					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: PII24					Dokumenta nosaukums: **CCTV un fiziskās uzraudzības privātuma 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/kontroles pasākums/pants	Piemērojamība	Pārklājuma veids	Piezīme
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Dokumentēti un operacionāli kontroles pasākumi
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.1.2.3; Annex A.1.2.6; Annex A.1.2.9	Controller	Primary	Nolūks, tiesiskais pamats, riska trigeris un ieraksti
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Apstrādātāja un kopīga pārziņa atbildības sadalījums
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10	Controller	Supporting	Datu subjektu pienākumi un pieprasījumi
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9	Controller	Primary	Vākšana, apstrāde, minimizēšana, glabāšana un likvidēšana
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Izpaušanas ieraksti un pieprasījumi
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Apstrādātāja vienošanās, norādījumi, atbalsts un ieraksti
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Apstrādātāja tiesības un atbalsts izpaušanā
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Ierakstu aizsardzība un žurnālu veidošana
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Principi un pārskatatbildība
GDPR	Article 6	Controller	Primary	Tiesiskais pamats

GDPR	Article 12; Article 13; Article 14	Controller	Primary	Pārredzamība un paziņojumi
GDPR	Article 15; Article 16; Article 17; Article 18; Article 21	Controller	Supporting	Tiesību īstenošanas pieprasījumi
GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Pārvaldība, apstrādātāji, ieraksti, drošība, DPIA un konsultācijas
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Controller	Supporting	Nolūks, vākšana, minimizēšana, glabāšana un izpaušana
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Pārredzamība, līdzdalība, pārskatatbildība, drošība un atbilstība
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	Privātuma risks un DPIA trigeri
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Both	Supporting	Personas datu aizsardzības privātuma kontroles pasākumi
ISO/IEC 29151:2022	Clause 9.2.3; Clause 9.4.2; Clause 11.1.3	Both	Supporting	Piekļuves un fiziskās ieejas kontroles pasākumi
ISO/IEC 27002:2022	Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15	Both	Supporting	PII, fiziskā uzraudzība, piekļuves ierobežošana un žurnālu veidošana

1. Piemērošanas joma

1.1 Šī politika attiecas uz CCTV, videonovērošanu, apmeklētāju uzraudzību, fiziskās piekļuves kontroles žurnāliem, apsardzes veiktiem uzraudzības ierakstiem, telpu un objektu uzraudzības sistēmām un saistītām fiziskās uzraudzības darbībām, kuru ietvaros tiek vākta vai citādi apstrādāta PII.

1.2 Šī politika attiecas uz organizācijām, kas darbojas kā PII pārziņi attiecībā uz savām telpām un fiziskās uzraudzības darbībām.

1.3 Šī politika attiecas arī uz apstrādātāja vai apakšapstrādātāja atbalsta darbībām, ja organizācija klienta vārdā ekspluatē, mitina, pārskata, glabā, izpauž, dzēš vai citādi apstrādā videonovērošanas ierakstus, apmeklētāju datus vai fiziskās piekļuves žurnālus.

1.4 Šī politika aptver uzraudzības nolūka definēšanu, apstiprināšanu, paziņojumus un uzraudzības informatīvās zīmes, piekļuves ierobežojumus, izpaušanu, glabāšanu, dzēšanu, ārpakalpojumu izmantošanu, incidentu eskalāciju, datu subjekta tiesību īstenošanas pieprasījumu maršrutēšanu, pārskatīšanu un pierādījumu pārvaldību.

1.5 Šī politika nesniedz konsultācijas darba tiesību jomā, juridiskus komentārus par darbinieku padomēm, tiesībaizsardzības procedūras vai atsevišķu CCTV reģistru.

1.6 Uzraudzībai specifiskie pierādījumi tiek uzturēti šajā politikā identificētajos kanoniskajos PIMS pierādījumu objektos.

2. Mērķis

2.1 Šīs politikas mērķis ir noteikt privātuma kontroles pasākumus CCTV un fiziskajai uzraudzībai, lai uzraudzības darbības būtu mērķtiecīgas, pārredzamas, samērīgas, ar kontrolētu piekļuvi, glabātas noteiktos termiņos, izpaustas tikai pa apstiprinātiem kanāliem un pamatotas ar auditējamiem PIMS pierādījumiem.

2.2 Šī politika atbalsta konsekventu videonovērošanas ierakstu, apmeklētāju ierakstu, fiziskās piekļuves žurnālu un saistītās uzraudzības PII apstrādi, neradot papildu reģistrus, komitejas, informācijas paneļus vai nekanoniskas lomas.

