

				Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: PII06				Titlul documentului: <b>Politica de management al drepturilor persoanelor vizate</b>							
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

<p><b>Notă juridică (drepturi de autor și restricții de utilizare)</b>  (C) 2025 Clarysec LLC. All rights reserved.</p> <p>Acest document este proprietatea intelectuală a Clarysec LLC. Nicio parte a acestui document nu poate fi copiată, reutilizată, distribuită sau modificată în scopuri comerciale sau de implementare fără autorizare prealabilă expresă, în scris.</p> <p>Utilizarea neautorizată este strict interzisă și poate conduce la acțiuni legale.</p> <p>Pentru licențiere, contactați: <a href="mailto:info@clarysec.com">info@clarysec.com</a></p>
--

## Aliniată la standardele și reglementările aplicabile

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Dovezi privind cererile de exercitare a drepturilor 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.1.3.2	Controller	Primary	Obligații față de persoanele vizate
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.7	Controller	Primary	Opoziție, acces, rectificare și ștergere
ISO/IEC 27701:2025	Annex A.1.3.8; Annex A.1.3.9	Controller	Primary	Notificarea terților și copia PII prelucrate
ISO/IEC 27701:2025	Annex A.1.3.10; Annex A.1.3.11	Controller	Primary	Gestionarea cererilor și obligațiile privind procesul decizional automatizat
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Evidențe de prelucrare ale operatorului
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Acord cu clientul, sprijin pentru obligații și evidențe ale persoanei împuternicite
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Sprijinul persoanei împuternicite pentru obligațiile față de persoana vizată
ISO/IEC 27701:2025	Annex A.3.14	Both	Supporting	Protejarea înregistrărilor privind cererile de exercitare a drepturilor
GDPR	Article 5(1)(a); Article 5(2)	Controller	Supporting	Transparență și responsabilitate
GDPR	Article 11; Article 12	Controller	Primary	Identificare, modalități de

				solicitare, termene și governanța răspunsurilor
GDPR	Article 15; Article 16; Article 17	Controller	Primary	Acces, rectificare și ștergere
GDPR	Article 18; Article 19; Article 20	Controller	Primary	Restricționare, notificare și portabilitate
GDPR	Article 21; Article 22	Controller	Primary	Opoziție și proces decizional automatizat
GDPR	Article 24	Controller	Supporting	Responsabilitatea operatorului și măsuri
GDPR	Article 26	Joint Controller	Supporting	Alocarea drepturilor între operatori asociați
GDPR	Article 28	Both	Primary	Asistența persoanei împuternicite pentru cererile de exercitare a drepturilor
GDPR	Article 30	Both	Supporting	Legătura cu evidențele activităților de prelucrare
GDPR	Article 32	Both	Supporting	Gestionarea securizată a dovezilor privind drepturile și a divulgărilor
GDPR	Article 39	Conditional	Supporting	Consilierea și monitorizarea DPO, acolo unde este aplicabil
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.12	Both	Supporting	Transparență, participarea persoanei, responsabilitate și conformitate
ISO/IEC 29151:2022	Annex A.10	Controller	Supporting	Participarea și accesul persoanei vizate

## **1. Domeniu de aplicare**

- 1.1 Prezenta politică definește cerințele obligatorii pentru primirea, validarea, evaluarea, îndeplinirea, refuzarea, prelungirea, închiderea, monitorizarea și dovedirea cererilor de exercitare a drepturilor persoanelor vizate.
- 1.2 Prezenta politică se aplică cererilor formulate de persoanele vizate sau de reprezentanții împuterniciți privind accesul, rectificarea, ștergerea, restricționarea, portabilitatea, opoziția, procesul decizional automatizat, direcționarea retragerii consimțământului, reclamațiile și întrebările conexe.
- 1.3 Prezenta politică se aplică în contexte de operator, operator asociat, persoană împuternicită și persoană subîmputernicită.
- 1.4 Obligațiile persoanei împuternicite și ale persoanei subîmputernicite se aplică numai atunci când organizația sprijină un operator, un client sau o persoană împuternicită din amonte în baza unor instrucțiuni documentate.

### **1.5 Prezenta politică nu înlocuiește:**

- 1.5.1 PII03 pentru inventarul prelucrărilor și înregistrările privind temeiul juridic;
- 1.5.2 PII04 pentru conținutul și publicarea notelor de informare privind confidențialitatea;
- 1.5.3 PII05 pentru îndeplinirea consimțământului și a preferințelor;
- 1.5.4 PII10 pentru executarea retenției, ștergerii și eliminării;
- 1.5.5 PII11 pentru guvernanta acuratetei și calității;
- 1.5.6 PII12 pentru guvernanta ciclului de viață al persoanelor împuternicite și subîmputernicite;
- 1.5.7 PII15 pentru gestionarea incidentelor și încălcărilor.

