

				Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: PII23				Naslov dokumenta: <b>Politika obdelovalca PII v oblaku</b>							
Različica: 1.0		Datum začetka veljavnosti: 01.01.2025		Lastnik dokumenta:							
X	Politika		Standard		Postopek		Obrazec		Register		Drugo

Zgodovina revizij				
Številka revizije	Datum revizije	Spremembe	Pregledal	Lastnik procesa

Odobritve			
Ime	Delovno mesto	Datum	Podpis

<p><b>Pravno obvestilo (avtorske pravice in omejitve uporabe)</b>  (C) 2025 Clarysec LLC. All rights reserved.</p> <p>Ta dokument je intelektualna lastnina družbe Clarysec LLC. Noben del tega dokumenta se ne sme kopirati, ponovno uporabiti, distribuirati ali spreminjati za komercialne ali implementacijske namene brez predhodnega izrecnega pisnega dovoljenja.</p> <p>Nepooblaščen uporaba je strogo prepovedana in lahko povzroči pravne ukrepe.</p> <p>Za licenciranje se obrnite na: <a href="mailto:info@clarysec.com">info@clarysec.com</a></p>
--

## Usklajenost s standardi in predpisi

Standard/predpis	Klavzula/kontrola/člen	Uporabljivost	Vrsta pokritosti	Komentar
ISO/IEC 27701:2025	Clause 4.1; Clause 6.1.3	Processor	Supporting	Vloga PIMS in uporabljivost kontrol
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Processor	Primary	Dokumentirana dokazila obdelovalca v oblaku in operativni nadzor
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Processor	Supporting	Spremljanje, neskladnost in korektivni ukrep
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	Dogovori z naročniki, navodila, podpora in evidence
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Pomoč naročniku pri obveznostih do posameznikov, na katere se nanašajo osebno določljivi podatki
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Primary	Začasne datoteke, vračilo, prenos, odstranjevanje in kontrole prenosa
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Supporting	Podlaga za prenos in lokacije
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Evidence razkritij in obravnava zahtev za razkritje
ISO/IEC 27701:2025	Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9	Processor	Primary	Razkritje podobdelovalcev, vključitev in obvestilo o spremembi
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	Dokazila o dostopu, evidencah, varnostnem kopiranju in beleženju
GDPR	Article 28	Processor	Primary	Obdelovalec, podobdelovalec, pomoč, revizija, izbris in vračilo

GDPR	Article 30	Processor	Supporting	Evidence obdelovalca
GDPR	Article 32; Article 33	Processor	Supporting	Varnost in obveščanje upravljavca o kršitvi
GDPR	Article 44	Conditional	Referenced	Usmerjanje mednarodnih prenosov
ISO/IEC 29100:2020	Clause 5.3; Clause 5.5; Clause 5.6	Processor	Supporting	Namen, minimizacija, uporaba, hramba in omejitve razkritja
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Processor	Supporting	Odgovornost, informacijska varnost in skladnost
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	Presoja obdelovalca, spremljanje, spremembe in kontrole hrambe
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	Uporabljenost kontrol, operativni nadzor in kontrole dobaviteljev/oblaka
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 dobaviteljev, oblaka, izbrisa, beleženja in spremljanja
ISO/IEC 27018:2020	Annex A.2.1; Annex A.3.1	Processor	Primary	Pomoč naročniku s strani obdelovalca v oblaku in omejitve namena
ISO/IEC 27018:2020	Annex A.6.1; Annex A.6.2; Annex A.8.1	Processor	Primary	Obvestila o razkritju v oblaku, evidence razkritij in preglednost podobdelovalcev
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	Vmesnik za kršitve v oblaku, izstop, pogodbeni ukrepi, podpogodbe in evidence lokacij

