					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: PII15					Dokumenta nosaukums: **Personas datu incidentu un personas datu aizsardzības pārkāpumu 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**

Saskaņots ar piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts/kontrole/pants	Piemērojamība	Pārklājuma veids	Piezīme
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	PIMS komunikācija un dokumentēti pārkāpumu pierādījumi
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Darbības kontroles pasākumi, privātuma risku izvērtēšana un saikne ar riska apstrādi
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Uzraudzība, izvērtēšana, neatbilstības, korektīvās darbības un uzlabošana
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Incidentu pārvaldības plānošana un sagatavošanās PII apstrādei
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Reaģēšana uz informācijas drošības incidentiem, kuros iesaistīta PII
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Juridiskās, normatīvās, regulatīvās un līgumiskās prasības un ierakstu aizsardzība
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Apstrādātāja klienta līgums un atbalsts klienta pienākumu izpildei
GDPR	Article 5(2); Article 24	Controller	Supporting	Pārskatatbildība un pārziņa atbildība
GDPR	Article 26	Joint Controller	Supporting	Kopīgo pārziņu atbildības koordinācija pārkāpuma gadījumā

GDPR	Article 28	Both	Supporting	Apstrādātāja palīdzība un apstrādātāja līgumsaistības
GDPR	Article 32	Both	Supporting	Apstrādes drošība un pārkāpumu atklāšanas spēja
GDPR	Article 33	Both	Primary	Paziņošana par personas datu aizsardzības pārkāpumu un pārkāpuma dokumentēšana
GDPR	Article 34	Controller	Primary	Personas datu aizsardzības pārkāpumu paziņošana skartajiem datu subjektiem
GDPR	Article 39	Conditional	Supporting	Datu aizsardzības speciālista konsultācijas, uzraudzība, sadarbība un kontaktpunkta atbalsts
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Informācijas drošības un privātuma atbilstības principi
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Atbildība par reaģēšanu uz PII incidentiem un notikumu ziņošana
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Incidentu plānošana, izvērtēšana, reaģēšana, gūtās mācības un pierādījumu vākšana
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Incidentu pārvaldības procesa dzīves cikls
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Incidentu politika, plāns, informētība,

				testēšana un gūtās mācības
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Atklāšanas, paziņošanas, triāžas, analīzes, reaģēšanas un ziņošanas darbības
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Mākoņpakalpojumu apstrādātāja paziņošanas un pārkāpumu ierakstu prasības
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Ziņošana par būtiskiem incidentiem, ja piemērojams
DORA Regulation (EU) 2022/2554	Article 17; Article 18; Article 19	Conditional	Supporting	IKT incidentu pārvaldība, klasifikācija un ziņošana, ja piemērojams

1. Piemērošanas joma

1.1 Šī politika nosaka prasības personas datu incidentu un personas datu aizsardzības pārkāpumu identificēšanai, ziņošanai, triāžai, izvērtēšanai, ierobežošanai, paziņošanai, dokumentēšanai, slēgšanai un no tiem izrietošai uzlabošanai PIMS darbības jomā.

1.2 Šī politika attiecas uz:

1.2.1 organizāciju, kas darbojas kā PII pārzinis;

1.2.2 organizāciju, kas darbojas kā kopīgs pārzinis, ja nepieciešama atbildības koordinācija pārkāpuma gadījumā;

1.2.3 organizāciju, kas darbojas kā PII apstrādātājs;

1.2.4 organizāciju, kas darbojas kā apakšapstrādātājs;

1.2.5 sistēmām, lietojumprogrammām, pakalpojumiem, procesiem, piegādātājiem, apstrādātājiem, apakšapstrādātājiem un trešajām pusēm, kas apstrādā, glabā, pārsūta, atbalsta, piekļūst vai citādi ietekmē PII PIMS darbības jomā.

1.3 Šajā politikā REG10 - PII incidentu un pārkāpumu reģistrs tiek izmantots kā galvenais pierādījumu objekts personas datu incidentu un personas datu aizsardzības pārkāpumu pārvaldībai.