## **2. Scop**

- 2.1 Scopul prezentei politici este de a asigura că cererile de exercitare a drepturilor persoanelor vizate sunt gestionate consecvent, legal, securizat, în termene definite și cu dovezi pregătite pentru audit.
- 2.2 Prezenta politică asigură că organizația poate demonstra responsabilitatea pentru primirea cererilor, verificarea identității, evaluare, îndeplinire, refuz, prelungire, cooperarea cu persoanele împuternicite, închidere și îmbunătățire continuă.

## **3. Obiective**

### **3.1 Obiectivele prezentei politici sunt:**

- 3.1.1 Să asigure primirea și urmărirea consecventă a tuturor cererilor de exercitare a drepturilor persoanelor vizate.
- 3.1.2 Să verifice identitatea sau autoritatea solicitantului înainte de divulgare, rectificare, ștergere, restricționare sau portabilitate.
- 3.1.3 Să evalueze cererile în raport cu evidențele de prelucrare, clasificarea rolului, obligațiile legale, obligațiile contractuale și fezabilitatea tehnică.
- 3.1.4 Să îndeplinească cererile valide în termene documentate.
- 3.1.5 Să înregistreze dovezi privind refuzul, îndeplinirea parțială, prelungirea și închiderea.
- 3.1.6 Să sprijine obligațiile operatorului atunci când organizația acționează ca persoană împuternicită sau persoană subîmputernicită.
- 3.1.7 Să protejeze înregistrările privind cererile de exercitare a drepturilor și pachetele de răspuns împotriva divulgării sau modificării neautorizate.
- 3.1.8 Să monitorizeze performanța gestionării cererilor de exercitare a drepturilor și să inițieze acțiuni corective atunci când este necesar.

## **4. Declarații de politică**

### **4.1 Primire, înregistrare și clasificare**

- 4.1.1 [All] Privacy Lead / PIMS Manager TREBUIE să înregistreze fiecare cerere de exercitare a drepturilor persoanei vizate în REG06 în termen de două zile lucrătoare de la primire.
- 4.1.2 [All] Privacy Lead / PIMS Manager TREBUIE să clasifice în REG06, înainte de începerea evaluării, tipul fiecărei cereri, canalul cererii, data cererii, referința privind identitatea solicitantului, responsabilul desemnat, termenul intern, termenul legal sau contractual și starea curentă.
- 4.1.3 [Controller] Privacy Lead / PIMS Manager TREBUIE să confirme primirea sau să furnizeze următoarea comunicare necesară către solicitant în termen de cinci zile lucrătoare de la primire și să înregistreze comunicarea în REG06.
- 4.1.4 [Controller] Process Owner / Business Owner TREBUIE să lege fiecare cerere de activitatea de prelucrare relevantă din REG02 înainte de alocarea acțiunilor de îndeplinire.
- 4.1.5 [Joint Controller] Privacy Lead / PIMS Manager TREBUIE să identifice, în REG02, REG06 sau REG08, partea operator asociat responsabilă cu gestionarea cererii înainte de începerea evaluării de fond.
- 4.1.6 [Processor] Privacy Lead / PIMS Manager TREBUIE să înregistreze în REG06 și REG08 fiecare instrucțiune a clientului privind o cerere de exercitare a drepturilor persoanei vizate înainte de începerea activității de sprijin.
- 4.1.7 [Subprocessor] Vendor / Procurement Owner TREBUIE să înregistreze în REG06 sau REG08 fiecare instrucțiune din amonte privind o cerere de exercitare a drepturilor persoanei vizate înainte de începerea activității de sprijin a persoanei subîmputernicite.
- 4.1.8 [All] Incident Response Coordinator TREBUIE să înregistreze o escaladare REG10 în termen de o zi lucrătoare atunci când o cerere de exercitare a drepturilor indică un posibil incident sau o posibilă încălcare PII.

