					Šeit ievadiet reģistrētās juridiskās personas nosaukumu						
Dokumenta numurs: PII07					Dokumenta nosaukums: **Privātuma risku izvērtēšanas un DPIA 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	Pārklājuma veids	Piezīme
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	PIMS 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 sasaiste ar SoA
ISO/IEC 27701:2025	Clause 6.3	Both	Supporting	Plānotās PIMS izmaiņas un riska atkārtota izvērtēšana
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumentēta informācija par privātuma risku un DPIA
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Darbības plānošana un kontrole
ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Operacionāla privātuma risku izvērtēšana
ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Operacionāla privātuma riska apstrāde
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Privātuma risku uzraudzība un mērīšana
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Vadības pārskatīšana par privātuma risku
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Ar risku saistīta neatbilstība un korektīvā darbība
ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Primary	Privātuma ietekmes novērtējums
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Apstrādes ieraksti, kas atbalsta risku izvērtēšanu
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Apstrādātāja klienta vienošanās un DPIA atbalsts

ISO/IEC 27701:2025	Annex A.2.2.6	Processor	Supporting	Apstrādātāja informācija klienta atbilstības atbalstam
GDPR	Article 5(2)	Controller	Supporting	Pārskatatbildības pierādījumi
GDPR	Article 24	Controller	Supporting	Pārziņa atbildība un pasākumi
GDPR	Article 25	Controller	Supporting	Datu aizsardzība pēc projektēšanas un pēc noklusējuma
GDPR	Article 28	Both	Supporting	Apstrādātāja atbalsts un norādījumi
GDPR	Article 30	Both	Supporting	Apstrādes ieraksti DPIA atbalstam
GDPR	Article 32	Both	Supporting	Drošības risks un drošības pasākumi
GDPR	Article 35	Controller	Primary	Datu aizsardzības ietekmes novērtējums
GDPR	Article 36	Controller	Primary	Iepriekšēja apspriešanās
GDPR	Article 39	Conditional	Supporting	Datu aizsardzības speciālista konsultācijas un uzraudzība, ja piemērojams
ISO/IEC 29100:2020	Clause 4.7; Clause 5.11; Clause 5.12	Both	Supporting	Privātuma kontroles pasākumi, informācijas drošība un privātuma atbilstība
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Primary	PIA piemērošanas joma, ieguvumi, ierosinātāji un sagatavošana
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2	Both	Supporting	PII aizsardzības programma un prasību identificēšana
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause	Both	Supporting	Organizācijas privātuma risku

	6.5; Clause 6.6; Clause 6.7			pārvaldības integrācija

1. Piemērošanas joma

1.1 Šī politika nosaka prasības privātuma risku izvērtēšanai, DPIA sākotnējai izvērtēšanai, pilna DPIA veikšanai, riska apstrādei, atlikušā riska pieņemšanai, apspriešanai, pārskatīšanai un pierādījumu pārvaldībai attiecībā uz PII apstrādi PIMS darbības jomā.

1.2 Šī politika attiecas uz:

1.2.1 jaunām un būtiski mainītām PII apstrādes darbībām;

1.2.2 pārziņa, kopīga pārziņa, apstrādātāja un apakšapstrādātāja apstrādes kontekstiem;

1.2.3 sistēmām, lietojumprogrammām, pakalpojumiem, biznesa procesiem, piegādātājiem, apstrādātājiem, apakšapstrādātājiem, starptautiskām nosūtīšanām un datu koplietošanas kārtībām, kas ietekmē PII apstrādi;

1.2.4 privātuma riska un DPIA pierādījumiem, kas tiek uzturēti REG04, un atbalsta pierādījumiem, kas tiek uzturēti REG02, REG03, REG08, REG09, REG10, REG11 un REG12.

1.3 Šī politika neaizstāj apstrādes uzskaites kontroles pasākumus, privātuma paziņojumu kontroles pasākumus, piekrišanas kontroles pasākumus, datu subjektu tiesību kontroles pasākumus, datu aizsardzības pēc projektēšanas kontroles pasākumus, piegādātāju kontroles pasākumus, starptautisko nosūtīšanu kontroles pasākumus, PII drošības kontroles pasākumus, incidentu kontroles pasākumus, dokumentētas informācijas kontroles pasākumus vai uzraudzības/audita/uzlabošanas kontroles pasākumus. Šīs prasības ir noteiktas saistītajās politikās, kas uzskaitītas 12. sadaļā.

