

				Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: PII23				Naziv dokumenta: Politika izvršitelja obrade PII-ja u oblaku							
Verzija: 1.0		Datum stupanja na snagu: 01.01.2025		Vlasnik dokumenta:							
X	Politika		Standard		Postupak		Obrazac		Registar		Drugo

Povijest revizija				
Broj revizije	Datum revizije	Promjene	Pregledao/la	Vlasnik procesa

Odobrenja			
Ime	Radno mjesto	Datum	Potpis

Pravna napomena (autorska prava i ograničenja uporabe)
(C) 2025 Clarysec LLC. All rights reserved.

Ovaj dokument intelektualno je vlasništvo društva Clarysec LLC. Nijedan dio ovog dokumenta ne smije se kopirati, ponovno upotrebljavati, distribuirati niti mijenjati u komercijalne svrhe ili svrhe implementacije bez izričitog prethodnog pisanog odobrenja.

Neovlaštena uporaba strogo je zabranjena i može rezultirati pravnim postupkom.

Za licenciranje kontaktirajte: info@clarysec.com

Usklađeno sa standardima i propisima

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 4.1; Clause 6.1.3	Processor	Supporting	Uloga u PIMS-u i primjenjivost kontrola
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Processor	Primary	Dokumentirani dokazi o izvršitelju obrade u oblaku i operativna kontrola
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Processor	Supporting	Praćenje, nesukladnost i korektivna radnja
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	Ugovori s klijentima, upute, podrška i zapisi
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Pomoć klijentima u vezi s obvezama prema ispitanicima
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Primary	Privremene datoteke, povrat, prijenos, zbrinjavanje i kontrole prijenosa podataka
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Supporting	Osnova prijenosa i lokacije
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Zapisi o otkrivanju podataka i postupanje sa zahtjevima za otkrivanje podataka
ISO/IEC 27701:2025	Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9	Processor	Primary	Objavljivanje podataka o podizvršiteljima, angažman i obavijest o promjeni
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	Dokazi o pristupu, zapisima, sigurnosnim kopijama i zapisivanju događaja

GDPR	Article 28	Processor	Primary	Izvršitelj obrade, podizvršitelj obrade, pomoć, revizija, brisanje i povrat
GDPR	Article 30	Processor	Supporting	Zapisi izvršitelja obrade
GDPR	Article 32; Article 33	Processor	Supporting	Sigurnost i obavješćivanje voditelja obrade o povredi
GDPR	Article 44	Conditional	Referenced	Usmjeravanje međunarodnih prijenosa
ISO/IEC 29100:2020	Clause 5.3; Clause 5.5; Clause 5.6	Processor	Supporting	Ograničenje svrhe, minimizacije, uporabe, zadržavanja i otkrivanja podataka
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Processor	Supporting	Odgovornost, informacijska sigurnost i usklađenost
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	Vrednovanje i praćenje izvršitelja obrade te kontrole promjena i zadržavanja
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	Primjenjivost kontrola, operativna kontrola i kontrole dobavljača/usluga u oblaku
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	Kontrole dobavljača, oblaka, brisanja, zapisivanja događaja i praćenja
ISO/IEC 27018:2020	Annex A.2.1; Annex A.3.1	Processor	Primary	Pomoć klijentima koju pruža izvršitelj obrade u oblaku i ograničenje svrhe
ISO/IEC 27018:2020	Annex A.6.1; Annex A.6.2; Annex A.8.1	Processor	Primary	Obavješćivanje o otkrivanju podataka

				u oblaku, zapisi o otkrivanju podataka i transparentnost podizvršitelja
ISO/IEC 27018:2020	Annex A.10.1; Annex A.10.3; Annex A.11.11; Annex A.11.12; Annex A.12.1	Processor	Primary	Sučelje za povrede u oblaku, izlaz, ugovorne mjere, podugovori i zapisi o lokacijama
ISO/IEC 27036-2:2022	Clause 6.1.1; Clause 6.1.2	Processor	Supporting	Strategija i upravljanje odnosima u opskrbi
ISO/IEC 27036-2:2022	Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5	Processor	Supporting	Planiranje, ugovaranje, upravljanje, praćenje i raskid odnosa s dobavljačima
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	Okvir i dokumentacija za brisanje
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	Provedba brisanja i iznimke