3. Mērķi

3.1 Šīs politikas mērķi ir:

3.1.1 definēt uzraudzības nolūkus un apstrādes tvērumu pirms uzraudzības sākšanas;

3.1.2 dokumentēt CCTV, fiziskās piekļuves, apmeklētāju uzraudzības un fiziskās uzraudzības darbības REG02;

3.1.3 identificēt uzraudzības darbības, kurām REG04 ir nepieciešama privātuma riska pārskatīšana vai DPIA sākotnējā izvērtēšana;

3.1.4 uzturēt pārredzamu paziņojumu un uzraudzības informatīvo zīmju pierādījumus REG07;

3.1.5 ierobežot piekļuvi uzraudzības PII, tās skatīšanu, eksportēšanu, izpaušanu un glabāšanu;

3.1.6 maršrutēt datu subjekta tiesību īstenošanas pieprasījumus caur REG06;

3.1.7 pārvaldīt ārpakalpojuma uzraudzības sniedzējus un datu koplietošanas pierādījumus caur REG08;

3.1.8 eskalēt aizdomas par ar uzraudzību saistītiem PII incidentiem caur REG10;

3.1.9 reģistrēt pārskatīšanas, izņēmumus, neatbilstības, korektīvās darbības, audita konstatējumus un uzlabojumus REG12.

4. Politikas prasības

4.1 Uzraudzības uzskaite, nolūks un apstiprināšana

4.1.1 [Controller] Process Owner / Business Owner ir jāreģistrē katra CCTV, apmeklētāju uzraudzības, fiziskās piekļuves kontroles žurnāla vai fiziskās uzraudzības darbība REG02 pirms darbības sākšanas.

4.1.2 [Controller] Privacy Lead / PIMS Manager ir jāvalidē REG02 ieraksts attiecībā uz nolūku, tiesisko pamatu, uzraudzīto atrašanās vietu, PII kategorijām, datu subjektu kategorijām, glabāšanu, paziņojumu, piekļuvi un izpaušanas laukiem pirms jaunas vai būtiski mainītas uzraudzības darbības aktivizēšanas.

4.1.3 [Controller] Process Owner / Business Owner ir jāreģistrē apstiprinātās uzraudzītās zonas, izslēgtās zonas un vākšanas robežas REG02 pirms kameru, sensoru, apmeklētāju žurnālu vai piekļuves kontroles žurnālu veidošanas iespējošanas.

4.1.4 [Conditional] Process Owner / Business Owner ir jāsaņem REG04 privātuma riska lēmums pirms tādas uzraudzības aktivizēšanas, kas ietver sistemātisku uzraudzību, audioierakstīšanu, biometrisku identifikāciju, ar analītiku iespējotu detektēšanu, sensitīvas atrašanās vietas, mazaizsargātas personas vai neacīmredzamu uzraudzību.

4.1.5 [Joint Controller] Privacy Lead / PIMS Manager ir jāreģistrē kopīgas uzraudzības atbildības sadalījums REG08 pirms kopīgas uzraudzības sākšanas ar iznomātāju, objektu apsaimniekošanas partneri, klientu vai citu kopīgu pārzini.

4.1.6 [Processor] Privacy Lead / PIMS Manager ir jāreģistrē klienta uzraudzības norādījumi un atļautās apstrādes robežas REG08 pirms videonovērošanas ierakstu, apmeklētāju ierakstu vai fiziskās piekļuves žurnālu apstrādes klienta vārdā.

4.2 Paziņojumi un pārredzamība

4.2.1 [Controller] Process Owner / Business Owner ir jānodrošina, ka uzraudzības informatīvo zīmju vai līdzvērtīga just-in-time paziņojuma pierādījumi tiek reģistrēti REG07 pirms uzraudzīto zonu atvēršanas datu subjektiem.

4.2.2 [Controller] Privacy Lead / PIMS Manager ir jāsaista katrs uzraudzības paziņojums REG07 ar attiecīgo REG02 apstrādes nolūku pirms publicēšanas vai būtiskas izmaiņas.

4.2.3 [Processor] Privacy Lead / PIMS Manager ir jāsniedz uzraudzības paziņojuma atbalsta informācija REG08, ja organizācija sniedz uzraudzības pakalpojumus saskaņā ar klienta norādījumiem.

4.2.4 [Conditional] Process Owner / Business Owner ir jāreģistrē alternatīvi pārredzamības pasākumi REG07 un REG04 pirms neacīmredzamas vai ārkārtas uzraudzības aktivizēšanas.

