentru clienți.

9.1.4 [All] Top Management MUST aproba în REG12 excepțiile privind riscurile de confidențialitate sau DPIA care afectează prelucrarea cu risc ridicat, domeniul de certificare, consultarea prealabilă sau riscul rezidual ridicat privind confidențialitatea nerezolvat, înainte ca excepția să producă efecte.

9.1.5 [All] The Privacy Lead / PIMS Manager MUST stabili în REG12, înainte de aprobare, o dată de expirare care să nu depășească 90 de zile pentru fiecare excepție aprobată privind riscurile de confidențialitate sau DPIA.

9.1.6 [All] The Process Owner / Business Owner MUST închide sau reevalua fiecare excepție privind riscurile de confidențialitate sau DPIA în REG12 în termen de cinci zile lucrătoare de la expirare.

10. Aplicare

10.1 Aplicarea cerințelor privind riscurile de confidențialitate și DPIA

10.1.1 [All] The Privacy Lead / PIMS Manager MUST înregistra dovezile REG04 privind riscurile de confidențialitate sau DPIA care lipsesc, sunt inexacte, incomplete, restante sau neaprobate ca neconformitate în REG12 în termen de cinci zile lucrătoare de la identificare.

10.1.2 [Controller] The Process Owner / Business Owner MUST suspenda prelucrarea nouă cu risc ridicat în calitate de operator atunci când dovezile necesare de aprobare DPIA în REG04 lipsesc înainte de lansare.

10.1.3 [Both] The System Owner / Application Owner MUST bloca intrarea în producție a sistemelor care prelucrează PII atunci când dovezile necesare REG04 privind tratamentul riscului lipsesc înainte de aprobarea intrării în producție.

10.1.4 [Both] The Vendor / Procurement Owner MUST bloca integrarea furnizorilor, persoanelor împuternicite, persoanelor subîmputernicite sau aranjamentelor de partajare a datelor atunci când dovezile necesare REG04 privind riscurile de confidențialitate sau asistența pentru DPIA lipsesc înainte de aprobarea acordului.

10.1.5 [All] Top Management MUST revizui neconformitățile majore nerezolvate privind riscurile de confidențialitate sau DPIA în REG12 în cadrul revizuirii de management.

10.1.6 [All] The Privacy Lead / PIMS Manager MUST escalada către Top Management în REG12, în termen de cinci zile lucrătoare după a doua apariție într-o perioadă de 12 luni, neîndeplinirea repetată a termenelor pentru evaluarea preliminară REG04, revizuirea DPIA sau tratamentul riscurilor.

10.1.7 [All] The Internal Audit / Compliance Reviewer MUST verifica eficacitatea acțiunilor corective pentru neconformitățile privind riscurile de confidențialitate și DPIA în REG12 la următorul audit programat sau în termen de 60 de zile de la închidere, oricare survine prima.

11. Revizuire și mentenanță

11.1 Revizuirea și mentenanța politicii

11.1.1 [All] The Privacy Lead / PIMS Manager MUST revizui această politică în REG12 anual și în termen de 30 de zile de la o modificare semnificativă a cerințelor privind riscurile de confidențialitate, DPIA, consultarea prealabilă, asistența acordată de persoana împuternicită sau certificarea.

11.1.2 [All] The Privacy Lead / PIMS Manager MUST revizui anual în REG12 criteriile de evaluare preliminară REG04, criteriile de declanșare DPIA, criteriile de rating al riscului și criteriile de acceptare a riscului rezidual.

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

11.1.4 [All] Top Management MUST aproba modificările semnificative aduse acestei politici în REG12 înainte de publicare.

11.1.5 [All] The Privacy Lead / PIMS Manager MUST actualiza REG03 și REG04 în termen de 15 zile lucrătoare după modificările aprobate ale politicii care schimbă aplicabilitatea controalelor, criteriile de risc sau cerințele de evaluare preliminară DPIA.

11.1.6 [All] The Privacy Lead / PIMS Manager MUST înregistra comunicarea modificărilor aprobate ale acestei politici 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 responsabilitatea în materie de confidențialitate

12.4 PII03 - Politica privind inventarul prelucrării PII și temeiul juridic

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

12.6 PII05 - Politica privind gestionarea consimțământului și preferințelor

12.7 PII06 - Politica privind gestionarea drepturilor persoanelor vizate

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

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

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 transferurile internaționale de PII

12.14 PII14 - Politica privind securitatea PII și controlul accesului

12.15 PII15 - Politica privind managementul incidentelor și încălcărilor PII

12.16 PII17 - Politica privind informațiile documentate și gestionarea dovezilor PIMS

12.17 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 6.1.1** - Mapată la identificarea și planificarea acțiunilor pentru riscurile și oportunitățile privind confidențialitatea, utilizând criterii de evaluare preliminară, praguri de risc, escaladare și intrări pentru revizuirea de management. Addressed by clauses [4.1.2; 4.4.5; 4.5.6; 6.1.1; 6.1.2; 8.1.2].

