					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: PII23					Názov dokumentu: **Politika cloudového sprostredkovateľa PII**							
Verzia: 1.0		Dátum nadobudnutia účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Štandard		Postup		Formulár		Register		Iné	

História revízií				
Číslo revízie	**Dátum revízie**	**Zmeny**	**Preskúmal**	**Vlastník procesu**

Schválenia			
Meno	**Pozícia**	**Dátum**	**Podpis**

Súlad s normami a predpismi

Norma / predpis	Kapitola / kontrola / článok	Uplatniteľnosť	Typ pokrytia	Poznámka
ISO/IEC 27701:2025	Clause 4.1; Clause 6.1.3	Processor	Supporting	Rola PIMS a uplatniteľnosť kontrol
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Processor	Primary	Zdokumentované dôkazy cloudového sprostredkovateľa a prevádzková kontrola
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Processor	Supporting	Monitorovanie, nezhody a nápravné opatrenie
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	Zákaznícke zmluvy, pokyny, podpora a záznamy
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Súčinnosť zákazníkom pri povinnostiach voči dotknutým osobám
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Primary	Kontroly dočasných súborov, vrátenia, prenosu, likvidácie a odosielania
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Supporting	Základ prenosu a umiestnenia
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Záznamy o poskytnutí údajov a vybavovanie žiadostí o poskytnutie údajov
ISO/IEC 27701:2025	Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9	Processor	Primary	Informovanie o ďalšom sprostredkovateľovi, jeho zapojenie a oznámenie zmeny
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	Dôkazy o prístupe, záznamoch, zálohovaní a logovaní
GDPR	Article 28	Processor	Primary	Sprostredkovateľ, ďalší sprostredkovateľ, súčinnosť, audit, výmaz a vrátenie
GDPR	Article 30	Processor	Supporting	Záznamy sprostredkovateľa

GDPR	Article 32; Article 33	Processor	Supporting	Bezpečnosť a oznámenie porušenia ochrany údajov prevádzkovateľovi
GDPR	Article 44	Conditional	Referenced	Smerovanie medzinárodných prenosov
ISO/IEC 29100:2020	Clause 5.3; Clause 5.5; Clause 5.6	Processor	Supporting	Účel, minimalizácia, použitie, uchovávanie a obmedzenie poskytovania
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Processor	Supporting	Preukázateľná zodpovednosť, informačná bezpečnosť a súlad
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	Hodnotenie, monitorovanie, zmena a kontroly uchovávania u sprostredkovateľa
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	Uplatniteľnosť kontrol, prevádzková kontrola a dodávateľské/cloudové kontroly
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	Kontroly dodávateľov, cloudu, výmazu, logovania a monitorovania
ISO/IEC 27018:2020	Annex A.2.1; Annex A.3.1	Processor	Primary	Súčinnosť zákazníkom a obmedzenie účelu pri cloudovom sprostredkovateľovi
ISO/IEC 27018:2020	Annex A.6.1; Annex A.6.2; Annex A.8.1	Processor	Primary	Cloudové oznamovanie poskytnutí, záznamy o poskytnutiach a transparentnosť ďalších sprostredkovateľov
ISO/IEC 27018:2020	Annex A.10.1; Annex A.10.3; Annex A.11.11;	Processor	Primary	Cloudové rozhranie pre porušenia, ukončenie služby, zmluvné opatrenia,

	Annex A.11.12; Annex A.12.1			subdodávky a záznamy o umiestneniach
ISO/IEC 27036-2:2022	Clause 6.1.1; Clause 6.1.2	Processor	Supporting	Stratégia a riadenie dodávateľských vzťahov
ISO/IEC 27036-2:2022	Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5	Processor	Supporting	Plánovanie, dohoda, riadenie, monitorovanie a ukončenie dodávateľského vzťahu
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	Rámec výmazu a dokumentácia
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	Implementácia výmazu a výnimky

1. Rozsah

1.1 Táto politika stanovuje povinné požiadavky na ochranu súkromia pre cloudové služby, pri ktorých organizácia vystupuje ako sprostredkovateľ alebo ďalší sprostredkovateľ PII, vrátane služieb SaaS, PaaS, IaaS, hostovaných aplikácií, spravovaného cloudu, cloudovej podpory, cloudového úložiska, cloudovej analytiky a služieb cloudovej infraštruktúry, ktoré spracúvajú PII v mene zákazníkov.