## **4.2 Verificarea identității, domeniul și evaluarea**

- 4.2.1 [Controller] Privacy Lead / PIMS Manager TREBUIE să verifice în REG06 identitatea solicitantului sau autoritatea reprezentantului înainte de a divulga PII sau de a efectua o modificare solicitată.
- 4.2.2 [Controller] Privacy Lead / PIMS Manager TREBUIE să solicite numai informațiile suplimentare minime necesare pentru verificare și să înregistreze cererea în REG06 atunci când identitatea sau autoritatea este insuficientă.
- 4.2.3 [Controller] Process Owner / Business Owner TREBUIE să identifice din REG02 sistemele, înregistrările, scopurile, categoriile de PII, destinatarii și constrângerile de retenție relevante înainte de evaluarea îndeplinirii.
- 4.2.4 [Controller] Data Protection Officer / Privacy Advisor TREBUIE să revizuiască în REG06 cererile cu risc ridicat, contestate, neclare, excesive, repetate, refuzate sau îndeplinite parțial înainte ca decizia să fie comunicată.
- 4.2.5 [Controller] System Owner / Application Owner TREBUIE să verifice faptul că extrasele de răspuns propuse exclud PII fără legătură cu cererea și date neautorizate ale terților înainte de eliberarea pachetului de răspuns.
- 4.2.6 [Controller] Information Security Lead TREBUIE să revizuiască metoda de transmitere a răspunsului în REG06 sau REG12 înainte de divulgarea PII în volum mare, sensibile, din categorii speciale sau cu risc ridicat.
- 4.2.7 [Controller] Data Protection Officer / Privacy Advisor TREBUIE să revizuiască în REG06 și REG04 cererile legate de procesul decizional automatizat sau de profilare înainte de îndeplinire, refuz sau escaladare.

- 4.2.8 [Both] Privacy Lead / PIMS Manager TREBUIE să înregistreze în REG06 rezultatul evaluării, tipul de cerere aplicabil, decizia, justificarea și acțiunea următoare înainte de îndeplinire sau refuz.

[ ... 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 o excepție în REG12 înainte de a se abate de la cerințele aprobate privind primirea, verificarea, îndeplinirea, răspunsul sau închiderea cererilor de exercitare a drepturilor.
- 9.1.2 [All] Privacy Lead / PIMS Manager TREBUIE să aprobe sau să respingă fiecare excepție privind gestionarea drepturilor în REG12 înainte de implementare.
- 9.1.3 [Controller] Data Protection Officer / Privacy Advisor TREBUIE să revizuiască orice excepție care implică refuz, îndeplinire parțială, incertitudine privind identitatea, PII sensibile, proces decizional automatizat, cereri referitoare la copii sau prelucrări cu risc ridicat înainte de aprobare.
- 9.1.4 [Both] System Owner / Application Owner TREBUIE să blocheze activitatea de divulgare, rectificare, ștergere, restricționare sau export atunci când o excepție necesară nu a fost aprobată în REG12 înainte de acțiune.
- 9.1.5 [All] Privacy Lead / PIMS Manager TREBUIE să atribuie o dată de expirare, un responsabil și un control compensatoriu pentru fiecare excepție aprobată privind gestionarea drepturilor în REG12 înainte ca excepția să devină activă.

## 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 unei înregistrări de cerere de exercitare a drepturilor restante, lipsă, incomplete, neverificate sau nesustținute.
- 10.1.2 [Controller] System Owner / Application Owner TREBUIE să suspende divulgarea răspunsului până când verificările privind identitatea, autoritatea și pachetul de răspuns sunt înregistrate în REG06.
- 10.1.3 [Both] Vendor / Procurement Owner TREBUIE să escaladeze necooperarea persoanelor împuternicite, persoanelor subîmputernicite sau terților în REG08 și REG12 în termen de cinci zile lucrătoare de la identificare.
- 10.1.4 [All] Top Management TREBUIE să atribuie responsabilitatea pentru acțiuni corective în REG12 atunci când eșecurile privind cererile de exercitare a drepturilor sunt sistemice, repetate sau relevante pentru certificare.
- 10.1.5 [All] Internal Audit / Compliance Reviewer TREBUIE să verifice în REG12, până la termenul atribuit, dovezile de închidere pentru acțiunile corective legate de drepturi.
- 10.1.6 [All] Incident Response Coordinator TREBUIE să inițieze o revizuire REG10 în termen de o zi lucrătoare atunci când o neconformitate privind cererile de exercitare a drepturilor indică divulgare neautorizată, pierdere, modificare, indisponibilitate sau alt incident PII suspectat.

## 11. Revizuire și mentenanță

- 11.1.1 [All] Privacy Lead / PIMS Manager TREBUIE să revizuiască prezenta politică anual și să înregistreze rezultatul revizuirii în REG12.
- 11.1.2 [All] Privacy Lead / PIMS Manager TREBUIE să revizuiască prezenta politică în termen de 30 de zile de la o modificare semnificativă a legislației privind cererile de exercitare a drepturilor, a domeniului activităților de prelucrare, a instrumentelor pentru drepturi, a metodei de verificare

a identității, a modelului de servicii al persoanelor împuternicite sau a cerințelor de certificare PIMS.

