					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: PII16					Dokumenta nosaukums: **Privātuma apmācības, informētības un kompetences 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 7.2; Clause 7.3	Both	Primary	Kompetence un informētība
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Komunikācija un dokumentēti pierādījumi
ISO/IEC 27701:2025	Clause 8.1; Clause 9.1; Clause 10.2	Both	Supporting	Darbības kontroles pasākumi, mērīšana un uzlabošana
ISO/IEC 27701:2025	Annex A.3.17	Both	Primary	Informētība, izglītošana un apmācība par PII apstrādi
GDPR	Article 5(2); Article 24; Article 28; Article 32; Article 39	Both	Supporting	Pārskatatbildība, apstrādātāju pārvaldība, drošība un DPO uzdevumi
ISO/IEC 27001:2022	Clause 7.2; Clause 7.3; Annex A control 6.3	Both	Supporting	Kompetence, informētība un apmācība
ISO/IEC 27002:2022	Control 6.3	Both	Supporting	Norādījumi par informētību, izglītošanu un apmācību
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Informācijas drošības un privātuma atbilstība

1. Piemērošanas joma

1.1 Šī politika nosaka organizācijas prasības privātuma apmācībām, informētībai un kompetencei privātuma informācijas pārvaldības sistēmā.

1.2 Šī politika attiecas uz personālu, līgumslēdzējiem, pagaidu darbiniekiem, attiecīgām trešajām pusēm, apstrādātājiem, apakšapstrādātājiem un citām ieinteresētajām pusēm, kuru darbs var ietekmēt PII apstrādi, PIMS veiktspēju, datu subjekta tiesības, privātuma risku, ar PII saistītu informācijas drošību, apstrādātāja norādījumus, privātuma incidentus, dokumentēto informāciju vai atbilstības pierādījumus.

1.3 Šī politika attiecas uz pārziņa, kopīga pārziņa, apstrādātāja un apakšapstrādātāja kontekstiem.

1.4 Šī politika aptver:

1.4.1 privātuma apmācību mērķauditorijas noteikšanu;

1.4.2 ievadapmācību;

1.4.3 ikgadējo atkārtoto apmācību;

1.4.4 uz lomām balstītu un notikumu ierosinātu apmācību;

1.4.5 apmācību pabeigšanas pierādījumus;

1.4.6 nepabeigšanas eskalāciju;

1.4.7 apmācību efektivitātes pārskatīšanu;

1.4.8 apstrādātāju, apakšapstrādātāju un trešo pušu apmācību apliecinājuma pierādījumus.

1.5 Šī politika neveido atsevišķu apmācību matricu, apmācību informācijas paneli, cilvēkresursu reģistru, kompetences reģistru, disciplināro reģistru vai klientu apmācību reģistru. Apmācību piešķīrumi, pabeigšana, atgādinājumi, kompetences pierādījumi un informētības pierādījumi tiek reģistrēti REG11, savukārt izņēmumi, eskalācijas, neatbilstības, korektīvās darbības un pārskatīšanas pierādījumi tiek reģistrēti REG12. Apstrādātāju, apakšapstrādātāju un trešo pušu apmācību apliecinājuma pierādījumi attiecīgajos gadījumos tiek reģistrēti REG08.

1.6 Šī politika nedublē:

1.6.1 lomu pārskatatbildības piešķiršanu PII02;

1.6.2 apstrādes uzskaites un tiesiskā pamata prasības PII03;

1.6.3 privātuma riska un DPIA metodoloģiju PII07;

1.6.4 integrētās datu aizsardzības kontrolpunktus PII08;

1.6.5 apstrādātāja dzīves cikla pārvaldību PII12;

1.6.6 PII drošības un piekļuves kontroles darbību PII14;

1.6.7 PII incidentu un pārkāpumu darbplūsmu PII15;

1.6.8 dokumentētās informācijas pārvaldību PII17;

1.6.9 uzraudzības, iekšējā audita un uzlabošanas pārvaldību PII18.

