					Sem zadajte názov registrovanej právnickej osoby						
Číslo dokumentu: PII15					Názov dokumentu: **Politika riadenia incidentov týkajúcich sa osobných údajov a porušení ochrany osobných údajov**						
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 7.4; Clause 7.5	Both	Supporting	Komunikácia PIMS a zdokumentované dôkazy o porušení ochrany osobných údajov
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Väzba na prevádzkové kontroly, posúdenie rizík ochrany súkromia a ošetrenie rizík
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorovanie, hodnotenie, nezhoda, nápravné opatrenie a zlepšovanie
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Plánovanie a príprava riadenia incidentov pri spracúvaní PII
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Reakcia na incidenty informačnej bezpečnosti týkajúce sa PII
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Právne, zákonné, regulačné a zmluvné požiadavky a ochrana záznamov
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Dohoda zákazníka so sprostredkovateľom a podpora povinností zákazníka
GDPR	Article 5(2); Article 24	Controller	Supporting	Preukázateľná zodpovednosť a zodpovednosť prevádzkovateľa
GDPR	Article 26	Joint Controller	Supporting	Koordinácia zodpovednosti spoločných prevádzkovateľov pri porušení

				ochrany osobných údajov
GDPR	Article 28	Both	Supporting	Súčinnosť sprostredkovateľa a zmluvné povinnosti sprostredkovateľa
GDPR	Article 32	Both	Supporting	Bezpečnosť spracúvania a schopnosť detegovať porušenia ochrany osobných údajov
GDPR	Article 33	Both	Primary	Oznámenie porušenia ochrany osobných údajov a dokumentovanie porušenia
GDPR	Article 34	Controller	Primary	Komunikácia porušení ochrany osobných údajov dotknutým osobám
GDPR	Article 39	Conditional	Supporting	Poradenstvo DPO, monitorovanie, spolupráca a podpora kontaktného miesta
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Zásady informačnej bezpečnosti a súladu v oblasti ochrany súkromia
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Zodpovednosti pri reakcii na incidenty týkajúce sa osobných údajov a hlásenie udalostí
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Plánovanie, posúdenie, reakcia, získané poznatky a zber dôkazov pri incidentoch
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Životný cyklus procesu riadenia incidentov
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Politika, plán, povedomie, testovanie a

				získané poznatky k incidentom
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Detekcia, oznamovanie, triáž, analýza, reakcia a operatívne vykazovanie incidentov
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Očakávania týkajúce sa oznámenia cloudového sprostredkovateľa a záznamu o porušení ochrany osobných údajov
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Hlásenie významných incidentov, ak je uplatniteľné
DORA Regulation (EU) 2022/2554	Article 17; Article 18; Article 19	Conditional	Supporting	Riadenie, klasifikácia a hlásenie ICT incidentov, ak je uplatniteľné

1. Rozsah

1.1 Táto politika stanovuje požiadavky na identifikáciu, nahlasovanie, triáž, posudzovanie, zamedzenie šírenia, oznamovanie, dokumentovanie, uzatváranie a zlepšovanie na základe incidentov týkajúcich sa osobných údajov a porušení ochrany osobných údajov v rozsahu PIMS.

1.2 Táto politika sa vzťahuje na tieto roly PIMS a prvky rozsahu:

1.2.1 organizáciu konajúcu ako prevádzkovateľ PII;

1.2.2 organizáciu konajúcu ako spoločný prevádzkovateľ, ak sa vyžaduje koordinácia zodpovednosti pri porušení ochrany osobných údajov;

1.2.3 organizáciu konajúcu ako sprostredkovateľ PII;

1.2.4 organizáciu konajúcu ako ďalší sprostredkovateľ;

1.2.5 systémy, aplikácie, služby, procesy, dodávateľov, sprostredkovateľov, ďalších sprostredkovateľov a tretie strany, ktoré spracúvajú, uchovávajú, prenášajú, podporujú, pristupujú k PII alebo inak ovplyvňujú PII v rozsahu PIMS.

1.3 Táto politika používa REG10 - Register incidentov týkajúcich sa osobných údajov a porušení ochrany osobných údajov ako primárny dôkazový objekt na riadenie incidentov týkajúcich sa osobných údajov a porušení ochrany osobných údajov.

