					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: PII08					Dokumenta nosaukums: **Datu aizsardzības pēc projektēšanas un pēc noklusējuma 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 6.1.2; Clause 6.1.3	Both	Supporting	Privātuma risku izvērtēšanas un privātuma riska apstrādes sasaiste
ISO/IEC 27701:2025	Clause 6.3; Clause 8.1	Both	Primary	Plānotās izmaiņas un darbības kontrole
ISO/IEC 27701:2025	Clause 7.5	Both	Supporting	Dokumentēti integrētās datu aizsardzības pierādījumi
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Uzraudzība un korektīvā darbība
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.6; Annex A.1.2.9	Controller	Supporting	Nolūki, PIA ierosinātājs un ieraksti
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3	Controller	Primary	Vākšanas un apstrādes ierobežošana
ISO/IEC 27701:2025	Annex A.1.4.4; Annex A.1.4.5	Controller	Supporting	Precizitātes un minimizēšanas mērķi
ISO/IEC 27701:2025	Annex A.1.4.6; Annex A.1.4.7	Controller	Supporting	Deidentifikācijas, dzēšanas projektēšanas un pagaidu datņu prasības
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Klienta vienošanās, atbalsts un apstrādātāja ieraksti
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Supporting	Apstrādātāja projektēšanas iespējas
ISO/IEC 27701:2025	Annex A.3.27; Annex A.3.29	Both	Supporting	Izstrādes dzīves cikls un inženierijas principi
GDPR	Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Supporting	Nolūka ierobežošana,

				minimizēšana un pārskatatbildība
GDPR	Article 24	Controller	Supporting	Pārziņa pasākumi
GDPR	Article 25	Controller	Primary	Datu aizsardzība pēc projektēšanas un pēc noklusējuma
GDPR	Article 28	Both	Supporting	Apstrādātāja norādījumi un palīdzība
GDPR	Article 30	Both	Supporting	Apstrādes ieraksti
GDPR	Article 35	Controller	Supporting	DPIA ierosinātāja sasaiste
ISO/IEC 29100:2020	Clause 4.7	Both	Supporting	Privātuma kontroles pasākumi pēc projektēšanas
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Nolūka, vākšanas, minimizēšanas un izmantošanas ierobežošana
ISO/IEC 29100:2020	Clause 5.7; Clause 5.10; Clause 5.12	Both	Supporting	Precizitāte, pārskatatbildība un atbilstība
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8	Both	Primary	PII aizsardzības principi un kontroles pasākumi

1. Piemērošanas joma

1.1 Šī politika nosaka prasības datu aizsardzības pēc projektēšanas un datu aizsardzības pēc noklusējuma iestrādāšanai jaunās un mainītās PII apstrādes darbībās, projektos, produktos, pakalpojumos, sistēmās, lietojumprogrammās, integrācijās, iepirkuma darbībās un biznesa procesu izmaiņās PIMS darbības jomas ietvaros.

1.2 Šī politika attiecas uz pārziņa, kopīga pārziņa, apstrādātāja un apakšapstrādātāja kontekstu. Apstrādātāja un apakšapstrādātāja pienākumi ir piemērojami, ja organizācija projektē, konfigurē, maina vai veic apstrādi klienta, pārziņa vai augšupējā apstrādātāja vārdā saskaņā ar dokumentētiem norādījumiem.

1.3 Šī politika aptver:

1.3.1 privātuma prasības projekta uzsākšanas posmā;

1.3.2 nolūka, datu minimizēšanas un noklusējuma iestatījumu projektēšanas kontroles pasākumus;

1.3.3 integrētās datu aizsardzības pārskatīšanu pirms nodošanas ražošanas vidē;

1.3.4 izmaiņu ierosinātu integrētās datu aizsardzības pārskatīšanu;

1.3.5 iepirkuma pārbaudes attiecībā uz datu aizsardzību pēc projektēšanas;

1.3.6 sasaisti ar privātuma risku, DPIA sākotnējo izvērtēšanu un korektīvās darbības pierādījumiem.