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

9. Izņēmumi

9.1 [All] Privacy Lead / PIMS Manager ir jāreģistrē katrs izņēmums no šīs politikas REG12 pirms izņēmuma izmantošanas.

9.2 [Conditional] Data Protection Officer / Privacy Advisor ir jādokumentē privātuma konsultācijas REG04 vai REG12 pirms tādu izņēmumu apstiprināšanas, kas ietver neacīmredzamu uzraudzību, audioierakstīšanu, biometrisku identifikāciju, ar analītiku iespējotu uzraudzību vai sensitīvas uzraudzības atrašanās vietas.

9.3 [All] Top Management ir jāapstiprina izņēmumi, kas pārsniedz 90 dienas, REG12 pirms pagarināšanas pēc sākotnējā izņēmuma perioda.

9.4 [All] Privacy Lead / PIMS Manager ir jāpārskata atvērtie uzraudzības izņēmumi REG12 vismaz reizi mēnesī līdz slēgšanai.

10. Piemērošana

10.1 [All] Privacy Lead / PIMS Manager ir jāreģistrē uzraudzības kontroles pasākumu kļūmes kā neatbilstības REG12 piecu darbdienu laikā pēc apstiprināšanas.

10.2 [Both] Information Security Lead ir jāaptur nesankcionēta piekļuve uzraudzības sistēmai vienas darbdienas laikā pēc apstiprināšanas un jāreģistrē darbība REG10 vai REG12.

10.3 [All] Top Management ir jāpiešķir korektīvās darbības īpašumtiesības REG12 10 darbdienu laikā atkārtotu vai būtisku politikas pārkāpumu gadījumā.

10.4 [Conditional] Incident Response Coordinator ir jāuzsāk PII incidenta darbplūsma REG10, ja pastāv aizdomas par uzraudzības PII nesankcionētu izpaušanu, zudumu vai kompromitēšanu.

11. Pārskatīšana un uzturēšana

11.1 [All] Privacy Lead / PIMS Manager ir jāpārskata šī politika un saistītie uzraudzības pierādījumi REG12 vismaz reizi gadā.

11.2 [Controller] Process Owner / Business Owner ir atkārtoti jāvalidē katrs aktīvais uzraudzības nolūks, paziņojums, atrašanās vietas tvērums un glabāšanas ieraksts REG02 un REG07 vismaz reizi gadā.

11.3 [Both] System Owner / Application Owner ir atkārtoti jāvalidē uzraudzības sistēmas piekļuves, žurnālu veidošanas, dzēšanas un eksportēšanas kontroles pasākumi REG12 vismaz reizi gadā un pēc būtiskas sistēmas izmaiņas.

11.4 [Conditional] Vendor / Procurement Owner ir atkārtoti jāvalidē ārpakalpojuma uzraudzības pakalpojumu sniedzēju pierādījumi REG08 vismaz reizi gadā un pirms līguma atjaunošanas.

11.5 [All] Privacy Lead / PIMS Manager ir jāatjaunina saistītie REG02, REG04, REG07, REG08, REG10 vai REG12 pierādījumi 30 kalendāro dienu laikā pēc apstiprinātām politikas izmaiņām.

