

				Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: PII19				Dokumenta nosaukums: <b>Darbinieku privātuma politika</b>							
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><b>Juridiskais paziņojums (autortiesības un lietošanas ierobežojumi)</b>  (C) 2025 Clarysec LLC. All rights reserved.</p> <p>Šis dokuments ir Clarysec LLC intelektuālais īpašums. Nevienam 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: <a href="mailto:info@clarysec.com">info@clarysec.com</a></p>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## 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	Darbinieku privātuma pierādījumi un darbības kontroles pasākumi
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Uzraudzība, neatbilstības un korektīvās darbības
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9	Controller	Primary	Personālvadības nolūki, sasaiste ar tiesisko pamatu, DPIA trigeris, kopīga atbildība un ieraksti
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Both	Supporting	Personālvadības apstrādātāju līgumi, norādījumi, palīdzība un ieraksti
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11	Controller	Supporting	Darbinieku pienākumi, tiesības un automatizētu lēmumu maršrutēšana
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	Vākšanas, apstrādes, minimizēšanas un glabāšanas sasaistes prasības
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Both	Supporting	Izpaušanas ieraksti un juridiski saistošas izpaušanas apstrāde
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Personālvadības ierakstu aizsardzība un žurnālfiksēšanas pierādījumi
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c);	Controller	Primary	Darbinieku privātuma principi un pārskatbildība

	Article 5(1)(e); Article 5(2)			
GDPR	Article 6; Article 9; Article 10	Controller	Supporting	Likumīgums, īpašu kategoriju dati un fona pārbaudes dati
GDPR	Article 12; Article 13; Article 14	Controller	Primary	Darbinieku informēšana un paziņojumi
GDPR	Article 15; Article 16; Article 17; Article 18; Article 21; Article 22	Controller	Supporting	Darbinieku tiesības un automatizētu lēmumu maršrutēšana
GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Pārvaldība, kopīgi pārziņi, apstrādātāji, ieraksti, drošība, DPIA un konsultēšana
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Controller	Supporting	Nolūks, vākšana, minimizēšana, izmantošana, 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 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Controller	Supporting	PII nolūks, vākšana, minimizēšana, glabāšana un datu subjekta līdzdalība
ISO/IEC 29151:2022	Clause 7.1.2; Clause 7.1.3; Clause 7.2.4; Clause 7.3.2	Controller	Supporting	Darbinieku dzīves cikla kontroles pasākumi PII aizsardzībai
ISO/IEC 29151:2022	Clause 15.1.2; Clause 15.2.2; Clause 15.2.3	Both	Supporting	Personālvadības apstrādātāju izvērtēšana, uzraudzība un izmaiņu kontrole
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	Personālvadības privātuma risks un sasaiste ar DPIA trigeri

ISO/IEC 27002:2022	Controls 5.34; 6.1; 6.2; 6.5; 6.6	Both	Supporting	PII aizsardzība un darbaspēka informācijas drošības dzīves cikls
ISO/IEC 27002:2022	Controls 8.15; 8.16	Both	Supporting	Žurnālfiksēšanas un uzraudzības darbības

## 1. Piemērošanas joma

- 1.1 Šī politika nosaka darbinieku privātuma prasības attiecībā uz darbinieku personas datu vākšanu, izmantošanu, izpaušanu, glabāšanas sasaisti, paziņojumiem, tiesību pieprasījumu apstrādi, uzraudzību, apstrādātāju atbalstu un pierādījumu pārvaldību privātuma informācijas pārvaldības sistēmā.
- 1.2 Šajā politikā "darbinieku personas dati" ietver PII, kas attiecas uz darbiniekiem, darba pretendentiem, bijušajiem darbiniekiem, līgumslēdzējiem, pagaidu personālu, praktikantiem, norīkotajiem darbiniekiem un citiem darbaspēka dalībniekiem, ja organizācija apstrādā viņu PII darbaspēka, personāla atlases, nodarbinātības, iesaistes, atlīdzības, labumu, drošības, atbilstības, darba vietas administrēšanas vai saistītu uzņēmējdarbības nolūku vajadzībām.
- 1.3 Šī politika attiecas uz pārziņa un kopīga pārziņa kontekstiem, kuros organizācija nosaka darbinieku personas datu apstrādes nolūkus un līdzekļus.
- 1.4 Šī politika attiecas arī uz apstrādātāja un apakšapstrādātāja kontekstiem, kuros organizācija apstrādā darbinieku personas datus klienta, augšupējā apstrādātāja vai cita pārziņa vārdā saskaņā ar dokumentētiem norādījumiem.