1.2 Táto politika sa vzťahuje na cloudové spracúvanie vykonávané podľa zákazníckych zmlúv, zdokumentovaných pokynov zákazníkov, pokynov nadradeného sprostredkovateľa, nastavení ďalšieho sprostredkovania, konfigurácie cloudových regiónov, prístupu cloudovej podpory, správy služby, zálohovania, replikácie, logovania, monitorovania, výmazu, vrátenia, podpory pri porušení ochrany údajov, podpory auditu a povinností súčinnosti zákazníkovi.

1.3 Táto politika pokrýva:

1.3.1 rozsah cloudového spracúvania PII a záznamy o pokynoch;

1.3.2 dôkazy o zákazníckej zmluve a zdieľanej zodpovednosti;

1.3.3 dôkazy o izolácii tenantov, cloudovom prístupe, administrátorskom prístupe a logovaní;

1.3.4 správu a riadenie ďalších sprostredkovateľov a cloudového dodávateľského reťazca;

1.3.5 umiestnenie, vzdialený prístup a smerovanie medzinárodných prenosov;

1.3.6 dôkazy o vrátení, prenose, výmaze, likvidácii a ukončení služby;

1.3.7 súčinnosť zákazníkom pri právach dotknutých osôb, DPIA, auditoch a reakcii na porušenie ochrany údajov;

1.3.8 dôkazy o monitorovaní, výnimkách, uplatňovaní politiky a zlepšovaní.

1.4 Táto politika nezriaďuje samostatný register zákazníckych zmlúv, register cloudových služieb, register izolácie tenantov, register prístupov, register logov, register výmazov, register žiadostí o podporu, register auditných dôkazov, register porušení ochrany údajov, register ďalších sprostredkovateľov ani výbor pre správu a riadenie cloudu.

1.5 Táto politika nenahrádza:

1.5.1 PII03 pre evidenciu spracúvania a vlastníctvo právneho základu;

1.5.2 PII06 pre úplný pracovný tok práv dotknutých osôb;

1.5.3 PII07 pre metodiku rizík ochrany súkromia a DPIA;

1.5.4 PII08 pre kontrolné brány ochrany súkromia už od návrhu a štandardne;

1.5.5 PII09 pre všeobecné kontroly zberu, použitia, poskytovania a zdieľania údajov;

1.5.6 PII10 pre metodiku uchovávania, výmazu a likvidácie;

1.5.7 PII12 pre všeobecnú správu a riadenie životného cyklu sprostredkovateľov, ďalších sprostredkovateľov a tretích strán;

1.5.8 PII13 pre posúdenie mechanizmov medzinárodného prenosu;

1.5.9 PII14 pre úplnú architektúru bezpečnosti PII a riadenia prístupu;

1.5.10 PII15 pre pracovný tok riadenia incidentov a porušení ochrany údajov;

1.5.11 PII17 pre riadenie zdokumentovaných informácií;

1.5.12 PII18 pre správu a riadenie monitorovania, auditu a zlepšovania PIMS.

2. Účel

2.1 Účelom tejto politiky je zabezpečiť, aby cloudové služby sprostredkovateľa a ďalšieho sprostredkovateľa PII boli prevádzkované na základe zdokumentovaných pokynov zákazníka, jasného rozsahu spracúvania, kontrolovaných nastavení ďalšieho sprostredkovania, primeraných cloudových bezpečnostných zodpovedností, zdokumentovaného umiestnenia a smerovania prenosov, povinností súčinnosti zákazníkovi, podpory pri porušení ochrany údajov, schopnosti výmazu/vrátenia a dôkazov pripravených na audit.