1.4 Šajā politikā atbalsta pierādījumu objekti tiek izmantoti šādi:

1.4.1 REG01 PIMS darbības jomai un piemērojamam ieinteresēto pušu, juridiskajam, līgumiskajam, nozares un klientu ziņošanas kontekstam.

1.4.2 REG02 skartajām apstrādes darbībām, PII kategorijām, datu subjektu kategorijām, nolūkiem un sistēmām.

1.4.3 REG03 Piemērojamības paziņojumam un kontroles pasākumu piemērojamības atjauninājumiem.

1.4.4 REG04 privātuma riska, DPIA un atlikušā riska saiknei.

1.4.5 REG08 apstrādātāju, apakšapstrādātāju, klientu, piegādātāju un trešo pušu incidentu saskarnes pierādījumiem.

1.4.6 REG09 starptautiskas datu nosūtīšanas saiknei, ja incidents ietekmē pārrobežu apstrādi.

1.4.7 REG11 apmācību, informētības un incidentu reaģēšanas kompetences pierādījumiem.

1.4.8 REG12 audita, neatbilstību, korektīvo darbību un uzlabošanas pierādījumiem.

1.5 Šī politika balstās uz saistītajām PIMS politikām specializētajiem kontroles pasākumiem:

1.5.1 PII03 regulē apstrādes uzskaiti un tiesiskā pamata ierakstus.

1.5.2 PII04 regulē privātuma paziņojuma un pārredzamības kontroles pasākumus ārpus ar pārkāpumu saistītas komunikācijas.

1.5.3 PII06 regulē datu subjektu tiesību īstenošanas pieprasījumus, kas rodas pirms incidenta, tā laikā vai pēc tā.

1.5.4 PII07 regulē privātuma risku izvērtēšanas un DPIA metodoloģiju.

1.5.5 PII08 regulē datu aizsardzības pēc projektēšanas un pēc noklusējuma kontroles pasākumus.

1.5.6 PII10 regulē glabāšanas, dzēšanas un likvidēšanas kontroles pasākumus.

1.5.7 PII12 regulē apstrādātāju, apakšapstrādātāju, piegādātāju un trešo pušu privātuma attiecību kontroles pasākumus.

1.5.8 PII13 regulē starptautiskas PII nosūtīšanas mehānismus un nosūtīšanas riska ierakstus.

1.5.9 PII14 regulē preventīvus un atklājošus PII drošības un piekļuves kontroles pasākumus.

1.5.10 PII16 regulē privātuma apmācību, informētību un kompetenci.

1.5.11 PII17 regulē dokumentētas informācijas un pierādījumu pārvaldību.

1.5.12 PII18 regulē uzraudzību, iekšējo auditu, vadības pārskatīšanu, neatbilstības, korektīvās darbības un nepārtrauktu uzlabošanu.

1.6 Šīs politikas vajadzībām:

1.6.1 "PII incident" nozīmē aizdomīgu vai apstiprinātu notikumu, kas ir ietekmējis, varētu būt ietekmējis vai pamatoti varētu ietekmēt PII konfidencialitāti, integritāti, pieejamību, likumīgu apstrādi vai autorizētu rīcību ar PII.

1.6.2 "PII breach" nozīmē apstiprinātu personas datu incidentu, kas ietver neatļautu, nelikumīgu, nejaušu vai neparedzētu PII iznīcināšanu, nozaudēšanu, izmainīšanu, izpaušanu, piekļuvi, nepieejamību vai kompromitēšanu.

1.6.3 "Breach assessment" nozīmē dokumentētu izvērtējumu par to, vai personas datu incidents ir personas datu aizsardzības pārkāpums, kāda PII un kuri datu subjekti ir skarti, kādi riski var rasties, kādi paziņojumi vai komunikācija ir nepieciešama un kādi novēršanas pasākumi ir vajadzīgi.

1.6.4 "Awareness" nozīmē brīdi, kad organizācijai ir pietiekama pārliecība, ka ir noticis drošības vai privātuma incidents un PII ir vai varētu būt kompromitēta.

