

				Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: PII13				Dokumenta nosaukums: Starptautiskas personas datu nosūtīšanas 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 / pants	Piemērojamība	Pārklājuma veids	Komentārs
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Datu nosūtīšanas pierādījumi un darbības kontroles pasākumi
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Uzraudzība, neatbilstība un korektīvā darbība
ISO/IEC 27701:2025	Annex A.1.2.8; Annex A.1.2.9	Controller / Joint Controller	Supporting	Kopīga atbildība un apstrādes ieraksti
ISO/IEC 27701:2025	Annex A.1.5.2; Annex A.1.5.3	Controller	Primary	Datu nosūtīšanas pamats un datu nosūtīšanas vietas
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Datu nosūtīšanas un izpaušanas ieraksti
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Supporting	Klienta vienošanās, norādījumi un apstrādātāja ieraksti
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Primary	Apstrādātāja datu nosūtīšanas pamats un vietas
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Apstrādātāja izpaušanas ieraksti un juridiski saistoša izpaušana
GDPR	Article 5(2); Article 24	Controller	Supporting	Pārskatatbildība un pārziņa pasākumi
GDPR	Article 26	Joint Controller	Supporting	Kopīgas atbildības sadalījums
GDPR	Article 28	Processor	Supporting	Apstrādātāja norādījumi un autorizācija
GDPR	Article 30	Both	Supporting	Datu nosūtīšanas ieraksti
GDPR	Article 44	Both	Primary	Vispārējais datu nosūtīšanas princips
GDPR	Article 45	Controller	Primary	Adekvatuma mehānisms

GDPR	Article 46	Controller	Primary	Atbilstoši aizsardzības pasākumi
GDPR	Article 47	Controller	Supporting	Saistošie uzņēmuma noteikumi
GDPR	Article 48	Both	Supporting	Publiskas iestādes datu izpaušanas pieprasījumi
GDPR	Article 49	Controller	Supporting	Atkāpes īpašās situācijās
ISO/IEC 29100:2020	Clause 5.6; Clause 5.10; Clause 5.12	Both	Supporting	Izpaušanas ierobežošana, pārskatatbildība un privātuma atbilstība
ISO/IEC 29151:2022	Annex A.7	Both	Supporting	Lietošanas, glabāšanas, izpaušanas un datu nosūtīšanas aizsardzība

1. Piemērošanas joma

- 1.1 Šī politika nosaka organizācijas prasības starptautisku personas datu nosūtīšanas gadījumā identificēšanai, apstiprināšanai, reģistrēšanai, pārskatīšanai, ierobežošanai un apturēšanai.
- 1.2 Šī politika attiecas uz pārziņa, kopīga pārziņa, apstrādātāja un apakšapstrādātāja darbībām, kurās PII tiek darīta pieejama, tai piekļūst no citas atrašanās vietas, tā tiek glabāta, mitināta, izpausta vai citādi nosūtīta uz valsti, teritoriju, starptautisku organizāciju vai saņēmēju ārpus apstiprinātās apstrādes robežas, kas reģistrēta REG02 vai REG09.
- 1.3 Šī politika attiecas uz datu nosūtīšanu, kurā iesaistīti iekšējie saistītie uzņēmumi, ārējie saņēmēji, apstrādātāji, apakšapstrādātāji, pakalpojumu sniedzēji, atbalsta piekļuve, mitināšanas vietas, attālināta administrēšana, turpmāka nosūtīšana, publiskas iestādes datu izpaušanas pieprasījumi un ar datu nosūtīšanu saistītas pakalpojumu izmaiņas.
- 1.4 Šī politika nesniedz juridiskas konsultācijas, nedefinē standarta līguma klauzulu tekstu, neveido atsevišķu datu nosūtīšanas ietekmes izvērtējuma reģistru, neveido atsevišķu SCC reģistru, nedefinē drošības kontroles pasākumu arhitektūru, nedefinē apstrādātāja dzīves cikla pārvaldību un nedefinē incidentu reaģēšanas darbplūsmu. Šie jautājumi tiek risināti, izmantojot saistītās politikas, klientam specifisku juridisko konfigurāciju vai apstiprinātus REG09 pierādījumus.
- 1.5 Šīs politikas vajadzībām būtiska datu nosūtīšanas izmaiņa ir jebkura izmaiņa datu nosūtīšanas galamērķī, saņēmējā, apstrādes lomā, mitināšanas vietā, atbalsta piekļuves vietā, datu nosūtīšanas mehānismā, turpmākas nosūtīšanas ceļā, apstrādātāja vai apakšapstrādātāja kārtībā, juridiskā vai regulatīvā datu nosūtīšanas nosacījumā, datu nosūtīšanas aizsardzības pasākumā vai atlikušajā datu nosūtīšanas riskā.