### 1.5 Šī politika aptver šādas darbinieku privātuma prasības:

- 1.5.1 darbinieku datu vākšana;
  - 1.5.2 personālvadības apstrādes nolūki;
  - 1.5.3 darbinieku privātuma paziņojumi;
  - 1.5.4 darbinieku tiesību pieprasījumu apstrāde;
  - 1.5.5 glabāšanas sasaiste;
  - 1.5.6 darbinieku uzraudzība;
  - 1.5.7 iekšēja izpaušana;
  - 1.5.8 attiecīgā gadījumā personālvadības apstrādātāju, algu aprēķina, HRIS, labumu, fona pārbaudes un ārpakalpojumā nodotu personālvadības pakalpojumu kontroles pasākumi;
  - 1.5.9 darbinieku personas datu incidenti, neatbilstības, korektīvās darbības un uzlabošanas pierādījumi.
- 1.6 Šī politika neizveido atsevišķu personālvadības privātuma reģistru, darbinieku privātuma reģistru, personālvadības apstrādes reģistru, darbinieku uzraudzības reģistru, fona pārbaudes reģistru, personālvadības piegādātāju reģistru, darbinieku tiesību reģistru vai darbinieku incidentu reģistru. Darbinieku apstrādes pierādījumi tiek ierakstīti REG02, REG04, REG06, REG07, REG08, REG10 un REG12.
  - 1.7 Šī politika nesniedz darba tiesību konsultācijas, darba attiecību konsultācijas, darbinieku padomes juridiskus komentārus, disciplinārās procedūras saturu, algu aprēķina darbības procedūru saturu vai konkrētai jurisdikcijai paredzētas nodarbinātības dokumentu veidnes.

### 1.8 Šī politika nedublē šādu PIMS saturu:

- 1.8.1 PIMS pārvaldību PII01;
- 1.8.2 lomu pārskatatbildību PII02;
- 1.8.3 apstrādes uzskaiti un atbildību par tiesisko pamatu PII03;
- 1.8.4 privātuma paziņojumu satura pārvaldību PII04;
- 1.8.5 piekrišanas un preferenču darbību PII05;
- 1.8.6 datu subjekta tiesību darbplūsmu PII06;
- 1.8.7 privātuma riska un DPIA metodoloģiju PII07;
- 1.8.8 datu aizsardzības pēc projektēšanas vērtus PII08;
- 1.8.9 vākšanas, izmantošanas, izpaušanas un koplietošanas pamatnoteikumus PII09;

- 1.8.10 glabāšanas, dzēšanas un likvidēšanas izpildi PII10;
- 1.8.11 precizitātes un kvalitātes pārvaldību PII11;
- 1.8.12 apstrādātāju, apakšapstrādātāju un trešo pušu dzīves cikla pārvaldību PII12;
- 1.8.13 starptautiskas nosūtīšanas mehānismu kontroles pasākumus PII13;
- 1.8.14 drošības un piekļuves kontroles ieviešanu PII14;
- 1.8.15 incidentu un pārkāpumu apstrādi PII15;
- 1.8.16 apmācību un informētības pārvaldību PII16;
- 1.8.17 dokumentētas informācijas kontroli PII17;
- 1.8.18 PIMS uzraudzības, audita un uzlabošanas pārvaldību PII18;
- 1.8.19 AI un automatizētas lēmumu pieņemšanas kontroles pasākumus PII21, ja šī izvēles politika ir iekļauta.