2. Mērķis

2.1 Šīs politikas mērķis ir nodrošināt, ka personas, kuru darbs ietekmē PII apstrādi, izprot savus privātuma pienākumus, pabeidz atbilstošas apmācības noteiktā periodiskumā, uztur lomai atbilstošu kompetenci un rada auditējamus pierādījumus par apmācībām, informētību un eskalāciju.

2.2 Šī politika atbalsta konsekventu PIMS ieviešanu, izmantojot REG11 kā galveno apmācību un informētības pierādījumu objektu un REG08, REG10 un REG12 kā atbalsta pierādījumu objektus.

3. Mērķi

3.1 Šīs politikas mērķi ir:

3.1.1 definēt privātuma apmācību mērķauditorijas;

3.1.2 definēt ievadapmācību prasības;

3.1.3 definēt ikgadējās atkārtotās apmācības prasības;

3.1.4 definēt uz lomām balstītas privātuma apmācības prasības;

3.1.5 reģistrēt pabeigšanas pierādījumus REG11;

3.1.6 eskalēt nepabeigšanu, izmantojot REG12;

3.1.7 attiecīgajos gadījumos uzturēt apstrādātāju, apakšapstrādātāju un trešo pušu apmācību apliecinājuma pierādījumus REG08;

3.1.8 pārskatīt apmācību efektivitāti, neveidojot pārmērīgu metriku vai dublējošus reģistrus;

3.1.9 nodrošināt, ka apmācību saturs saglabā atbilstību aktuālajām PIMS politikām un būtiskajiem privātuma pienākumiem.

4. Politikas paziņojumi

4.1 Apmācību mērķauditorija un piešķiršana

4.1.1 [All] Privacy Lead / PIMS Manager ir jādefinē PIMS apmācību mērķauditorijas kategorijas REG11 pirms katra ikgadējā apmācību cikla sākuma.

4.1.2 [All] Process Owner / Business Owner ir jāidentificē personāls, kura pienākumi ietver PII apstrādi, REG11 pirms ievadīšanas, lomas piešķiršanas vai būtiskas pienākumu maiņas.

4.1.3 [Conditional] System Owner / Application Owner ir jāidentificē lietotāji, kuriem nepieciešama PII sistēmas, privileģētas piekļuves vai administratīvā privātuma apmācība, REG11 pirms piekļuves iespējošanas vai būtiskas maiņas.

4.1.4 [Joint Controller] Privacy Lead / PIMS Manager ir jāreģistrē kopīgo pārziņu apmācību atbildības sadalījums REG11 vai REG08 pirms kopīgas apstrādes darbības sākuma vai būtiskas maiņas.

4.1.5 [Conditional] Data Protection Officer / Privacy Advisor ir jāidentificē pastiprinātas privātuma apmācības vajadzības REG11 pirms apmācības piešķiršanas lomām, kas veic augsta riska apstrādi, īpašu kategoriju personas datu apstrādi, datu subjekta tiesību īstenošanu, DPIAs, starptautisku personas datu nosūtīšanu vai pārkāpuma izvērtēšanu.

4.1.6 [All] Privacy Lead / PIMS Manager ir jāreģistrē piešķirtā apmācību mērķauditorija, apmācību veids, obligātais pabeigšanas datums un pierādījumu īpašnieks REG11 pirms katra ikgadējā apmācību cikla sākuma.

4.2 Ievadapmācības un ikgadējo apmācību periodiskums

4.2.1 [All] Privacy Lead / PIMS Manager ir jāpiešķir pamata privātuma informētības apmācība REG11 10 darba dienu laikā pēc ievadīšanas personālam, kam ir piekļuve PII vai PIMS pienākumi.