ISO/IEC 27036-2:2022	Clause 6.1.1; Clause 6.1.2	Processor	Supporting	Strategija in upravljanje dobavnih razmerij
ISO/IEC 27036-2:2022	Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5	Processor	Supporting	Načrtovanje, dogovor, upravljanje, spremljanje in prenehanje razmerja z dobaviteljem
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 izbrisa in dokumentacija
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	Izvedba izbrisa in izjeme

## 1. Področje uporabe

1.1 Ta politika določa obvezne zahteve glede zasebnosti za storitve v oblaku, pri katerih organizacija deluje kot obdelovalec ali podobdelovalec PII, vključno s storitvami SaaS, PaaS, IaaS, gostovanimi aplikacijami, upravljanim oblakom, podporo v oblaku, shrambo v oblaku, analitiko v oblaku in infrastrukturo v oblaku, ki obdelujejo PII v imenu naročnikov.

1.2 Ta politika se uporablja za obdelavo v oblaku, ki se izvaja na podlagi dogovorov z naročniki, dokumentiranih navodil naročnika, navodil nadrejenega obdelovalca, ureditev s podobdelovalci, konfiguracije regije v oblaku, dostopa podpore v oblaku, administracije storitev, varnostnega kopiranja, replikacije, beleženja, spremljanja, izbrisa, vračila, podpore pri kršitvah, podpore pri revizijah in obveznosti pomoči naročniku.

### 1.3 Ta politika zajema:

1.3.1 obseg obdelave PII v oblaku in evidence navodil;

1.3.2 dokazila o dogovorih z naročniki in deljeni odgovornosti;

1.3.3 dokazila o izolaciji najemnikov, dostopu v oblaku, administrativnem dostopu in beleženju;

1.3.4 upravljanje podobdelovalcev in dobavne verige v oblaku;

1.3.5 lokacijo, oddaljeni dostop in usmerjanje mednarodnih prenosov;

1.3.6 dokazila o vračilu, prenosu, izbrisu, odstranjevanju in izstopu;

1.3.7 pomoč naročniku pri pravicah posameznikov, na katere se nanašajo osebno določljivi podatki, DPIA, revizijah in odzivu na kršitve;

1.3.8 dokazila o spremljanju, izjemah, uveljavljanju in izboljševanju.

1.4 Ta politika ne vzpostavlja ločenega registra pogodb z naročniki, registra storitev v oblaku, registra izolacije najemnikov, registra dostopov, registra dnevnikov, registra izbrisov, registra zahtevkov za podporo, registra revizijskih dokazil, registra kršitev, registra podobdelovalcev ali odbora za upravljanje oblaka.

### 1.5 Ta politika ne nadomešča:

1.5.1 PII03 za popis dejavnosti obdelave in lastništvo pravnih podlag;

1.5.2 PII06 za celoten delovni tok pravic posameznikov, na katere se nanašajo osebno določljivi podatki;

1.5.3 PII07 za metodologijo tveganj za zasebnost in DPIA;

1.5.4 PII08 za kontrolne točke varstva zasebnosti že pri načrtovanju in privzeto;

1.5.5 PII09 za splošne kontrole zbiranja, uporabe, razkritja in deljenja;

1.5.6 PII10 za metodologijo hrambe, izbrisa in odstranjevanja;

1.5.7 PII12 za splošno upravljanje življenjskega cikla obdelovalcev, podobdelovalcev in tretjih oseb;

1.5.8 PII13 za presojo mehanizmov mednarodnega prenosa;

1.5.9 PII14 za celotno varnostno arhitekturo in arhitekturo nadzora dostopa za PII;

1.5.10 PII15 za delovni tok upravljanja incidentov in kršitev;

1.5.11 PII17 za nadzor dokumentiranih informacij;

1.5.12 PII18 za upravljanje spremljanja, revizij in izboljševanja PIMS.

## 2. Namen

2.1 Namen te politike je zagotoviti, da se storitve obdelovalca in podobdelovalca PII v oblaku izvajajo na podlagi dokumentiranih navodil naročnika, jasnega obsega obdelave, nadzorovanih ureditev s podobdelovalci, ustreznih varnostnih odgovornosti v oblaku, dokumentiranih lokacij in usmerjanja prenosov, obveznosti pomoči naročniku, podpore pri kršitvah, zmožnosti izbrisa/vračila ter dokazil, pripravljenih za revizijo.