1. Opseg

1.1 Ova politika definira obvezne zahtjeve privatnosti za usluge u oblaku u kojima organizacija djeluje kao izvršitelj obrade ili podizvršitelj obrade PII-ja, uključujući SaaS, PaaS, IaaS, hostirane aplikacije, upravljani oblak, podršku u oblaku, pohranu u oblaku, analitiku u oblaku i usluge infrastrukture oblaka koje obrađuju PII u ime klijenata.

1.2 Ova se politika primjenjuje na obradu u oblaku koja se provodi na temelju ugovora s klijentima, dokumentiranih uputa klijenta, uputa uzvodnog izvršitelja obrade, aranžmana podizvršitelja obrade, konfiguracije regije u oblaku, pristupa podrške u oblaku, administriranja usluge, sigurnosnog kopiranja, replikacije, zapisivanja događaja, praćenja, brisanja, povrata, podrške u vezi s povredama, revizijske podrške i obveza pomoći klijentima.

1.3 Ova politika obuhvaća:

1.3.1 opseg obrade PII-ja u oblaku i zapise o uputama;

1.3.2 ugovor s klijentom i dokaze o granici podijeljene odgovornosti;

1.3.3 dokaze o izolaciji zakupaca, pristupu oblaku, administrativnom pristupu i zapisivanju događaja;

1.3.4 upravljanje podizvršiteljima obrade i opskrbnim lancem u oblaku;

1.3.5 lokaciju, udaljeni pristup i usmjeravanje međunarodnih prijenosa;

1.3.6 dokaze o povratu, prijenosu, brisanju, zbrinjavanju i izlaznom postupku;

1.3.7 pomoć klijentima u vezi s pravima ispitanika, DPIA-ama, revizijama i odgovorom na povredu;

1.3.8 dokaze o praćenju, iznimkama, provedbi i poboljšanjima.

1.4 Ova politika ne uspostavlja zaseban registar ugovora s klijentima, registar usluga u oblaku, registar izolacije zakupaca, registar pristupa, registar dnevnčkih zapisa, registar brisanja, registar zahtjeva za podršku, registar revizijskih dokaza, registar povreda, registar podizvršitelja obrade niti odbor za upravljanje oblakom.

1.5 Ova politika ne zamjenjuje:

1.5.1 PII03 za popis obrada i vlasništvo nad pravnom osnovom;

1.5.2 PII06 za cjeloviti tijek rada za prava ispitanika;

1.5.3 PII07 za metodologiju procjene rizika za privatnost i DPIA-e;

1.5.4 PII08 za kontrolne točke ugrađene zaštite privatnosti i zaštite privatnosti prema zadanim postavkama;

1.5.5 PII09 za opće kontrole prikupljanja, uporabe, otkrivanja i dijeljenja podataka;

1.5.6 PII10 za metodologiju zadržavanja, brisanja i zbrinjavanja;

1.5.7 PII12 za opće upravljanje životnim ciklusom izvršitelja obrade, podizvršitelja obrade i trećih strana;

1.5.8 PII13 za procjenu mehanizama međunarodnog prijenosa;

1.5.9 PII14 za cjelovitu sigurnosnu arhitekturu i arhitekturu kontrole pristupa za PII;

1.5.10 PII15 za tijek rada upravljanja incidentima i povredama;

1.5.11 PII17 za upravljanje dokumentiranim informacijama;

1.5.12 PII18 za upravljanje praćenjem, revizijom i poboljšanjem PIMS-a.

2. Svrha

2.1 Svrha je ove politike osigurati da se usluge izvršitelja obrade i podizvršitelja obrade PII-ja u oblaku pružaju na temelju dokumentiranih uputa klijenta, jasnog opsega obrade, kontroliranih aranžmana podizvršitelja obrade, odgovarajućih sigurnosnih odgovornosti u oblaku, dokumentiranih lokacija i

usmjeravanja prijenosa, obveza pomoći klijentima, podrške u vezi s povredama, mogućnosti brisanja/povrata i dokaza spremnih za reviziju.