13.2.2 **Clause 6.1.2** - Mapată la efectuarea evaluării preliminare a riscurilor privind confidențialitatea, evaluării riscurilor privind confidențialitatea, ratingului de risc, reevaluării și evaluării declanșatorilor DPIA înainte ca prelucrarea nouă sau modificată semnificativ să continue. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.6; 4.2.1; 4.2.4; 4.3.1; 4.3.7; 4.6.1].

13.2.3 **Clause 6.1.3** - Mapată la planificarea tratamentului riscurilor privind confidențialitatea, actualizările aplicabilității controalelor, implementarea tratamentului, acceptarea riscului rezidual și legătura cu SoA. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 6.1.5; 7.1.7; 11.1.5].

13.2.4 **Clause 6.3** - Mapată la modificările PIMS și ale prelucrării planificate care declanșează reevaluarea riscurilor privind confidențialitatea și revizuirea DPIA. Addressed by clauses [4.2.4; 4.6.1; 11.1.1].

13.2.5 **Clause 7.5** - Mapată la informațiile documentate controlate pentru evaluarea preliminară a riscurilor privind confidențialitatea, dovezile DPIA, tratamentul riscului, acceptarea riscului rezidual, deciziile privind consultarea prealabilă, excepțiile, neconformitățile și dovezile de revizuire a politicii. Addressed by clauses [4.1.6; 4.3.7; 4.4.1; 4.5.1; 5.1.2; 7.1.1; 9.1.1; 10.1.1; 11.1.1].

13.2.6 **Clause 8.1** - Mapată la operarea controalelor privind riscurile de confidențialitate și DPIA înainte de intrarea în producție, integrare, aprobarea prelucrării, închiderea tratamentului și legătura cu acțiunile corective. Addressed by clauses [4.1.1; 4.1.5; 7.1.2; 7.1.3; 7.1.4; 7.1.5; 7.1.6; 7.1.7; 7.1.8].

13.2.7 **Clause 8.2** - Mapată la evaluarea operațională a riscurilor privind confidențialitatea pentru modificări de prelucrare noi, modificate, de sistem, furnizor, transfer și determinate de incidente. Addressed by clauses [4.1.1; 4.2.4; 4.3.1; 4.3.5; 4.5.5; 4.6.1].

13.2.8 **Clause 8.3** - Mapată la tratamentul operațional al riscurilor privind confidențialitatea, atribuirea tratamentului, implementarea tratamentului, escaladarea tratamentului restant și verificarea eficacității. Addressed by clauses [4.4.1; 4.4.3; 4.4.4; 4.4.6; 4.4.7; 8.1.3; 10.1.7].

13.2.9 **Clause 9.1** - Mapată la monitorizarea și măsurarea acoperirii evaluării preliminare, stării DPIA, riscurilor deschise, acțiunilor restante de tratament, acțiunilor furnizorilor, acțiunilor de tratament al securității, acțiunilor de reevaluare după incidente și constatărilor de audit. Addressed by clauses [4.6.3; 4.6.4; 4.6.5; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 8.1.8].

13.2.10 **Clause 9.3** - Mapată la revizuirea de management a riscurilor reziduale ridicate privind confidențialitatea, acțiunilor restante de tratament, stării DPIA complete, deciziilor privind consultarea prealabilă și excepțiilor majore privind riscurile de confidențialitate. Addressed by clauses [4.6.6; 6.1.1; 6.1.2; 6.1.3; 10.1.5].

13.2.11 **Clause 10.2** - Mapată la neconformitățile privind riscurile de confidențialitate și DPIA, excepții, deschiderea acțiunilor corective, escaladare și verificarea eficacității. Addressed by clauses [4.4.6; 9.1.1; 9.1.2; 9.1.4; 9.1.6; 10.1.1; 10.1.5; 10.1.6; 10.1.7].

13.2.12 **Annex A.1.2.6** - Mapată la evaluarea necesității unei evaluări a impactului asupra confidențialității și implementarea acesteia, după caz, pentru prelucrări noi sau modificate în calitate de operator. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.2.13 **Annex A.1.2.9** - Mapată la evidențele de prelucrare care susțin intrările evaluării riscurilor privind confidențialitatea și ale DPIA, inclusiv scopul, categoriile, sistemele, destinatarii, transferurile și furnizorii. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.2.14 **Annex A.2.2.2** - Mapată la acordurile dintre persoanele împuternicite și clienți și obligațiile de asistență pentru DPIA pentru clienți. Addressed by clauses [4.1.4; 4.2.5; 4.5.4; 5.1.7; 7.1.6].

