					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: PII01					Dokumenta nosaukums: **Privātuma informācijas pārvaldības sistēmas 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**

Saskaņots ar piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts / kontrole / pants	Piemērojamība	Aptvēruma veids	Piezīme
ISO/IEC 27701:2025	Clause 4.1	Both	Primary	Konteksta un PIMS lomas noteikšana
ISO/IEC 27701:2025	Clause 4.2	Both	Primary	Ieinteresētās puses un prasības
ISO/IEC 27701:2025	Clause 4.3	Both	Primary	PIMS darbības joma
ISO/IEC 27701:2025	Clause 4.4	Both	Primary	PIMS izveide un uzlabošana
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Vadība un apņemšanās
ISO/IEC 27701:2025	Clause 5.2	Both	Primary	Privātuma politika
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	Lomas un pilnvaras
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	Riski un iespējas
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Privātuma risku izvērtēšana
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Privātuma riska apstrāde un SoA
ISO/IEC 27701:2025	Clause 6.2	Both	Primary	Privātuma mērķi
ISO/IEC 27701:2025	Clause 6.3	Both	Primary	Plānotās PIMS izmaiņas
ISO/IEC 27701:2025	Clause 7.1	Both	Primary	Resursi
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Kompetence
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Informētība
ISO/IEC 27701:2025	Clause 7.4	Both	Primary	Komunikācija
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumentēta informācija
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Darbības plānošana un kontrole
ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Darbības līmeņa privātuma risku izvērtēšana
ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Darbības līmeņa privātuma riska apstrāde
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Uzraudzība un izvērtēšana

ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Iekšējais audits
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Vadības pārskatīšana
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Nepārtraukta uzlabošana
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	Neatbilstība un korektīvā darbība
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9	Controller	Primary	Pārziņa pārvaldības ieraksti
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3	Processor	Primary	Apstrādātāja vienošanās un nolūki
ISO/IEC 27701:2025	Annex A.3.3	Both	Primary	Sasaiste ar PII drošības politiku
GDPR	Article 5(2)	Controller	Supporting	Pārskatatbildības pierādījumi
GDPR	Article 24	Controller	Supporting	Pārziņa pasākumi un politika
GDPR	Article 26	Joint Controller	Supporting	Kopīgu pārziņu kārtība
GDPR	Article 28	Both	Supporting	Apstrādātāju pārvaldība
GDPR	Article 30	Both	Supporting	Apstrādes ieraksti
GDPR	Article 32	Both	Supporting	Apstrādes drošība
GDPR	Article 35	Controller	Supporting	DPIA pārvaldība
ISO/IEC 29100:2020	Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12	Both	Supporting	Privātuma kontroles pasākumi un principi
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	PIA process un sagatavošana
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2; Annex A.2	Controller	Supporting	PII aizsardzības programma un politika
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1	Both	Supporting	Organizācijas privātuma riska integrācija

1. Piemērošanas joma

1.1 Šī politika nosaka organizācijas privātuma informācijas pārvaldības sistēmu PII apstrādei pārziņa, kopīga pārziņa, apstrādātāja un apakšapstrādātāja kontekstos.

1.2 Šī politika attiecas uz:

1.2.1 PIMS darbības jomu, kontekstu, ieinteresētajām pusēm un organizācijas robežām;

1.2.2 PIMS lomas noteikšanu PII apstrādes darbībām;

1.2.3 privātuma politiku, privātuma mērķiem, privātuma risku izvērtēšanu, privātuma riska apstrādi un PIMS piemērojamības paziņojumu;

1.2.4 PIMS pārvaldību, uzraudzību, iekšējo auditu, vadības pārskatīšanu, neatbilstībām, korektīvajām darbībām un nepārtrauktu uzlabošanu;

1.2.5 dokumentēto informāciju un pierādījumiem, kas nepieciešami PIMS atbilstības un pārskatatbildības pierādīšanai.