2. Mērķis

- 2.1 Šīs politikas mērķis ir nodrošināt, ka starptautiska personas datu nosūtīšana tiek identificēta pirms tās veikšanas, ir pamatota ar apstiprinātiem datu nosūtīšanas mehānisma pierādījumiem, tiek pārskatīta datu nosūtīšanas riska kontekstā, tiek pārvaldīta attiecībā uz turpmāku nosūtīšanu un tiek apturēta vai tiek novērsti trūkumi, ja netiek uzturēti nepieciešamie pierādījumi vai aizsardzības pasākumi.
- 2.2 Šī politika ļauj organizācijai demonstrēt pārskatatbildīgu datu nosūtīšanas pārvaldību, izmantojot REG09 kā primāro datu nosūtīšanas pierādījumu objektu un REG02, REG08 un REG12 kā atbalstošus pierādījumu objektus.

3. Mērķi

3.1 Šīs politikas mērķi ir:

- 3.1.1 identificēt starptautisku personas datu nosūtīšanu pirms apstrādes sākšanas vai izmaiņu veikšanas;
- 3.1.2 uzturēt apstiprinātus datu nosūtīšanas ierakstus REG09;
- 3.1.3 dokumentēt datu nosūtīšanas mehānismus un atbalstošos pierādījumus;
- 3.1.4 definēt datu nosūtīšanas riska pārskatīšanas un apstiprināšanas prasības;
- 3.1.5 kontrolēt apstrādātāja, apakšapstrādātāja un turpmākas nosūtīšanas autorizāciju;
- 3.1.6 pārskatīt aktīvos datu nosūtīšanas gadījumus noteiktā periodiskumā;
- 3.1.7 apturēt datu nosūtīšanu vai novērst trūkumus, ja netiek uzturēti nepieciešamie pierādījumi, autorizācija vai aizsardzības pasākumi;
- 3.1.8 izvairīties no nevajadzīga juridisko konsultāciju teksta, dublētiem reģistriem un dublētiem piegādātāju pārvaldības kontroles pasākumiem.

4. Politikas prasības

4.1 Datu nosūtīšanas identificēšana un reģistrēšana

- 4.1.1 [Controller] Process Owner / Business Owner ir jāidentificē starptautiskas personas datu nosūtīšanas galamērķi, saņēmēju kategorijas un piekļuves vietas REG02 pirms apstrādes darbības sākšanas vai būtiskas izmaiņas.
- 4.1.2 [Controller] Privacy Lead / PIMS Manager ir jāizveido vai jāatjaunina REG09 datu nosūtīšanas ieraksts pirms jebkuras jaunas vai būtiski mainītas pārziņa starptautiskas personas datu nosūtīšanas sākšanas.
- 4.1.3 [Processor] Vendor / Procurement Owner ir jāreģistrē klienta autorizētie apstrādātāja datu nosūtīšanas galamērķi, pakalpojumu vietas un attālinātās piekļuves vietas REG08 un REG09 pirms apstrādātāja datu nosūtīšanas darbības sākšanas vai izmaiņām.
- 4.1.4 [Joint Controller] Privacy Lead / PIMS Manager ir jāreģistrē kopīga pārziņa atbildības sadalījums attiecībā uz starptautiskas datu nosūtīšanas lēmumiem REG08 un REG09 pirms kopīgas datu nosūtīšanas darbības sākšanas vai izmaiņām.
- 4.1.5 [Both] Process Owner / Business Owner ir jāidentificē turpmākas nosūtīšanas maršruti, turpmāko saņēmēju kategorijas un turpmākas nosūtīšanas nosacījumi REG09 pirms turpmākas nosūtīšanas apstiprināšanas.