1.4 Šī politika neaizstāj:

1.4.1 PII03 attiecībā uz apstrādes uzskaiti, nolūkiem, tiesisko pamatu un ROPA ierakstiem;

1.4.2 PII04 attiecībā uz privātuma paziņojumu saturu un publicēšanu;

1.4.3 PII05 attiecībā uz piekrišanas un preferenču kontroles pasākumiem;

1.4.4 PII06 attiecībā uz datu subjekta tiesību īstenošanas pārvaldību;

1.4.5 PII07 attiecībā uz privātuma risku izvērtēšanas un DPIA metodoloģiju;

1.4.6 PII09 attiecībā uz vākšanas, izmantošanas, izpaušanas un koplietošanas kontroles pasākumiem;

1.4.7 PII10 attiecībā uz glabāšanas, dzēšanas un likvidēšanas izpildi;

1.4.8 PII11 attiecībā uz precizitātes un kvalitātes darbību;

1.4.9 PII12 attiecībā uz apstrādātāju, apakšapstrādātāju un trešo pušu dzīves cikla pārvaldību;

1.4.10 PII13 attiecībā uz starptautiskās PII nosūtīšanas mehānismiem;

1.4.11 PII14 attiecībā uz PII drošību un piekļuves kontroles darbību;

1.4.12 PII18 attiecībā uz PIMS mēroga uzraudzību, auditu, korektīvo darbību un uzlabojumu pārvaldību.

2. Mērķis

2.1 Šīs politikas mērķis ir nodrošināt, ka privātuma prasības tiek identificētas, ieviestas un pierādītas pirms PII apstrādes sākšanas vai būtiskas maiņas un ka sistēmas un procesi pēc noklusējuma tiek konfigurēti tā, lai ierobežotu PII vākšanu, izmantošanu, ekspozīciju, glabāšanas atkarību, izpaušanas atkarību un identificējamību līdz tam, kas nepieciešams dokumentētajam nolūkam.

3. Mērķi

3.1 Šīs politikas mērķi ir:

3.1.1 iestrādāt privātuma prasības projektu uzsākšanas, projektēšanas, iepirkuma, izmaiņu un nodošanas ražošanas vidē lēmumos;

3.1.2 nodrošināt, ka PII apstrādes risinājumi ir sasaistīti ar dokumentētiem nolūkiem un REG02 apstrādes ierakstiem;

3.1.3 ieviest datu minimizēšanu un datu aizsardzību veicinošus noklusējuma iestatījumus pirms apstrādes sākšanas;

3.1.4 nodrošināt, ka tiek ierosināta privātuma riska un DPIA sākotnējā izvērtēšana, nedublējot PII07 metodoloģiju;

3.1.5 nodrošināt, ka iepirkuma un apstrādātāja projektēšanas prasības tiek reģistrētas, nedublējot PII12 dzīves cikla pārvaldību;

3.1.6 nodrošināt, ka neatrisinātās projektēšanas problēmas tiek eskalētas, izmantojot REG12;

3.1.7 uzturēt auditam gatavus projektēšanas pierādījumus REG02, REG04, REG08 un REG12.

4. Politikas noteikumi

4.1 Projekta uzsākšana un privātuma prasības

4.1.1 [Both] Process Owner / Business Owner ir jāreģistrē integrētās datu aizsardzības ieraksts REG04 pirms jebkura projekta, produkta, pakalpojuma, sistēmas, lietojumprogrammas, integrācijas vai biznesa procesa izmaiņas uzsākšanas, ja tā ietver PII.

4.1.2 [Both] Process Owner / Business Owner ir jāsasaista katrs integrētās datu aizsardzības ieraksts REG04 ar esošu vai projekta stadijā esošu REG02 apstrādes darbību pirms funkcionālo prasību apstiprināšanas.

4.1.3 [Controller] Privacy Lead / PIMS Manager ir jāreģistrē pārziņa datu aizsardzības pēc projektēšanas prasības REG04 pirms pārziņa funkcionālā risinājuma apstiprināšanas.

4.1.4 [Processor] Vendor / Procurement Owner ir jāreģistrē klienta privātuma projektēšanas norādījumi un līgumiskie projektēšanas ierobežojumi REG08 pirms apstrādātāja pakalpojuma projektēšanas vai būtiskas pakalpojuma izmaiņas apstiprināšanas.

4.1.5 [Conditional] Data Protection Officer / Privacy Advisor ir jāreģistrē konsultācija REG04 pirms augsta riska, jauna, sensitīva, automatizēta, liela mēroga vai būtiski mainīta PII risinājuma apstiprināšanas.

4.1.6 [Both] Information Security Lead ir jāreģistrē PII drošības kontroles pasākumu atkarības, kas atbalsta privātuma risinājumu, REG04 pirms arhitektūras apstiprināšanas.