1.3 Šīs politikas vajadzībām būtiska izmaiņa ir jebkura izmaiņa, kas ietekmē PIMS darbības jomu, PII apstrādes nolūkus, PII kategorijas, datu subjektu kategorijas, apstrādes vietas, pārziņa vai apstrādātāja lomu sadalījumu, sistēmas arhitektūru, piegādātāju vai apakšapstrādātāju kārtību, privātuma riska profilu, piemērojamos juridiskos vai līgumiskos pienākumus vai sertifikācijas tvērumu.

2. Mērķis

2.1 Šī politika nosaka obligātās pārvaldības prasības PIMS izveidei, ieviešanai, uzturēšanai, uzraudzībai un nepārtrauktai uzlabošanai.

2.2 Šīs politikas mērķis ir nodrošināt, ka organizācija spēj pierādīt pārskatatbildīgu, uz risku balstītu un pierādījumos pamatotu PII apstrādes pārvaldību visās piemērojamajās PIMS lomās.

3. Mērķi

3.1 Šīs politikas mērķi ir:

3.1.1 definēt PIMS darbības jomu, kontekstu, robežas un lomu piemērojamību;

3.1.2 piešķirt pārvaldības pārskatatbildību par PIMS, izmantojot kanoniskās PIMS lomas;

3.1.3 noteikt privātuma mērķus un izmērāmas PIMS veiktspējas prasības;

3.1.4 uzturēt PIMS piemērojamības paziņojumu atlasītajiem un izslēgtajiem kontroles pasākumiem;

3.1.5 integrēt privātuma risku izvērtēšanu, privātuma riska apstrādi un DPIA pārvaldību PIMS darbībā;

3.1.6 nodrošināt, ka pārziņa, kopīga pārziņa, apstrādātāja un apakšapstrādātāja pienākumi tiek identificēti pirms apstrādes uzsākšanas;

3.1.7 uzturēt auditam gatavus pierādījumus gatavībai sertifikācijai un nepārtrauktai uzlabošanai;

3.1.8 izvairīties no nevajadzīgām lomām, reģistriem, veidlapām un dublējošiem darbības kontroles pasākumiem.

4. Politikas noteikumi

4.1 PIMS izveide, konteksts un darbības joma

4.1.1 [Both] Top Management ir jāapstiprina PIMS darbības joma REG01 pirms sākotnējās PIMS ieviešanas un 30 dienu laikā pēc jebkuras būtiskas izmaiņas.

4.1.2 [Both] Privacy Lead / PIMS Manager ik gadu un 30 dienu laikā pēc jebkuras būtiskas izmaiņas REG01 ir jādokumentē ārējie un iekšējie privātuma konteksta jautājumi.

4.1.3 [Both] Privacy Lead / PIMS Manager ik gadu un 30 dienu laikā pēc jebkuras būtiskas izmaiņas REG01 ir jādokumentē attiecīgās ieinteresētās puses un to PIMS prasības.

4.1.4 [Both] Privacy Lead / PIMS Manager pirms katras vadības pārskatīšanas REG01 ir jāuztur PIMS procesu mijiedarbības kopsavilkums.

4.2 PIMS lomas noteikšana

4.2.1 [Both] Process Owner / Business Owner pirms apstrādes darbības uzsākšanas REG02 ir jāklasificē organizācijas PIMS loma katrai PII apstrādes darbībai.

4.2.2 [Joint Controller] Vendor / Procurement Owner pirms kopīgas apstrādes uzsākšanas REG08 ir jādokumentē kopīgu pārziņu atbildības sadalījums.

4.2.3 [Processor] Vendor / Procurement Owner pirms pakalpojuma ieviešanas REG08 ir jādokumentē klienta apstrādes norādījumi apstrādātāja darbībām.

4.2.4 [Subprocessor] Vendor / Procurement Owner pirms apakšapstrādes uzsākšanas REG08 ir jādokumentē augšupējā klienta norādījumi un apstiprinātā apakšapstrādes kārtība.

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

9. Izņēmumi

9.1 Izņēmuma pieprasīšana un apstiprināšana

9.1.1 [All] Process Owner / Business Owner pirms atkāpes iestāšanās REG12 ir jādokumentē jebkurš pieprasītais izņēmums no šīs politikas.