1.4 Šīs politikas izpratnē privātuma risku izvērtēšana nozīmē dokumentētu potenciālu nelabvēlīgu privātuma ietekmju identificēšanu, analīzi, novērtēšanu, apstrādi, pārskatīšanu un uzraudzību, kas izriet no PII apstrādes.

1.5 Šīs politikas izpratnē DPIA nozīmē dokumentētu novērtējumu, ko izmanto pārziņa apstrādei, kura, visticamāk, radīs augstu risku datu subjektiem un kurā tiek izvērtēta apstrādes nepieciešamība, samērīgums, riski, drošības pasākumi, atlikušais risks, apspriešanās vajadzības un apstiprināšanas nosacījumi.

1.6 Šīs politikas izpratnē augsts atlikušais privātuma risks nozīmē privātuma risku, kas pēc ierosinātās vai īstenotās riska apstrādes joprojām pārsniedz apstiprināto pieņemšanas slieksni.

1.7 Šīs politikas izpratnē būtiska izmaiņa nozīmē jebkuru izmaiņu, kas ietekmē PIMS darbības jomu, apstrādes nolūku, tiesisko pamatu, PII kategorijas, datu subjektu kategorijas, apstrādes mērogu, apstrādes tehnoloģiju, uzraudzību vai profilēšanu, automatizētu lēmumu pieņemšanu, neaizsargātus datu subjektus, saņēmējus, apstrādātājus, apakšapstrādātājus, starptautiskas nosūtīšanas, glabāšanu, drošības kontroles pasākumus, riska profilu, klienta norādījumus vai sertifikācijas darbības jomu.

2. Mērķis

2.1 Šīs politikas mērķis ir nodrošināt, ka privātuma riski un DPIA pienākumi tiek identificēti, izvērtēti, apstrādāti, apstiprināti, pārskatīti un apliecināti ar pierādījumiem, pirms PII apstrāde rada nepieņemamu risku datu subjektiem vai PIMS.

2.2 Šī politika ļauj organizācijai pierādīt uz risku balstītu privātuma pārvaldību, pārziņa DPIA pārskatatbildību, apstrādātāja DPIA atbalstu, dokumentētu riska apstrādi, atlikušā riska apstiprināšanu, lēmumu pieņemšanu par iepriekšēju apspriešanos un nepārtrauktu privātuma kontroles pasākumu uzlabošanu.

3. Mērķi

3.1 Šīs politikas mērķi ir:

3.1.1 definēt obligātos privātuma riska sākotnējās izvērtēšanas ierosinātājus;

3.1.2 definēt, kad ir nepieciešams pilns DPIA;

3.1.3 nodrošināt, ka pārziņa DPIA lēmumi ir dokumentēti un pārskatāmi;

3.1.4 nodrošināt, ka apstrādātāja un apakšapstrādātāja DPIA atbalsts ir dokumentēts, ja to prasa klienta norādījums vai vienošanās;

3.1.5 nodrošināt, ka privātuma riski tiek izvērtēti pirms jaunas vai būtiski mainītas PII apstrādes uzsākšanas;

3.1.6 nodrošināt, ka privātuma riska apstrādes pasākumi tiek piešķirti, īstenoti un verificēti;

3.1.7 nodrošināt, ka augsti atlikušie privātuma riski tiek eskalēti un apstiprināti pirms apstrādes sākšanas vai turpināšanas;

3.1.8 nodrošināt, ka lēmumi par iepriekšēju apspriešanos tiek dokumentēti, ja saglabājas augsts atlikušais risks;

3.1.9 nodrošināt, ka privātuma riska un DPIA pierādījumi tiek uzturēti REG04 un sasaistīti ar saistītajiem pierādījumu objektiem;

3.1.10 nepieļaut atsevišķu DPIA, risku vai apspriešanās reģistru izveidi ārpus REG04.

4. Politikas prasības

4.1 Privātuma riska sākotnējā izvērtēšana

4.1.1 [Both] Process Owner / Business Owner ir jāuzsāk privātuma riska sākotnējā izvērtēšana REG04 pirms jaunas vai būtiski mainītas PII apstrādes, kas reģistrēta REG02, sākšanas.