4.2 Datu minimizēšana un datu aizsardzības pēc noklusējuma projektēšana

4.2.1 [Controller] Process Owner / Business Owner ir jādokumentē minimālās PII kategorijas, datu subjektu kategorijas, avoti un nolūki REG02 un REG04 pirms vākšanas vai importēšanas risinājuma apstiprināšanas.

4.2.2 [Both] System Owner / Application Owner ir jākonfigurē apstrādes noklusējuma iestatījumi atbilstoši minimālajai PII vākšanai un apstrādei, kas nepieciešama dokumentētajam nolūkam, un pirms nodošanas ražošanas vidē jāreģistrē pierādījumi REG04.

4.2.3 [Controller] Process Owner / Business Owner ir jādokumentē neobligātie PII lauki, neobligātās apstrādes izvēles un pēc noklusējuma izslēgti iestatījumi REG02 un REG04 pirms lietotāja saskarnes, veidlapas vai darbplūsmas apstiprināšanas.

4.2.4 [Both] System Owner / Application Owner ir jādokumentē privātuma ekspozīcijas noklusējuma iestatījumi skatiem, pārskatiem, eksportiem, saskarnēm un automatizētām darbplūsmām REG04 pirms nodošanas ražošanas vidē.

4.2.5 [Both] Process Owner / Business Owner ir jādokumentē deidentifikācijas, pseidonimizācijas, agregēšanas vai neidentificējamas apstrādes iespējamība REG04 pirms identificējamas PII apstiprināšanas testēšanai, analītikai, ziņošanai vai sekundārai operatīvai izmantošanai.

4.2.6 [Both] System Owner / Application Owner ir jādokumentē pagaidu PII artefaktu apstrāde, tostarp pagaidu datnes, kešatmiņas, žurnāli vai sagatavošanas ieraksti, REG04 pirms nodošanas ražošanas vidē.

4.2.7 [Both] Process Owner / Business Owner ir jānovirza projektēšanas prasības, par kurām atbild PII10, PII11, PII13 vai PII14, uz attiecīgās politikas pierādījumu ceļu REG04 piecu darbdienu laikā pēc atkarības identificēšanas.

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

9. Izņēmumi

9.1 Integrētās datu aizsardzības izņēmumi

9.1.1 [Both] Process Owner / Business Owner ir jāpieprasa integrētās datu aizsardzības izņēmums REG12 pirms tāda risinājuma vai izmaiņas apstiprināšanas, kas nevar izpildīt piemērojamu integrētās datu aizsardzības prasību.

9.1.2 [Both] Privacy Lead / PIMS Manager ir jāizvērtē katra integrētās datu aizsardzības izņēmuma ietekme, kompensējošie kontroles pasākumi un termiņš REG12 piecu darbdienu laikā pēc pieprasījuma.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor ir jāreģistrē konsultācija REG12 pirms integrētās datu aizsardzības izņēmuma apstiprināšanas, ja tas ietver augsta riska, sensitīvu, automatizētu, liela mēroga, apstrīdētu vai juridiski būtisku apstrādi.

9.1.4 [All] Top Management ir jāapstiprina integrētās datu aizsardzības izņēmums, kas ietekmē augstas ietekmes apstrādi, sertifikācijas tvērumu, neatrisinātu būtisku risku vai juridisku pienākumu, REG12 pirms izņēmuma stāšanās spēkā.

9.1.5 [Both] Privacy Lead / PIMS Manager ir jānosaka derīguma termiņš, kas nepārsniedz 90 dienas, REG12 katram apstiprinātam integrētās datu aizsardzības izņēmumam pirms apstiprināšanas.

9.1.6 [Both] Privacy Lead / PIMS Manager ir jāslēdz vai atkārtoti jāizvērtē katrs integrētās datu aizsardzības izņēmums REG12 piecu darbdienu laikā pēc termiņa beigām.

10. Piemērošana

10.1 Piemērošana un neatbilstību apstrāde

10.1.1 [Both] Privacy Lead / PIMS Manager ir jāreģistrē trūkstoša integrētās datu aizsardzības pārskatīšana, trūkstoši minimizēšanas pierādījumi, neatrisināta noklusējuma iestatījumu kļūme vai nesankcionēta nodošana ražošanas vidē kā neatbilstība REG12 piecu darbdienu laikā pēc identificēšanas.