2.2 Ova politika podupire spremnost za certifikaciju prema ISO/IEC 27701:2025 PIMS-u za izvršitelje obrade u oblaku i podizvršitelje obrade u oblaku, uz zadržavanje integracije s postojećim skupom PIMS politika i kanonskim objektima dokaza.

3. Ciljevi

3.1 Ciljevi su ove politike:

- 3.1.1 Definirati opseg obrade PII-ja u oblaku prije uvođenja klijenta ili značajne promjene.
- 3.1.2 Osigurati da se upute klijenta evidentiraju, pregledavaju i slijede.
- 3.1.3 Održavati dokaze o izvršitelju obrade i podizvršitelju obrade u oblaku u kanonskim PIMS registrima.
- 3.1.4 Definirati dokaze o granici podijeljene odgovornosti, izolaciji zakupaca, pristupu, zapisivanju događaja i lokaciji bez dupliciranja politike sigurnosti PII-ja.
- 3.1.5 Kontrolirati dokaze o uvođenju, promjeni, prenesenim obvezama i praćenju podizvršitelja obrade.
- 3.1.6 Podržati klijente u vezi s pravima ispitanika, DPIA-ama, zahtjevima za reviziju i odgovorom na povredu.
- 3.1.7 Osigurati zadržavanje dokaza o povratu, brisanju, prijenosu i zbrinjavanju pri izlazu.
- 3.1.8 Pratiti kontrole izvršitelja obrade u oblaku i pokretati korektivne radnje putem REG12.

4. Izjave politike

4.1 Opseg obrade u oblaku i upute klijenta

- 4.1.1 [Processor] Privacy Lead / PIMS Manager mora evidentirati svaku uslugu obrade PII-ja u oblaku, ulogu obrade za klijenta, izvor uputa klijenta, kategorije PII-ja, kategorije ispitanika, svrhu usluge, lokaciju obrade, ovisnost o podizvršitelju obrade, ovisnost o brisanju i oznaku prijenosa u REG02 i REG08 prije uvođenja klijenta ili značajne promjene usluge.
- 4.1.2 [Processor] Process Owner / Business Owner mora evidentirati dokumentirane upute klijenta za obradu PII-ja u oblaku u REG08 prije početka obrade.
- 4.1.3 [Subprocessor] Process Owner / Business Owner mora evidentirati upute uzvodnog izvršitelja obrade ili upute koje je odobrio klijent u REG08 prije obrade PII-ja kao podizvršitelj obrade u oblaku.
- 4.1.4 [Processor] Privacy Lead / PIMS Manager mora evidentirati primjenjivost kontrola izvršitelja obrade u oblaku u REG03 prije puštanja u rad ili značajne promjene nove usluge obrade PII-ja u oblaku.
- 4.1.5 [Processor] Data Protection Officer / Privacy Advisor mora pregledati svaku uputu klijenta koja se čini neusklađenom s dokumentiranim obvezama klijenta, zahtjevima PIMS-a ili odobrenim opsegom usluge u REG12 prije nego što organizacija postupi po toj uputi.
- 4.1.6 [Processor] Process Owner / Business Owner mora evidentirati svaku predloženu obradu PII-ja klijenta izvan dokumentiranih uputa klijenta u REG12 i ishoditi odobrenje Privacy Lead / PIMS Manager prije obrade.

