

				Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: PII23				Dokumendi pealkiri: Pilve PII volitatud töötaja poliitika							
Versioon: 1.0		Jõustumiskuupäev: 01.01.2025		Dokumendi omanik:							
X	Poliitika		Standard		Protseduur		Vorm		Register		Muu

Muudatuste ajalugu				
Muudatuse number	Muudatuse kuupäev	Muudatused	Läbi vaadanud	Protsessi omanik

Kinnitused			
Nimi	Ametikoht	Kuupäev	Allkiri

<p>Õiguslik teatis (autoriõigus ja kasutuspiirangud) (C) 2025 Clarysec LLC. All rights reserved.</p> <p>Käesolev dokument on Clarysec LLC intellektuaalomand. Selle dokumendi ühtegi osa ei tohi ilma eelneva selgesõnalise kirjaliku loata kopeerida, taaskasutada, levitada ega muuta äriilistel või rakendamise eesmärkidel.</p> <p>Loata kasutamine on rangelt keelatud ja võib kaasa tuua õiguslikke meetmeid.</p> <p>Litsentsimise küsimustes võtke ühendust: info@clarysec.com</p>
--

Kooskõla standardite ja regulatsioonidega

Standard / õigusnorm	Punkt / kontrollimeede / artikkel	Kohaldatavus	Katvuse tüüp	Kommentaar
ISO/IEC 27701:2025	Clause 4.1; Clause 6.1.3	Processor	Supporting	PIMS-i roll ja kontrollimeetme kohaldatavus
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Processor	Primary	Dokumenteeritud pilve volitatud töötaja tõendusmaterjal ja tegevuslik ohje
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Processor	Supporting	Seire, mittevastavus ja parandusmeetmed
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	Kliendilepingud, juhised, tugi ja kirjed
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Kliendi abistamine isikuandmesubjektiga seotud kohustuste täitmisel
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Primary	Ajutised failid, tagastamine, edastamine, kõrvaldamine ja edastuskontrollid
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Supporting	Edastamise alus ja asukohad
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Avalikustamise kirjed ja avalikustamistaotluste käsitlemine
ISO/IEC 27701:2025	Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9	Processor	Primary	Alltöötaja avalikustamine, kaasamine ja muudatustest teavitamine
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	Juurdepääsu, kirjete, varunduse ja logimise tõendusmaterjal
GDPR	Article 28	Processor	Primary	Volitatud töötaja, alltöötaja, abi, audit, kustutamine ja tagastamine

GDPR	Article 30	Processor	Supporting	Volitatud töötleja kirjed
GDPR	Article 32; Article 33	Processor	Supporting	Turvalisus ja rikkumisest vastutavale töötlejale teatamine
GDPR	Article 44	Conditional	Referenced	Rahvusvahelise edastuse marsruutimine
ISO/IEC 29100:2020	Clause 5.3; Clause 5.5; Clause 5.6	Processor	Supporting	Eesmärk, minimaalsus, kasutamine, säilitamine ja avalikustamise piirang
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Processor	Supporting	Vastutus, infoturve ja vastavus
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	Volitatud töötleja hindamise, seire, muudatuste ja säilitamise kontrollimeetmed
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	Kontrollimeetme kohaldatavus, tegevuslik ohje ning tarnija- ja pilvekontrollid
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	Tarnija-, pilve-, kustutamise-, logimis- ja seirekontrollid
ISO/IEC 27018:2020	Annex A.2.1; Annex A.3.1	Processor	Primary	Pilve volitatud töötleja kliendiabi ja eesmärgi piirang
ISO/IEC 27018:2020	Annex A.6.1; Annex A.6.2; Annex A.8.1	Processor	Primary	Pilve avalikustamise teavitus, avalikustamise kirjed ja alltöötlejate läbipaistvus
ISO/IEC 27018:2020	Annex A.10.1; Annex A.10.3; Annex A.11.11;	Processor	Primary	Pilve rikkumislüües, lõpetamine, lepingulised meetmed,