9.1.2 [Both] Privacy Lead / PIMS Manager pirms apstiprināšanas REG04 ir jāizvērtē katra pieprasītā izņēmuma privātuma risks.

9.1.3 [Both] Top Management pirms ieviešanas REG12 ir jāapstiprina izņēmumi, kas pārsniedz pieņemtos privātuma riska sliekšņus.

9.1.4 [Both] Privacy Lead / PIMS Manager reizi ceturksnī līdz slēgšanai REG12 ir jāpārskata aktīvie PIMS izņēmumi.

9.2 Izņēmuma slēgšana

9.2.1 [All] Process Owner / Business Owner līdz apstiprinātajam izņēmuma beigu datumam REG12 ir jādokumentē izņēmuma slēgšanas pierādījumi.

9.2.2 [Both] Internal Audit / Compliance Reviewer nākamā plānotā iekšējā audita laikā REG12 ir jāpārbauda pierādījumi par beigušos izņēmumu slēgšanu.

10. Piemērošana

10.1 Neatbilstību apstrāde

10.1.1 [All] Privacy Lead / PIMS Manager piecu darbdienu laikā pēc identificēšanas REG12 ir jāreģistrē aizdomas par neatbilstībām šai politikai.

10.1.2 [All] Process Owner / Business Owner pēc neatbilstības apstiprināšanas REG12 ir jāievieš apstiprinātās korektīvās darbības līdz piešķirtajam izpildes termiņam.

10.1.3 [All] Top Management katrā vadības pārskatīšanā REG12 ir jāpārskata neatrisinātās būtiskās PIMS neatbilstības.

10.1.4 [All] Internal Audit / Compliance Reviewer 30 dienu laikā pēc ziņotās slēgšanas REG12 ir jāpārbauda korektīvās darbības efektivitāte.

10.2 Eskalācija

10.2.1 [All] Privacy Lead / PIMS Manager piecu darbdienu laikā pēc izpildes termiņa REG12 ir jāeskalē nokavētās būtiskās korektīvās darbības Top Management.

10.2.2 [All] Top Management 15 darbdienu laikā pēc eskalācijas REG12 ir jāreģistrē lēmumi par nokavētajām būtiskajām korektīvajām darbībām.

11. Pārskatīšana un uzturēšana

11.1 Politikas pārskatīšana

11.1.1 [All] Privacy Lead / PIMS Manager ik gadu un 30 dienu laikā pēc jebkuras būtiskas juridiskas, organizatoriskas, apstrādes, tehnoloģiju vai sertifikācijas tvēruma izmaiņas REG12 ir jāpārskata šī politika.

11.1.2 [All] Data Protection Officer / Privacy Advisor pirms politikas apstiprināšanas, ja būtiski mainās privātuma pienākumi, REG12 ir jāsniedz dokumentēta konsultācija.

11.1.3 [All] Top Management pirms publicēšanas REG12 ir jāapstiprina būtiskas šīs politikas izmaiņas.

11.1.4 [All] Privacy Lead / PIMS Manager 15 darbdienu laikā pēc apstiprinātām politikas izmaiņām, kas maina PIMS darbības jomu vai kontroles pasākumu piemērojamību, ir jāatjaunina REG01 un REG03.

11.1.5 [All] Privacy Lead / PIMS Manager 30 dienu laikā pēc publicēšanas REG11 ir jāreģistrē apstiprināto politikas izmaiņu komunikācija.