## **2. Mērķis**

- 2.1 Šīs politikas mērķis ir nodrošināt, ka darbinieku personas dati tiek apstrādāti tikai dokumentētiem, apstiprinātiem, pārredzamiem, samērīgiem un pārskatatbildīgiem darbaspēka nolūkiem un ka darbinieku privātuma pierādījumi tiek uzturēti kanoniskajos PIMS reģistros, neveidojot atsevišķu personālvadības privātuma pierādījumu slāni.
- 2.2 Šī politika atbalsta konsekvētu darbinieku apstrādes pārvaldību, sasaistot darbinieku apstrādes darbības ar REG02, darbinieku privātuma paziņojumus ar REG07, darbinieku tiesību pieprasījumus ar REG06, personālvadības privātuma risku un DPIA triggerus ar REG04, personālvadības apstrādātājus un algu aprēķina vai HRIS piegādātājus ar REG08, darbinieku personas datu incidentus ar REG10 un izņēmumus, neatbilstības, korektīvās darbības un uzraudzības pierādījumus ar REG12.

## **3. Mērķi**

### **3.1 Šīs politikas mērķi ir:**

- 3.1.1 uzturēt darbinieku apstrādes uzskaites pierādījumus REG02;
- 3.1.2 dokumentēt darbinieku vākšanas avotus, PII kategorijas, nolūkus, sistēmas, saņēmējus un glabāšanas sasaisti;
- 3.1.3 uzturēt darbinieku privātuma paziņojumu pierādījumus REG07;
- 3.1.4 virzīt darbinieku privātuma riska un DPIA triggerus caur REG04;
- 3.1.5 virzīt darbinieku tiesību pieprasījumus caur REG06;
- 3.1.6 uzturēt personālvadības apstrādātāju, algu aprēķina, HRIS, labumu, fona pārbaudes un ārpakalpojumā nodotu personālvadības pakalpojumu pierādījumus REG08;
- 3.1.7 nodrošināt, ka darbinieku uzraudzība ir dokumentēta, samērīga, pārskatīta un attiecīgā gadījumā eskalēta caur REG04 un REG12;
- 3.1.8 virzīt aizdomīgus darbinieku personas datu incidentus caur REG10;
- 3.1.9 ierakstīt darbinieku privātuma izņēmumus, neatbilstības, korektīvās darbības un uzlabošanas darbības REG12;
- 3.1.10 nepieļaut darba tiesību konsultācijas un darbinieku padomes juridiskus komentārus operatīvajās klauzulās;
- 3.1.11 nepieļaut dublējošus reģistrus, lomas, veidlapas, informācijas paneļus vai personālvadībai specifiskus pierādījumu objektus.

## **4. Politikas paziņojumi**

### **4.1 Darbinieku apstrādes uzskaitē un personālvadības apstrādes nolūki**

- 4.1.1 [Controller] Process Owner / Business Owner IR JĀIERAKSTA katra darbinieku apstrādes darbība REG02, pirms darbinieku personas dati tiek vākti, ģenerēti, importēti, izmantoti vai izpausti.
- 4.1.2 [Controller] Process Owner / Business Owner IR JĀDOKUMENTĒ darbinieku PII kategorijas, darbinieku populācija, vākšanas avots, apstrādes nolūks, sistēma, iekšējo saņēmēju kategorija, ārējo saņēmēju kategorija un glabāšanas sasaiste REG02, pirms apstrādes darbība tiek apstiprināta.
- 4.1.3 [Controller] Privacy Lead / PIMS Manager IR JĀPĀRSKATA katra jauna vai būtiski mainīta darbinieku apstrādes darbība REG02, pirms apstrādes darbība tiek apstiprināta darbībai.
- 4.1.4 [Conditional] Data Protection Officer / Privacy Advisor IR JĀIERAKSTA privātuma konsultācija REG04, pirms tiek apstiprināta darbinieku apstrāde, kas ietver īpašu kategoriju personas datus, datus par noziedzīgiem nodarījumiem, fona pārbaudi, arodveselības datus, biometriskos datus, atrašanās vietas datus, darbinieku uzraudzību vai apstrādi, kas var būtiski ietekmēt darbinieku.
- 4.1.5 [Processor] Privacy Lead / PIMS Manager IR JĀIERAKSTA klienta norādījums, pakalpojuma nolūks, klienta darbinieku PII kategorijas un apstrādātāja lomas sasaiste REG08, pirms tiek apstrādāti klienta darbinieku personas dati ārpakalpojumā sniegta personālvadības, algu aprēķina, labumu, HRIS, pārbaudes vai darbaspēka atbalsta pakalpojuma ietvaros.
- 4.1.6 [Joint Controller] Privacy Lead / PIMS Manager IR JĀIERAKSTA kopīgā pārziņa atbildības sadalījums par darbinieku personas datu apstrādi REG08, pirms sākas kopīgā darbinieku apstrādes darbība.

