

				Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: PII23				Dokumenta nosaukums: Mākoņpakalpojumu PII apstrādātāja 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

<p>Juridiskais paziņojums (autortiesības un lietošanas ierobežojumi) (C) 2025 Clarysec LLC. All rights reserved.</p> <p>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.</p> <p>Neautorizēta lietošana ir stingri aizliegta un var izraisīt tiesvedību.</p> <p>Par licencēšanu sazinieties: info@clarysec.com</p>
--

Saskaņots ar piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts/kontrole/pant	Piemērojamība	Pārklājuma veids	Piezīme
ISO/IEC 27701:2025	Clause 4.1; Clause 6.1.3	Processor	Supporting	PIMS loma un kontroles pasākumu piemērojamība
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Processor	Primary	Dokumentēti mākoņpakalpojumu apstrādātāja pierādījumi un darbības kontrole
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Processor	Supporting	Uzraudzība, neatbilstība un korektīvā darbība
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.5; Annex A.2.2.6; Annex A.2.2.7	Processor	Primary	Klientu vienošanās, norādījumi, atbalsts un ieraksti
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Palīdzība klientam saistībā ar pienākumiem pret datu subjektiem
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Primary	Pagaidu datnes, atdošana, nosūtīšana, likvidēšana un pārsūtīšanas kontroles pasākumi
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Supporting	Nosūtīšanas pamats un atrašanās vietas
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Izpaušanas ieraksti un izpaušanas pieprasījumu apstrāde
ISO/IEC 27701:2025	Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9	Processor	Primary	Apakšapstrādātāju izpaušana, piesaiste un paziņošana par izmaiņām
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9; Annex A.3.14; Annex A.3.24; Annex A.3.25	Processor	Supporting	Piekluves, ierakstu, rezerves kopiju un žurnālfiksēšanas pierādījumi
GDPR	Article 28	Processor	Primary	Apstrādātājs, apakšapstrādātājs, palīdzība, audits, dzēšana un atdošana
GDPR	Article 30	Processor	Supporting	Apstrādātāja ieraksti
GDPR	Article 32; Article 33	Processor	Supporting	Drošība un paziņošana pārzinim par pārkāpumu
GDPR	Article 44	Conditional	Reference	Starptautiskas nosūtīšanas maršrutēšana

ISO/IEC 29100:2020	Clause 5.3; Clause 5.5; Clause 5.6	Processor	Supporting	Nolūka, minimizēšanas, izmantošanas, glabāšanas un izpaušanas ierobežošana
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Processor	Supporting	Pārskatbūve, informācijas drošība un atbilstība
ISO/IEC 29151:2022	Clause 15.1.2; Clause 15.2.2; Clause 15.2.3; Annex A.7; Annex A.7.2	Processor	Supporting	Apstrādātāja izvērtēšana, uzraudzība, izmaiņas un glabāšanas kontroles pasākumi
ISO/IEC 27001:2022	Clause 6.1.3; Clause 8.1; Annex A controls 5.19; 5.20; 5.21; 5.22; 5.23	Processor	Supporting	Kontroles pasākumu piemērojamība, darbības kontrole un piegādātāju/mākoņpakalpojumu kontroles pasākumi
ISO/IEC 27002:2022	Control 5.19; Control 5.20; Control 5.21; Control 5.22; Control 5.23; Control 8.10; Control 8.15; Control 8.16	Processor	Supporting	Piegādātāju, mākoņpakalpojumu, dzēšanas, žurnālfiksēšanas un uzraudzības kontroles pasākumi
ISO/IEC 27018:2020	Annex A.2.1; Annex A.3.1	Processor	Primary	Mākoņpakalpojumu apstrādātāja palīdzība klientam un nolūka ierobežošana
ISO/IEC 27018:2020	Annex A.6.1; Annex A.6.2; Annex A.8.1	Processor	Primary	Paziņošana par izpaušanu mākonī, izpaušanas ieraksti un apakšuzņēmēju pārredzamība
ISO/IEC 27018:2020	Annex A.10.1; Annex A.10.3; Annex A.11.11; Annex A.11.12; Annex A.12.1	Processor	Primary	Mākoņpakalpojumu pārkāpumu saskarne, izstāšanās, līgumiskie pasākumi, apakšlīgumi un atrašanās vietu ieraksti
ISO/IEC 27036-2:2022	Clause 6.1.1; Clause 6.1.2	Processor	Supporting	Piegādes attiecību stratēģija un pārvaldība
ISO/IEC 27036-2:2022	Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5	Processor	Supporting	Piegādātāju attiecību plānošana, vienošanās, pārvaldība, uzraudzība un izbeigšana
ISO/IEC 27555:2025	Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8	Processor	Supporting	Dzēšanas ietvars un dokumentācija
ISO/IEC 27555:2025	Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause	Processor	Supporting	Dzēšanas īstenošana un izņēmumi