12. Saistītās politikas

12.1 Šo politiku atbalsta šādas saistītās politikas:

12.2 PII02 - Privātuma lomu, pienākumu un pārskatatbildības politika

12.3 PII03 - PII apstrādes uzskaites un tiesiskā pamata politika

12.4 PII07 - Privātuma risku izvērtēšanas un DPIA politika

12.5 PII08 - Privātuma pēc projektēšanas un pēc noklusējuma politika

12.6 PII12 - Apstrādātāju, apakšapstrādātāju un datu kopīgošanas politika

12.7 PII14 - PII drošības un piekļuves kontroles politika

12.8 PII15 - PII incidentu un pārkāpumu pārvaldības politika

12.9 PII16 - Privātuma apmācību, informētības un kompetences politika

12.10 PII17 - PIMS dokumentētās informācijas un pierādījumu pārvaldības politika

12.11 PII18 - PIMS uzraudzības, audita un uzlabošanas politika

13. Atsauces standarti un ietvari

13.1 Šī politika ir sasaistīta ar šādiem standartiem un regulējumiem. Sasaistes apraksts paskaidro, kā politika atbalsta citētās prasības, un identificē iekšējos punktus, kas tās ievieš vai atbalsta.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 4.1** - Sasaistīts ar organizācijas konteksta, privātuma konteksta jautājumu un pārziņa vai apstrādātāja lomas piemērojamības noteikšanu PIMS darbībām. Addressed by clauses [4.1.2; 4.2.1; 6.1.3].

13.2.2 **Clause 4.2** - Sasaistīts ar ieinteresēto pušu, datu subjektu, klientu, uzraudzības iestāžu, apstrādātāju, apakšapstrādātāju un to attiecīgo PIMS prasību identificēšanu. Addressed by clauses [4.1.3; 7.2.1; 11.1.1].

13.2.3 **Clause 4.3** - Sasaistīts ar dokumentētās PIMS darbības jomas definēšanu, apstiprināšanu, uzturēšanu un mainīšanu. Addressed by clauses [4.1.1; 6.1.3; 11.1.4].

13.2.4 **Clause 4.4** - Sasaistīts ar PIMS procesu un to mijiedarbību izveidi, ieviešanu, uzturēšanu un uzlabošanu. Addressed by clauses [4.1.4; 7.1.1; 7.2.1].

13.2.5 **Clause 5.1** - Sasaistīts ar Top Management apstiprinājumu, resursiem, pārvaldības pārskatīšanu un vadību pār PIMS efektivitāti un uzlabošanu. Addressed by clauses [4.3.1; 5.1.1; 6.1.1; 8.1.4; 10.1.3].

13.2.6 **Clause 5.2** - Sasaistīts ar šīs privātuma politikas uzturēšanu kā apstiprinātu dokumentētu informāciju un politikas izmaiņu komunikāciju. Addressed by clauses [4.3.1; 11.1.1; 11.1.3; 11.1.5].

13.2.7 **Clause 5.3** - Sasaistīts ar PIMS lomu, pienākumu un pilnvaru piešķiršanu un komunikāciju. Addressed by clauses [5.1.1; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.8 **Clause 6.1.1** - Sasaistīts ar darbību plānošanu PIMS risku un iespēju pārvaldībai, izmantojot kontekstu, ieinteresēto pušu prasības, mērķus un uzlabošanas ievaddatus. Addressed by clauses [4.1.2; 4.1.3; 4.4.1; 6.1.1; 8.1.1].

13.2.9 **Clause 6.1.2** - Sasaistīts ar prasību veikt privātuma risku izvērtēšanu pirms jaunas vai būtiski mainītas apstrādes un uzturēt privātuma riska pierādījumus. Addressed by clauses [4.4.1; 5.1.3; 8.2.4; 9.1.2].

13.2.10 **Clause 6.1.3** - Sasaistīts ar privātuma riska apstrādi, kontroles pasākumu atlasi, sasaisti ar informācijas drošības programmu un Piemērojamības paziņojuma uzturēšanu. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.3; 7.1.4; 8.2.2].

13.2.11 **Clause 6.2** - Sasaistīts ar PIMS mērķu noteikšanu, mērīšanu, uzraudzību, komunikāciju un atjaunināšanu. Addressed by clauses [4.3.1; 4.3.2; 8.1.2; 8.1.4].

13.2.12 **Clause 6.3** - Sasaistīts ar plānotām PIMS izmaiņām un tādu izmaiņu kontroli, kas ietekmē darbības jomu, lomas, kontroles pasākumus un dokumentēto informāciju. Addressed by clauses [4.1.1; 6.1.3; 7.1.1; 11.1.4].