## **4.2 Darbinieku datu vākšana un darbinieku privātuma paziņojumi**

- 4.2.1 [Controller] Process Owner / Business Owner IR JĀIEROBEŽO darbinieku personas datu vākšana līdz REG02 dokumentētajām kategorijām, pirms sākas vākšana personāla atlasei, ievadīšanai, nodarbinātības administrēšanai, labumu administrēšanai, algu aprēķina veikšanai, pārbaudei, uzraudzībai vai darba attiecību izbeigšanai.
- 4.2.2 [Controller] Process Owner / Business Owner IR JĀIERAKSTA no trešām pusēm vākta darbinieku personas datu avots REG02, pirms tiek izmantots trešās puses vākšanas avots.
- 4.2.3 [Controller] Privacy Lead / PIMS Manager IR JĀUZTUR darbinieku privātuma paziņojuma ieraksts REG07, pirms darbinieku personas dati tiek vākti tieši vai netieši jaunam vai būtiski mainītam nolūkam.
- 4.2.4 [Controller] Process Owner / Business Owner IR JĀAPSTIPRINA, ka REG07 ierakstītais aktuālais darbinieku privātuma paziņojums ir pieejams, pirms notiek personāla atlases datu vākšana, ievadīšanas datu vākšana, uzraudzības aktivizēšana, pieteikšanās labumiem, fona pārbaude vai būtiska darbinieku apstrādes izmaiņa.
- 4.2.5 [Conditional] Data Protection Officer / Privacy Advisor IR JĀPĀRSKATA REG07 darbinieku privātuma paziņojuma ieraksts pirms publicēšanas, ja paziņojums aptver darbinieku uzraudzību, fona pārbaudi, īpašu kategoriju personas datus, datus par noziedzīgiem nodarījumiem, automatizētu lēmumu pieņemšanu vai būtiski mainītu darbinieku apstrādes nolūku.
- 4.2.6 [Processor] Vendor / Procurement Owner IR JĀIERAKSTA darbiniekiem paredzēto vākšanas kanālu atbildības REG08, pirms apstrādātāja vadīts personālvadības, algu aprēķina, HRIS, labumu, pārbaudes vai ārpakalpojuma personālvadības pakalpojums vāc darbinieku personas datus klienta vārdā.

[ ... 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 JĀIERAKSTA izņēmuma pieprasījums REG12, pirms tiek veikta atkāpe no jebkuras šīs politikas prasības.
- 9.1.2 [Conditional] Data Protection Officer / Privacy Advisor IR JĀIERAKSTA konsultācija REG12, pirms tiek apstiprināts izņēmums, kas ietekmē darbinieku uzraudzību, darbinieku tiesību pieprasījumu apstrādi, fona pārbaudi, īpašu kategoriju personas datus, datus par noziedzīgiem nodarījumiem vai augstas ietekmes darbinieku apstrādi.
- 9.1.3 [Conditional] Top Management IR JĀAPSTIPRINA darbinieku privātuma izņēmumi REG12 pirms aktivizēšanas, ja izņēmums ietekmē augsta riska darbinieku apstrādi, darbinieku uzraudzību, ārēju izpaušanu, paļaušanos uz apstrādātāju vai neatrisinātu korektīvo darbību.
- 9.1.4 [All] Privacy Lead / PIMS Manager IR JĀPIEŠĶIR katram darbinieku privātuma izņēmumam REG12 beigu datums, kas nepārsniedz 90 dienas, pirms izņēmums tiek aktivizēts.
- 9.1.5 [All] Privacy Lead / PIMS Manager IR JĀPĀRSKATA katrs darbinieku privātuma izņēmums REG12 piecu darbdienu laikā pirms termiņa beigām.
- 9.1.6 [All] Privacy Lead / PIMS Manager IR JĀSLĒDZ vai jāeskalē katrs termiņu pārsniedzis darbinieku privātuma izņēmums REG12 piecu darbdienu laikā pēc termiņa beigām.