13.2.15 **Annex A.2.2.6** - Mapată la furnizarea de către persoana împuternicită a informațiilor necesare pentru conformitatea clientului, inclusiv asistența pentru DPIA și dovezile de suport pentru client. Addressed by clauses [4.2.5; 4.2.6; 4.5.4; 8.1.5].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapată la dovezile privind responsabilitatea pentru evaluarea preliminară DPIA, deciziile privind DPIA completă, tratamentul riscului, acceptarea riscului rezidual, deciziile privind consultarea prealabilă, excepțiile, constatările de audit și acțiunile corective. Addressed by clauses [4.1.6; 4.3.7; 4.4.5; 4.5.1; 4.6.4; 10.1.1; 10.1.7].

13.3.2 **Article 24** - Mapată la responsabilitatea operatorului pentru măsuri adecvate privind riscurile de confidențialitate, revizuirea riscului rezidual ridicat, aprobarea de management și menținerea politicii. Addressed by clauses [4.4.5; 4.5.3; 6.1.2; 10.1.5; 11.1.4].

13.3.3 **Article 25** - Mapată la dovezile privind protecția datelor încă din faza de proiectare și protecția datelor în mod implicit utilizate în evaluarea riscurilor și înainte de aprobarea intrării în producție. Addressed by clauses [4.1.5; 4.3.4; 7.1.5].

13.3.4 **Article 28** - Mapată la asistența pentru DPIA din partea persoanelor împuternicite și persoanelor subîmputernicite, gestionarea instrucțiunilor clientului și dovezile privind tratamentul riscurilor furnizorilor. Addressed by clauses [4.1.4; 4.2.5; 4.2.6; 4.4.4; 4.5.4; 7.1.6; 8.1.5].

13.3.5 **Article 30** - Mapată la evidențele de prelucrare care susțin intrările evaluării riscurilor privind confidențialitatea și ale DPIA. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.3.6 **Article 32** - Mapată la intrările privind riscurile de securitate PII, selectarea măsurilor de protecție, tratamentul riscurilor de securitate și actualizările stării controalelor de securitate. Addressed by clauses [4.1.5; 4.3.3; 4.4.2; 8.1.6].

13.3.7 **Article 35** - Mapată la evaluarea preliminară DPIA, stabilirea cerinței de DPIA completă, conținutul DPIA, consilierea DPO, revizuirea și blocarea prelucrării cu risc ridicat fără aprobarea DPIA necesară. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.3.6; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.3.8 **Article 36** - Mapată la procesul decizional privind consultarea prealabilă, consilierea DPO, aprobarea Top Management și acțiunile de continuare, suspendare, reproiectare sau consultare atunci când rămâne un risc rezidual ridicat. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 6.1.2].

13.3.9 **Article 39** - Mapată la consilierea și monitorizarea de către Data Protection Officer / Privacy Advisor, acolo unde este aplicabil, pentru deciziile DPIA, prelucrarea cu risc ridicat, consultarea prealabilă și modificările politicii. Addressed by clauses [4.2.3; 4.3.6; 4.5.2; 5.1.3; 6.1.3; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.11; Clause 5.12** - Mapată la identificarea controalelor de confidențialitate, măsurile de protecție a securității, conformitatea privind confidențialitatea, dovezile privind riscurile de confidențialitate, monitorizare și revizuire. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.7; 4.6.3; 4.6.5; 8.1.6; 10.1.7].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Mapată la domeniul de aplicare al procesului PIA, beneficii, stabilirea declanșatorului, pregătire, intrări ale evaluării, dovezi ale părților interesate și structura raportului DPIA menținută în REG04. Addressed by clauses [4.1.1; 4.1.3; 4.1.6; 4.2.1; 4.3.1; 4.3.2; 4.3.7; 7.1.1].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2** - Mapată la cerințele programului de protecție PII, identificarea cerințelor de protecție PII, selectarea controalelor bazată pe risc și legătura cu tratamentul riscurilor privind confidențialitatea. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 6.1.5].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7** - Mapată la principiile organizaționale privind riscurile de confidențialitate, leadership, integrare, evaluarea riscurilor, tratamentul riscurilor, monitorizare și revizuire, precum și înregistrare și raportare. Addressed by clauses [4.1.2; 4.3.1; 4.3.7; 4.4.1; 4.4.5; 4.6.3; 4.6.4; 5.1.1; 6.1.1; 6.1.2; 8.1.1; 8.1.3].