

				Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: PII06				Dokumenta nosaukums: Datu subjekta tiesību pārvaldības politika							
Versija: 1.0		Spēkā stāšanās datums: 01.01.2025		Dokumenta īpašnieks:							
X	Politika		Standarts		Procedūra		Veidlapa		Reģistrs		Cits

Pārskatījumu vēsture				
Pārskatījuma numurs	Pārskatījuma datums	Izmaiņas	Pārskatīja	Procesa īpašnieks

Apstiprinājumi			
Vārds	Amats	Datums	Paraksts

Juridiskais paziņojums (autortiesības un lietošanas ierobežojumi)
(C) 2025 Clarysec LLC. All rights reserved.

Šis dokuments ir Clarysec LLC intelektuālais īpašums. Nevienu šī dokumenta daļu nedrīkst kopēt, atkārtoti izmantot, izplatīt vai grozīt komerciāliem vai ieviešanas nolūkiem bez iepriekšējas skaidras rakstiskas atļaujas.

Neautorizēta lietošana ir stingri aizliegta un var izraisīt tiesvedību.

Par licencēšanu sazinieties: info@clarysec.com

Saskaņots ar piemērojamiem standartiem un regulējumu

Standarts / regulējums	Punkts / kontrole / pants	Piemērojamība	Pārklājuma veids	Komentārs
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Datu subjekta tiesību īstenošanas pieprasījumu pierādījumi un darbības kontroles pasākumi
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Uzraudzība, neatbilstības un korektīvās darbības
ISO/IEC 27701:2025	Annex A.1.3.2	Controller	Primary	Pienākumi pret datu subjektiem
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.7	Controller	Primary	Iebildumi, piekļuve, labošana un dzēšana
ISO/IEC 27701:2025	Annex A.1.3.8; Annex A.1.3.9	Controller	Primary	Trešo pušu informēšana un apstrādātās PII kopija
ISO/IEC 27701:2025	Annex A.1.3.10; Annex A.1.3.11	Controller	Primary	Pieprasījumu apstrāde un automatizētas lēmumu pieņemšanas pienākumi
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Pārziņa apstrādes ieraksti
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Klienta līgums, pienākumu atbalsts un apstrādātāja ieraksti
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Apstrādātāja atbalsts pienākumiem pret datu subjektiem
ISO/IEC 27701:2025	Annex A.3.14	Both	Supporting	Datu subjekta tiesību īstenošanas pieprasījumu ierakstu aizsardzība
GDPR	Article 5(1)(a); Article 5(2)	Controller	Supporting	Pārredzamība un pārskatatbildība
GDPR	Article 11; Article 12	Controller	Primary	Identifikācija, pieprasījumu

				iesniegšanas veidi, termiņi un atbilžu pārvaldība
GDPR	Article 15; Article 16; Article 17	Controller	Primary	Pieklūve, labošana un dzēšana
GDPR	Article 18; Article 19; Article 20	Controller	Primary	Ierobežošana, paziņošana un pārnēsamība
GDPR	Article 21; Article 22	Controller	Primary	Iebildumi un automatizēta lēmumu pieņemšana
GDPR	Article 24	Controller	Supporting	Pārziņa atbildība un pasākumi
GDPR	Article 26	Joint Controller	Supporting	Kopīgu pārziņu tiesību sadalījums
GDPR	Article 28	Both	Primary	Apstrādātāja palīdzība datu subjekta tiesību īstenošanas pieprasījumu izpildē
GDPR	Article 30	Both	Supporting	Sasaiste ar apstrādes ierakstiem
GDPR	Article 32	Both	Supporting	Tiesību pierādījumu un izpaušanas droša apstrāde
GDPR	Article 39	Conditional	Supporting	Datu aizsardzības speciālista konsultācijas un uzraudzība, ja piemērojams
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.12	Both	Supporting	Pārredzamība, personas līdzdalība, pārskatatbildība un atbilstība
ISO/IEC 29151:2022	Annex A.10	Controller	Supporting	Datu subjekta līdzdalība un pieklūve