2.2 Táto politika podporuje pripravenosť na certifikáciu PIMS podľa ISO/IEC 27701:2025 pre cloudových sprostredkovateľov a cloudových ďalších sprostredkovateľov, pričom zostáva integrovaná s existujúcim súborom politík PIMS a kanonickými dôkazovými objektmi.

3. Ciele

3.1 Cieľmi tejto politiky je:

3.1.1 Definovať rozsah cloudového spracúvania PII pred onboardingom zákazníka alebo podstatnou zmenou.

3.1.2 Zabezpečiť, aby boli pokyny zákazníka zaznamenané, preskúmané a dodržiavané.

3.1.3 Udržiavať dôkazy cloudového sprostredkovateľa a ďalšieho sprostredkovateľa v kanonických registroch PIMS.

3.1.4 Definovať dôkazy o zdieľanej zodpovednosti, izolácii tenantov, prístupe, logovaní a umiestnení bez duplikovania politiky bezpečnosti PII.

3.1.5 Riadiť dôkazy o onboardingu ďalších sprostredkovateľov, zmenách, prenesených povinnostiach a monitorovaní.

3.1.6 Poskytovať zákazníkom podporu pri právach dotknutých osôb, DPIA, auditných žiadostiach a reakcii na porušenie ochrany údajov.

3.1.7 Zabezpečiť uchovávanie dôkazov o vrátení, výmaze, prenose a likvidácii pri ukončení služby.

3.1.8 Monitorovať kontroly cloudového sprostredkovateľa a iniciovať nápravné opatrenia prostredníctvom REG12.

4. Vyhlásenia politiky

4.1 Rozsah cloudového spracúvania a pokyny zákazníka

4.1.1 [Processor] Privacy Lead / PIMS Manager musí pred onboardingom zákazníka alebo podstatnou zmenou služby zaznamenať každú službu cloudového spracúvania PII, rolu zákazníka pri spracúvaní, zdroj pokynu zákazníka, kategórie PII, kategórie dotknutých osôb, účel služby, miesto spracúvania, závislosť od ďalšieho sprostredkovateľa, závislosť výmazu a príznak prenosu v REG02 a REG08.

4.1.2 [Processor] Process Owner / Business Owner musí pred začatím spracúvania zaznamenať zdokumentované pokyny zákazníka pre cloudové spracúvanie PII v REG08.

4.1.3 [Subprocessor] Process Owner / Business Owner musí pred spracúvaním PII ako cloudový ďalší sprostredkovateľ zaznamenať pokyny nadradeného sprostredkovateľa alebo pokyny schválené zákazníkom v REG08.

4.1.4 [Processor] Privacy Lead / PIMS Manager musí pred uvoľnením alebo podstatnou zmenou novej služby cloudového spracúvania PII zaznamenať uplatniteľnosť kontrol cloudového sprostredkovateľa v REG03.

4.1.5 [Processor] Data Protection Officer / Privacy Advisor musí pred tým, ako organizácia koná podľa pokynu, preskúmať v REG12 každý pokyn zákazníka, ktorý sa javí ako nezlučiteľný so zdokumentovanými povinnosťami zákazníka, požiadavkami PIMS alebo schváleným rozsahom služby.

4.1.6 [Processor] Process Owner / Business Owner musí pred uskutočnením spracúvania zaznamenať v REG12 každé navrhované spracúvanie zákazníckych PII mimo zdokumentovaných pokynov zákazníka a získať schválenie Privacy Lead / PIMS Manager.

4.2 Cloudová konfigurácia, izolácia tenantov, prístup a logovanie

4.2.1 [Processor] Information Security Lead musí pred onboardingom zákazníka alebo podstatnou zmenou služby zaznamenať hranicu zdieľanej zodpovednosti v cloude pre prístup

k PII, administráciu, logovanie, zálohovanie, šifrovanie, riadenie zraniteľností a výmaz v REG08.