	Annex A.11.12; Annex A.12.1			alltöövõtulepingud ja asukohakirjed
ISO/IEC 27036- 2:2022	Clause 6.1.1; Clause 6.1.2	Processor	Supporting	Tarnehela suhte strateegia ja juhtimine
ISO/IEC 27036- 2:2022	Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5	Processor	Supporting	Tarnijasuhete planeerimine, kokkulepe, haldamine, seire ja lõpetamine
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	Kustutamise raamistik ja dokumentatsioon
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	Processor	Supporting	Kustutamise rakendamine ja erandid

1. Kohaldamisala

1.1 Käesolev poliitika määrab kohustuslikud privaatsusnõuded pilveteenustele, mille puhul organisatsioon tegutseb PII volitatud töötaja või alltöötajana, sealhulgas SaaS, PaaS, IaaS, pilvekeskkonnas majutatud rakenduste, hallatud pilve, pilvetoe, pilvesalvestuse, pilveanalüütika ja pilvetaristu teenused, mis töötlevad PII-d klientide nimel.

1.2 Käesolevat poliitikat kohaldatakse pilvetöötlustele, mida tehakse kliendilepingute, dokumenteeritud kliendi juhiste, ülesvoolu volitatud töötaja juhiste, alltöötajate kokkulepete, pilveregiooni konfiguratsiooni, pilvetoe juurdepääsu, teenuse halduse, varundamise, replikatsiooni, logimise, seire, kustutamise, tagastamise, rikkumistoega seotud tegevuste, audititoe ja kliendi abistamise kohustuste alusel.

1.3 Käesolev poliitika hõlmab järgmist:

1.3.1 pilve PII töötluste kohaldamisala ja juhiste kirjed;

1.3.2 kliendilepingu ja jagatud vastutuse tõendusmaterjal;

1.3.3 rentnike isoleerimise, pilvejuurdepääsu, haldusjuurdepääsu ja logimise tõendusmaterjal;

1.3.4 alltöötajate ja pilve tarneahela juhtimine;

1.3.5 asukoha, kaugjuurdepääsu ja rahvusvahelise edastuse marsruutimine;

1.3.6 tagastamise, edastamise, kustutamise, kõrvaldamise ja lõpetamise tõendusmaterjal;

1.3.7 kliendi abistamine isikuandmesubjekti õiguste, DPIA-de, auditite ja rikkumistele reageerimisega;

1.3.8 seire, erandite, rakendamise ja parendamise tõendusmaterjal.

1.4 Käesolev poliitika ei loo eraldi kliendilepingute registrit, pilveteenuste registrit, rentnike isoleerimise registrit, juurdepääsuregistrit, logiregistrit, kustutamisregistrit, tugitaotluste registrit, audititõendite registrit, rikkumiste registrit, alltöötajate registrit ega pilve juhtimiskomiteed.

1.5 Käesolev poliitika ei asenda:

1.5.1 PII03 töötlemisregistri ja õigusliku aluse vastutuse kohta;

1.5.2 PII06 isikuandmesubjekti õiguste täieliku töövoogu kohta;

1.5.3 PII07 privaatsusriskide ja DPIA meetodika kohta;

1.5.4 PII08 lõimitud ja vaikumisi andmekaitse kontrollivärvate kohta;

1.5.5 PII09 kogumise, kasutamise, avalikustamise ja jagamise üldiste kontrollimeetmete kohta;

1.5.6 PII10 säilitamise, kustutamise ja kõrvaldamise meetodika kohta;

1.5.7 PII12 volitatud töötajate, alltöötajate ja kolmandate osapoolte üldise elutsükli juhtimise kohta;

1.5.8 PII13 rahvusvahelise edastusmehhanismi hindamise kohta;

1.5.9 PII14 PII turvalisuse ja juurdepääsukontrolli täieliku arhitektuuri kohta;

1.5.10 PII15 intsidendi- ja rikkumishalduse töövoogu kohta;

1.5.11 PII17 dokumenteeritud teabe ohje kohta;

1.5.12 PII18 PIMS-i seire, auditi ja parendamise juhtimise kohta.

2. Eesmärk

2.1 Käesoleva poliitika eesmärk on tagada, et pilve PII volitatud töötaja ja alltöötaja teenuseid osutatakse dokumenteeritud kliendi juhiste, selge töötlemisulatus, ohjatud alltöötajate kokkulepete, asjakohaste pilveturbe vastutuste, dokumenteeritud asukoha ja edastuste marsruutimise, kliendi abistamise kohustuste, rikkumistoetuse, kustutamise/tagastamise võimekuse ning auditiks valmis tõendusmaterjali alusel.