## 10. Piemērošana

- 10.1.1 [All] Privacy Lead / PIMS Manager IR JĀIERAKSTA neatbilstība REG12 piecu darbdienu laikā, ja darbinieku personas datu apstrādei trūkst nepieciešamo REG02, REG07, REG08, REG04 vai REG06 pierādījumu.
- 10.1.2 [Conditional] Incident Response Coordinator IR JĀIERAKSTA aizdomīga neatļauta piekļuve darbinieku personas datiem, izpaušana, zudums vai kompromitēšana REG10 vienas darbdienu laikā pēc identificēšanas.
- 10.1.3 [Controller] Privacy Lead / PIMS Manager IR JĀNOVĒRŠ jaunas darbinieku uzraudzības apstiprināšana REG12, ja trūkst nepieciešamo REG02, REG04 vai REG07 pierādījumu.
- 10.1.4 [Both] Vendor / Procurement Owner IR JĀAPTUR jauna darbinieku personas datu izpaušana personālvadības piegādātājam REG08, ja trūkst nepieciešamo apstrādātāja, apakšapstrādātāja, norādījumu vai palīdzības pierādījumu.
- 10.1.5 [All] Top Management IR JĀPĀRSKATA atkārtotas darbinieku privātuma neatbilstības REG12, ja viena un tā pati kategorija rodas divas vai vairāk reizes slīdošā 12 mēnešu periodā.
- 10.1.6 [All] Internal Audit / Compliance Reviewer IR JĀPĀRBAUDA slēgšanas pierādījumi REG12, pirms tiek slēgti audita konstatējumi, kas ietver darbinieku privātuma apstrādi, darbinieku paziņojumus, darbinieku uzraudzību, darbinieku tiesības vai personālvadības piegādātājus.

## 11. Pārskatīšana un uzturēšana

- 11.1.1 [All] Privacy Lead / PIMS Manager IR JĀPĀRSKATA šī politika REG12 vismaz reizi gadā.
- 11.1.2 [Conditional] Privacy Lead / PIMS Manager IR JĀPĀRSKATA šī politika REG12 30 dienu laikā pēc būtiskas izmaiņas darbinieku apstrādē, darbinieku uzraudzībā, personālvadības sistēmās, algu aprēķina kārtībā, HRIS pakalpojumu sniedzējos, labumu pakalpojumu sniedzējos, fona pārbaudes pakalpojumu sniedzējos vai ārpakalpojuma personālvadības pakalpojumos.
- 11.1.3 [Conditional] Data Protection Officer / Privacy Advisor IR JĀPĀRSKATA ierosinātās būtiskās izmaiņas šajā politikā REG12 pirms Top Management apstiprināšanas.
- 11.1.4 [All] Top Management IR JĀAPSTIPRINA būtiskas izmaiņas šajā politikā REG12 pirms publicēšanas.

11.1.5 [All] Privacy Lead / PIMS Manager IR JĀATJAUNINA REG02, REG07 vai REG08 15 darbdienu laikā pēc tam, kad apstiprināta politikas izmaiņa ietekmē darbinieku apstrādes ierakstus, darbinieku privātuma paziņojumus vai personālvadības piegādātāju pierādījumus.

11.1.6 [All] Internal Audit / Compliance Reviewer IR JĀIERAKSTA šīs politikas pārskatīšanas efektivitātes novērojumi REG12 plānotā PIMS iekšējā audita cikla laikā.

## 12. Saistītās politikas

- 12.1 Šo politiku atbalsta šādas saistītās politikas:
- 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 PII11 - PII precizitātes un kvalitātes politika
- 12.13 PII12 - Apstrādātāju, apakšapstrādātāju un trešo pušu privātuma pārvaldības politika
- 12.14 PII13 - Starptautiskas PII nosūtīšanas politika
- 12.15 PII14 - PII drošības un piekļuves kontroles politika
- 12.16 PII15 - PII incidentu un pārkāpumu pārvaldības politika
- 12.17 PII16 - Privātuma apmācību, informētības un kompetences politika
- 12.18 PII17 - PIMS dokumentētas informācijas un pierādījumu pārvaldības politika
- 12.19 PII18 - PIMS uzraudzības, audita un uzlabošanas politika
- 12.20 PII21 - AI un automatizētas lēmumu pieņemšanas privātuma politika, ja tā ir iekļauta izvēles papildinājuma laidiena tvērumā

## 13. Atsauces standarti un ietvari

13.1 Šī politika ir kartēta uz turpmāk norādītajiem standartiem un regulējumu. Kartējums paskaidro, kā politika atbalsta minētās prasības, un identificē iekšējās klauzulas, kas tās īsteno vai atbalsta.