4.2.2 [Processor] System Owner / Application Owner musí pred produkčným použitím a po podstatnej zmene architektúry validovať kontroly izolácie tenantov alebo oddelenia zákazníkov v REG12.

4.2.3 [Processor] System Owner / Application Owner smie udeliť cloudový administrátorský prístup k zákazníckym PII až po zaznamenaní schválenej obchodnej potreby, rozsahu prístupu, trvania prístupu a frekvencie preskúmania v REG12.

4.2.4 [Processor] Information Security Lead musí najmenej štvrťročne preskúmať privilegovaný cloudový prístup, prístup podpory, prístup k zákazníckym PII a pokrytie logovania v REG12.

4.2.5 [Processor] System Owner / Application Owner musí pred uvoľnením a po podstatnej zmene prostredia validovať oddelenie produkčných, staging, testovacích a podporných prostredí pre zákaznícke PII v REG12.

4.2.6 [Processor] System Owner / Application Owner musí pred povolením alebo zmenou týchto umiestnení zaznamenať umiestnenia záloh, replikácií, úložísk logov a prístupu podpory pre cloudové zákaznícke PII v REG02, REG08 alebo REG09.

[... Sekcie 4.3–8 nie sú súčasťou tohto náhľadu. Pre prístup k úplnému obsahu si zakúpte celý dokument. ...]

9. Výnimky

9.1 [Processor] Process Owner / Business Owner musí pred onboardingom, uvoľnením, obnovením alebo pokračujúcim používaním požiadať o výnimku cloudového sprostredkovateľa v REG12, ak sú požadované dôkazy o pokyne zákazníka, ďalšom sprostredkovateľovi, umiestnení, prístupe, logovaní, výmaze alebo incidentnom rozhraní neúplné.

9.2 [Processor] Data Protection Officer / Privacy Advisor musí pred schválením preskúmať v REG12 žiadosti o výnimku cloudového sprostredkovateľa významné z hľadiska ochrany súkromia, ak výnimka ovplyvňuje pokyny zákazníka, súčinnosť pri právach dotknutých osôb, prenosy, ďalších sprostredkovateľov, výmaz, podporu pri porušení ochrany údajov alebo PII s vysokým dopadom.

9.3 [Processor] Top Management musí pred nadobudnutím účinnosti výnimky schváliť vysokorizikové alebo podstatné výnimky cloudového sprostredkovateľa v REG12.

9.4 [Processor] Privacy Lead / PIMS Manager musí pred schválením priradiť dátum uplynutia platnosti, vlastníka nápravy, dátum preskúmania a poznámku k zostatkovému riziku v REG12 pre každú schválenú výnimku cloudového sprostredkovateľa.

10. Uplatňovanie politiky

10.1 [Processor] Privacy Lead / PIMS Manager musí zablokovať onboarding zákazníka, uvoľnenie služby, obnovenie alebo pokračujúce spracúvanie, ak požadované dôkazy v REG02, REG03, REG08, REG09, REG10 alebo REG12 chýbajú pred začatím alebo pokračovaním spracúvania.

10.2 [Processor] System Owner / Application Owner musí do jedného pracovného dňa po rozhodnutí o uplatnení politiky zakázať neschválený cloudový prístup, neschválené použitie regiónu, neschválenú replikáciu, neschválený prístup podpory alebo neschválený tok údajov k ďalšiemu sprostredkovateľovi a zaznamenať dokončenie v REG08 alebo REG12.

10.3 [Processor] Vendor / Procurement Owner musí pozastaviť nové spracúvanie PII neschváleným alebo nevyhovujúcim cloudovým ďalším sprostredkovateľom, kým nie sú dokončené dôkazy o nápravnom opatrení v REG08.