4.2 Konfiguracija oblaka, izolacija zakupaca, pristup i zapisivanje događaja

- 4.2.1 [Processor] Information Security Lead mora evidentirati granicu podijeljene odgovornosti u oblaku za pristup PII-ju, administraciju, zapisivanje događaja, sigurnosno kopiranje, šifriranje, upravljanje ranjivostima i brisanje u REG08 prije uvođenja klijenta ili značajne promjene usluge.

- 4.2.2 [Processor] System Owner / Application Owner mora potvrditi kontrole izolacije zakupaca ili segregacije klijenata u REG12 prije produkcijske uporabe i nakon značajne promjene arhitekture.
- 4.2.3 [Processor] System Owner / Application Owner smije dodijeliti administrativni pristup PII-ju klijenta u oblaku tek nakon što se u REG12 evidentiraju odobrena poslovna potreba, opseg pristupa, trajanje pristupa i učestalost pregleda.
- 4.2.4 [Processor] Information Security Lead mora najmanje tromjesečno pregledati privilegirani pristup oblaku, pristup podrške, pristup PII-ju klijenta i obuhvat zapisivanja događaja u REG12.
- 4.2.5 [Processor] System Owner / Application Owner mora potvrditi razdvajanje produkcijskih, pripremnih, testnih i podržnih okruženja za PII klijenta u REG12 prije izdanja i nakon značajne promjene okruženja.
- 4.2.6 [Processor] System Owner / Application Owner mora evidentirati lokacije sigurnosnih kopija, replikacije, pohrane dnevnčkih zapisa i pristupa podrške za PII klijenta u oblaku u REG02, REG08 ili REG09 prije omogućavanja ili promjene tih lokacija.

[... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ...]

9. Iznimke

- 9.1 [Processor] Process Owner / Business Owner mora zatražiti iznimku izvršitelja obrade u oblaku u REG12 prije uvođenja, izdanja, obnove ili nastavka uporabe kada su potrebni dokazi o uputama klijenta, podizvršitelju obrade, lokaciji, pristupu, zapisivanju događaja, brisanju ili sučelju za incidente nepotpuni.
- 9.2 [Processor] Data Protection Officer / Privacy Advisor mora pregledati zahtjeve za iznimku izvršitelja obrade u oblaku značajne za privatnost u REG12 prije odobrenja kada iznimka utječe na upute klijenta, pomoć ispitanicima, prijenose, podizvršitelje obrade, brisanje, podršku u vezi s povredama ili PII visokog utjecaja.
- 9.3 [Processor] Top Management mora odobriti visokorizične ili značajne iznimke izvršitelja obrade u oblaku u REG12 prije stupanja iznimke na snagu.
- 9.4 [Processor] Privacy Lead / PIMS Manager mora dodijeliti datum isteka, vlasnika otklanjanja, datum pregleda i napomenu o preostalom riziku u REG12 za svaku odobrenu iznimku izvršitelja obrade u oblaku prije odobrenja.

10. Provedba

- 10.1 [Processor] Privacy Lead / PIMS Manager mora blokirati uvođenje klijenta, izdanje usluge, obnovu ili nastavak obrade kada nedostaju potrebni dokazi u REG02, REG03, REG08, REG09, REG10 ili REG12 prije početka ili nastavka obrade.
- 10.2 [Processor] System Owner / Application Owner mora onemogućiti neodobreni pristup oblaku, neodobrenu uporabu regije, neodobrenu replikaciju, neodobreni pristup podrške ili neodobreni tok podataka prema podizvršitelju obrade u roku od jednog radnog dana nakon odluke o provedbi i evidentirati dovršetak u REG08 ili REG12.
- 10.3 [Processor] Vendor / Procurement Owner mora obustaviti novu obradu PII-ja od strane neodobrenog ili nesukladnog podizvršitelja obrade u oblaku dok dokazi o korektivnoj radnji u REG08 ne budu potpuni.
- 10.4 [Processor] Incident Response Coordinator mora eskalirati propuštene rokove za obavješćivanje klijenata o incidentima u REG10 i REG12 u roku od jednog radnog dana nakon utvrđivanja.
- 10.5 [Processor] Internal Audit / Compliance Reviewer mora provjeriti djelotvornost korektivnih radnji za veće ili ponavljajuće nesukladnosti izvršitelja obrade u oblaku u REG12 u roku od 60 dana nakon zatvaranja korektivne radnje.