13.2.13 **Clause 7.1** - Sasaistīts ar resursu noteikšanu un nodrošināšanu PIMS izveidei, darbībai, uzturēšanai un uzlabošanai. Addressed by clauses [5.1.1; 6.1.1; 7.1.1].

13.2.14 **Clause 7.2** - Sasaistīts ar kompetences prasībām un pierādījumiem, kas atbalsta PIMS pienākumus un lomu izpildi. Addressed by clauses [5.1.3; 5.1.8; 11.1.5].

13.2.15 **Clause 7.3** - Sasaistīts ar informētību par privātuma politiku, ieguldījumu PIMS efektivitātē un neatbilstības sekām. Addressed by clauses [11.1.5; 10.1.1; 10.2.1].

13.2.16 **Clause 7.4** - Sasaistīts ar PIMS pārvaldībai, politikas izmaiņām un eskalācijai nozīmīgu iekšējo un ārējo komunikāciju. Addressed by clauses [6.2.1; 10.2.1; 11.1.5].

13.2.17 **Clause 7.5** - Sasaistīts ar dokumentētas informācijas izveidi, uzturēšanu, kontroli, pierādījumu gatavību un glabāšanu. Addressed by clauses [4.5.1; 4.5.3; 7.1.6; 11.1.4].

13.2.18 **Clause 8.1** - Sasaistīts ar PIMS darbības procesu un ārēji nodrošināto procesu plānošanu, ieviešanu un kontroli. Addressed by clauses [4.4.4; 7.1.3; 7.1.5; 7.2.1].

13.2.19 **Clause 8.2** - Sasaistīts ar privātuma risku izvērtēšanas veikšanu plānotos intervālos un gadījumos, kad tiek ierosinātas vai notiek būtiskas izmaiņas. Addressed by clauses [4.4.1; 8.2.4; 9.1.2].

13.2.20 **Clause 8.3** - Sasaistīts ar privātuma riska apstrādes plānu ieviešanu un apstrādes rezultātu pierādījumu saglabāšanu. Addressed by clauses [4.4.3; 7.1.3; 8.2.2].

13.2.21 **Clause 9.1** - Sasaistīts ar uzraudzību, mērīšanu, analīzi, izvērtēšanu, metrikām un PIMS efektivitātes ziņošanu. Addressed by clauses [8.1.1; 8.1.2; 8.1.4; 8.2.1; 8.2.2; 8.2.3; 8.2.4].

13.2.22 **Clause 9.2** - Sasaistīts ar iekšējā audita plānošanu, pierādījumu izlasi, audita rezultātiem un neatkarīgu pārskatīšanu. Addressed by clauses [5.1.9; 6.2.1; 8.1.3; 9.2.2].

13.2.23 **Clause 9.3** - Sasaistīts ar vadības pārskatīšanas ievaddatiem, veiktspējas pārskatīšanu, vadības pārskatīšanas rezultātiem un uzlabošanas lēmumiem. Addressed by clauses [6.1.1; 6.1.2; 8.1.4; 10.1.3].

13.2.24 **Clause 10.1** - Sasaistīts ar nepārtrauktu uzlabošanu, izmantojot vadības pārskatīšanu, metrikas, korektīvo darbību izsekošanu un politikas uzturēšanu. Addressed by clauses [6.1.1; 6.2.2; 10.1.4; 11.1.1].

13.2.25 **Clause 10.2** - Sasaistīts ar neatbilstību apstrādi, korektīvajām darbībām, eskalāciju, slēgšanu un efektivitātes pārbaudi. Addressed by clauses [4.5.2; 6.2.2; 6.2.3; 10.1.1; 10.1.2; 10.1.4; 10.2.1; 10.2.2].

13.2.26 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9** - Sasaistīts ar pārziņa puses apstrādes nolūku ierakstiem, tiesiskā pamata sasaisti, DPIA nepieciešamības noteikšanu, kopīgu pārziņu atbildības sadalījumu un apstrādes pierādījumu ierakstiem. Addressed by clauses [4.2.1; 4.2.2; 4.4.2; 4.5.1; 7.1.2; 8.2.1].