1.6.5 "High-impact PII incident" nozīmē personas datu incidentu, kas ietver augsta riska apstrādi, īpašu kategoriju vai ļoti sensitīvu PII, liela mēroga PII, neaizsargātas personas, reglamentētus klientus, ietekmi vairākās jurisdikcijās, būtisku ietekmi uz klientu, privileģētas piekļuves kompromitēšanu, publisku ekspozīciju, izspiedējprogrammatūru, pakalpojuma nepieejamību vai būtisku operacionālu vai reputācijas ietekmi.

1.6.6 "Material incident change" nozīmē jaunu vai mainītu informāciju, kas ietekmē incidenta tvērumu, smaguma pakāpi, PII kategorijas, ietekmi uz datu subjektiem, paziņošanas lēmumu, ietekmi uz klientu, pamatcēloni, ierobežošanu, atjaunošanu, korektīvo darbību vai ārējās ziņošanas pienākumus.

2. Mērķis

2.1 Šīs politikas mērķis ir nodrošināt, ka personas datu incidenti un personas datu aizsardzības pārkāpumi tiek pārvaldīti konsekventi, savlaicīgi, likumīgi, droši un ar auditam gataviem pierādījumiem.

2.2 Šī politika atbalsta pārskatatbildību, pieprasot personas datu incidentus un personas datu aizsardzības pārkāpumus reģistrēt REG10 un, ja to nosaka incidenta fakti, sasaistīt tos ar skartajiem apstrādes ierakstiem, privātuma riskiem, apstrādātāju un apakšapstrādātāju attiecībām, nosūtīšanas ierakstiem, korektīvajām darbībām un apmācību ierakstiem.

2.3 Šī politika nodrošina, ka pārziņa, kopīga pārziņa, apstrādātāja un apakšapstrādātāja pienākumi tiek pārvaldīti, izmantojot atšķirīgus piemērojamības noteikumus, vienlaikus saglabājot vienotu incidentu un pārkāpumu pierādījumu modeli.

3. Mērķi

3.1 Šīs politikas mērķi ir:

3.1.1 nodrošināt, ka aizdomīgi personas datu incidenti tiek savlaicīgi ziņoti un reģistrēti;

3.1.2 nodrošināt, ka personas datu incidentiem tiek veikta triāža un klasifikācija, izmantojot konsekventus kritērijus;

3.1.3 nodrošināt, ka pārkāpuma izvērtēšanā tiek ņemta vērā skartā PII, datu subjekti, sistēmas, apstrādes darbības, apstrādātāji, apakšapstrādātāji, nosūtīšanas, riski un novēršanas pasākumi;

3.1.4 nodrošināt, ka tiek dokumentēti pārziņa paziņošanas un datu subjektu informēšanas lēmumi;

3.1.5 nodrošināt, ka apstrādātāja un apakšapstrādātāja paziņojumi par pārkāpumu klientiem vai augšupējām pusēm tiek veikti bez nepamatotas kavēšanās un saskaņā ar piemērojamajiem līgumiem;

3.1.6 nodrošināt, ka incidenta pārvaldības laikā pierādījumi tiek saglabāti un aizsargāti;

3.1.7 nodrošināt, ka ierobežošana, izskaušana, atjaunošana un validācija tiek izsekota REG10;

3.1.8 nodrošināt, ka reglamentētās, līgumiskās, klientu un nozares ziņošanas ierosinātāji tiek izvērtēti, ja piemērojams;

3.1.9 nodrošināt, ka incidentos gūtās mācības rada korektīvas darbības un nepārtrauktu uzlabošanu;

3.1.10 nodrošināt, ka incidentu un pārkāpumu ieraksti ir pieejami auditam, vadības pārskatīšanai, klientu apliecinājumam un regulatīvai pārskatīšanai, ja piemērojams.