4.2 Datu nosūtīšanas mehānisma izvēle un apstiprināšana

- 4.2.1 [Controller] Privacy Lead / PIMS Manager ir jāreģistrē apstiprinātais datu nosūtīšanas mehānisms un atbalstošie pierādījumi REG09 pirms pārziņa starptautiskas personas datu nosūtīšanas sākšanas.
- 4.2.2 [Controller] Data Protection Officer / Privacy Advisor ir jāpārskata datu nosūtīšanas mehānisma pierādījumi REG09 pirms jaunas, būtiski mainītas vai augstāka riska starptautiskas personas datu nosūtīšanas apstiprināšanas.
- 4.2.3 [Processor] Vendor / Procurement Owner ir jāiegūst dokumentēta klienta autorizācija vai norādījums REG08 un REG09 pirms jebkuras apstrādātāja starptautiskas personas datu nosūtīšanas sākšanas.
- 4.2.4 [Subprocessor] Vendor / Procurement Owner ir jāreģistrē apakšapstrādātāja datu nosūtīšanas autorizācija un piemērojami tālāk nododamie datu nosūtīšanas nosacījumi REG08 un REG09 pirms apakšapstrādātāja datu nosūtīšanas darbības sākšanas.
- 4.2.5 [Both] Privacy Lead / PIMS Manager ir jābloķē vai jāatliek starptautiska personas datu nosūtīšana REG09, ja pirms plānotās datu nosūtīšanas sākuma datu nosūtīšanas mehānisms, galamērķis, saņēmējs, lomu sadalījums vai atbalstošie pierādījumi ir nepilnīgi.

[... 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 jāiesniedz jebkurš pieprasījums turpināt darbību ar nepilnīgiem, aizkavētiem vai izņēmuma datu nosūtīšanas pierādījumiem REG12 pirms izņēmums kļūst aktīvs.
- 9.1.2 [All] Privacy Lead / PIMS Manager ir jāapstiprina vai jānoraida datu nosūtīšanas izņēmuma pieprasījumi REG12 pirms izņēmums kļūst aktīvs.
- 9.1.3 [All] Data Protection Officer / Privacy Advisor ir jāreģistrē padoms REG12 pirms jebkura datu nosūtīšanas izņēmuma apstiprināšanas, ja tas ietver augstāka riska apstrādi, trūkstošus datu nosūtīšanas mehānisma pierādījumus, publiskas iestādes izpaušanu, turpmāku nosūtīšanu vai ietekmi uz sertifikāciju.
- 9.1.4 [All] Top Management ir jāapstiprina datu nosūtīšanas izņēmumi, kas pārsniedz 90 dienas, ietekmē augstāka riska apstrādi, ietekmē atkārtotu datu nosūtīšanas darbību vai ietekmē ārējo apliecinājumu, REG12 pirms izņēmums kļūst aktīvs.

- 9.1.5 [All] Privacy Lead / PIMS Manager katram apstiprinātam datu nosūtīšanas izņēmumam REG12 ir jāpiešķir īpašnieks, beigu datums, kompensējošais kontroles pasākums un pārskatīšanas biežums.
- 9.1.6 [All] Privacy Lead / PIMS Manager ir jāpārskata katrs atvērtais datu nosūtīšanas izņēmums REG12 vismaz reizi mēnesī līdz tā slēgšanai.