1. Piemērošanas joma

- 1.1 Šī politika nosaka obligātās prasības datu subjekta tiesību īstenošanas pieprasījumu saņemšanai, validācijai, izvērtēšanai, izpildei, atteikšanai, pagarināšanai, slēgšanai, uzraudzībai un pierādīšanai.
- 1.2 Šī politika attiecas uz datu subjektu vai pilnvaroto pārstāvju pieprasījumiem par piekļuvi, labošanu, dzēšanu, ierobežošanu, pārnēsāšanu, iebildumiem, automatizētu lēmumu pieņemšanu, piekrišanas atsaukšanas maršrutēšanu, sūdzībām un saistītiem jautājumiem.
- 1.3 Šī politika attiecas uz pārziņa, kopīga pārziņa, apstrādātāja un apakšapstrādātāja kontekstiem. Apstrādātāja un apakšapstrādātāja pienākumi ir piemērojami tikai tad, ja organizācija atbalsta pārziņi, klientu vai augšupēju apstrādātāju saskaņā ar dokumentētiem norādījumiem.

1.4 Šī politika neaizstāj:

- 1.4.1 PII03 attiecībā uz apstrādes uzskaiti un tiesiskā pamata ierakstiem;
- 1.4.2 PII04 attiecībā uz privātuma paziņojumu saturu un publicēšanu;
- 1.4.3 PII05 attiecībā uz piekrišanas un preferenču izpildi;
- 1.4.4 PII10 attiecībā uz glabāšanas, dzēšanas un likvidēšanas izpildi;
- 1.4.5 PII11 attiecībā uz precizitātes un kvalitātes pārvaldību;
- 1.4.6 PII12 attiecībā uz apstrādātāja un apakšapstrādātāja dzīves cikla pārvaldību;
- 1.4.7 PII15 attiecībā uz incidentu un pārkāpumu apstrādi.

2. Mērķis

- 2.1 Šīs politikas mērķis ir nodrošināt, ka datu subjekta tiesību īstenošanas pieprasījumi tiek apstrādāti konsekventi, likumīgi, droši, noteiktajos termiņos un ar auditam gataviem pierādījumiem.
- 2.2 Šī politika nodrošina, ka organizācija var pierādīt pārskatatbildību par pieprasījumu pieņemšanu, identitātes pārbaudi, izvērtēšanu, izpildi, atteikšanu, pagarināšanu, apstrādātāju sadarbību, slēgšanu un nepārtrauktu uzlabošanu.

3. Mērķi

3.1 Šīs politikas mērķi ir:

- 3.1.1 Nodrošināt konsekventu visu datu subjekta tiesību īstenošanas pieprasījumu pieņemšanu un izsekošanu.
- 3.1.2 Pirms izpaušanas, labošanas, dzēšanas, ierobežošanas vai pārnēsāšanas pārbaudīt pieprasītāja identitāti vai pilnvarojumu.
- 3.1.3 Izvērtēt pieprasījumus, ņemot vērā apstrādes ierakstus, lomas klasifikāciju, juridiskos pienākumus, līgumiskos pienākumus un tehnisko iespējamību.
- 3.1.4 Izpildīt derīgus pieprasījumus dokumentētajos termiņos.
- 3.1.5 Reģistrēt atteikuma, daļējas izpildes, pagarināšanas un slēgšanas pierādījumus.
- 3.1.6 Atbalstīt pārziņa pienākumus, ja organizācija darbojas kā apstrādātājs vai apakšapstrādātājs.
- 3.1.7 Aizsargāt datu subjekta tiesību īstenošanas pieprasījumu ierakstus un atbilžu pakotnes pret nesankcionētu izpaušanu vai izmaiņšanu.
- 3.1.8 Uzraudzīt datu subjekta tiesību īstenošanas pieprasījumu veikspēju un, ja nepieciešams, virzīt korektīvās darbības.

4. Politikas prasības

4.1 Pieņemšana, reģistrēšana un klasifikācija

- 4.1.1 [All] Privacy Lead / PIMS Manager ir jāreģistrē katrs datu subjekta tiesību īstenošanas pieprasījums REG06 divu darba dienu laikā pēc tā saņemšanas.