4.2.2 [All] Process Owner / Business Owner ir jānodrošina, ka piešķirtais personāls pabeidz ievadapmācību privātuma jomā REG11 pirms neuzraudzītas piekļuves PII apstiprināšanas vai 30 dienu laikā pēc ievadīšanas atkarībā no tā, kas notiek agrāk.

4.2.3 [All] Privacy Lead / PIMS Manager ir jāpiešķir ikgadējā privātuma atkārtotā apmācība REG11 vismaz reizi 12 mēnešos.

4.2.4 [All] Process Owner / Business Owner ir jāapstiprina piešķirtā personāla ikgadējās atkārtotās apmācības pabeigšanas statuss REG11 līdz publicētajam ikgadējam termiņam.

4.2.5 [Conditional] Privacy Lead / PIMS Manager ir jāpiešķir mērķtiecīga atkārtota apmācība REG11 30 dienu laikā pēc būtiskām privātuma politikas izmaiņām, būtiskām PIMS procesa izmaiņām, audita konstatējuma, atkārtotas apmācību neizpildes vai attiecīgas PII incidenta mācības.

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

9. Izņēmumi

9.1.1 [All] Process Owner / Business Owner ir jāreģistrē privātuma apmācības izņēmuma pieprasījums REG12 pirms obligātā pabeigšanas termiņa pagarināšanas.

9.1.2 [All] Privacy Lead / PIMS Manager ir jāapstiprina vai jānoraida privātuma apmācības izņēmuma pieprasījumi REG12 pirms izņēmums kļūst aktīvs.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor ir jāsniedz padomi par apmācību izņēmumiem REG12 pirms apstiprināšanas, ja izņēmums ietekmē augsta riska apstrādi, īpašu kategoriju personas datus, tiesību īstenošanu, incidentu apstrādi, starptautisku nosūtīšanu vai sertifikācijas pierādījumus.

9.1.4 [Conditional] Top Management ir jāapstiprina privātuma apmācības izņēmumi REG12 pirms aktivizēšanas, ja izņēmums ietekmē atkārtotu nepabeigšanu, privileģētu PII piekļuvi, augstas ietekmes PII apstrādi vai regulatoram iesniedzamus pierādījumus.

9.1.5 [All] Privacy Lead / PIMS Manager ir jādefinē izņēmuma īpašnieks, termiņa beigu datums, kompensējošā darbība un pārskatīšanas datums REG12 pirms jebkura privātuma apmācības izņēmuma apstiprināšanas.

9.1.6 [All] Process Owner / Business Owner ir jāslēdz vai jāatjauno apstiprinātie privātuma apmācības izņēmumi REG12 pirms izņēmuma termiņa beigām.

10. Piemērošana

10.1.1 [All] Privacy Lead / PIMS Manager ir jāreģistrē apmācību neatbilstība REG12 piecu darba dienu laikā, ja obligātās privātuma apmācības pierādījumi trūkst, ir nepilnīgi, kavēti vai nav izsekojami līdz REG11.

10.1.2 [All] Process Owner / Business Owner ir jānodrošina, ka kavēta obligātā privātuma apmācība tiek pabeigta vai eskalēta REG11 vai REG12 10 darba dienu laikā pēc kavējuma statusa reģistrēšanas.

10.1.3 [Conditional] System Owner / Application Owner ir jāierobežo jauna augstas ietekmes PII piekļuve REG12, ja obligātā ievadapmācība vai uz lomām balstītā privātuma apmācība pēc eskalācijas joprojām nav pabeigta.

10.1.4 [Processor] Vendor / Procurement Owner ir jāeskalē trūkstoši apstrādātāja, apakšapstrādātāja vai ārējā darbaspēka apmācību apliecinājuma pierādījumi REG08 un REG12 piecu darba dienu laikā pēc identificēšanas.

10.1.5 [Conditional] Incident Response Coordinator ir jāsasaista ar apmācībām saistītās piemērošanas darbības ar REG10 vienas darba dienas laikā, ja apmācību neizpilde veicināja aizdomas par PII incidentu vai apstiprinātu PII incidentu.