11. Pregled i održavanje

- 11.1 [Processor] Privacy Lead / PIMS Manager mora jednom godišnje i u roku od 30 dana nakon značajne promjene obveza izvršitelja obrade u oblaku, arhitekture oblaka, upravljanja podizvršiteljima obrade, pomoći klijentima, mogućnosti brisanja ili zahtjeva certifikacije pregledati ovu politiku u REG12.
- 11.2 [Processor] Vendor / Procurement Owner mora pregledati zapise o podizvršiteljima obrade u oblaku i ovisnostima o uslugama u oblaku u REG08 najmanje jednom godišnje i prije obnove.
- 11.3 [Processor] System Owner / Application Owner mora pregledati dokaze o izolaciji zakupaca, privilegiranom pristupu, zapisivanju događaja, sigurnosnom kopiranju, replikaciji i brisanju u REG12 najmanje jednom godišnje i nakon značajne promjene arhitekture.
- 11.4 [Processor] Privacy Lead / PIMS Manager mora pregledati zapise o lokacijama u oblaku i usmjeravanju prijenosa u REG09 najmanje jednom godišnje i u roku od 15 radnih dana nakon značajne promjene lokacije, pristupa podrške, sigurnosnog kopiranja ili podizvršitelja obrade.
- 11.5 [Processor] Privacy Lead / PIMS Manager mora ažurirati REG03 u roku od 15 radnih dana nakon odobrenih izmjena politike koje utječu na primjenjivost kontrola izvršitelja obrade u oblaku.
- 11.6 [All] Top Management mora odobriti značajne izmjene ove politike u REG12 prije objave.

12. Povezane politike

- 12.1 Ovu politiku podupiru sljedeće povezane politike:
- 12.2 PII01 - Politika sustava upravljanja informacijama o privatnosti
- 12.3 PII02 - Politika uloga, odgovornosti i odgovornosti za postupanje u području privatnosti
- 12.4 PII03 - Politika popisa obrada PII-ja i pravne osnove
- 12.5 PII06 - Politika upravljanja pravima ispitanika
- 12.6 PII07 - Politika procjene rizika za privatnost i DPIA-e
- 12.7 PII08 - Politika ugrađene zaštite privatnosti i zaštite privatnosti prema zadanim postavkama
- 12.8 PII09 - Politika prikupljanja, uporabe, otkrivanja i dijeljenja PII-ja
- 12.9 PII10 - Politika zadržavanja, brisanja i zbrinjavanja PII-ja
- 12.10 PII12 - Politika upravljanja privatnošću izvršitelja obrade, podizvršitelja obrade i trećih strana
- 12.11 PII13 - Politika međunarodnog prijenosa PII-ja
- 12.12 PII14 - Politika sigurnosti i kontrole pristupa za PII
- 12.13 PII15 - Politika upravljanja incidentima i povredama PII-ja
- 12.14 PII17 - Politika upravljanja dokumentiranim informacijama i dokazima PIMS-a
- 12.15 PII18 - Politika praćenja, revizije i poboljšanja PIMS-a
- 12.16 PII20 - Politika privatnosti djece
- 12.17 PII21 - Politika privatnosti za AI i automatizirano donošenje odluka
- 12.18 PII22 - Politika privatnosti u marketingu i kolačića
- 12.19 PII24 - Politika privatnosti za CCTV i fizičko praćenje

13. Referentni standardi i okviri

- 13.1 Ova je politika mapirana na sljedeće standarde i propise. Mapiranje objašnjava kako politika podupire navedene zahtjeve i utvrđuje interne točke koje ih provode ili podupiru.
- 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].