- 4.1.2 [All] Privacy Lead / PIMS Manager pirms izvērtēšanas sākšanas REG06 ir jāklasificē katrs pieprasījuma veids, pieprasījuma kanāls, pieprasījuma datums, pieprasītāja identitātes atsauce, piešķirtais īpašnieks, iekšējais izpildes termiņš, tiesību aktos vai līgumā noteiktais izpildes termiņš un pašreizējais statuss.
- 4.1.3 [Controller] Privacy Lead / PIMS Manager piecu darba dienu laikā pēc pieprasījuma pieņemšanas ir jāapstiprina saņemšana vai jāsniedz pieprasītājam nākamā nepieciešamā komunikācija un jāreģistrē šī komunikācija REG06.
- 4.1.4 [Controller] Process Owner / Business Owner pirms izpildes darbību piešķiršanas katrs pieprasījums ir jāsaista ar attiecīgo REG02 apstrādes darbību.
- 4.1.5 [Joint Controller] Privacy Lead / PIMS Manager pirms saturiskās izvērtēšanas sākšanas REG02, REG06 vai REG08 ir jāidentificē kopīgā pārziņa puse, kas ir atbildīga par pieprasījuma apstrādi.
- 4.1.6 [Processor] Privacy Lead / PIMS Manager pirms atbalsta darbību sākšanas REG06 un REG08 ir jāreģistrē katrs klienta norādījums, kas attiecas uz datu subjekta tiesību īstenošanas pieprasījumu.
- 4.1.7 [Subprocessor] Vendor / Procurement Owner pirms apakšapstrādātāja atbalsta darbību sākšanas REG06 vai REG08 ir jāreģistrē katrs augšupējais norādījums, kas attiecas uz datu subjekta tiesību īstenošanas pieprasījumu.
- 4.1.8 [All] Incident Response Coordinator vienas darba dienas laikā ir jāreģistrē REG10 eskalācija, ja datu subjekta tiesību īstenošanas pieprasījums norāda uz iespējamu PII incidentu vai pārkāpumu.

4.2 Identitātes pārbaude, tvērums un izvērtēšana

- 4.2.1 [Controller] Privacy Lead / PIMS Manager pirms PII izpaušanas vai pieprasītas izmaiņas veikšanas REG06 ir jāpārbauda pieprasītāja identitāte vai pārstāvja pilnvarojums.
- 4.2.2 [Controller] Privacy Lead / PIMS Manager verifikācijai ir jāpieprasa tikai minimāli nepieciešamā papildu informācija un, ja identitāte vai pilnvarojums nav pietiekams, pieprasījums jāreģistrē REG06.
- 4.2.3 [Controller] Process Owner / Business Owner pirms izpildes izvērtēšanas no REG02 ir jāidentificē attiecīgās sistēmas, ieraksti, nolūki, PII kategorijas, saņēmēji un glabāšanas ierobežojumi.
- 4.2.4 [Controller] Data Protection Officer / Privacy Advisor pirms lēmuma paziņošanas REG06 ir jāpārskata augsta riska, apstrīdēti, neskaidri, pārmērīgi, atkārtoti, atteikti vai daļēji izpildīti pieprasījumi.
- 4.2.5 [Controller] System Owner / Application Owner pirms atbildes pakotnes izsniegšanas ir jāpārbauda, ka piedāvātie atbildes izraksti neietver nesaistītu PII un nesankcionētus trešo pušu datus.
- 4.2.6 [Controller] Information Security Lead pirms liela apjoma, sensitīvas, īpašu kategoriju vai augsta riska PII izpaušanas REG06 vai REG12 ir jāpārskata atbildes piegādes metode.
- 4.2.7 [Controller] Data Protection Officer / Privacy Advisor pirms izpildes, atteikuma vai eskalācijas REG06 un REG04 ir jāpārskata ar automatizētu lēmumu pieņemšanu vai profilēšanu saistīti pieprasījumi.
- 4.2.8 [Both] Privacy Lead / PIMS Manager pirms izpildes vai atteikuma REG06 ir jāreģistrē izvērtēšanas rezultāts, piemērojamais pieprasījuma veids, lēmums, pamatojums un nākamā darbība.

[... Sadaļas 4.3–8 nav iekļautas šajā priekšskatījumā. Iegādājieties pilnu dokumentu, lai piekļūtu pilnam saturam. ...]