10. Piemērošana

- 10.1.1 [All] Privacy Lead / PIMS Manager ir jāreģistrē neatbilstība REG12 piecu darbdienu laikā pēc neregistrētas datu nosūtīšanas, neatbalstīta datu nosūtīšanas mehānisma, trūkstošas apstrādātāja autorizācijas, nokavētas pārskatīšanas, trūkstošu turpmākas nosūtīšanas pierādījumu vai neatļautas datu nosūtīšanas turpināšanas identificēšanas.
- 10.1.2 [Controller] Privacy Lead / PIMS Manager ir jāaptur pārziņa starptautiska personas datu nosūtīšana REG09, ja pirms plānotās datu nosūtīšanas sākuma nav nepieciešamo datu nosūtīšanas mehānisma pierādījumu.
- 10.1.3 [Processor] Vendor / Procurement Owner ir jāaptur apstrādātāja starptautiskās datu nosūtīšanas darbība REG08 un REG09, ja pirms datu nosūtīšanas darbības sākšanas trūkst nepieciešamās klienta autorizācijas.
- 10.1.4 [Subprocessor] Vendor / Procurement Owner ir jāeskalē neatļauta apakšapstrādātāja starptautiskās datu nosūtīšanas darbība REG08 un REG12 piecu darbdienu laikā pēc identificēšanas.
- 10.1.5 [All] Top Management ir jāpiešķir korektīvās darbības īpašumtiesības REG12 10 darbdienu laikā atkārtotu, ilgstošu, augsta riska vai sertifikācijai būtisku datu nosūtīšanas nepilnību gadījumā.
- 10.1.6 [All] Internal Audit / Compliance Reviewer ir jāpārbauda korektīvo darbību efektivitāte attiecībā uz ar datu nosūtīšanu saistītām neatbilstībām 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 reizi gadā un jādokumentē pārskatīšanas rezultāts REG12.
- 11.1.2 [All] Privacy Lead / PIMS Manager ir jāpārskata šī politika 30 dienu laikā pēc būtiskas izmaiņas datu nosūtīšanas tiesiskajā regulējumā, datu nosūtīšanas mehānisma pieejamībā, apstrādātāja pakalpojuma modelī, mitināšanas vietā, atbalsta piekļuves vietā, apakšapstrādātāja kārtībā, datu nosūtīšanas aizsardzības pasākumā vai PIMS sertifikācijas prasībās.
- 11.1.3 [All] Data Protection Officer / Privacy Advisor ir jāpārskata privātam nozīmīgas šīs 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 jāreģistrē apstiprināto politikas izmaiņu komunikācija REG11 30 dienu laikā pēc publicēšanas.

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 pārskatbildības politika
- 12.4 PII03 - PII apstrādes uzskaites un tiesiskā pamata politika
- 12.5 PII04 - Privātuma paziņojumu un pārredzamības politika

- 12.6 PII07 - Privātuma risku izvērtēšanas un DPIA politika
- 12.7 PII08 - Datu aizsardzības pēc projektēšanas un pēc noklusējuma politika
- 12.8 PII09 - PII vākšanas, lietošanas, izpaušanas un koplietošanas politika
- 12.9 PII12 - Apstrādātāju, apakšapstrādātāju un trešo pušu privātuma pārvaldības politika
- 12.10 PII14 - PII drošības un piekļuves kontroles politika
- 12.11 PII17 - PIMS dokumentētās informācijas un pierādījumu pārvaldības politika
- 12.12 PII18 - PIMS uzraudzības, audita un uzlabošanas politika

13. Atsauces standarti un ietvari

- 13.1 Šī politika ir kartēta pret šādiem standartiem un regulējumiem. Kartējums izskaidro, kā politika atbalsta citētās prasības, un identificē iekšējos punktus, kas tās ievieš vai atbalsta.