10.4 [Processor] Incident Response Coordinator musí do jedného pracovného dňa po identifikácii eskalovať zmeškané termíny zákazníckeho oznámenia incidentu v REG10 a REG12.

10.5 [Processor] Internal Audit / Compliance Reviewer musí do 60 dní po uzavretí nápravného opatrenia overiť účinnosť nápravného opatrenia pri závažných alebo opakovaných nezhodách cloudového sprostredkovateľa v REG12.

11. Preskúmanie a údržba

11.1 [Processor] Privacy Lead / PIMS Manager musí každoročne a do 30 dní po podstatnej zmene povinností cloudového sprostredkovateľa, cloudovej architektúry, správy a riadenia ďalších sprostredkovateľov, súčinnosti zákazníkovi, schopnosti výmazu alebo certifikačných požiadaviek preskúmať túto politiku v REG12.

11.2 [Processor] Vendor / Procurement Owner musí najmenej raz ročne a pred obnovením preskúmať záznamy cloudových ďalších sprostredkovateľov a závislostí od cloudových služieb v REG08.

11.3 [Processor] System Owner / Application Owner musí najmenej raz ročne a po podstatnej zmene architektúry preskúmať dôkazy o izolácii tenantov, privilegovanom prístupe, logovaní, zálohovaní, replikácii a výmaze v REG12.

11.4 [Processor] Privacy Lead / PIMS Manager musí najmenej raz ročne a do 15 pracovných dní po podstatnej zmene umiestnenia, prístupu podpory, zálohovania alebo ďalšieho sprostredkovateľa preskúmať záznamy o cloudových umiestneniach a smerovaní prenosov v REG09.

11.5 [Processor] Privacy Lead / PIMS Manager musí do 15 pracovných dní po schválených zmenách politiky, ktoré ovplyvňujú uplatniteľnosť kontrol cloudového sprostredkovateľa, aktualizovať REG03.

11.6 [All] Top Management musí pred zverejnením schváliť podstatné revízie tejto politiky v REG12.

12. Súvisiace politiky

12.1 Túto politiku podporujú tieto súvisiace politiky:

12.2 PII01 - Politika systému manažérstva informácií o súkromí

12.3 PII02 - Politika rolí, zodpovedností a preukázateľnej zodpovednosti v oblasti ochrany súkromia

12.4 PII03 - Politika evidencie spracúvania PII a právneho základu

12.5 PII06 - Politika riadenia práv dotknutých osôb

12.6 PII07 - Politika posúdenia rizík ochrany súkromia a DPIA

12.7 PII08 - Politika ochrany súkromia už od návrhu a štandardne

12.8 PII09 - Politika zberu, použitia, poskytovania a zdieľania PII

12.9 PII10 - Politika uchovávania, výmazu a likvidácie PII

12.10 PII12 - Politika riadenia ochrany súkromia sprostredkovateľov, ďalších sprostredkovateľov a tretích strán

12.11 PII13 - Politika medzinárodného prenosu PII

12.12 PII14 - Politika bezpečnosti PII a riadenia prístupu

12.13 PII15 - Politika riadenia incidentov a porušení ochrany PII

12.14 PII17 - Politika zdokumentovaných informácií a správy dôkazov PIMS

12.15 PII18 - Politika monitorovania, auditu a zlepšovania PIMS

12.16 PII20 - Politika ochrany súkromia detí

12.17 PII21 - Politika ochrany súkromia pri AI a automatizovanom rozhodovaní

12.18 PII22 - Politika ochrany súkromia pri marketingu a súboroch cookie

12.19 PII24 - Politika ochrany súkromia pri CCTV a fyzickom monitorovaní

13. Referenčné normy a rámce

13.1 Táto politika je namapovaná na tieto normy a predpisy. Mapovanie vysvetľuje, ako politika podporuje citované požiadavky, a identifikuje interné ustanovenia, ktoré ich implementujú alebo podporujú.

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].