	9.5; Clause 9.6; Clause 9.7			
--	--------------------------------	--	--	--

1. Piemērošanas joma

1.1 Šī politika nosaka obligātās privātuma prasības mākoņpakalpojumiem, kuros organizācija darbojas kā PII apstrādātājs vai apakšapstrādātājs, tostarp SaaS, PaaS, IaaS, mākoņvidē mitinātu lietotņu, pārvaldītu mākoņpakalpojumu, mākoņatbalsta, mākoņkrātuvju, mākoņanalītikas un mākoņinfrastruktūras pakalpojumiem, kas apstrādā PII klientu vārdā.

1.2 Šī politika attiecas uz mākoņapstrādi, kas tiek veikta saskaņā ar klientu vienošanos, dokumentētiem klienta norādījumiem, augšupējā apstrādātāja norādījumiem, apakšapstrādātāju kārtību, mākoņreģiona konfigurāciju, mākoņatbalsta piekļuvi, pakalpojuma administrēšanu, rezerves kopiju veidošanu, replicēšanu, žurnālfiksēšanu, uzraudzību, dzēšanu, atdošanu, atbalstu pārkāpumu gadījumā, audita atbalstu un pienākumiem palīdzēt klientam.

1.3 Šī politika aptver:

1.3.1 mākoņpakalpojumu PII apstrādes jomu un norādījumu ierakstus;

1.3.2 klientu vienošanās un kopīgās atbildības pierādījumus;

1.3.3 nomnieku izolācijas, mākoņpiekļuves, administratīvās piekļuves un žurnālfiksēšanas pierādījumus;

1.3.4 apakšapstrādātāju un mākoņpakalpojumu piegādes ķēdes pārvaldību;

1.3.5 atrašanās vietu, attālinātas piekļuves un starptautiskas nosūtīšanas maršrutēšanu;

1.3.6 atdošanas, nosūtīšanas, dzēšanas, likvidēšanas un izstāšanās pierādījumus;

1.3.7 palīdzību klientam saistībā ar datu subjektu tiesībām, DPIA, auditiem un reaģēšanu uz pārkāpumiem;

1.3.8 uzraudzības, izņēmumu, politikas piemērošanas un uzlabošanas pierādījumus.

1.4 Šī politika neveido atsevišķu klientu līgumu reģistru, mākoņpakalpojumu reģistru, nomnieku izolācijas reģistru, piekļuves reģistru, žurnālu reģistru, dzēšanas reģistru, atbalsta pieprasījumu reģistru, audita pierādījumu reģistru, pārkāpumu reģistru, apakšapstrādātāju reģistru vai mākoņpakalpojumu pārvaldības komiteju.

1.5 Šī politika neaizstāj:

1.5.1 PII03 attiecībā uz apstrādes uzskaiti un tiesiskā pamata atbildību;

1.5.2 PII06 attiecībā uz pilnu datu subjektu tiesību īstenošanas darbplūsmu;

1.5.3 PII07 attiecībā uz privātuma risku un DPIA metodoloģiju;

1.5.4 PII08 attiecībā uz datu aizsardzības pēc projektēšanas un pēc noklusējuma kontroles vārtiem;

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

1.5.6 PII10 attiecībā uz glabāšanas, dzēšanas un likvidēšanas metodoloģiju;

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

1.5.8 PII13 attiecībā uz starptautiskas nosūtīšanas mehānisma izvērtēšanu;

1.5.9 PII14 attiecībā uz pilnu PII drošības un piekļuves kontroles arhitektūru;

1.5.10 PII15 attiecībā uz incidentu un pārkāpumu pārvaldības darbplūsmu;

1.5.11 PII17 attiecībā uz dokumentētas informācijas kontroli;

1.5.12 PII18 attiecībā uz PIMS uzraudzības, audita un uzlabošanas pārvaldību.

2. Mērķis

2.1 Šīs politikas mērķis ir nodrošināt, ka mākoņpakalpojumu PII apstrādātāja un apakšapstrādātāja pakalpojumi tiek sniegti saskaņā ar dokumentētiem klienta norādījumiem, skaidru apstrādes jomu, kontrolētu apakšapstrādātāju kārtību, atbilstošām mākoņdrošības atbildībām, dokumentētu

atrašanās vietu un nosūtīšanas maršrutēšanu, pienākumiem palīdzēt klientam, atbalstu pārkāpumu gadījumā, dzēšanas/atdošanas spēju un auditam gataviem pierādījumiem.