13.2.27 **Annex A.2.2.2; Annex A.2.2.3** - Sasaistīts ar apstrādātāja klientu vienošanām, dokumentētiem klienta norādījumiem un apstrādātāja nolūku ierobežojumiem. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.2.28 **Annex A.3.3** - Sasaistīts ar PII drošības politikas sasaisti, PII drošības kontroles pasākumu pamatlīmeņa īpašumtiesībām un informācijas drošības kontroles pasākumu statusu PIMS piemērojamības paziņojumā. Addressed by clauses [4.3.4; 5.1.4; 7.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Sasaistīts ar pārskatatbildības pierādījumiem, politikas apstiprināšanu, apstrādes lomas klasifikāciju, kontroles pasākumu piemērojamību, uzraudzību, auditu un korektīvo darbību ierakstiem. Addressed by clauses [4.3.1; 4.5.1; 4.5.2; 6.1.1; 8.1.3].

13.3.2 **Article 24** - Sasaistīts ar pārziņa pārvaldības pasākumiem, politikas apstiprināšanu, PIMS mērķiem, efektivitātes pārskatīšanu un dokumentētiem pārziņa pārskatatbildības pierādījumiem. Addressed by clauses [4.3.1; 4.3.2; 6.1.1; 8.1.4; 11.1.1].

13.3.3 **Article 26** - Sasaistīts ar kopīgu pārziņu atbildības sadalījuma noteikšanu un dokumentēšanu pirms kopīgas apstrādes uzsākšanas. Addressed by clauses [4.2.2; 5.1.7; 7.1.5].

13.3.4 **Article 28** - Sasaistīts ar apstrādātāju un apakšapstrādātāju pārvaldības ierakstiem, klienta apstrādes norādījumiem un ārēji nodrošinātu procesu kontroli. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.3.5 **Article 30** - Sasaistīts ar apstrādes darbību ierakstiem, lomu klasifikāciju, apstrādes pārskatatbildības ierakstiem un auditējamībai saglabātiem pierādījumiem. Addressed by clauses [4.2.1; 5.1.5; 7.1.2; 8.2.1].

13.3.6 **Article 32** - Sasaistīts ar PII drošības pamatlīmeņa pārvaldību, drošības kontroles pasākumu īpašumtiesībām, drošības ieviešanas statusu un darbības kontroles pasākumu apstiprināšanu. Addressed by clauses [4.3.4; 4.4.4; 5.1.4; 7.1.4].

13.3.7 **Article 35** - Sasaistīts ar DPIA nepieciešamības noteikšanu un privātuma risku izvērtēšanu pirms augsta riska vai būtiski mainītas pārziņa veiktas apstrādes turpināšanas. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12** - Sasaistīts ar privātuma kontroles pasākumu identificēšanu, privātuma principiem, informācijas drošību, privātuma atbilstību, auditu, pierādījumiem un uz risku balstītu privātuma pārvaldību. Addressed by clauses [4.3.3; 4.3.4; 4.4.1; 4.5.1; 8.1.3; 10.1.4].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Sasaistīts ar PIA pārvaldību, DPIA ierosinātāju noteikšanu, PIA sagatavošanu, privātuma riska kritērijiem un dokumentētiem privātuma risku izvērtēšanas pierādījumiem. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4; 9.1.2].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2; Annex A.2** - Sasaistīts ar PII aizsardzības programmas prasībām, PII aizsardzības prasību identificēšanu, uz privātuma risku balstītu kontroles pasākumu atlasi un PII aizsardzības politikas virzienu. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.4].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1** - Sasaistīts ar organizācijas privātuma riska principiem, vadības apņemšanos, privātuma riska integrāciju PIMS pārvaldībā un organizācijas lomas izpratni PII apstrādē. Addressed by clauses [4.1.2; 4.2.1; 4.4.1; 4.4.3; 6.1.1].