9. Izņēmumi

- 9.1.1 [All] Process Owner / Business Owner pirms atkāpšanās no apstiprinātajām tiesību pieņemšanas, verifikācijas, izpildes, atbildes vai slēgšanas prasībām REG12 ir jāpieprasa izņēmums.
- 9.1.2 [All] Privacy Lead / PIMS Manager pirms ieviešanas REG12 ir jāapstiprina vai jānoraida katrs tiesību apstrādes izņēmums.
- 9.1.3 [Controller] Data Protection Officer / Privacy Advisor pirms apstiprināšanas ir jāpārskata jebkurš izņēmums, kas saistīts ar atteikumu, daļēju izpildi, identitātes nenoteiktību, sensitīvu PII, automatizētu lēmumu pieņemšanu, ar bērniem saistītiem pieprasījumiem vai augsta riska apstrādi.
- 9.1.4 [Both] System Owner / Application Owner ir jābloķē izpaušanas, labošanas, dzēšanas, ierobežošanas vai eksportēšanas darbība, ja nepieciešamais izņēmums pirms darbības nav apstiprināts REG12.
- 9.1.5 [All] Privacy Lead / PIMS Manager pirms izņēmuma stāšanās spēkā REG12 katram apstiprinātam tiesību apstrādes izņēmumam ir jāpiešķir derīguma beigu datums, īpašnieks un kompensējošais kontroles pasākums.

10. Piemērošana

- 10.1.1 [All] Privacy Lead / PIMS Manager piecu darba dienu laikā pēc nokavēta, trūkstoša, nepilnīga, neverificēta vai neatbalstīta datu subjekta tiesību īstenošanas pieprasījuma ieraksta identificēšanas REG12 ir jāreģistrē neatbilstība.
- 10.1.2 [Controller] System Owner / Application Owner ir jāaptur atbildes izpaušana līdz brīdim, kad REG06 ir reģistrētas identitātes, pilnvarojuma un atbildes pakotnes pārbaudes.
- 10.1.3 [Both] Vendor / Procurement Owner piecu darba dienu laikā pēc identificēšanas REG08 un REG12 ir jāeskalē apstrādātāja, apakšapstrādātāja vai trešās puses nesadarbošanās.
- 10.1.4 [All] Top Management, ja datu subjekta tiesību īstenošanas pieprasījumu neizpildes ir sistēmiskas, atkārtotas vai būtiskas sertifikācijai, REG12 ir jāpiešķir korektīvās darbības īpašumtiesības.
- 10.1.5 [All] Internal Audit / Compliance Reviewer līdz piešķirtajam izpildes termiņam REG12 ir jāpārbauda ar tiesībām saistīto korektīvo darbību slēgšanas pierādījumi.
- 10.1.6 [All] Incident Response Coordinator vienas darba dienas laikā ir jāuzsāk REG10 pārskatīšana, ja datu subjekta tiesību īstenošanas pieprasījuma neatbilstība norāda uz nesankcionētu izpaušanu, zudumu, izmaiņšanu, nepieejamību vai citu iespējamu PII incidentu.

11. Pārskatīšana un uzturēšana

- 11.1.1 [All] Privacy Lead / PIMS Manager reizi gadā ir jāpārskata šī politika un pārskatīšanas rezultāts jāreģistrē REG12.
- 11.1.2 [All] Privacy Lead / PIMS Manager šī politika ir jāpārskata 30 dienu laikā pēc būtiskām izmaiņām datu subjekta tiesību īstenošanas pieprasījumu regulējumā, apstrādes darbību tvērumā, tiesību rīkos, identitātes pārbaudes metodē, apstrādātāja pakalpojumu modelī vai PIMS sertifikācijas prasībās.
- 11.1.3 [All] Data Protection Officer / Privacy Advisor pirms apstiprināšanas REG12 ir jāpārskata šīs politikas izmaiņas, kas ir būtiskas privātumam.
- 11.1.4 [All] Top Management pirms publicēšanas REG12 ir jāapstiprina būtiskas izmaiņas šajā politikā.
- 11.1.5 [All] Privacy Lead / PIMS Manager 30 dienu laikā pēc publicēšanas REG11 ir jāreģistrē komunikācija par apstiprinātajām politikas izmaiņām.