10.1.2 [Both] System Owner / Application Owner ir jānovērš PII apstrādes sistēmas nodošana ražošanas vidē, ja REG04 integrētās datu aizsardzības pārskatīšana nav pabeigta, un jāreģistrē lēmums REG12 pirms nodošanas ražošanas vidē.

10.1.3 [Both] Vendor / Procurement Owner ir jānovērš piegādātāja sākotnējā piesaiste vai līguma parakstīšana, ja nav nepieciešamo REG08 integrētās datu aizsardzības pierādījumu, un jāreģistrē lēmums REG12 pirms sākotnējās piesaistes vai parakstīšanas.

10.1.4 [Both] Process Owner / Business Owner ir jāaptur jauna vai mainīta PII apstrādes risinājuma izmantošana, līdz ir pabeigta REG04 pārskatīšana, REG02 atjauninājumi un nepieciešamie REG12 izņēmumi.

10.1.5 [All] Top Management ir jāpieprasa korektīvā darbība REG12 10 darbdienu laikā atkārtotas, ilgstošas vai augstas ietekmes integrētās datu aizsardzības kļūmes gadījumā.

10.1.6 [All] Internal Audit / Compliance Reviewer ir jāpārbauda korektīvās darbības efektivitāte attiecībā uz integrētās datu aizsardzības neatbilstībām REG12 nākamajā plānotajā PIMS auditā vai 60 dienu laikā pēc slēgšanas atkarībā no tā, kas iestājas agrāk.

11. Pārskatīšana un uzturēšana

11.1 Politikas un projektēšanas kontroles pasākumu pārskatīšana

11.1.1 [All] Privacy Lead / PIMS Manager ir jāpārskata šī politika REG12 reizi gadā un 30 dienu laikā pēc būtiskām tiesiskām, apstrādes, tehnoloģiju, sertifikācijas tvēruma vai PIMS kontroles pasākumu izmaiņām.

11.1.2 [Both] Process Owner / Business Owner ir jāpārskata aktīvās REG02 apstrādes darbības attiecībā uz integrētās datu aizsardzības atkarību izmaiņām reizi gadā un 30 dienu laikā pēc būtiskām apstrādes izmaiņām.

11.1.3 [Both] System Owner / Application Owner ir jāpārskata datu aizsardzības pēc noklusējuma konfigurācijas pierādījumi REG04 reizi gadā un 30 dienu laikā pēc būtiskām sistēmas izmaiņām.

11.1.4 [Both] Vendor / Procurement Owner ir jāpārskata piegādātāju, apstrādātāju, apakšapstrādātāju un trešo pušu integrētās datu aizsardzības pienākumi REG08 pirms atjaunošanas un 30 dienu laikā pēc būtiskām attiecību izmaiņām.

11.1.5 [Conditional] Data Protection Officer / Privacy Advisor ir jāpārskata būtisku politikas izmaiņu ietekme uz privātumu REG12 pirms apstiprināšanas.

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

12. Saistītās politikas

12.1 PII01 - Privātuma informācijas pārvaldības sistēmas politika

12.2 PII02 - Privātuma lomu, pienākumu un pārskatatbildības politika

12.3 PII03 - PII apstrādes uzskaites un tiesiskā pamata politika

12.4 PII04 - Privātuma paziņojumu un pārredzamības politika

12.5 PII05 - Piekrišanas un preferenču pārvaldības politika

12.6 PII06 - Datu subjektu tiesību pārvaldības politika

12.7 PII07 - Privātuma risku izvērtēšanas un DPIA politika

12.8 PII09 - PII vākšanas, izmantošanas, izpaušanas un koplietošanas politika

12.9 PII10 - PII glabāšanas, dzēšanas un likvidēšanas politika

12.10 PII11 - PII precizitātes un kvalitātes politika

12.11 PII12 - Apstrādātāju, apakšapstrādātāju un trešo pušu privātuma pārvaldības politika

12.12 PII13 - Starptautiskās PII nosūtīšanas politika

12.13 PII14 - PII drošības un piekļuves kontroles politika

12.14 PII17 - PIMS dokumentētās informācijas un pierādījumu pārvaldības politika

12.15 PII18 - PIMS uzraudzības, audita un uzlabošanas politika

13. Atsauces standarti un ietvari

13.1 Šī politika ir kartēta pret šādiem standartiem un regulējumu. Kartējums izskaidro, kā politika atbalsta citētās prasības, un identificē iekšējos punktus, kas tās ievieš vai atbalsta.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.2; Clause 6.1.3** - Kartēts uz privātuma riska sākotnējo izvērtēšanu, riska apstrādes darbību sasaisti, projektēšanas atkarību analīzi, eskalāciju un korektīvo darbību, nedublējot pilnu privātuma risku un DPIA metodoloģiju. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.5; 5.1.3; 7.1.7].