1.4 Táto politika používa podporné dôkazové objekty takto:

1.4.1 REG01 pre rozsah PIMS a kontext príslušných zainteresovaných strán, právnych, zmluvných, odvetvových a zákazníckych požiadaviek na hlásenie.

1.4.2 REG02 pre dotknuté spracovateľské činnosti, kategórie PII, kategórie dotknutých osôb, účely a systémy.

1.4.3 REG03 pre Vyhlásenie o uplatniteľnosti a aktualizácie uplatniteľnosti kontrol.

1.4.4 REG04 pre väzbu na riziká ochrany súkromia, DPIA a zostatkové riziko.

1.4.5 REG08 pre dôkazy o rozhraniach incidentov so sprostredkovateľmi, ďalšími sprostredkovateľmi, zákazníkmi, dodávateľmi a tretími stranami.

1.4.6 REG09 pre väzbu na medzinárodný prenos, ak incident ovplyvňuje cezhraničné spracúvanie.

1.4.7 REG11 pre dôkazy o školení, povedomí a spôsobilosti na reakciu na incidenty.

1.4.8 REG12 pre dôkazy o audite, nezhode, nápravnom opatrení a zlepšovaní.

1.5 Táto politika sa pri špecializovaných kontrolách opiera o súvisiace politiky PIMS:

1.5.1 PII03 upravuje evidenciu spracúvania a záznamy o právnom základe.

1.5.2 PII04 upravuje oznámenie o ochrane údajov a kontroly transparentnosti mimo komunikácie špecifickej pre porušenia ochrany osobných údajov.

1.5.3 PII06 upravuje žiadosti dotknutých osôb o uplatnenie práv, ktoré vzniknú pred incidentom, počas incidentu alebo po incidente.

1.5.4 PII07 upravuje metodiku posúdenia rizík ochrany súkromia a DPIA.

1.5.5 PII08 upravuje ochranu súkromia už od návrhu a štandardne.

1.5.6 PII10 upravuje kontroly uchovávania, výmazu a likvidácie.

1.5.7 PII12 upravuje kontroly vzťahov v oblasti ochrany súkromia so sprostredkovateľmi, ďalšími sprostredkovateľmi, dodávateľmi a tretími stranami.

1.5.8 PII13 upravuje mechanizmy medzinárodného prenosu PII a záznamy o rizikách prenosu.

1.5.9 PII14 upravuje preventívne a detekčné bezpečnostné kontroly PII a kontroly prístupu.

1.5.10 PII16 upravuje školenie, povedomie a spôsobilosť v oblasti ochrany súkromia.

1.5.11 PII17 upravuje zdokumentované informácie a správu dôkazov.

1.5.12 PII18 upravuje monitorovanie, vnútorný audit, preskúmanie manažmentom, nezhodu, nápravné opatrenie a neustále zlepšovanie.

1.6 Na účely tejto politiky sa používajú tieto pojmy:

1.6.1 „Incident týkajúci sa osobných údajov“ znamená podozrivú alebo potvrdenú udalosť, ktorá ovplyvnila, mohla ovplyvniť alebo by primerane mohla ovplyvniť dôvernosť, integritu, dostupnosť, zákonné spracúvanie alebo oprávnené nakladanie s PII.

1.6.2 „Porušenie ochrany osobných údajov“ znamená potvrdený incident týkajúci sa osobných údajov zahŕňajúci neoprávnené, nezákonné, náhodné alebo neúmyselné zničenie, stratu, zmenu, sprístupnenie, prístup k, nedostupnosť alebo kompromitáciu PII.

1.6.3 „Posúdenie porušenia ochrany osobných údajov“ znamená zdokumentované hodnotenie toho, či je incident týkajúci sa osobných údajov porušením ochrany osobných údajov, ktoré PII a dotknuté osoby sú dotknuté, aké riziká môžu vzniknúť, aké oznámenia alebo komunikácie sú vyžadované a aké nápravné opatrenia sú potrebné.

1.6.4 „Nadobudnutie vedomosti“ znamená okamih, v ktorom má organizácia primeranú mieru istoty, že došlo k bezpečnostnému incidentu alebo incidentu ochrany súkromia a že PII boli alebo mohli byť kompromitované.