13.2 ISO/IEC 27701:2025

- 13.2.1 **Clause 7.5; Clause 8.1** - Kartēts pret dokumentētiem datu nosūtīšanas pierādījumiem, datu nosūtīšanas darbības kontroli, REG09 datu nosūtīšanas laukiem, datu nosūtīšanas apstiprinājumiem, datu nosūtīšanas ieviešanas ierakstiem un datu nosūtīšanas pierādījumu saskaņošanu. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.2.5; 7.1.1; 7.1.2; 7.1.3; 7.1.5; 7.1.6].
- 13.2.2 **Clause 9.1; Clause 10.2** - Kartēts pret starptautiskās datu nosūtīšanas kontroles pasākumu uzraudzību, metrikām, pārskatīšanu, apturēšanu, neatbilstību un korektīvo darbību. Addressed by clauses [4.3.4; 4.5.1; 4.5.3; 6.1.1; 6.1.2; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.6; 10.1.1; 10.1.5; 10.1.6].
- 13.2.3 **Annex A.1.2.8; Annex A.1.2.9** - Kartēts pret kopīga pārziņa atbildības pierādījumiem un pārziņa apstrādes ierakstiem, kas ietver starptautiskās datu nosūtīšanas informāciju. Addressed by clauses [4.1.1; 4.1.4; 4.1.5; 4.5.5; 6.1.4; 7.1.5].
- 13.2.4 **Annex A.1.5.2; Annex A.1.5.3** - Kartēts pret pārziņa datu nosūtīšanas pamatu, datu nosūtīšanas mehānisma pierādījumiem, valstīm, starptautiskām organizācijām, galamērķiem un datu nosūtīšanas pārskatīšanas pierādījumiem REG09. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.3.1; 4.5.1].
- 13.2.5 **Annex A.1.5.4; Annex A.1.5.5** - Kartēts pret datu nosūtīšanas un izpaušanas ierakstiem, turpmākas nosūtīšanas maršrutu identificēšanu un pabeigtas datu nosūtīšanas vai izpaušanas pierādījumiem. Addressed by clauses [4.1.5; 4.4.3; 4.4.5; 7.1.7].
- 13.2.6 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Kartēts pret apstrādātāja klientu vienošanos, dokumentētiem klienta norādījumiem, apstrādātāja ierakstiem un autorizācijas pierādījumiem apstrādātāja starptautiskai datu nosūtīšanai. Addressed by clauses [4.1.3; 4.2.3; 4.2.4; 4.4.2; 6.1.5; 7.1.6; 10.1.3].
- 13.2.7 **Annex A.2.5.2; Annex A.2.5.3** - Kartēts pret apstrādātāja datu nosūtīšanas pamatu, klienta autorizētiem datu nosūtīšanas galamērķiem, pakalpojumu vietām un datu nosūtīšanas vietas pierādījumiem. Addressed by clauses [4.1.3; 4.2.3; 4.2.4; 4.5.2; 7.1.6].
- 13.2.8 **Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Kartēts pret apstrādātāja izpaušanas ierakstiem, izpaušanas pieprasījumu apstrādes pierādījumiem, publiskas iestādes datu izpaušanas pieprasījumu maršrutēšanu un turpmākas nosūtīšanas pierādījumiem. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 10.1.4].

13.3 GDPR

- 13.3.1 **Article 5(2); Article 24** - Kartēts pret pārskatatbildību, pārziņa pārvaldību, datu nosūtīšanas pierādījumiem, datu nosūtīšanas riska pārskatīšanu, izņēmumu pārvaldību un korektīvo darbību. Addressed by clauses [4.1.2; 4.2.1; 4.3.1; 4.3.4; 4.3.5; 6.1.2; 8.1.1; 9.1.2; 9.1.3; 10.1.1; 11.1.1].