13.2.2 **Clause 6.3; Clause 8.1** - Kartēts uz plānotām privātuma izmaiņām, projekta uzsākšanu, operatīvu integrētās datu aizsardzības pārskatīšanu, nodošanas ražošanas vidē kontroli un būtisku izmaiņu pārskatīšanu. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.3; 4.3.5; 4.5.1; 4.5.3; 4.5.4; 4.5.6; 7.1.2; 7.1.5; 10.1.2].

13.2.3 **Clause 7.5** - Kartēts uz dokumentētiem integrētās datu aizsardzības pierādījumiem, kas tiek glabāti REG02, REG04, REG08 un REG12. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.2.3; 4.4.1; 4.4.2; 4.4.3; 5.1.2; 5.1.5; 5.1.6; 5.1.7; 7.1.1; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1; Clause 10.2** - Kartēts uz integrētās datu aizsardzības metrikām, pierādījumu izlases pārbaudēm, neatbilstību reģistrēšanu, korektīvo darbību un efektivitātes pārbaudi. Addressed by clauses [4.3.6; 4.4.5; 4.5.5; 6.1.1; 6.1.2; 6.1.4; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 10.1.1; 10.1.5; 10.1.6].

13.2.5 **Annex A.1.2.2; Annex A.1.2.6; Annex A.1.2.9** - Kartēts uz apstrādes nolūku dokumentēšanu, apstrādes ierakstiem, integrētās datu aizsardzības sasaisti un privātuma riska vai DPIA sākotnējās izvērtēšanas ierosinātājiem pārziņa apstrādei. Addressed by clauses [4.1.2; 4.2.1; 4.3.1; 4.4.2; 4.5.2; 5.1.5; 7.1.3; 11.1.2].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3** - Kartēts uz PII vākšanas un apstrādes ierobežošanu, izmantojot uz nolūku balstītas minimālās datu prasības, pēc noklusējuma izslēgtu neobligāto apstrādi un minimālos noklusējuma apstrādes iestatījumus. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.5.4; 7.1.5; 11.1.3].

13.2.7 **Annex A.1.4.4; Annex A.1.4.5** - Kartēts uz precizitātes atkarību novirzīšanu, minimizēšanas mērķiem, deidentifikācijas iespējamību un projektēšanas pierādījumiem identificējamas PII minimizēšanai. Addressed by clauses [4.2.5; 4.2.7; 4.3.2; 4.5.2; 7.1.3; 11.1.2].

13.2.8 **Annex A.1.4.6; Annex A.1.4.7** - Kartēts uz deidentifikācijas, dzēšanas atkarības, pagaidu PII artefaktu identificēšanu projektēšanas posmā un novirzīšanu uz dzīves cikla kontroles pasākumiem, nedublējot glabāšanas vai likvidēšanas izpildi. Addressed by clauses [4.2.5; 4.2.6; 4.2.7; 4.3.3; 4.5.4; 7.1.5; 11.1.3].

13.2.9 **Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7** - Kartēts uz apstrādātāja klienta norādījumiem, klienta atbalsta informāciju, apstrādātāja projektēšanas ierakstiem un klienta autorizētām pakalpojuma projektēšanas izmaiņām. Addressed by clauses [4.1.4; 4.4.1; 4.4.3; 4.4.6; 5.1.7; 7.1.4; 11.1.4].

13.2.10 **Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4** - Kartēts uz apstrādātāja projektēšanas iespējām attiecībā uz pagaidu datnēm, atgriešanas vai likvidēšanas atkarību un pārsūtīšanas kontroles atkarību, kas reģistrētas kā projektēšanas pierādījumi, nedublējot operatīvās dzēšanas vai drošības kontroles pasākumu procedūras. Addressed by clauses [4.2.6; 4.2.7; 4.4.3; 4.4.4; 4.4.6; 7.1.4; 7.1.6; 11.1.4].