2.2 Šī politika atbalsta ISO/IEC 27701:2025 PIMS gatavību sertifikācijai mākoņpakalpojumu apstrādātājiem un mākoņpakalpojumu apakšapstrādātājiem, vienlaikus saglabājot integrāciju ar esošo PIMS politiku kopumu un kanoniskajiem pierādījumu objektiem.

3. Mērķi

3.1 Šīs politikas mērķi ir:

- 3.1.1 Noteikt mākoņpakalpojumu PII apstrādes jomu pirms klienta piesaistes vai būtiskas izmaiņas.
- 3.1.2 Nodrošināt, ka klienta norādījumi tiek reģistrēti, pārskatīti un ievēroti.
- 3.1.3 Uzturēt mākoņpakalpojumu apstrādātāja un apakšapstrādātāja pierādījumus kanoniskajos PIMS reģistros.
- 3.1.4 Noteikt kopīgās atbildības, nomnieku izolācijas, piekļuves, žurnālfiksēšanas un atrašanās vietu pierādījumus, nedublējot PII drošības politiku.
- 3.1.5 Kontrolēt apakšapstrādātāju piesaistes, izmaiņu, tālāk nododamo pienākumu un uzraudzības pierādījumus.
- 3.1.6 Atbalstīt klientus saistībā ar datu subjektu tiesībām, DPIA, audita pieprasījumiem un reaģēšanu uz pārkāpumiem.
- 3.1.7 Nodrošināt, ka izstāšanās brīdī tiek saglabāti atdošanas, dzēšanas, nosūtīšanas un likvidēšanas pierādījumi.
- 3.1.8 Uzraudzīt mākoņpakalpojumu apstrādātāja kontroles pasākumus un virzīt korektīvo darbību, izmantojot REG12.

4. Politikas prasības

4.1 Mākoņapstrādes joma un klienta norādījumi

- 4.1.1 [Processor] Privacy Lead / PIMS Manager ir jāreģistrē katrs mākoņpakalpojumu PII apstrādes pakalpojums, klienta apstrādes loma, klienta norādījumu avots, PII kategorijas, datu subjektu kategorijas, pakalpojuma nolūks, apstrādes atrašanās vieta, apakšapstrādātāja atkarība, dzēšanas atkarība un nosūtīšanas pazīme REG02 un REG08 pirms klienta piesaistes vai būtiskas pakalpojuma izmaiņas.
- 4.1.2 [Processor] Process Owner / Business Owner ir jāreģistrē dokumentētie klienta norādījumi mākoņpakalpojumu PII apstrādei REG08 pirms apstrādes sākšanas.
- 4.1.3 [Subprocessor] Process Owner / Business Owner ir jāreģistrē augšupējā apstrādātāja vai klienta apstiprinātie norādījumi REG08 pirms PII apstrādes mākoņpakalpojumu apakšapstrādātāja statusā.
- 4.1.4 [Processor] Privacy Lead / PIMS Manager ir jāreģistrē mākoņpakalpojumu apstrādātāja kontroles pasākumu piemērojamība REG03 pirms jauna mākoņpakalpojumu PII apstrādes pakalpojuma izlaišanas vai būtiskas maiņas.
- 4.1.5 [Processor] Data Protection Officer / Privacy Advisor ir jāpārskata jebkurš klienta norādījums, kas šķiet neatbilstošs dokumentētajiem klienta pienākumiem, PIMS prasībām vai apstiprinātajai pakalpojuma jomai, REG12 pirms organizācija rīkojas saskaņā ar šo norādījumu.
- 4.1.6 [Processor] Process Owner / Business Owner ir jāreģistrē jebkura ierosināta klienta PII apstrāde ārpus dokumentētajiem klienta norādījumiem REG12 un jāsaņem Privacy Lead / PIMS Manager apstiprinājums pirms apstrādes veikšanas.