### 13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Kartēts uz dokumentētiem darbinieku privātuma pierādījumiem, operatīvās apstiprināšanas vārtiem, personālvadības apstrādātāju ierakstiem, darbinieku paziņojumiem, uzraudzības ierakstiem, izņēmumu apstrādi un ieviešanas pierādījumiem. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.3; 4.3.1; 4.4.1; 4.5.1; 4.7.1; 7.1.1; 7.1.3].

13.2.2 **Clause 9.1; Clause 10.2** - Kartēts uz darbinieku privātuma uzraudzību, metrikām, audita pierādījumiem, darbinieku uzraudzības izlasi, neatbilstību apstrādi, korektīvajām darbībām un uzlabošanu. Addressed by clauses [4.3.6; 4.4.5; 4.5.5; 4.6.7; 8.1.1; 8.1.4; 8.1.7; 10.1.1; 10.1.5].

13.2.3 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9** - Kartēts uz darbinieku apstrādes nolūkiem, tiesiskā pamata sasaisti, privātuma riska un DPIA maršrutēšanu, kopīgā pārziņa atbildības sadalījumu un apstrādes ierakstiem REG02 un REG04. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.6; 4.2.2; 4.6.1; 4.6.2].

- 13.2.4 **Annex A.1.2.7; Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7** - Kartēts uz personālvadības apstrādātāju līgumiem, dokumentētiem norādījumiem, klienta darbinieku PII apstrādi, apstrādātāja palīdzību un apstrādātāja ierakstiem REG08. Addressed by clauses [4.1.5; 4.2.6; 4.4.4; 4.5.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5].
- 13.2.5 **Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11** - Kartēts uz darbinieku tiesību pieprasījumu apstrādi, sarežģītu tiesību pieprasījumu konsultācijām un automatizētu lēmumu vai augstas ietekmes apstrādes maršrutēšanu caur REG06 un REG04. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.3].
- 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** - Kartēts uz darbinieku datu vākšanas ierobežošanu, apstiprinātu iekšēju izmantošanu, minimizēšanu, glabāšanas sasaisti un glabāšanas izņēmumu maršrutēšanu. Addressed by clauses [4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.6.1].
- 13.2.7 **Annex A.1.5.4; Annex A.1.5.5; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Kartēts uz ārējām darbinieku PII izpaušanām, datu koplietošanas ierakstiem, apstrādātāja izpaušanas autorizāciju un ar izpaušanu saistītu incidentu maršrutēšanu. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.7.6].
- 13.2.8 **Annex A.3.14; Annex A.3.25** - Kartēts uz darbinieku privātuma ierakstu aizsardzību, darbinieku uzraudzības žurnālu pierādījumiem un aizdomīgu darbinieku uzraudzības datu nepareizu lietošanu vai kompromitēšanu. Addressed by clauses [4.6.4; 4.6.6; 4.6.7; 7.1.2].

### 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)** - Kartēts uz likumīgu, godprātīgu, pārredzamu, nolūkam ierobežotu, minimizētu, ar glabāšanu sasaistītu un pārskatatbildīgu darbinieku PII apstrādi. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.1; 4.3.3; 4.4.1; 4.4.5].
- 13.3.2 **Article 6; Article 9; Article 10** - Kartēts uz tiesiskā pamata sasaisti, ģipašu kategoriju darbinieku PII maršrutēšanu, ar arodveselību un nodarbinātību saistītu sensitīvu PII maršrutēšanu un datu par noziedzīgiem nodarījumiem vai fona pārbaudes datu maršrutēšanu. Addressed by clauses [4.1.2; 4.1.3; 4.1.4; 4.2.2; 4.7.3].
- 13.3.3 **Article 12; Article 13; Article 14** - Kartēts uz darbinieku informēšanu, darbinieku privātuma paziņojumu ierakstiem, tiešas un netiešas vākšanas paziņojumu trigeriem un uzraudzības paziņojumu pierādījumiem. Addressed by clauses [4.2.3; 4.2.4; 4.2.5; 4.6.5].
- 13.3.4 **Article 15; Article 16; Article 17; Article 18; Article 21; Article 22** - Kartēts uz darbinieku tiesību pieprasījumu maršrutēšanu, pieprasījumu pierādījumiem, sarežģītu pieprasījumu konsultācijām un automatizētu lēmumu maršrutēšanu. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.3].
- 13.3.5 **Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39** - Kartēts uz pārziņa pārvaldību, kopīgā pārziņa atbildības sadalījumu, personālvadības apstrādātāju pārvaldību, apstrādes ierakstiem, drošu apstrādi, DPIA maršrutēšanu un privātuma konsultēšanas iesaisti. Addressed by clauses [4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.3.4; 4.3.5; 4.6.2; 4.6.3; 4.6.6; 4.7.1; 4.7.6].