4. Politikas prasības

4.1 Gatavība incidentiem un pieņemšana

4.1.1 [Both] Privacy Lead / PIMS Manager ir jāuztur PII incidentu un pārkāpumu apstrādes kritēriji REG10 vismaz reizi gadā un pēc jebkādām būtiskām izmaiņām PIMS darbības jomā, juridiskajā kontekstā, līgumiskajās saistībās vai augsta riska apstrādē.

4.1.2 [All] Incident Response Coordinator ir jāreģistrē katrs paziņotais vai atklātais aizdomīgais personas datu incidents REG10 vienas darba dienas laikā pēc saņemšanas vai ātrāk, ja var tikt aktivizēts piemērojams paziņošanas vai klientu ziņošanas termiņš.

4.1.3 [Both] System Owner / Application Owner ir jāsaglabā attiecīgie sistēmas žurnāli, brīdinājumi, piekļuves ieraksti, konfigurācijas pierādījumi un atjaunošanas pierādījumi, kas saistīti ar REG10, ja aizdomīgs incidents ietekmē sistēmu vai lietojumprogrammu, kas apstrādā PII.

4.1.4 [Both] Information Security Lead ir jāpabeidz sākotnējā tehniskā triāža par jebkuru drošības notikumu, kurā iesaistīta PII, 24 stundu laikā pēc atklāšanas un REG10 jāreģistrē sākotnējā smaguma pakāpe, skartie aktīvi un ierobežošanas statuss.

4.2 Klasifikācija un pārkāpuma izvērtēšana

4.2.1 [Both] Incident Response Coordinator ir jāklasificē katrs REG10 ieraksts kā ar PII nesaistīts notikums, aizdomīgs personas datu incidents, apstiprināts personas datu incidents vai apstiprināts personas datu aizsardzības pārkāpums 24 stundu laikā pēc pieņemšanas vai jāatjaunina REG10 ieraksts ar iemeslu, kāpēc klasifikācija vēl nav pabeigta.

4.2.2 [Both] Privacy Lead / PIMS Manager ir jāidentificē skartā apstrādes darbība, PII kategorijas, datu subjektu kategorijas, sistēmas, apstrādātāji, apakšapstrādātāji, nosūtīšanas vietas un privātuma riski REG02, REG04, REG08, REG09 un REG10 pirms tiek galīgi pieņemts lēmums par paziņošanu par pārkāpumu.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor ir jāizvērtē risks skartajiem datu subjektiem katram apstiprinātam vai pamatoti aizdomīgam personas datu aizsardzības pārkāpumam un REG10 jāreģistrē paziņošanas ieteikums, riska pamatojums un konsultācija pirms tiek pieņemts ārējās paziņošanas lēmums.

4.2.4 [Processor] Privacy Lead / PIMS Manager ir jāidentificē skartais pārzinis vai klients un piemērojamās līgumiskās paziņošanas prasības, tiklīdz organizācija uzzina par personas datu aizsardzības pārkāpumu, kas ietekmē klienta PII, un rezultāts jāreģistrē REG08 un REG10.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager ir jāpārbauda saskaņotā atbildība par pārkāpumu, vadošā atbildība par komunikāciju un koordinācijas kārtība pirms jebkādas ārējas paziņošanas vai komunikācijas, ko veic kopīgs pārzinis, un lēmums jāreģistrē REG08 un REG10.

4.2.6 [Conditional] Privacy Lead / PIMS Manager ir jāizvērtē piemērojamie juridiskie, nozares, finanšu sektora, kiberdrošības, līgumiskie, klientu un pakalpojuma saņēmēju ziņošanas ierosinātāji katram augstas ietekmes personas datu incidentam un piemērojamības rezultāts jāreģistrē REG01, REG08 un REG10.

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

9. Izņēmumi

9.1.1 [Both] Privacy Lead / PIMS Manager ir jāreģistrē jebkurš šīs politikas izņēmums REG12 pirms ieviešanas vai 24 stundu laikā pēc ārkārtas darbības, ja iepriekšējs apstiprinājums nebija iespējams.