4.2 Mākoņkonfigurācija, nomnieku izolācija, piekļuve un žurnālfiksēšana

- 4.2.1 [Processor] Information Security Lead ir jāreģistrē mākoņpakalpojumu kopīgās atbildības robeža attiecībā uz PII piekļuvi, administrēšanu, žurnālfiksēšanu, rezerves kopijām, šifrēšanu, ievainojamību pārvaldību un dzēšanu REG08 pirms klienta piesaistes vai būtiskas pakalpojuma izmaiņas.
- 4.2.2 [Processor] System Owner / Application Owner ir jāvalidē nomnieku izolācijas vai klientu nodalīšanas kontroles pasākumi REG12 pirms izmantošanas ražošanas vidē un pēc būtiskas arhitektūras izmaiņas.
- 4.2.3 [Processor] System Owner / Application Owner drīkst piešķirt mākoņvides administratīvo piekļuvi klienta PII tikai pēc tam, kad REG12 ir reģistrēta apstiprināta biznesa vajadzība, piekļuves joma, piekļuves ilgums un pārskatīšanas biežums.
- 4.2.4 [Processor] Information Security Lead ir jāpārskata priviliģēta mākoņpiekļuve, atbalsta piekļuve, piekļuve klienta PII un žurnālfiksēšanas pārklājums REG12 vismaz reizi ceturksnī.
- 4.2.5 [Processor] System Owner / Application Owner ir jāvalidē ražošanas, sagatavošanas, testa un atbalsta vides nodalīšana klienta PII vajadzībām REG12 pirms izlaišanas un pēc būtiskas vides izmaiņas.
- 4.2.6 [Processor] System Owner / Application Owner ir jāreģistrē rezerves kopiju, replicēšanas, žurnālu glabāšanas un atbalsta piekļuves atrašanās vietas mākoņvidē apstrādātai klienta PII REG02, REG08 vai REG09 pirms šo atrašanās vietu iespējošanas vai maiņas.

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

9. Izņēmumi

- 9.1 [Processor] Process Owner / Business Owner ir jāpieprasa mākoņpakalpojumu apstrādātāja izņēmums REG12 pirms piesaistes, izlaišanas, atjaunošanas vai turpmākas izmantošanas, ja nepieciešamie klienta norādījumu, apakšapstrādātāja, atrašanās vietas, piekļuves, žurnālfiksēšanas, dzēšanas vai incidentu saskarnes pierādījumi ir nepilnīgi.
- 9.2 [Processor] Data Protection Officer / Privacy Advisor ir jāpārskata privātumam nozīmīgi mākoņpakalpojumu apstrādātāja izņēmumu pieprasījumi REG12 pirms apstiprināšanas, ja izņēmums ietekmē klienta norādījumus, palīdzību datu subjektam, nosūtīšanu, apakšapstrādātājus, dzēšanu, atbalstu pārkāpumu gadījumā vai augstas ietekmes PII.
- 9.3 [Processor] Top Management ir jāapstiprina augsta riska vai būtiski mākoņpakalpojumu apstrādātāja izņēmumi REG12 pirms izņēmuma stāšanās spēkā.
- 9.4 [Processor] Privacy Lead / PIMS Manager ir jāpiešķir derīguma beigu datums, novēršanas īpašnieks, pārskatīšanas datums un atlikušā riska piezīme REG12 katram apstiprinātam mākoņpakalpojumu apstrādātāja izņēmumam pirms apstiprināšanas.

10. Politikas piemērošana

- 10.1 [Processor] Privacy Lead / PIMS Manager ir jābloķē klienta piesaiste, pakalpojuma izlaišana, atjaunošana vai turpmāka apstrāde, ja nepieciešamie REG02, REG03, REG08, REG09, REG10 vai REG12 pierādījumi trūkst pirms apstrādes sākšanas vai turpināšanas.
- 10.2 [Processor] System Owner / Application Owner ir jāatspējo neapstiprināta mākoņpiekļuve, neapstiprināta reģiona izmantošana, neapstiprināta replicēšana, neapstiprināta atbalsta piekļuve vai neapstiprināta apakšapstrādātāja datu plūsma vienas darba dienas laikā pēc politikas piemērošanas lēmuma un jāreģistrē pabeigšana REG08 vai REG12.
- 10.3 [Processor] Vendor / Procurement Owner ir jāaptur jauna PII apstrāde, ko veic neapstiprināts vai neatbilstošs mākoņpakalpojumu apakšapstrādātājs, līdz REG08 korektīvās darbības pierādījumi ir pilnīgi.

- 10.4 [Processor] Incident Response Coordinator ir jāeskalē nokavētie klienta incidenta paziņošanas termiņi REG10 un REG12 vienas darba dienas laikā pēc identificēšanas.
- 10.5 [Processor] Internal Audit / Compliance Reviewer ir jāpārbauda korektīvās darbības efektivitāte attiecībā uz būtiskām vai atkārtotām mākoņpakalpojumu apstrādātāja neatbilstībām REG12 60 dienu laikā pēc korektīvās darbības slēgšanas.