4.1.2 [Both] Privacy Lead / PIMS Manager ir jāuztur privātuma riska sākotnējās izvērtēšanas kritēriji REG04 pirms PIMS sākotnējās darbības un pēc tam reizi gadā.

4.1.3 [Controller] Process Owner / Business Owner ir jāpabeidz DPIA sākotnējā izvērtēšana REG04 pirms pārziņa apstrādes, kas atbilst privātuma riska sākotnējās izvērtēšanas kritērijiem, sākšanas.

4.1.4 [Processor] Vendor / Procurement Owner ir jāreģistrē klienta DPIA atbalsta prasības REG08 pirms apstrādātāja apstrādes sākšanas, ja klienta vienošanās vai dokumentēts norādījums prasa DPIA atbalstu.

4.1.5 [Both] System Owner / Application Owner ir jāsniedz sistēmas projektējuma, piekļuves, drošības, žurnālfiksēšanas un datu plūsmas pierādījumi REG04 pirms privātuma risku izvērtēšanas apstiprināšanas jaunām vai būtiski mainītām sistēmām, kas apstrādā PII.

4.1.6 [Both] Privacy Lead / PIMS Manager ir jāreģistrē sākotnējās izvērtēšanas rezultāts un pilna DPIA lēmuma pamatojums REG04 pirms apstrādes darbības turpināšanas.

4.2 DPIA ierosinātāji un prasības noteikšana

4.2.1 [Controller] Privacy Lead / PIMS Manager ir jāpieprasa pilns DPIA REG04 pirms pārziņa apstrādes, kura, visticamāk, radīs augstu risku, sākšanas.

4.2.2 [Controller] Process Owner / Business Owner ir jānodod Privacy Lead / PIMS Manager izvērtēšanai REG04 apstrāde, kas ietver lielu mērogu, sistemātisku uzraudzību, profilēšanu, automatizētus lēmumus, īpašu kategoriju personas datus, datus par sodāmību vai pārkāpumiem, neaizsargātus datu subjektus, inovatīvu tehnoloģiju vai būtiski mainītu apstrādi, pirms apstrādes sākšanas.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor ir jāreģistrē konsultācija REG04 pirms lēmuma par pilna DPIA prasību apstiprināšanas augsta riska pārziņa apstrādei.

4.2.4 [Both] Process Owner / Business Owner ir jāveic atkārtota privātuma riska sākotnējā izvērtēšana REG04 pirms PII izmantošanas jaunam nolūkam, jauna saņēmēja pievienošanas, jauna apstrādātāja vai apakšapstrādātāja ieviešanas, sistēmas arhitektūras maiņas vai jaunas starptautiskas nosūtīšanas sākšanas.

4.2.5 [Processor] Privacy Lead / PIMS Manager ir jādokumentē REG08, vai ir nepieciešams apstrādātāja DPIA atbalsts, 10 darbdienu laikā pēc klienta DPIA atbalsta pieprasījuma saņemšanas.

4.2.6 [Subprocessor] Vendor / Procurement Owner ir jādokumentē augšupējās DPIA atbalsta prasības REG08 pirms apakšapstrādes sākšanas, ja augšupējā klienta vai apstrādātāja vienošanās prasa šādu atbalstu.

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

9. Izņēmumi

9.1 Privātuma riska un DPIA izņēmumi

9.1.1 [All] Process Owner / Business Owner ir jāpieprasa jebkurš izņēmums no šīs politikas REG12 pirms atkāpes rašanās.

9.1.2 [All] Privacy Lead / PIMS Manager ir jāizvērtē katra pieprasītā izņēmuma privātuma, tiesiskā, sertifikācijas, operacionālā un datu subjektu ietekme REG04 vai REG12 10 darbdienu laikā pēc pieprasījuma.

9.1.3 [All] Data Protection Officer / Privacy Advisor ir jāreģistrē konsultācija REG12 pirms jebkura izņēmuma apstiprināšanas, kas ietekmē augsta riska apstrādi, pilna DPIA pabeigšanu, iepriekšēju apspriešanos, augstu atlikušo privātuma risku vai klienta DPIA atbalstu.