12. Saistītās politikas

12.1 PII02 - Privātuma lomu, pienākumu un pārskatatbildības politika

12.2 PII03 - PII apstrādes uzskaites un tiesiskā pamata politika

12.3 PII04 - Privātuma paziņojumu un pārredzamības politika

12.4 PII06 - Datu subjektu tiesību pārvaldības politika

12.5 PII07 - Privātuma risku izvērtēšanas un DPIA politika

12.6 PII08 - Datu aizsardzības pēc projektēšanas un pēc noklusējuma politika

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

12.8 PII10 - PII glabāšanas, dzēšanas un likvidēšanas politika

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

12.10 PII13 - Starptautiskas PII nosūtīšanas politika

12.11 PII14 - PII drošības un piekļuves kontroles politika

12.12 PII15 - PII incidentu un pārkāpumu pārvaldības politika

12.13 PII17 - PIMS dokumentētas informācijas un pierādījumu pārvaldības politika

12.14 PII18 - PIMS uzraudzības, audita un uzlabošanas politika

12.15 PII19 - Darbinieku privātuma politika

12.16 PII21 - Mākslīgā intelekta un automatizētas lēmumu pieņemšanas privātuma politika

12.17 PII23 - Mākoņvides PII apstrādātāja politika

13. Atsauces standarti un ietvari

13.1 Šī politika ir sasaistīta ar šādiem standartiem un regulējumiem. Sasaistījums skaidro, kā politika atbalsta norādītās prasības, un identificē iekšējos punktus, ar kuriem tās tiek ieviestas vai atbalstītas.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Sasaistīts ar dokumentētiem uzraudzības pierādījumiem, operacionālo plānošanu, aktivizēšanas kontroles pasākumiem, nolūka ierakstiem, paziņojumu sasaisti, piekļuves konfigurāciju, glabāšanas konfigurāciju un izmaiņu kontroli CCTV un fiziskās uzraudzības darbībām. Addressed by clauses [4.1.1; 4.1.2; 4.2.2; 4.3.1; 4.4.1; 6.2; 7.1; 11.5].

13.2.2 **Clause 9.1; Clause 10.2** - Sasaistīts ar uzraudzības kontroles pasākumu mērīšanu, pakalpojumu sniedzēju pārskatīšanu, piekļuves pārskatīšanu, audita konstatējumiem, neatbilstībām, korektīvajām darbībām, kavētu darbību eskalāciju un uzlabojumu pierādījumiem. Addressed by clauses [4.6.4; 6.4; 6.5; 6.6; 8.1; 8.7; 10.1; 11.1].

13.2.3 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9** - Sasaistīts ar pārziņa veiktu uzraudzības nolūka definēšanu, tiesiskā pamata dokumentēšanu, privātuma riska trigera lēmumiem un uzraudzības apstrādes darbību ierakstiem REG02 un REG04. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.4.1; 6.2; 7.1; 11.2].

13.2.4 **Annex A.1.2.7; Annex A.1.2.8** - Sasaistīts ar ārpakalpojuma uzraudzības pakalpojumu sniedzēju atbildības sadalījumu, kopīgas uzraudzības atbildības sadalījumu un apstrādātāja vai kopīga pārziņa pierādījumiem REG08. Addressed by clauses [4.1.5; 4.6.1; 4.6.2; 5.7; 6.2; 7.6].

13.2.5 **Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10** - Sasaistīts ar uzraudzību saistītiem datu subjektu pienākumiem, pieprasījumu maršrutēšanu, saglabāšanu, kas nepieciešama pieprasījumu izvērtēšanai, un pārvaldības pierādījumiem tiesību atbalstam. Addressed by clauses [4.5.1; 4.5.2; 5.2; 7.2; 11.5].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9** - Sasaistīts ar uzraudzības vākšanas ierobežošanu, apstrādes robežām, minimizēšanu, glabāšanas termiņiem, dzēšanu, pārrakstīšanu, glabāšanas aizturēšanu un izvilkto kopiju kontroli. Addressed by clauses [4.1.3; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 7.3; 7.5; 8.4].

13.2.7 **Annex A.1.5.4; Annex A.1.5.5** - Sasaistīts ar ārējas izpaušanas ierakstiem, izpaušanas pieprasījumu apstrādi, minimizēšanu pirms izpaušanas un ar incidentiem saistītu izpaušanu, kas ietver uzraudzības PII. Addressed by clauses [4.3.4; 4.5.4; 7.8; 10.4].

13.2.8 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7** - Sasaistīts ar apstrādātāja klienta norādījumiem, atļautajām apstrādes robežām, paziņojumu atbalstu, glabāšanas un dzēšanas norādījumiem, palīdzību tiesību īstenošanā un apstrādātāja ierakstiem ārpakalpojuma uzraudzības pakalpojumiem. Addressed by clauses [4.1.6; 4.2.3; 4.4.5; 4.5.3; 4.6.3].

13.2.9 **Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Sasaistīts ar apstrādātāja atbalstu klienta pienākumiem, izpaušanas atļauju, izpaušanas ierakstiem, paziņošanu par izpaušanas pieprasījumiem un juridiski saistošu izpaušanas apstrādi attiecībā uz uzraudzības PII. Addressed by clauses [4.3.5; 4.5.3; 4.6.2; 4.6.3].

13.2.10 **Annex A.3.14; Annex A.3.25** - Sasaistīts ar uzraudzības ierakstu aizsardzību, ierobežotu piekļuvi, privileģētās piekļuves pārskatīšanu, piekļuves žurnālu veidošanu, nesankcionētas piekļuves ierobežošanu un uzraudzības sistēmu žurnālu pierādījumiem. Addressed by clauses [4.3.2; 4.3.3; 4.5.5; 5.4; 7.4; 10.2; 11.3].