### 13.4 ISO/IEC 29100:2020

- 13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Kartēts uz darbinieku nolūka noteikšanu, vākšanas ierobežošanu, minimizēšanu, izmantošanas ierobežošanu, glabāšanas ierobežošanu un izpaušanas ierobežošanu. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.4.1; 4.4.2; 4.6.1].
- 13.4.2 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12** - Kartēts uz pārredzamību, darbinieku līdzdalību, darbinieku tiesību atbalstu, pārskatatbildību, informācijas

drošību un privātuma atbilstības pierādījumiem. Addressed by clauses [4.2.3; 4.2.4; 4.5.1; 4.5.2; 4.5.5; 4.6.4; 4.6.6; 4.6.7; 4.7.6].

### **13.5 ISO/IEC 29151:2022**

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10** - Kartēts uz PII nolūka ierakstiem, vākšanas kontroles pasākumiem, minimizēšanu, glabāšanas sasaisti, izpaušanas ierobežošanu un darbinieku līdzdalības vai piekļuves atbalstu. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.3.1; 4.3.4; 4.4.1; 4.4.2; 4.5.1; 4.5.4].

13.5.2 **Clause 7.1.2; Clause 7.1.3; Clause 7.2.4; Clause 7.3.2** - Kartēts uz PII aizsardzībai paredzētiem darbaspēka dzīves cikla kontroles pasākumiem, kas attiecas uz pārbaudi, noteikumiem, privātuma pārkāpumu piemērošanas sasaisti un glabāšanas pārskatīšanu darba attiecību izbeigšanas vai nodarbinātības izmaiņu gadījumā. Addressed by clauses [4.1.4; 4.2.2; 4.4.2; 4.4.5; 10.1.1; 10.1.5].

13.5.3 **Clause 15.1.2; Clause 15.2.2; Clause 15.2.3** - Kartēts uz personālvadības apstrādātāju izvērtēšanu, personālvadības apstrādātāju uzraudzību, personālvadības piegādātāju pārskatīšanu un pakalpojumu izmaiņu pierādījumiem REG08. Addressed by clauses [4.4.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.6].

### **13.6 ISO/IEC 29134:2020**

13.6.1 **Clause 5.1; Clause 6.2** - Kartēts uz privātuma ietekmes novērtējuma ieguvumiem un personālvadības privātuma riska vai DPIA trigeru noteikšanu darbinieku uzraudzībai un augstas ietekmes personālvadības apstrādei, nedublējot DPIA metodi. Addressed by clauses [4.1.4; 4.3.3; 4.6.2; 4.6.3].

### **13.7 ISO/IEC 27002:2022**

13.7.1 Controls 5.34; 6.1; 6.2; 6.5; 6.6 - Kartēts uz PII aizsardzību, pārbaudi, darbaspēka noteikumiem, pienākumiem pēc nodarbinātības izmaiņām un konfidencialitātes gaidām kā PII atbalstošiem darbaspēka dzīves cikla kontroles pasākumiem. Addressed by clauses [4.1.4; 4.2.2; 4.4.2; 4.4.4; 4.7.2; 4.7.3].

13.7.2 Controls 8.15; 8.16 - Kartēts uz darbinieku uzraudzības žurnāliem, uzraudzības darbībām, žurnālu nolūka ierobežošanu un uzraudzības pierādījumu pārskatīšanu. Addressed by clauses [4.6.1; 4.6.2; 4.6.4; 4.6.6; 4.6.7].