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

11.1.4 [All] Top Management TREBUIE să aprobe modificările semnificative ale prezentei 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 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 răspunderea în domeniul confidențialității

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 de gestionare a consimțământului și preferințelor

12.7 PII07 - Politica privind evaluarea riscurilor privind confidențialitatea și DPIA

12.8 PII08 - Politica privind protecția datelor încă din faza de proiectare și protecția datelor 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 de management al confidențialității pentru persoanele împuternicite, persoanele subîmputernicite și terți

12.13 PII13 - Politica privind transferul internațional de PII

12.14 PII14 - Politica privind securitatea PII și controlul accesului

12.15 PII15 - Politica de management al incidentelor și încălcărilor PII

12.16 PII16 - Politica privind instruirea, conștientizarea și competența în domeniul confidențialității

12.17 PII17 - Politica privind informațiile documentate și gestionarea dovezilor PIMS

12.18 PII18 - Politica de monitorizare, audit și îmbunătățire 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 7.5; Clause 8.1** - Mapate la înregistrările documentate ale cererilor de exercitare a drepturilor, fluxul operațional al cererilor, verificarea identității, îndeplinire, răspuns, închidere și dovezi privind sprijinul persoanelor împuternicite. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.8; 4.3.10; 4.4.5; 7.1.1; 7.1.2; 7.1.3].

13.2.2 **Clause 9.1; Clause 10.2** - Mapate la metricile cererilor de exercitare a drepturilor, monitorizarea cererilor restante, eșantionarea de audit, înregistrarea neconformităților, acțiunea corectivă și verificarea eficacității. Addressed by clauses [4.5.6; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 10.1.1; 10.1.3; 10.1.4; 10.1.5].

- 13.2.3 **Annex A.1.3.2** - Mapată la determinarea și îndeplinirea obligațiilor față de persoanele vizate prin categorii documentate de drepturi, canale de primire, verificare, evaluare, răspuns și criterii de închidere. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.2.8; 4.4.1; 4.4.4; 6.1.1; 7.1.1].
- 13.2.4 **Annex A.1.3.6; Annex A.1.3.7** - Mapate la gestionarea opoziției, accesului, rectificării, ștergerii și restricționării, verificare, îndeplinire și gestionarea acurateței contestate. Addressed by clauses [4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.6; 4.4.6].
- 13.2.5 **Annex A.1.3.8; Annex A.1.3.9** - Mapate la notificarea terților în urma rezultatelor privind drepturile și la furnizarea de copii sau pachete de răspuns portabile. Addressed by clauses [4.3.5; 4.3.8; 4.5.5].
- 13.2.6 **Annex A.1.3.10; Annex A.1.3.11** - Mapate la gestionarea documentată a cererilor legitime, termenelor, prelungirilor, refuzului, închiderii și revizuirii cererilor privind procesul decizional automatizat. Addressed by clauses [4.1.2; 4.2.4; 4.2.7; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5].
- 13.2.7 **Annex A.1.2.9** - Mapată la legarea cererilor de exercitare a drepturilor de evidențele de prelucrare, scopurile prelucrării, sisteme, categorii, destinatari și constrângeri de retenție. Addressed by clauses [4.1.4; 4.2.3; 4.3.8; 7.1.3].
- 13.2.8 **Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7** - Mapate la instrucțiunile din acordurile cu clienții, sprijinul persoanelor împuternicite pentru obligațiile clientului și evidențele persoanelor împuternicite pentru activitățile de sprijin privind drepturile. Addressed by clauses [4.1.6; 4.1.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 7.1.7].
- 13.2.9 **Annex A.2.3.2** - Mapată la mijloacele persoanei împuternicite de sprijinire a obligațiilor operatorului față de persoanele vizate, inclusiv sprijin pentru regăsire, rectificare, restricționare, ștergere și export în baza unei instrucțiuni documentate. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 7.1.7].
- 13.2.10 **Annex A.3.14** - Mapată la protejarea înregistrărilor privind cererile de exercitare a drepturilor, gestionarea securizată a pachetelor de răspuns, verificările transiterii răspunsurilor și protejarea dovezilor de închidere. Addressed by clauses [4.2.5; 4.2.6; 4.4.5; 4.4.7; 7.1.4; 7.1.5; 10.1.2].