9.1.4 [All] Top Management ir jāapstiprina privātuma riska vai DPIA izņēmumi, kas ietekmē augsta riska apstrādi, sertifikācijas darbības jomu, iepriekšēju apspriešanos vai neatrisinātu augstu atlikušo privātuma risku, REG12 pirms izņēmuma stāšanās spēkā.

9.1.5 [All] Privacy Lead / PIMS Manager ir jānosaka derīguma termiņš, kas nepārsniedz 90 dienas, REG12 katram apstiprinātajam privātuma riska vai DPIA izņēmumam pirms apstiprināšanas.

9.1.6 [All] Process Owner / Business Owner ir jāslēdz vai atkārtoti jāizvērtē katrs privātuma riska vai DPIA izņēmums REG12 piecu darbdienu laikā pēc termiņa beigām.

10. Izpildes nodrošināšana

10.1 Privātuma riska un DPIA izpildes nodrošināšana

10.1.1 [All] Privacy Lead / PIMS Manager ir jāreģistrē trūkstoši, neprecīzi, nepilnīgi, nokavēti vai neapstiprināti REG04 privātuma riska vai DPIA pierādījumi kā neatbilstība REG12 piecu darbdienu laikā pēc identificēšanas.

10.1.2 [Controller] Process Owner / Business Owner ir jāaptur jauna augsta riska pārziņa apstrāde, ja pirms palaišanas trūkst nepieciešamo REG04 DPIA apstiprināšanas pierādījumu.

10.1.3 [Both] System Owner / Application Owner ir jābloķē sistēmu, kas apstrādā PII, nodošana ražošanas vidē, ja pirms nodošanas ražošanas vidē apstiprināšanas trūkst nepieciešamo REG04 riska apstrādes pierādījumu.

10.1.4 [Both] Vendor / Procurement Owner ir jābloķē piegādātāja, apstrādātāja, apakšapstrādātāja vai datu koplietošanas sākotnējā piesaiste, ja pirms vienošanās apstiprināšanas trūkst nepieciešamo REG04 privātuma riska vai DPIA atbalsta pierādījumu.

10.1.5 [All] Top Management ir jāpārskata neatrisinātas būtiskas privātuma riska vai DPIA neatbilstības REG12 vadības pārskatīšanas laikā.

10.1.6 [All] Privacy Lead / PIMS Manager ir jāeskalē atkārtoti nokavēti REG04 sākotnējās izvērtēšanas, DPIA pārskatīšanas vai riska apstrādes termiņi Top Management REG12 piecu darbdienu laikā pēc otrā gadījuma 12 mēnešu periodā.

10.1.7 [All] Internal Audit / Compliance Reviewer ir jāverificē korektīvo darbību efektivitāte privātuma riska un DPIA neatbilstībām REG12 nākamajā plānotajā auditā vai 60 dienu laikā pēc slēgšanas atkarībā no tā, kas iestājas agrāk.

11. Pārskatīšana un uzturēšana

11.1 Politikas pārskatīšana un uzturēšana

11.1.1 [All] Privacy Lead / PIMS Manager ir jāpārskata šī politika REG12 reizi gadā un 30 dienu laikā pēc būtiskām izmaiņām privātuma riska, DPIA, iepriekšējas apspriešanās, apstrādātāja atbalsta vai sertifikācijas prasībās.

11.1.2 [All] Privacy Lead / PIMS Manager ir jāpārskata REG04 sākotnējās izvērtēšanas kritēriji, DPIA ierosinātāju kritēriji, riska vērtēšanas kritēriji un atlikušā riska pieņemšanas kritēriji REG12 reizi gadā.

11.1.3 [All] Data Protection Officer / Privacy Advisor ir jāpārskata privātumam būtiskas izmaiņas šajā politikā REG12 pirms apstiprināšanas.

11.1.4 [All] Top Management ir jāapstiprina būtiskas izmaiņas šajā politikā REG12 pirms publicēšanas.

11.1.5 [All] Privacy Lead / PIMS Manager ir jāatjaunina REG03 un REG04 15 darbdienu laikā pēc apstiprinātām politikas izmaiņām, kas maina kontroles pasākumu piemērojamību, riska kritērijus vai DPIA sākotnējās izvērtēšanas prasības.