11. Pārskatīšana un uzturēšana

- 11.1 [Processor] Privacy Lead / PIMS Manager ir jāpārskata šī politika REG12 reizi gadā un 30 dienu laikā pēc būtiskas izmaiņas mākoņpakalpojumu apstrādātāja pienākumos, mākoņarhitektūrā, apakšapstrādātāju pārvaldībā, palīdzībā klientam, dzēšanas spējā vai sertifikācijas prasībās.
- 11.2 [Processor] Vendor / Procurement Owner ir jāpārskata mākoņpakalpojumu apakšapstrādātāju un mākoņpakalpojumu atkarību ieraksti REG08 vismaz reizi gadā un pirms atjaunošanas.
- 11.3 [Processor] System Owner / Application Owner ir jāpārskata nomnieku izolācijas, privilēģētās piekļuves, žurnālfiksēšanas, rezerves kopiju, replicēšanas un dzēšanas pierādījumi REG12 vismaz reizi gadā un pēc būtiskas arhitektūras izmaiņas.
- 11.4 [Processor] Privacy Lead / PIMS Manager ir jāpārskata REG09 mākoņpakalpojumu atrašanās vietu un nosūtīšanas maršrutēšanas ieraksti vismaz reizi gadā un 15 darba dienu laikā pēc būtiskas atrašanās vietas, atbalsta piekļuves, rezerves kopiju vai apakšapstrādātāja izmaiņas.
- 11.5 [Processor] Privacy Lead / PIMS Manager ir jāatjaunina REG03 15 darba dienu laikā pēc apstiprinātām politikas izmaiņām, kas ietekmē mākoņpakalpojumu apstrādātāja kontroles pasākumu piemērojamību.
- 11.6 [All] Top Management ir jāapstiprina būtiski šīs politikas grozījumi REG12 pirms publicēšanas.

12. Saistītās politikas

12.1 Šo politiku atbalsta šādas saistītās politikas:

- 12.1.1 PII01 - Privātuma informācijas pārvaldības sistēmas politika
- 12.1.2 PII02 - Privātuma lomu, pienākumu un pārskatatbildības politika
- 12.1.3 PII03 - PII apstrādes uzskaites un tiesiskā pamata politika
- 12.1.4 PII06 - Datu subjektu tiesību pārvaldības politika
- 12.1.5 PII07 - Privātuma risku izvērtēšanas un DPIA politika
- 12.1.6 PII08 - Datu aizsardzības pēc projektēšanas un pēc noklusējuma politika
- 12.1.7 PII09 - PII vākšanas, izmantošanas, izpaušanas un koplietošanas politika
- 12.1.8 PII10 - PII glabāšanas, dzēšanas un likvidēšanas politika
- 12.1.9 PII12 - Apstrādātāju, apakšapstrādātāju un trešo pušu privātuma pārvaldības politika
- 12.1.10 PII13 - Starptautiskas PII nosūtīšanas politika
- 12.1.11 PII14 - PII drošības un piekļuves kontroles politika
- 12.1.12 PII15 - PII incidentu un pārkāpumu pārvaldības politika
- 12.1.13 PII17 - PIMS dokumentētās informācijas un pierādījumu pārvaldības politika
- 12.1.14 PII18 - PIMS uzraudzības, audita un uzlabošanas politika
- 12.1.15 PII20 - Bērnu privātuma politika
- 12.1.16 PII21 - Mākslīgā intelekta un automatizētas lēmumu pieņemšanas privātuma politika
- 12.1.17 PII22 - Mārketinga privātuma un sīkdatņu politika
- 12.1.18 PII24 - Videonovērošanas un fiziskās novērošanas privātuma politika