13.3 GDPR

13.3.1 **Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)** - Sasaistīts ar likumību, godprātību, pārredzamību, nolūka ierobežošanu, datu minimizēšanu, glabāšanas ierobežošanu un pārskatatbildības pierādījumiem uzraudzības darbībām. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.4.1; 4.4.2; 4.4.3; 6.1; 8.1; 11.2].

13.3.2 Article 6 - Sasaistīts ar tiesiskā pamata dokumentēšanu CCTV, apmeklētāju uzraudzībai, fiziskās piekļuves žurnāliem un citām fiziskās uzraudzības darbībām. Addressed by clauses [4.1.2; 4.1.4; 7.1].

13.3.3 **Article 12; Article 13; Article 14** - Sasaistīts ar pārredzamiem uzraudzības paziņojumiem, uzraudzības informatīvo zīmju pierādījumiem, paziņojumu sasaisti ar apstrādes nolūkiem, apstrādātāja paziņojumu atbalsta informāciju un alternatīviem pārredzamības pasākumiem. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 7.2; 8.2; 11.2].

13.3.4 **Article 15; Article 16; Article 17; Article 18; Article 21** - Sasaistīts ar piekļuvi, labošanu, dzēšanu, ierobežošanu, iebildumiem, pieprasījumu maršrutēšanu, saglabāšanu, kas nepieciešama pieprasījumu izvērtēšanai, un ar uzraudzību saistītu klienta atbalstu. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 7.8; 11.5].

13.3.5 **Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39** - Sasaistīts ar pārziņa pārvaldību, kopīga pārziņa atbildības sadalījumu, apstrādātāja pārvaldību, apstrādes ierakstiem, uzraudzības sistēmu drošību, privātuma riska pārskatīšanu, DPIA trigeriem un privātuma konsultācijām. Addressed by clauses [4.1.4; 4.1.5; 4.1.6; 4.3.2; 4.3.3; 4.5.4; 4.6.1; 4.6.2; 4.6.4; 5.1; 5.3; 6.3; 8.5; 10.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Sasaistīts ar nolūka noteikšanu, vākšanas ierobežošanu, datu minimizēšanu, izmantošanas ierobežošanu, glabāšanas ierobežošanu un izpaušanas ierobežošanu attiecībā uz uzraudzības PII. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.4; 4.4.1; 4.4.2; 4.4.4; 7.8].

13.4.2 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12** - Sasaistīts ar pārredzamību, individuālu līdzdalību, pārskatatbildību, informācijas drošību, atbilstības pārskatīšanu, piekļuves pārskatīšanu, tiesību īstenošanas pieprasījumu maršrutēšanu, incidentu eskalāciju un korektīvo darbību pierādījumiem. Addressed by clauses [4.2.1; 4.2.2; 4.3.2; 4.3.3; 4.5.1; 4.5.4; 6.1; 8.7; 10.1].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 5.1; Clause 6.2** - Sasaistīts ar privātuma riska un DPIA trigera sākotnējo izvērtēšanu sistemātiskai, neacīmredzamai, audio, biometriskai, ar analītiku iespējotai, sensitīvas atrašanās vietas, mazaizsargātu personu vai citai augstāka riska fiziskai uzraudzībai. Addressed by clauses [4.1.4; 4.2.4; 5.3; 6.3; 7.5; 9.2].

13.6 ISO/IEC 29151:2022

13.6.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10** - Sasaistīts ar PII aizsardzības kontroles pasākumiem attiecībā uz nolūku, vākšanu, minimizēšanu, glabāšanu, izpaušanu un datu subjektu līdzdalību uzraudzības kontekstos. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.4.1; 4.4.3; 4.5.1; 7.2; 8.2].

13.6.2 **Clause 9.2.3; Clause 9.4.2; Clause 11.1.3** - Sasaistīts ar piekļuves piešķiršanu, informācijas piekļuves ierobežošanu un fiziskās ieejas kontroles pasākumiem, kas attiecas uz piekļuvi uzraudzības sistēmām un fiziskās piekļuves kontroles ierakstiem. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.5.5; 5.4; 7.4; 10.2; 11.3].

13.7 ISO/IEC 27002:2022

13.7.1 Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15 - Sasaistīts ar PII privātumu un aizsardzību, fizisko ieeju, fiziskās drošības uzraudzību, privileģēto piekļuvi, informācijas piekļuves ierobežošanu un žurnālu veidošanas kontroles pasākumiem CCTV un fiziskās uzraudzības sistēmām. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.5.5; 5.4; 7.3; 7.4; 8.3; 10.2; 11.3].