- 13.3.2 **Article 26** - Kartēts pret kopīga pārziņa starptautiskās datu nosūtīšanas atbildības sadalījumu. Addressed by clauses [4.1.4; 6.1.4].
- 13.3.3 **Article 28** - Kartēts pret apstrādātāja un apakšapstrādātāja datu nosūtīšanas autorizāciju, klienta norādījumiem, tālāk nododamo pienākumu pierādījumiem un apturēšanu, ja autorizācijas trūkst. Addressed by clauses [4.1.3; 4.2.3; 4.2.4; 4.4.2; 4.5.2; 6.1.5; 10.1.3; 10.1.4].
- 13.3.4 **Article 30** - Kartēts pret apstrādes darbību ierakstiem un datu nosūtīšanas ierakstiem REG02, REG08 un REG09. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.4.5; 4.5.5; 7.1.5].
- 13.3.5 **Article 44** - Kartēts pret vispārējo datu nosūtīšanas pārvaldību, datu nosūtīšanas mehānisma apstiprināšanu, datu nosūtīšanas riska pārskatīšanu, apturēšanu trūkstošu pierādījumu gadījumā un datu nosūtīšanas atkārtotu izvērtēšanu. Addressed by clauses [4.1.2; 4.2.1; 4.2.5; 4.3.1; 4.5.3; 4.5.4].
- 13.3.6 **Article 45** - Kartēts pret uz adekvātumu balstīta datu nosūtīšanas mehānisma pierādījumiem, pārskatīšanu un apstiprināšanu REG09. Addressed by clauses [4.2.1; 4.2.2; 4.5.1].
- 13.3.7 **Article 46** - Kartēts pret atbilstošiem aizsardzības pasākumiem, aizsardzības pasākumu pierādījumiem, tehnisko aizsardzības pasākumu atkarības maršrutēšanu un datu nosūtīšanas apturēšanu, ja aizsardzības pasākumu trūkst vai tie nav derīgi. Addressed by clauses [4.2.1; 4.2.2; 4.3.2; 4.3.3; 4.5.3; 4.5.4].
- 13.3.8 **Article 47** - Kartēts pret saistošajiem uzņēmuma noteikumiem kā datu nosūtīšanas mehānisma iespēju, ja piemērojams un reģistrēts REG09. Addressed by clauses [4.2.1; 4.2.2; 4.3.1].
- 13.3.9 **Article 48** - Kartēts pret ārvalstu publiskas iestādes datu izpaušanas pieprasījumu reģistrēšanu un privātuma padomu pirms atbildes sniegšanas, ja tas ir praktiski iespējams. Addressed by clauses [4.4.3; 4.4.4].
- 13.3.10 **Article 49** - Kartēts pret izņēmuma datu nosūtīšanas mehānisma pierādījumiem un izņēmuma apstiprināšanu, ja tiek izmantotas atkāpes īpašās situācijās. Addressed by clauses [4.2.1; 4.2.2; 9.1.3].

13.4 ISO/IEC 29100:2020

- 13.4.1 **Clause 5.6; Clause 5.10; Clause 5.12** - Kartēts pret izpaušanas ierobežošanu, pārskatatbildīgu datu nosūtīšanas pārvaldību, datu nosūtīšanas atbilstības pierādījumiem, pārskatīšanu un korektīvo darbību. Addressed by clauses [4.1.2; 4.1.5; 4.3.5; 4.4.1; 4.5.1; 6.1.1; 8.1.1; 10.1.1].

13.5 ISO/IEC 29151:2022

- 13.5.1 **Annex A.7** - Kartēts pret datu nosūtīšanas aizsardzību, izpaušanas ierobežošanu, datu nosūtīšanas aizsardzības pasākumu pierādījumiem, turpmākas nosūtīšanas kontroli un apturēšanu, ja datu nosūtīšanas aizsardzības pasākumu trūkst vai tie nav derīgi. Addressed by clauses [4.2.1; 4.3.2; 4.3.3; 4.4.1; 4.5.3; 7.1.4].