2.2 Käesolev poliitika toetab ISO/IEC 27701:2025 PIMS-i valmisolekut sertifitseerimiseks pilve volitatud töötajate ja pilve alltöötajate puhul, jäädes samal ajal integreerituks olemasoleva PIMS-i poliitikakogumi ja kanooniliste tõendusobjektidega.

3. Eesmärgid

3.1 Käesoleva poliitika eesmärgid on järgmised:

- 3.1.1 Määratleda pilve PII töötajate ulatus enne kliendi kasutuselevõttu või olulist muudatust.
- 3.1.2 Tagada, et kliendi juhised registreeritakse, vaadatakse läbi ja neid järgitakse.
- 3.1.3 Säilitada pilve volitatud töötajate ja alltöötajate tõendusmaterjal kanoonilistes PIMS-i registrites.
- 3.1.4 Määratleda jagatud vastutuse, rentnike isoleerimise, juurdepääsu, logimise ja asukoha tõendusmaterjal ilma PII turbepoliitikat dubleerimata.
- 3.1.5 Ohjata alltöötajate kasutuselevõttu, muudatusi, edasiantavate kohustuste ja seire tõendusmaterjali.
- 3.1.6 Toetada kliente isikuandmesubjekti õiguste, DPIA-de, audititaotluste ja rikkumistele reageerimisega.
- 3.1.7 Tagada, et tagastamise, kustutamise, edastamise ja kõrvaldamise tõendusmaterjal säilitatakse teenuse lõpetamisel.
- 3.1.8 Seirata pilve volitatud töötajate kontrollimeetmeid ja juhtida parandusmeetmeid REG12 abil.

4. Poliitika nõuded

4.1 Pilvetöötajate ulatus ja kliendi juhised

- 4.1.1 [Processor] Privacy Lead / PIMS Manager PEAB enne kliendi kasutuselevõttu või olulist teenusemuudatust registreerima iga pilve PII töötlemise teenuse, kliendi töötlemisrolli, kliendi juhise allika, PII kategooriad, isikuandmesubjektide kategooriad, teenuse eesmärgi, töötlemiskoha, alltöötajate sõltuvuse, kustutamise sõltuvuse ja edastuse märgise registrites REG02 ja REG08.
- 4.1.2 [Processor] Process Owner / Business Owner PEAB enne töötlemise alustamist registreerima pilve PII töötlemise dokumenteeritud kliendi juhised registris REG08.
- 4.1.3 [Subprocessor] Process Owner / Business Owner PEAB enne PII töötlemist pilve alltöötajana registreerima ülesvoolu volitatud töötajate või kliendi heakskiidetud juhised registris REG08.
- 4.1.4 [Processor] Privacy Lead / PIMS Manager PEAB enne uue pilve PII töötlemise teenuse väljalaskmist või olulist muutmist registreerima pilve volitatud töötajate kontrollimeetmete kohaldatavuse registris REG03.
- 4.1.5 [Processor] Data Protection Officer / Privacy Advisor PEAB enne organisatsiooni tegutsemist juhise alusel läbi vaatama registris REG12 iga kliendi juhise, mis näib olevat vastuolus dokumenteeritud kliendi kohustuste, PIMS-i nõuete või heakskiidetud teenuse ulatusega.
- 4.1.6 [Processor] Process Owner / Business Owner PEAB registreerima registris REG12 iga kavandatud kliendi PII töötlemise väljaspool dokumenteeritud kliendi juhiseid ning saama Privacy Lead / PIMS Manager heakskiidu enne töötlemise toimumist.

4.2 Pilve konfiguratsioon, rentnike isoleerimine, juurdepääs ja logimine

- 4.2.1 [Processor] Information Security Lead PEAB enne kliendi kasutuselevõttu või olulist teenusemuudatust registreerima registris REG08 pilve jagatud vastutuse piiri PII juurdepääsu, halduse, logimise, varundamise, krüptimise, haavatavuste halduse ja kustutamise kohta.