9.1.2 [Both] Top Management ir jāapstiprina jebkurš izņēmums, kas būtiski ietekmē paziņošanas par pārkāpumu termiņus, publisko komunikāciju, klienta saistības, pierādījumu saglabāšanu vai risku datu subjektiem pirms incidenta slēgšanas, apstiprinājuma pierādījumus saglabājot REG10 un REG12.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor ir jādokumentē konsultācija par jebkuru kavētu paziņošanu, nepaziņošanas lēmumu vai izņēmuma komunikācijas pieeju pirms incidenta slēgšanas, konsultāciju saglabājot REG10.

9.1.4 [Both] Vendor / Procurement Owner ir jāreģistrē piegādātāja, apstrādātāja, apakšapstrādātāja vai klienta izraisīti izņēmumi, kas ietekmē reaģēšanu uz incidentu, REG08 un REG12 piecu darba dienu laikā pēc izņēmuma identificēšanas.

10. Piemērošana

10.1.1 [All] Process Owner / Business Owner ir jāeskalē nespēja ziņot par aizdomīgu personas datu incidentu, saglabāt pierādījumus, izpildīt piešķirtās darbības vai sadarboties pārkāpuma izvērtēšanā Privacy Lead / PIMS Manager divu darba dienu laikā pēc atklāšanas, pierādījumus saglabājot REG12.

10.1.2 [Both] Privacy Lead / PIMS Manager ir jāreģistrē REG12 neatbilstība, ja šīs politikas pārkāpums ietekmē incidenta pieņemšanu, triāžu, ierobežošanu, paziņošanu, pierādījumu integritāti, komunikāciju vai korektīvo darbību.

10.1.3 [Both] Vendor / Procurement Owner ir jāuzsāk piegādātāja vai apstrādātāja trūkumu novēršana, izmantojot REG08 un REG12, piecu darba dienu laikā, ja apstrādātājs, apakšapstrādātājs, piegādātājs vai cita trešā puse neizpilda saskaņotos incidentu vai pārkāpumu pienākumus.

10.1.4 [Both] Top Management ir jāpārskata būtiskas vai atkārtotas incidentu pārvaldības neatbilstības nākamajā plānotajā vadības pārskatīšanā, lēmumus un nepieciešamās darbības saglabājot REG12.

11. Pārskatīšana un uzturēšana

11.1.1 [Both] Privacy Lead / PIMS Manager ir jāpārskata šī politika vismaz reizi gadā un REG12 jāreģistrē pārskatīšanas rezultāts, nepieciešamās izmaiņas un apstiprinājuma statuss.

11.1.2 [Both] Incident Response Coordinator ir jāierosina šīs politikas pēcincidenta pārskatīšana 30 kalendāro dienu laikā pēc jebkura augstas ietekmes personas datu incidenta vai apstiprināta personas datu aizsardzības pārkāpuma slēgšanas, pārskatīšanas pierādījumus saglabājot REG10 un REG12.

11.1.3 [Conditional] Privacy Lead / PIMS Manager ir jāpārskata šī politika 30 kalendāro dienu laikā pēc tam, kad kļūst zināms par būtiskām izmaiņām piemērojamajās juridiskajās, nozares, klientu, līgumiskajās, apstrādātāju, apakšapstrādātāju vai ar nosūtīšanu saistītajās incidentu

ziņošanas prasībās, pārskatīšanas pierādījumus saglabājot REG01, REG08, REG09 un REG12.

11.1.4 [Both] Internal Audit / Compliance Reviewer ir vismaz reizi gadā jāpārskata šīs politikas ieviešana PIMS iekšējā audita programmas ietvaros, audita konstatējumus un korektīvās darbības saglabājot REG12.

11.1.5 [Both] Top Management ir plānotās vadības pārskatīšanas laikā jāpārskata incidentu tendences, būtiski pārkāpumi, paziņošanas veiktspēja, nokavētas korektīvās darbības un politikas efektivitāte, rezultātus saglabājot REG12.