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

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 PII06 - Datu subjektu tiesību pārvaldības politika

12.8 PII08 - Datu aizsardzības pēc projektēšanas un pēc noklusējuma politika

12.9 PII09 - PII vākšanas, izmantošanas, izpaušanas un koplietošanas 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 - Starptautiskas PII nosūtīšanas politika

12.14 PII14 - PII drošības un piekļuves kontroles politika

12.15 PII15 - PII incidentu un pārkāpumu pārvaldības politika

12.16 PII17 - PIMS dokumentētas informācijas un pierādījumu pārvaldības politika

12.17 PII18 - PIMS uzraudzības, audita un uzlabošanas politika

13. Atsauces standarti un ietvari

13.1 Šī politika ir sasaistīta ar šādiem standartiem un regulējumu. Sasaistes skaidrojums norāda, kā politika atbalsta minētās prasības, un identificē iekšējos punktus, ar kuriem tās tiek īstenotas vai atbalstītas.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.1** - Sasaistīts ar privātuma risku un iespēju identificēšanu un darbību plānošanu, izmantojot sākotnējās izvērtēšanas kritērijus, riska sliekšņus, eskalāciju un vadības pārskatīšanas ievaddatus. 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** - Sasaistīts ar privātuma riska sākotnējās izvērtēšanas, privātuma risku izvērtēšanas, riska vērtēšanas, atkārtotas izvērtēšanas un DPIA ierosinātāju izvērtēšanas veikšanu pirms jaunas vai būtiski mainītas apstrādes turpināšanas. 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** - Sasaistīts ar privātuma riska apstrādes plānošanu, kontroles pasākumu piemērojamības atjauninājumiem, apstrādes īstenošanu, atlikušā riska pieņemšanu un sasaisti ar 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** - Sasaistīts ar plānotām PIMS un apstrādes izmaiņām, kas ierosina privātuma riska atkārtotu izvērtēšanu un DPIA pārskatīšanu. Addressed by clauses [4.2.4; 4.6.1; 11.1.1].

13.2.5 **Clause 7.5** - Sasaistīts ar kontrolētu dokumentēto informāciju par privātuma riska sākotnējo izvērtēšanu, DPIA pierādījumiem, riska apstrādi, atlikušā riska pieņemšanu, lēmumiem par iepriekšēju apspriešanos, izņēmumiem, neatbilstībām un politikas pārskatīšanas pierādījumiem. 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** - Sasaistīts ar privātuma riska un DPIA kontroles pasākumu darbību pirms nodošanas ražošanas vidē, sākotnējās piesaistes, apstrādes apstiprināšanas, apstrādes slēgšanas un sasaistes ar korektīvajām darbībām. 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** - Sasaistīts ar operacionālu privātuma risku izvērtēšanu jaunām, mainītām, sistēmu, piegādātāju, nosūtīšanas un incidentu izraisītām apstrādes izmaiņām. 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** - Sasaistīts ar operacionālu privātuma riska apstrādi, apstrādes piešķiršanu, apstrādes īstenošanu, nokavētas apstrādes eskalāciju un efektivitātes verifikāciju. 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** - Sasaistīts ar sākotnējās izvērtēšanas pārklājuma, DPIA statusa, atvērto risku, nokavēto apstrādes darbību, piegādātāju darbību, drošības apstrādes darbību, incidentu atkārtotas izvērtēšanas darbību un audita konstatējumu uzraudzību un mērīšanu. 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** - Sasaistīts ar vadības pārskatīšanu par augstiem atlikušajiem privātuma riskiem, nokavētām apstrādes darbībām, pilna DPIA statusu, lēmumiem par iepriekšēju apspriešanos un būtiskiem privātuma riska izņēmumiem. Addressed by clauses [4.6.6; 6.1.1; 6.1.2; 6.1.3; 10.1.5].