- 4.2.2 [Processor] System Owner / Application Owner PEAB enne tootmiskasutust ja pärast olulist arhitektuurimuudatust valideerima rentnike isoleerimise või kliendi eraldamise kontrollimeetmed registris REG12.
- 4.2.3 [Processor] System Owner / Application Owner PEAB andma pilve haldusjuurdepääsu kliendi PII-le ainult pärast seda, kui heakskiidetud ärivajadus, juurdepääsu ulatus, juurdepääsu kestus ja läbivaatamise sagedus on registreeritud registris REG12.
- 4.2.4 [Processor] Information Security Lead PEAB vähemalt kord kvartalis läbi vaatama privilegeeritud pilvejuurdepääsu, tugijuurdepääsu, kliendi PII juurdepääsu ja logimise katvuse registris REG12.
- 4.2.5 [Processor] System Owner / Application Owner PEAB enne väljalaset ja pärast olulist keskkonnamuudatust valideerima kliendi PII jaoks tootmis-, vahe-, test- ja tugikeskkondade lahususe registris REG12.
- 4.2.6 [Processor] System Owner / Application Owner PEAB enne pilve kliendi PII varundus-, replikatsiooni-, logisalvestus- ja tugijuurdepääsu asukohtade lubamist või muutmist registreerima need asukohad registris REG02, REG08 või REG09.

[... Jaotised 4.3–8 ei ole selles eelvaates. Täieliku sisu saamiseks ostke täisdokument. ...]

9. Erandid

- 9.1 [Processor] Process Owner / Business Owner PEAB enne kasutuselevõttu, väljalaset, uuendamist või jätkuvat kasutamist taotlema registris REG12 pilve volitatud töötleja erandit, kui nõutav kliendi juhise, alltöötleja, asukoha, juurdepääsu, logimise, kustutamise või intsidendiliidese tõendusmaterjal on puudulik.
- 9.2 [Processor] Data Protection Officer / Privacy Advisor PEAB enne heakskiitu läbi vaatama privaatsuse seisukohast olulised pilve volitatud töötleja eranditaotlused registris REG12, kui erand mõjutab kliendi juhiseid, isikuandmesubjekti abistamist, edastusi, alltöötlejaid, kustutamist, rikkumistoetust või suure mõjuga PII-d.
- 9.3 [Processor] Top Management PEAB enne erandi jõustumist heaks kiitma kõrge riskiga või olulised pilve volitatud töötleja erandid registris REG12.
- 9.4 [Processor] Privacy Lead / PIMS Manager PEAB enne heakskiitu määrama igale heakskiidetud pilve volitatud töötleja erandile registris REG12 aegumiskuupäeva, parandusmeetme omaniku, läbivaatamise kuupäeva ja jääkriski märkuse.

10. Järgimise tagamine

- 10.1 [Processor] Privacy Lead / PIMS Manager PEAB blokeerima kliendi kasutuselevõtu, teenuse väljalaske, uuendamise või jätkuva töötlemise, kui nõutav REG02, REG03, REG08, REG09, REG10 või REG12 tõendusmaterjal puudub enne töötlemise algust või jätkumist.
- 10.2 [Processor] System Owner / Application Owner PEAB ühe tööpäeva jooksul pärast rakendamisotsust keelama heakskiitmata pilvejuurdepääsu, heakskiitmata regiooni kasutamise, heakskiitmata replikatsiooni, heakskiitmata tugijuurdepääsu või heakskiitmata alltöötleja andmevoo ning registreerima lõpetamise registris REG08 või REG12.
- 10.3 [Processor] Vendor / Procurement Owner PEAB peatama uue PII töötlemise heakskiitmata või mittevastava pilve alltöötleja poolt kuni REG08 parandusmeetmete tõendusmaterjal on täielik.
- 10.4 [Processor] Incident Response Coordinator PEAB eskaleerima kliendi intsidenditeavituse tähtaegade ületamise registrites REG10 ja REG12 ühe tööpäeva jooksul pärast tuvastamist.
- 10.5 [Processor] Internal Audit / Compliance Reviewer PEAB 60 päeva jooksul pärast parandusmeetme sulgemist kontrollima parandusmeetme tõhusust oluliste või korduvate pilve volitatud töötleja mittevastavuste puhul registris REG12.