12. Saistītās politikas

12.1 Šī politika jālasa kopā ar:

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 paziņojuma un pārredzamības politika

12.6 PII06 - Datu subjektu tiesību pārvaldības politika

12.7 PII07 - Privātuma risku izvērtēšanas un DPIA politika

12.8 PII08 - Datu aizsardzības pēc projektēšanas un pēc noklusējuma politika

12.9 PII10 - PII glabāšanas, dzēšanas un likvidēšanas politika

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

12.11 PII13 - Starptautiskas PII nosūtīšanas politika

12.12 PII14 - PII drošības un piekļuves kontroles politika

12.13 PII16 - Privātuma apmācības, informētības un kompetences politika

12.14 PII17 - PIMS dokumentētas informācijas un pierādījumu pārvaldības politika

12.15 PII18 - PIMS uzraudzības, audita un uzlabošanas politika

13. Atsauces standarti un ietvari

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.7; 4.5.1; 4.5.3; 4.5.4; 5.2.2; 6.2.2; 7.1.1; 7.1.7; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.2.2; 4.3.4; 4.6.3; 6.3.1; 7.1.4; 11.1.2].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 6.4.1; 6.5.1; 8.1.1; 8.1.4; 10.1.2; 11.1.4; 11.1.5].

13.4 ISO/IEC 27701:2025 - Annex A.3.11. Addressed by clauses [4.1.1; 4.1.2; 4.2.6; 4.4.1; 5.1.1; 5.4.1; 7.1.1; 7.1.2; 7.1.6].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.4; 4.2.1; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.3; 4.4.4; 4.5.1; 4.5.4; 6.3.1].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.2.6; 4.4.6; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.4; 6.2.2; 9.1.2; 11.1.3].

13.7 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.6. Addressed by clauses [4.2.4; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5; 10.1.3].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.2; 4.4.1; 4.5.1; 4.5.3; 4.5.4; 4.6.2; 5.2.1; 6.3.1; 8.1.3; 11.1.5].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.1; 4.4.3; 5.3.1; 6.2.2; 11.1.3].

13.10 GDPR - Article 28. Addressed by clauses [4.2.4; 4.3.5; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5; 10.1.3].

13.11 GDPR - Article 32. Addressed by clauses [4.1.3; 4.1.4; 4.3.2; 4.3.3; 4.5.2; 4.6.3; 5.5.1; 7.1.4; 8.1.2; 11.1.2].

13.12 GDPR - Article 33. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.1; 4.5.4; 8.1.3; 9.1.3].

13.13 GDPR - Article 34. Addressed by clauses [4.2.3; 4.2.5; 4.4.2; 4.4.3; 4.4.7; 4.5.4; 8.1.3; 9.1.3].

13.14 GDPR - Article 39. Addressed by clauses [4.2.3; 4.4.2; 5.3.1; 6.2.2; 9.1.3; 11.1.3].

13.15 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.2.2; 4.3.2; 4.3.3; 4.5.3; 4.6.2; 4.6.3; 5.2.2; 6.4.1; 8.1.4; 11.1.4].

13.16 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.2.3; 4.4.1; 4.4.3; 4.6.5; 7.1.3; 7.1.6].

13.17 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.5.1; 4.5.2; 4.6.1; 4.6.2; 7.1.2; 7.1.6].

13.18 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.2; 4.6.1; 5.4.1; 7.1.6; 11.1.2].

13.19 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.1; 4.6.1; 4.6.5; 5.1.1; 7.1.1; 7.1.3; 7.1.6; 8.1.6; 11.1.1; 11.1.2].

13.20 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.4.1; 4.4.4; 4.5.1; 5.4.2; 6.1.2; 8.1.2].

13.21 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.4; 4.3.5; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5].

13.22 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.2.6; 4.4.6; 4.4.7; 5.3.1; 6.2.2; 8.1.3; 11.1.3].

13.23 DORA Regulation (EU) 2022/2554 - Article 17; Article 18; Article 19. Addressed by clauses [4.2.1; 4.2.6; 4.4.6; 4.4.7; 5.1.2; 6.2.1; 8.1.3; 11.1.3; 11.1.5].