12. Saistītās politikas

- 12.1 Šo politiku atbalsta šādas saistītās politikas:
- 12.2 PII01 - Privātuma informācijas pārvaldības sistēmas politika
- 12.3 PII02 - Privātuma lomu, pienākumu un pārskatatbildības politika
- 12.4 PII03 - PII apstrādes uzskaites un tiesiskā pamata politika
- 12.5 PII04 - Privātuma paziņojumu un pārredzamības politika
- 12.6 PII05 - Piekrišanas un preferenču pārvaldības politika
- 12.7 PII07 - Privātuma risku izvērtēšanas un DPIA politika
- 12.8 PII08 - Datu aizsardzības pēc projektēšanas un pēc noklusējuma politika
- 12.9 PII09 - PII vākšanas, izmantošanas, izpaušanas un kopīgošanas politika
- 12.10 PII10 - PII glabāšanas, dzēšanas un likvidēšanas politika
- 12.11 PII11 - PII precizitātes un kvalitātes politika
- 12.12 PII12 - Apstrādātāju, apakšapstrādātāju un trešo pušu privātuma pārvaldības politika
- 12.13 PII13 - Starptautisku PII pārsūtījumu politika
- 12.14 PII14 - PII drošības un piekļuves kontroles politika
- 12.15 PII15 - PII incidentu un pārkāpumu pārvaldības politika
- 12.16 PII16 - Privātuma apmācības, informētības un kompetences politika
- 12.17 PII17 - PIMS dokumentētās informācijas un pierādījumu pārvaldības politika
- 12.18 PII18 - PIMS uzraudzības, audita un uzlabošanas politika

13. Atsauces standarti un ietvari

- 13.1 Šī politika ir kartēta uz šādiem standartiem un regulējumiem. Kartējums skaidro, kā politika atbalsta norādītās prasības, un identificē iekšējos punktus, kas tās ievieš vai atbalsta.