11. Läbivaatamine ja ajakohastamine

- 11.1 [Processor] Privacy Lead / PIMS Manager PEAB käesoleva poliitika registris REG12 läbi vaatama kord aastas ning 30 päeva jooksul pärast olulist muudatust pilve volitatud töötaja kohustustes, pilvearhitektuuris, alltöötajate juhtimises, kliendi abistamises, kustutamise võimekuses või sertifitseerimisnõuetes.
- 11.2 [Processor] Vendor / Procurement Owner PEAB vähemalt kord aastas ja enne uuendamist läbi vaatama pilve alltöötaja ja pilveteenuse sõltuvuse kirjed registris REG08.
- 11.3 [Processor] System Owner / Application Owner PEAB vähemalt kord aastas ja pärast olulist arhitektuurimuudatust läbi vaatama rentnike isoleerimise, privilegeeritud juurdepääsu, logimise, varunduse, replikatsiooni ja kustutamise tõendusmaterjali registris REG12.
- 11.4 [Processor] Privacy Lead / PIMS Manager PEAB vähemalt kord aastas ja 15 tööpäeva jooksul pärast olulist asukoha, tugijuurdepääsu, varunduse või alltöötaja muudatust läbi vaatama registri REG09 pilve asukoha ja edastuse marsruutimise kirjed.
- 11.5 [Processor] Privacy Lead / PIMS Manager PEAB 15 tööpäeva jooksul pärast heakskiidetud poliitikamuudatust, mis mõjutavad pilve volitatud töötaja kontrollimeetmete kohaldatavust, uuendama registrit REG03.
- 11.6 [All] Top Management PEAB enne avaldamist heaks kiitma käesoleva poliitika olulised muudatused registris REG12.

12. Seotud poliitikad

- 12.1 Käesolevat poliitikat toetavad järgmised seotud poliitikad:
- 12.2 PII01 - Privaatsusteabe haldussüsteemi poliitika
- 12.3 PII02 - Privaatsusrollide, vastutuste ja vastutuse poliitika
- 12.4 PII03 - PII töötlemisregistri ja õigusliku aluse poliitika
- 12.5 PII06 - Isikuandmesubjekti õiguste halduse poliitika
- 12.6 PII07 - Privaatsusriskide hindamise ja DPIA poliitika
- 12.7 PII08 - Lõimitud ja vaikimisi andmekaitse poliitika
- 12.8 PII09 - PII kogumise, kasutamise, avalikustamise ja jagamise poliitika
- 12.9 PII10 - PII säilitamise, kustutamise ja kõrvaldamise poliitika
- 12.10 PII12 - Volitatud töötaja, alltöötaja ja kolmanda osapoole privaatsushalduse poliitika
- 12.11 PII13 - Rahvusvahelise PII edastamise poliitika
- 12.12 PII14 - PII turvalisuse ja juurdepääsukontrolli poliitika
- 12.13 PII15 - PII intsidendi- ja rikkumishalduse poliitika
- 12.14 PII17 - PIMS-i dokumenteeritud teabe ja tõendusmaterjali halduse poliitika
- 12.15 PII18 - PIMS-i seire, auditi ja parendamise poliitika
- 12.16 PII20 - Laste privaatsuse poliitika
- 12.17 PII21 - Tehisintellekti ja automatiseeritud otsuste tegemise privaatsuspoliitika
- 12.18 PII22 - Turunduse privaatsuse ja küpsiste poliitika
- 12.19 PII24 - Videovalve ja füüsilise jälgimise privaatsuspoliitika

13. Viitestandardid ja raamistikud

- 13.1 Käesolev poliitika on vastendatud järgmiste standardite ja regulatsioonidega. Vastendus selgitab, kuidas poliitika toetab viidatud nõudeid, ning tuvastab sisemised punktid, mis neid rakendavad või toetavad.
- 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].