10.1.6 [All] Internal Audit / Compliance Reviewer ir jāpārbauda apmācību korektīvo darbību slēgšanas pierādījumi REG12 nākamajā plānotajā auditā vai 60 dienu laikā pēc slēgšanas atkarībā no tā, kas notiek agrāk.

11. Pārskatīšana un uzturēšana

11.1.1 [All] Privacy Lead / PIMS Manager ir jāpārskata šī politika un apmācību saturs vismaz reizi gadā un jāreģistrē pārskatīšanas rezultāts REG11 vai REG12.

11.1.2 [All] Privacy Lead / PIMS Manager ir jāpārskata šī politika 30 dienu laikā pēc būtiskām izmaiņām PIMS darbības jomā, privātuma tiesību aktos, apstrādes darbībās, lomu modelī, incidentu mācībās, audita konstatējumos vai apmācību efektivitātes rezultātos.

11.1.3 [Conditional] Data Protection Officer / Privacy Advisor ir jāpārskata privātumam nozīmīgas politikas izmaiņas REG12 pirms apstiprināšanas.

11.1.4 [All] Top Management ir jāapstiprina būtiskas šīs politikas izmaiņas REG12 pirms publicēšanas.

11.1.5 [All] Privacy Lead / PIMS Manager ir jāatjaunina REG11 apmācību saturs un piešķīrumu pierādījumi 30 dienu laikā pēc apstiprinātām būtiskām politikas izmaiņām.

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 paziņojumu un pārredzamības politika;

12.6 PII05 - Piekrišanas un preferenču pārvaldības politika;

12.7 PII06 - Datu subjekta tiesību pārvaldības politika;

12.8 PII07 - Privātuma risku izvērtēšanas un DPIA politika;

12.9 PII08 - Datu aizsardzības pēc projektēšanas un pēc noklusējuma politika;

12.10 PII09 - PII vākšanas, izmantošanas, izpaušanas un koplietošanas politika;

12.11 PII10 - PII glabāšanas, dzēšanas un likvidēšanas 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 dokumentētās informācijas un pierādījumu pārvaldības politika;

12.17 PII18 - PIMS uzraudzības, audita un uzlabošanas politika.

13. Atsauces standarti un ietvari

13.1 ISO/IEC 27701:2025 - Clause 7.2; Clause 7.3; Clause 7.4. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 7.1.1; 7.1.2; 7.1.3; 11.1.1; 11.1.5].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.4; 4.6.5; 6.1.1; 6.1.2; 6.1.3; 6.1.5; 7.1.7; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 9.1.1; 9.1.2; 9.1.5; 10.1.1; 10.1.2; 10.1.6; 11.1.1; 11.1.2; 11.1.4].

13.3 ISO/IEC 27701:2025 - Annex A.3.17. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 11.1.5].

13.4 GDPR - Article 5(2); Article 24; Article 28; Article 32; Article 39. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.4.4; 4.5.3; 4.5.4; 4.5.5; 5.1.1; 5.1.3; 5.1.7; 6.1.2; 6.1.3; 6.1.4; 7.1.4; 7.1.5; 9.1.3; 9.1.4; 10.1.3; 10.1.4; 10.1.5; 11.1.3].

13.5 ISO/IEC 27001:2022 - Clause 7.2; Clause 7.3; Annex A control 6.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.3; 4.3.1; 4.3.5; 4.4.1; 4.4.3; 4.5.1; 4.5.2; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 6.1.1; 7.1.1; 7.1.2; 8.1.1; 8.1.2; 8.1.3; 11.1.1].

13.6 ISO/IEC 27002:2022 - Control 6.3. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 10.1.2].

13.7 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.5.5; 4.6.4; 4.6.5; 5.1.3; 6.1.2; 6.1.3; 6.1.5; 8.1.5; 9.1.3; 10.1.1; 10.1.6; 11.1.2].