13.2.11 **Annex A.3.27; Annex A.3.29** - Kartēts uz privātuma prasībām izstrādes dzīves ciklā, inženierijas principiem, PII aizsardzības kontrolpunktiem un datu aizsardzības pēc noklusējuma konfigurācijas pierādījumiem. Addressed by clauses [4.1.6; 4.3.3; 4.3.4; 4.4.4; 4.5.1; 4.5.4; 5.1.4; 5.1.6; 7.1.5; 7.1.6; 10.1.2; 11.1.3].

13.3 GDPR

13.3.1 **Article 5(1)(b); Article 5(1)(c); Article 5(2)** - Kartēts uz nolūka ierobežošanu, minimālu PII projektēšanu, apstrādes ierakstu sasaisti, noklusējuma minimizēšanu, pierādījumiem un pārskatatbildību. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.4.2; 4.5.2; 5.1.5; 8.1.1; 10.1.1].

13.3.2 **Article 24** - Kartēts uz pārziņa pasākumiem, pārvaldības pārskatīšanu, izņēmumu apstiprināšanu, korektīvo darbību un politikas uzturēšanu datu aizsardzības pēc projektēšanas ieviešanai. Addressed by clauses [4.1.3; 4.5.6; 5.1.1; 6.1.2; 9.1.2; 9.1.4; 10.1.5; 11.1.6].

13.3.3 **Article 25** - Kartēts uz projekta uzsākšanu, projektēšanas posma privātuma prasībām, datu aizsardzības pēc noklusējuma iestatījumiem, minimizēšanu, iepirkuma projektēšanas pārbaudēm, nodošanas ražošanas vidē pārskatīšanu un izmaiņu ierosinātu pārskatīšanu.

Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.5; 4.4.1; 4.5.1; 4.5.3; 4.5.4; 10.1.2].

13.3.4 **Article 28** - Kartēts uz apstrādātāja norādījumiem, apstrādātāja projektēšanas atbalstu, piegādātāja integrētās datu aizsardzības pierādījumiem un klienta autorizētām projektēšanas izmaiņām. Addressed by clauses [4.1.4; 4.4.1; 4.4.3; 4.4.5; 4.4.6; 5.1.7; 7.1.4; 10.1.3; 11.1.4].

13.3.5 **Article 30** - Kartēts uz apstrādes ierakstu sasaisti, REG02 atjauninājumiem, apstrādes darbību projektēšanas atkarībām un apstrādes ierakstu pierādījumiem. Addressed by clauses [4.1.2; 4.2.1; 4.4.2; 4.5.2; 5.1.5; 7.1.3; 11.1.2].

13.3.6 **Article 35** - Kartēts uz projektēšanas posma privātuma riska un DPIA sākotnējās izvērtēšanas ierosinātājiem, augsta riska konsultācijām un pārbaudēm pēc ieviešanas, nedublējot DPIA metodoloģiju. Addressed by clauses [4.1.5; 4.3.1; 4.3.6; 5.1.3; 6.1.3; 9.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7** - Kartēts uz privātuma kontroles pasākumu identificēšanu projektēšanas posmā, privātuma riska sasaisti un projektēšanas pierādījumiem kontroles pasākumu ieviešanai. Addressed by clauses [4.1.1; 4.1.3; 4.1.5; 4.3.1; 4.3.2; 4.3.3; 4.3.5; 4.5.1].

13.4.2 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Kartēts uz nolūka noteikšanu, vākšanas ierobežošanu, datu minimizēšanu, ierobežotu izmantošanu un noklusējuma apstrādes iestatījumiem. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.4.2; 4.5.2].

13.4.3 **Clause 5.7; Clause 5.10; Clause 5.12** - Kartēts uz precizitātes atkarību novirzīšanu, pārskatatbildības pierādījumiem, integrētās datu aizsardzības uzraudzību, auditu un korektīvo darbību. Addressed by clauses [4.2.7; 4.3.6; 4.5.5; 6.1.1; 6.1.4; 8.1.1; 8.1.2; 10.1.1; 10.1.6].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8** - Kartēts uz nolūka leģitimitāti, vākšanas ierobežošanu, datu minimizēšanu, izmantošanas un izpaušanas ierobežošanu, glabāšanas atkarību, pagaidu datņu apstrādi un precizitātes atkarību projektēšanas kontroles pasākumiem. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.4.2; 4.5.2; 4.5.4; 7.1.3; 7.1.5].