2.2 Ta politika podpira pripravljenost na certifikacijo PIMS po ISO/IEC 27701:2025 za obdelovalce v oblaku in podobdelovalce v oblaku, pri čemer ostaja integrirana z obstoječim naborom politik PIMS in kanoničnimi dokaznimi objekti.

### 3. Cilji

#### 3.1 Cilji te politike so:

- 3.1.1 Določiti obseg obdelave PII v oblaku pred uvedbo naročnika ali bistveno spremembo.
- 3.1.2 Zagotoviti, da so navodila naročnika evidentirana, pregledana in upoštevana.
- 3.1.3 Vzdrževati dokazila o obdelovalcih in podobdelovalcih v oblaku v kanoničnih registrih PIMS.
- 3.1.4 Določiti dokazila o deljeni odgovornosti, izolaciji najemnikov, dostopu, beleženju in lokaciji brez podvajanja politike varnosti PII.
- 3.1.5 Nadzorovati dokazila o uvajanju podobdelovalcev, spremembah, prenesenih obveznostih in spremljanju.
- 3.1.6 Podpirati naročnike pri pravicah posameznikov, na katere se nanašajo osebno določljivi podatki, DPIA, revizijskih zahtevah in odzivu na kršitve.
- 3.1.7 Zagotoviti, da se dokazila o vračilu, izbrisu, prenosu in odstranjevanju hranijo ob izstopu.
- 3.1.8 Spremljati kontrole obdelovalca v oblaku in usmerjati korektivne ukrepe z uporabo REG12.

### 4. Izjave politike

#### 4.1 Obseg obdelave v oblaku in navodila naročnika

- 4.1.1 [Processor] Privacy Lead / PIMS Manager mora v REG02 in REG08 pred uvedbo naročnika ali bistveno spremembo storitve evidentirati vsako storitev obdelave PII v oblaku, vlogo naročnika pri obdelavi, vir navodil naročnika, kategorije PII, kategorije posameznikov, na katere se nanašajo osebno določljivi podatki, namen storitve, lokacijo obdelave, odvisnost od podobdelovalca, odvisnost pri izbrisu in oznako prenosa.
- 4.1.2 [Processor] Process Owner / Business Owner mora dokumentirana navodila naročnika za obdelavo PII v oblaku evidentirati v REG08 pred začetkom obdelave.
- 4.1.3 [Subprocessor] Process Owner / Business Owner mora navodila nadrejenega obdelovalca ali navodila, ki jih je odobril naročnik, evidentirati v REG08 pred obdelavo PII kot podobdelovalec v oblaku.
- 4.1.4 [Processor] Privacy Lead / PIMS Manager mora v REG03 evidentirati uporabljivost kontrol obdelovalca v oblaku, preden se nova storitev obdelave PII v oblaku sprosti v uporabo ali bistveno spremeni.
- 4.1.5 [Processor] Data Protection Officer / Privacy Advisor mora v REG12 pregledati vsako navodilo naročnika, za katero se zdi, da ni skladno z dokumentiranimi obveznostmi naročnika, zahtevami PIMS ali odobrenim obsegom storitve, preden organizacija ravna po navodilu.
- 4.1.6 [Processor] Process Owner / Business Owner mora v REG12 evidentirati vsako predlagano obdelavo PII naročnika zunaj dokumentiranih navodil naročnika in pridobiti odobritev Privacy Lead / PIMS Manager, preden se obdelava izvede.