13.2 ISO/IEC 27701:2025

- 13.2.1 **Clause 7.5; Clause 8.1** - Kartēts uz dokumentētiem datu subjekta tiesību īstenošanas pieprasījumu ierakstiem, operatīvu pieprasījumu darbplūsmu, identitātes pārbaudi, izpildi, atbildi, slēgšanu un apstrādātāja atbalsta pierādījumiem. 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** - Kartēts uz datu subjekta tiesību īstenošanas pieprasījumu metriku, nokavētu pieprasījumu uzraudzību, audita izlases pārbaudēm, neatbilstību reģistrēšanu, korektīvajām darbībām un efektivitātes pārbaudi. 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** - Kartēts uz pienākumu pret datu subjektiem noteikšanu un izpildi, izmantojot dokumentētas tiesību kategorijas, pieņemšanas kanālus, verifikācijas, izvērtēšanas, atbildes un slēgšanas kritērijus. 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** - Kartēts uz iebildumu, piekļuves, labošanas, dzēšanas un ierobežošanas apstrādi, verifikāciju, izpildi un apstrīdētas precizitātes apstrādi. 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** - Kartēts uz trešo pušu informēšanu pēc tiesību rezultātiem un kopiju vai pārnesamu atbildes pakotņu nodrošināšanu. 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** - Kartēts uz likumīgu pieprasījumu, termiņu, pagarinājumu, atteikumu, slēgšanas un automatizētas lēmumu pieņemšanas pieprasījumu pārskatīšanas dokumentētu apstrādi. 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** - Kartēts uz datu subjekta tiesību īstenošanas pieprasījumu sasaisti ar apstrādes ierakstiem, apstrādes nolūkiem, sistēmām, kategorijām, saņēmējiem un glabāšanas ierobežojumiem. 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** - Kartēts uz klientu līgumu norādījumiem, apstrādātāja atbalstu klienta pienākumiem un apstrādātāja ierakstiem par tiesību atbalsta darbībām. 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** - Kartēts uz apstrādātāja līdzekļiem, ar kuriem atbalsta pārziņa pienākumus pret datu subjektiem, tostarp izgūšanas, labošanas, ierobežošanas, dzēšanas un eksportēšanas atbalstu saskaņā ar dokumentētu norādījumu. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 7.1.7].
- 13.2.10 **Annex A.3.14** - Kartēts uz datu subjekta tiesību īstenošanas pieprasījumu ierakstu aizsardzību, drošu atbildes pakotņu apstrādi, atbildes piegādes pārbaudēm un slēgšanas pierādījumu aizsardzību. 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)** - Kartēts uz pārredzamu tiesību apstrādi, pārskatatbildības pierādījumiem, pieprasījumu žurnāliem, atbilžu ierakstiem, audita izlases pārbaudēm un korektīvajām darbībām. 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** - Kartēts uz identifikāciju, papildu informāciju, ja tā nepieciešama, atbildes termiņiem, komunikāciju, pagarinājumu, atteikumu un pieprasījuma slēgšanu. 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** - Kartēts uz piekļuves meklēšanas rezultātiem, labošanu, dzēšanu, verifikāciju, izpildes pierādījumiem un atbildes pakotnes piegādi. 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** - Kartēts uz ierobežošanu, attiecīgo pušu informēšanu par tiesību rezultātiem un pārnesamības vai kopijas piegādi. Addressed by clauses [4.3.4; 4.3.5; 4.3.8; 4.5.5].
- 13.3.5 **Article 21; Article 22** - Kartēts uz iebildumu izvērtēšanu un automatizētas lēmumu pieņemšanas vai profilēšanas pieprasījumu pārskatīšanu. Addressed by clauses [4.2.7; 4.3.6; 4.3.7].
- 13.3.6 **Article 24** - Kartēts uz pārziņa pārvaldības pasākumiem, lomām, darbplūsmas īpašumtiesībām, pārskatīšanu, izņēmumiem, korektīvajām darbībām un vadības pārraudzību tiesību apstrādē. 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** - Kartēts uz kopīgā pārziņa atbildības identificēšanu pieprasījumu apstrādei pirms saturiskās izvērtēšanas sākšanas. Addressed by clauses [4.1.5; 6.1.5].
- 13.3.8 **Article 28** - Kartēts uz apstrādātāja un apakšapstrādātāja palīdzību, dokumentētiem klienta norādījumiem, atbalsta termiņiem, aizliegumu sniegt tiešu atbildi bez autorizācijas un nesadarbošanās eskalāciju. 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** - Kartēts uz datu subjekta tiesību īstenošanas pieprasījumu sasaisti ar apstrādes ierakstiem, apstrādes darbībām, sistēmām, PII kategorijām, saņēmējiem un apstrādātāja ierakstiem. Addressed by clauses [4.1.4; 4.2.3; 4.3.8; 4.5.1; 7.1.3].
- 13.3.10 **Article 32** - Kartēts uz drošu datu subjekta tiesību īstenošanas pieprasījumu apstrādi, atbildes piegādes aizsardzību, nesankcionētas izpaušanas novēršanu un tiesību pierādījumu aizsardzību. 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** - Kartēts uz Data Protection Officer / Privacy Advisor konsultācijām un uzraudzību attiecībā uz augsta riska, apstrīdētiem, atteiktiem, pagarinātiem un ar automatizētu lēmumu pieņemšanu saistītiem datu subjekta tiesību īstenošanas pieprasījumiem. 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** - Kartēts uz tiesību kanālu pārredzamību, personas līdzdalību un piekļuvi, pārskatatbildību, sūdzību un tiesiskās aizsardzības procedūrām, privātuma atbilstības uzraudzību un audita pierādījumiem. 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** - Kartēts uz datu subjekta līdzdalību un piekļuvi, identitātes pārbaudi, piekļuvi, labošanu, dzēšanu, statusa atjauninājumiem, apstrādātāja atbalstu un sūdzību/tiesiskās aizsardzības mehānismiem. 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 Iekšējās prasības

13.6.1 Iekšējā prasība - Punkti, kas nosaka REG06 kā primāro tiesību pierādījumu objektu, apmācību, nestandarta darbplūsmas apstiprināšanu, izņēmumu derīguma termiņu, politikas pārskatīšanu un politikas izmaiņu komunikāciju, atbalsta ieviešanas konsekvenci, bet nav tieši kartēti uz vienu ārēju punktu. 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].