### 13.3 GDPR

- 13.3.1 **Article 5(1)(a); Article 5(2)** - Mapate la gestionarea transparentă a drepturilor, dovezile privind responsabilitatea, registrele cererilor, înregistrările răspunsurilor, eșantionarea de audit și acțiunea corectivă. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.4.4; 4.4.5; 8.1.5; 10.1.1].
- 13.3.2 **Article 11; Article 12** - Mapate la identificare, informații suplimentare atunci când sunt necesare, termene de răspuns, comunicări, prelungire, refuz și închiderea cererilor. Addressed by clauses [4.2.1; 4.2.2; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5].
- 13.3.3 **Article 15; Article 16; Article 17** - Mapate la rezultatele căutării pentru acces, rectificare, ștergere, verificare, dovezi de îndeplinire și transmiterea pachetului de răspuns. Addressed by clauses [4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.5; 4.3.10].
- 13.3.4 **Article 18; Article 19; Article 20** - Mapate la restricționare, notificarea rezultatelor privind drepturile către părțile relevante și portabilitate sau transmiterea copieii. Addressed by clauses [4.3.4; 4.3.5; 4.3.8; 4.5.5].
- 13.3.5 **Article 21; Article 22** - Mapate la evaluarea opoziției și la revizuirea cererilor privind procesul decizional automatizat sau profilarea. Addressed by clauses [4.2.7; 4.3.6; 4.3.7].
- 13.3.6 **Article 24** - Mapat la măsurile de guvernanta ale operatorului, roluri, responsabilitatea pentru fluxul de lucru, revizuire, excepții, acțiune corectivă și supravegherea conducerii pentru gestionarea drepturilor. Addressed by clauses [5.1.1; 5.1.2; 6.1.1; 6.1.3; 6.1.4; 9.1.1; 9.1.2; 10.1.4; 11.1.1].

13.3.7 **Article 26** - Mapat la identificarea responsabilității operatorului asociat pentru gestionarea cererilor înainte de începerea evaluării de fond. Addressed by clauses [4.1.5; 6.1.5].

13.3.8 **Article 28** - Mapat la asistența persoanelor împuternicite și subîmputernicite, instrucțiuni documentate ale clientului, termene de sprijin, lipsa unui răspuns direct fără autorizare și escaladarea necooperării. Addressed by clauses [4.1.6; 4.1.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.6; 6.1.6].

13.3.9 **Article 30** - Mapat la legarea cererilor de exercitare a drepturilor de evidențele de prelucrare, activitățile de prelucrare, sisteme, categorii de PII, destinatari și evidențe ale persoanelor împuternicite. Addressed by clauses [4.1.4; 4.2.3; 4.3.8; 4.5.1; 7.1.3].

13.3.10 **Article 32** - Mapat la gestionarea securizată a cererilor de exercitare a drepturilor, protecția transmiterii răspunsurilor, prevenirea divulgării neautorizate și protejarea dovezilor privind drepturile. Addressed by clauses [4.2.5; 4.2.6; 7.1.4; 7.1.5; 10.1.2; 10.1.6].

13.3.11 **Article 39** - Mapat la consilierea și monitorizarea de către Data Protection Officer / Privacy Advisor pentru cererile de exercitare a drepturilor cu risc ridicat, contestate, refuzate, prelungite și legate de procesul decizional automatizat. Addressed by clauses [4.2.4; 4.2.7; 4.3.7; 4.4.3; 6.1.3; 9.1.3; 11.1.3].

#### **13.4 ISO/IEC 29100:2020**

13.4.1 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.12** - Mapate la transparența canalelor de exercitare a drepturilor, participarea și accesul persoanei, responsabilitate, proceduri de reclamație/remediere, monitorizarea conformității în materie de confidențialitate și dovezi de audit. Addressed by clauses [4.1.3; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.8; 4.4.6; 7.1.1; 8.1.5; 10.1.1].

#### **13.5 ISO/IEC 29151:2022**

13.5.1 **Annex A.10** - Mapată la participarea și accesul persoanei vizate, verificarea identității, acces, rectificare, ștergere, actualizări de stare, sprijinul persoanei împuternicite și mecanisme de reclamație/remediere. Addressed by clauses [4.1.1; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.4.4; 4.5.1; 4.5.4; 8.1.6].

#### **13.6 Cerințe interne**

13.6.1 Cerință internă - Clauzele care definesc REG06 ca obiect principal de dovezi privind drepturile, instruirea, aprobarea fluxurilor de lucru nestandard, expirarea excepțiilor, revizuirea politicii și comunicarea modificărilor politicii susțin consecvența implementării, dar nu sunt mapate direct la o singură clauză externă. Addressed by clauses [5.1.2; 6.1.7; 7.1.6; 9.1.4; 9.1.5; 11.1.2; 11.1.4; 11.1.5].