13.2.11 **Clause 10.2** - Sasaistīts ar privātuma riska un DPIA neatbilstībām, izņēmumiem, korektīvo darbību atvēršanu, eskalāciju un efektivitātes verifikāciju. 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** - Sasaistīts ar privātuma ietekmes novērtējuma nepieciešamības izvērtēšanu un, ja piemērojams, īstenošanu jaunai vai mainītai pārziņa apstrādei. 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** - Sasaistīts ar apstrādes ierakstiem, kas atbalsta privātuma riska un DPIA izvērtēšanas ievaddatus, tostarp nolūku, kategorijas, sistēmas, saņēmējus, nosūtīšanas un piegādātājus. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.2.14 **Annex A.2.2.2** - Sasaistīts ar apstrādātāja klientu vienošanos un klienta DPIA atbalsta pienākumiem. 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** - Sasaistīts ar apstrādātāja sniegto informāciju, kas nepieciešama klienta atbilstībai, tostarp DPIA atbalstu un klienta atbalsta pierādījumiem. Addressed by clauses [4.2.5; 4.2.6; 4.5.4; 8.1.5].

13.3 GDPR

13.3.1 **Article 5(2)** - Sasaistīts ar pārskatatbildības pierādījumiem DPIA sākotnējai izvērtēšanai, pilna DPIA lēmumiem, riska apstrādei, atlikušā riska pieņemšanai, lēmumiem par iepriekšēju apspriešanos, izņēmumiem, audita konstatējumiem un korektīvajām darbībām. 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** - Sasaistīts ar pārziņa atbildību par atbilstošiem privātuma riska pasākumiem, augsta atlikušā riska pārskatīšanu, vadības apstiprinājumu un politikas uzturēšanu. Addressed by clauses [4.4.5; 4.5.3; 6.1.2; 10.1.5; 11.1.4].

13.3.3 **Article 25** - Sasaistīts ar datu aizsardzības pēc projektēšanas un datu aizsardzības pēc noklusējuma pierādījumiem, kas tiek izmantoti risku izvērtēšanā un pirms nodošanas ražošanas vidē apstiprināšanas. Addressed by clauses [4.1.5; 4.3.4; 7.1.5].

13.3.4 **Article 28** - Sasaistīts ar apstrādātāja un apakšapstrādātāja DPIA atbalstu, klienta norādījumu apstrādi un piegādātāju riska apstrādes pierādījumiem. 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** - Sasaistīts ar apstrādes ierakstiem, kas atbalsta privātuma risku izvērtēšanas un DPIA ievaddatus. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.3.6 **Article 32** - Sasaistīts ar PII drošības riska ievaddatiem, drošības pasākumu izvēli, drošības riska apstrādi un drošības kontroles pasākumu statusa atjauninājumiem. Addressed by clauses [4.1.5; 4.3.3; 4.4.2; 8.1.6].

13.3.7 **Article 35** - Sasaistīts ar DPIA sākotnējo izvērtēšanu, pilna DPIA prasības noteikšanu, DPIA saturu, DPO konsultāciju, pārskatīšanu un augsta riska apstrādes bloķēšanu bez nepieciešamā DPIA apstiprinājuma. 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** - Sasaistīts ar lēmumu pieņemšanu par iepriekšēju apspriešanos, DPO konsultāciju, Top Management apstiprinājumu un turpināšanas, apturēšanas, pārprojektēšanas vai apspriešanās darbībām, ja saglabājas augsts atlikušais risks. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 6.1.2].

13.3.9 **Article 39** - Sasaistīts ar Data Protection Officer / Privacy Advisor konsultācijām un uzraudzību, ja piemērojams, attiecībā uz DPIA lēmumiem, augsta riska apstrādi, iepriekšēju apspriešanos un politikas izmaiņām. 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** - Sasaistīts ar privātuma kontroles pasākumu identificēšanu, drošības pasākumiem, privātuma atbilstību, privātuma riska pierādījumiem, uzraudzību un pārskatīšanu. 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** - Sasaistīts ar PIA procesa piemērošanas jomu, ieguvumiem, ierosinātāju noteikšanu, sagatavošanu, izvērtēšanas ievaddatiem, iesaistīto pušu pierādījumiem un DPIA ziņojuma struktūru, kas tiek uzturēta 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** - Sasaistīts ar PII aizsardzības programmas prasībām, PII aizsardzības prasību identificēšanu, uz risku balstītu kontroles pasākumu izvēli un privātuma riska apstrādes sasaisti. 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** - Sasaistīts ar organizācijas privātuma riska principiem, vadību, integrāciju, risku izvērtēšanu, riska apstrādi, uzraudzību un pārskatīšanu, kā arī reģistrēšanu un ziņošanu. 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].