#### 4.2 Konfiguracija oblaka, izolacija najemnikov, dostop in beleženje

- 4.2.1 [Processor] Information Security Lead mora v REG08 pred uvedbo naročnika ali bistveno spremembo storitve evidentirati mejo deljene odgovornosti v oblaku za dostop do PII, administracijo, beleženje, varnostno kopiranje, šifriranje, upravljanje ranljivosti in izbris.
- 4.2.2 [Processor] System Owner / Application Owner mora v REG12 validirati kontrole izolacije najemnikov ali ločevanja naročnikov pred produkcijsko uporabo in po bistveni spremembi arhitekture.

- 4.2.3 [Processor] System Owner / Application Owner sme dodeliti administrativni dostop v oblaku do PII naročnika šele po tem, ko so v REG12 evidentirani odobrena poslovna potreba, obseg dostopa, trajanje dostopa in pogostost pregleda.
- 4.2.4 [Processor] Information Security Lead mora najmanj četrletno v REG12 pregledati privilegirani dostop v oblaku, dostop podpore, dostop do PII naročnika in pokritost beleženja.
- 4.2.5 [Processor] System Owner / Application Owner mora v REG12 validirati ločevanje produkcijskih, pripravljalnih, testnih in podpornih okolij za PII naročnika pred izdajo in po bistveni spremembi okolja.
- 4.2.6 [Processor] System Owner / Application Owner mora v REG02, REG08 ali REG09 evidentirati lokacije varnostnih kopij, replikacije, hrambe dnevnikov in dostopa podpore za PII naročnika v oblaku, preden omogoči ali spremeni te lokacije.

[ ... Razdelki 4.3–8 niso vključeni v ta predogled. Kupite celoten dokument za dostop do celotne vsebine. ... ]

## 9. Izjeme

- 9.1 [Processor] Process Owner / Business Owner mora v REG12 zahtevati izjemo obdelovalca v oblaku pred uvedbo, izdajo, podaljšanjem ali nadaljnjo uporabo, kadar so zahtevana dokazila o navodilih naročnika, podobdelovalcih, lokaciji, dostopu, beleženju, izbrisu ali stični točki za obravnavo incidentov nepopolna.
- 9.2 [Processor] Data Protection Officer / Privacy Advisor mora v REG12 pred odobritvijo pregledati zahteve za izjeme obdelovalca v oblaku, pomembne z vidika zasebnosti, kadar izjema vpliva na navodila naročnika, pomoč posameznikom, na katere se nanašajo osebno določljivi podatki, prenose, podobdelovalce, izbris, podporo pri kršitvah ali PII z velikim vplivom.
- 9.3 [Processor] Top Management mora visoko tvegane ali bistvene izjeme obdelovalca v oblaku odobriti v REG12, preden izjema začne veljati.
- 9.4 [Processor] Privacy Lead / PIMS Manager mora za vsako odobreno izjemo obdelovalca v oblaku v REG12 pred odobritvijo dodeliti datum poteka, nosilca sanacije, datum pregleda in opombo o preostalem tveganju.

## 10. Uveljavljanje

- 10.1 [Processor] Privacy Lead / PIMS Manager mora blokirati uvedbo naročnika, izdajo storitve, podaljšanje ali nadaljnjo obdelavo, kadar zahtevana dokazila v REG02, REG03, REG08, REG09, REG10 ali REG12 manjkajo pred začetkom ali nadaljevanjem obdelave.
- 10.2 [Processor] System Owner / Application Owner mora v enem delovnem dnevu po odločitvi o uveljavljanju onemogočiti neodobren dostop v oblaku, neodobreno uporabo regije, neodobreno replikacijo, neodobren dostop podpore ali neodobren tok podatkov do podobdelovalca ter dokončanje evidentirati v REG08 ali REG12.
- 10.3 [Processor] Vendor / Procurement Owner mora začasno ustaviti novo obdelavo PII pri neodobrenem ali neskladnem podobdelovalcu v oblaku, dokler dokazila o korektivnem ukrepu v REG08 niso popolna.
- 10.4 [Processor] Incident Response Coordinator mora zamujene roke za obveščanje naročnika o incidentih eskalirati v REG10 in REG12 v enem delovnem dnevu po ugotovitvi.
- 10.5 [Processor] Internal Audit / Compliance Reviewer mora v REG12 preveriti učinkovitost korektivnih ukrepov za večje ali ponavljajoče se neskladnosti obdelovalca v oblaku v 60 dneh po zaprtju korektivnega ukrepa.