13. Atsauces standarti un ietvari

- 13.1 Šī politika ir kartēta uz turpmāk minētajiem standartiem un regulējumu. Kartējums skaidro, kā politika atbalsta norādītās prasības, un identificē iekšējos punktus, kas tās īsteno vai atbalsta.
- 13.2 ISO/IEC 27701:2025 - Clause 4.1; Clause 6.1.3. Addressed by clauses [4.1.1; 4.1.4; 5.2; 7.1; 11.5].
- 13.3 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.3.1; 4.4.1; 4.6.1; 4.7.1; 4.8.1; 7.1; 7.2; 7.3].
- 13.4 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.3.5; 4.6.6; 4.8.1; 4.8.2; 4.8.4; 6.1; 6.2; 8.1; 8.2; 8.3; 8.4; 8.5; 10.5; 11.1].
- 13.5 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.5; Annex A.2.2.6; Annex A.2.2.7. Addressed by clauses [4.1.2; 4.1.3; 4.1.5; 4.1.6; 4.3.1; 4.7.5; 7.2].
- 13.6 ISO/IEC 27701:2025 - Annex A.2.3.2. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5].
- 13.7 ISO/IEC 27701:2025 - Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].
- 13.8 ISO/IEC 27701:2025 - Annex A.2.5.2; Annex A.2.5.3. Addressed by clauses [4.2.6; 4.4.4; 4.5.1; 4.5.2; 7.5; 11.4].
- 13.9 ISO/IEC 27701:2025 - Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.5.3; 4.5.4; 4.7.2; 4.7.5].
- 13.10 ISO/IEC 27701:2025 - Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6].
- 13.11 ISO/IEC 27701:2025 - Annex A.3.8; Annex A.3.9; Annex A.3.14; Annex A.3.24; Annex A.3.25. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.7.3; 5.4; 5.6; 11.3].
- 13.12 GDPR - Article 28. Addressed by clauses [4.1.2; 4.1.3; 4.3.1; 4.3.2; 4.3.4; 4.4.2; 4.4.3; 4.4.5; 4.6.1; 4.6.3; 4.6.5; 4.7.2].
- 13.13 GDPR - Article 30. Addressed by clauses [4.1.1; 4.1.3; 4.4.1; 4.8.1; 7.1].
- 13.14 GDPR - Article 32; Article 33. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 7.6].
- 13.15 GDPR - Article 44. Addressed by clauses [4.2.6; 4.4.4; 4.5.1; 4.5.2; 7.5; 11.4].
- 13.16 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.1.6; 4.2.6; 4.5.1; 4.6.1; 4.6.3].
- 13.17 ISO/IEC 29100:2020 - Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.2.4; 4.3.5; 4.8.1; 4.8.4; 6.1; 8.5; 10.5].
- 13.18 ISO/IEC 29151:2022 - Clause 15.1.2; Clause 15.2.2; Clause 15.2.3; Annex A.7; Annex A.7.2. Addressed by clauses [4.4.1; 4.4.6; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.8.3].
- 13.19 ISO/IEC 27001:2022 - Clause 6.1.3; Clause 8.1; Annex A controls 5.19; 5.20; 5.21; 5.22; 5.23. Addressed by clauses [4.1.4; 4.2.1; 4.4.1; 4.4.3; 4.4.6; 4.8.1; 4.8.3; 6.1; 7.1; 11.5].
- 13.20 ISO/IEC 27002:2022 - Control 5.19; Control 5.20; Control 5.21; Control 5.22; Control 5.23; Control 8.10; Control 8.15; Control 8.16. Addressed by clauses [4.2.1; 4.2.4; 4.4.1; 4.4.3; 4.4.6; 4.6.1; 4.6.3; 4.7.3; 4.8.3; 11.3].
- 13.21 ISO/IEC 27018:2020 - Annex A.2.1; Annex A.3.1. Addressed by clauses [4.1.2; 4.1.6; 4.3.1; 4.3.2; 4.3.3; 4.3.5].
- 13.22 ISO/IEC 27018:2020 - Annex A.6.1; Annex A.6.2; Annex A.8.1. Addressed by clauses [4.4.1; 4.4.2; 4.4.5; 4.5.3; 4.5.4].

- 13.23 ISO/IEC 27018:2020 - Annex A.10.1; Annex A.10.3; Annex A.11.11; Annex A.11.12; Annex A.12.1. Addressed by clauses [4.2.6; 4.4.3; 4.4.4; 4.6.1; 4.6.3; 4.6.5; 4.7.1; 4.7.2; 4.7.5].
- 13.24 ISO/IEC 27036-2:2022 - Clause 6.1.1; Clause 6.1.2. Addressed by clauses [4.1.1; 4.2.1; 4.4.1; 4.4.6; 6.1; 7.2].
- 13.25 ISO/IEC 27036-2:2022 - Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.4.6; 4.8.2; 4.8.3; 10.3; 11.2].
- 13.26 ISO/IEC 27555:2025 - Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].
- 13.27 ISO/IEC 27555:2025 - Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7. Addressed by clauses [4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6; 9.1; 9.4].