## 11. Pregled in vzdrževanje

- 11.1 [Processor] Privacy Lead / PIMS Manager mora to politiko v REG12 pregledati letno in v 30 dneh po bistveni spremembi obveznosti obdelovalca v oblaku, arhitekture oblaka, upravljanja podobdelovalcev, pomoči naročniku, zmožnosti izbrisa ali certifikacijskih zahtev.
- 11.2 [Processor] Vendor / Procurement Owner mora evidence podobdelovalcev v oblaku in odvisnosti od storitev v oblaku v REG08 pregledati najmanj letno in pred podaljšanjem.
- 11.3 [Processor] System Owner / Application Owner mora dokazila o izolaciji najemnikov, privilegiranem dostopu, beleženju, varnostnem kopiranju, replikaciji in izbrisu v REG12 pregledati najmanj letno in po bistveni spremembi arhitekture.
- 11.4 [Processor] Privacy Lead / PIMS Manager mora evidence o lokacijah v oblaku in usmerjanju prenosov v REG09 pregledati najmanj letno in v 15 delovnih dneh po bistveni spremembi lokacije, dostopa podpore, varnostnega kopiranja ali podobdelovalca.
- 11.5 [Processor] Privacy Lead / PIMS Manager mora REG03 posodobiti v 15 delovnih dneh po odobrenih spremembah politike, ki vplivajo na uporabljivost kontrol obdelovalca v oblaku.
- 11.6 [All] Top Management mora bistvene revizije te politike odobriti v REG12 pred objavo.

## 12. Povezane politike

- 12.1 To politiko podpirajo naslednje povezane politike:
- 12.2 PII01 - Politika sistema upravljanja informacij o zasebnosti
- 12.3 PII02 - Politika vlog, odgovornosti in odgovornosti za zasebnost
- 12.4 PII03 - Politika popisa obdelave PII in pravne podlage
- 12.5 PII06 - Politika upravljanja pravic posameznikov, na katere se nanašajo osebno določljivi podatki
- 12.6 PII07 - Politika ocenjevanja tveganj za zasebnost in DPIA
- 12.7 PII08 - Politika varstva zasebnosti že pri načrtovanju in privzeto
- 12.8 PII09 - Politika zbiranja, uporabe, razkritja in deljenja PII
- 12.9 PII10 - Politika hrambe, izbrisa in odstranjevanja PII
- 12.10 PII12 - Politika upravljanja zasebnosti obdelovalcev, podobdelovalcev in tretjih oseb
- 12.11 PII13 - Politika mednarodnih prenosov PII
- 12.12 PII14 - Politika varnosti PII in nadzora dostopa
- 12.13 PII15 - Politika upravljanja incidentov in kršitev v zvezi s PII
- 12.14 PII17 - Politika upravljanja dokumentiranih informacij in dokazil PIMS
- 12.15 PII18 - Politika spremljanja, revizij in izboljševanja PIMS
- 12.16 PII20 - Politika zasebnosti otrok
- 12.17 PII21 - Politika zasebnosti pri AI in avtomatiziranem sprejemanju odločitev
- 12.18 PII22 - Politika zasebnosti pri trženju in piškotkih
- 12.19 PII24 - Politika zasebnosti pri CCTV in fizičnem spremljanju

## 13. Referenčni standardi in okviri

- 13.1 Ta politika je preslikana na naslednje standarde in predpise. Preslikava pojasnjuje, kako politika podpira navedene zahteve, in opredeljuje notranje klavzule, ki jih izvajajo ali podpirajo.
- 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].