1.6.5 „Incident s vysokým dopadom týkajúci sa osobných údajov“ znamená incident týkajúci sa osobných údajov zahŕňajúci vysoko rizikové spracúvanie, osobitné kategórie alebo veľmi citlivé PII, veľký rozsah PII, zraniteľné osoby, regulovaných zákazníkov, dopad vo viacerých jurisdikciách, podstatný dopad na zákazníka, kompromitáciu privilegovaného prístupu, verejné sprístupnenie, ransomvér, nedostupnosť služby alebo významný prevádzkový či reputačný dopad.

1.6.6 „Podstatná zmena incidentu“ znamená nové alebo zmenené informácie ovplyvňujúce rozsah incidentu, závažnosť, kategórie PII, dopad na dotknuté osoby, rozhodnutie o oznámení, dopad na zákazníka, koreňovú príčinu, zamedzenie šírenia, obnovu, nápravné opatrenie alebo externé oznamovacie povinnosti.

2. Účel

2.1 Účelom tejto politiky je zabezpečiť, aby sa incidenty týkajúce sa osobných údajov a porušenia ochrany osobných údajov riešili konzistentne, bezodkladne, zákonne, bezpečne a s dôkazmi pripravenými na audit.

2.2 Táto politika podporuje preukázateľnú zodpovednosť tým, že vyžaduje zaznamenanie incidentov týkajúcich sa osobných údajov a porušení ochrany osobných údajov v REG10 a ich prepojenie s dotknutými záznamami o spracúvaní, rizikami ochrany súkromia, vzťahmi so sprostredkovateľmi a ďalšími sprostredkovateľmi, záznamami o prenosoch, nápravnými opatreniami a záznamami o školení, ak sú aktivované.

2.3 Táto politika zabezpečuje, aby sa povinnosti prevádzkovateľa, spoločného prevádzkovateľa, sprostredkovateľa a ďalšieho sprostredkovateľa riešili podľa odlišných pravidiel uplatniteľnosti pri zachovaní jedného integrovaného dôkazového modelu pre incidenty a porušenia ochrany osobných údajov.

3. Ciele

3.1 Cieľmi tejto politiky je:

3.1.1 zabezpečiť bezodkladné nahlásenie a zaznamenanie podozrivých incidentov týkajúcich sa osobných údajov;

3.1.2 zabezpečiť triáž a klasifikáciu incidentov týkajúcich sa osobných údajov podľa konzistentných kritérií;

3.1.3 zabezpečiť, aby posúdenia porušenia ochrany osobných údajov zohľadňovali dotknuté PII, dotknuté osoby, systémy, spracovateľské činnosti, sprostredkovateľov, ďalších sprostredkovateľov, prenosy, riziká a nápravné opatrenia;

3.1.4 zabezpečiť dokumentovanie rozhodnutí o oznámení prevádzkovateľom a komunikácii s dotknutými osobami;

3.1.5 zabezpečiť, aby oznámenia porušení ochrany osobných údajov zákazníkom alebo nadradeným stranám zo strany sprostredkovateľa a ďalšieho sprostredkovateľa boli vykonané bez zbytočného odkladu a v súlade s príslušnými dohodami;

3.1.6 zabezpečiť zachovanie a ochranu dôkazov počas riešenia incidentu;

3.1.7 zabezpečiť sledovanie zamedzenia šírenia, odstránenia, obnovy a validácie prostredníctvom REG10;

3.1.8 zabezpečiť vyhodnotenie spúšťačov regulovaného, zmluvného, zákazníckeho a odvetvového hlásenia, ak sú uplatniteľné;

3.1.9 zabezpečiť, aby získané poznatky z incidentov viedli k nápravným opatreniam a neustálemu zlepšovaniu;

3.1.10 zabezpečiť dostupnosť záznamov o incidentoch a porušeniach ochrany osobných údajov na audit, preskúmanie manažmentom, uistenie zákazníkov a regulačné preskúmanie, ak je uplatniteľné.

4. Vyhlásenia politiky

4.1 Pripravenosť na incidenty a prijatie hlásenia

4.1.1 [Both] Privacy Lead / PIMS Manager MUSÍ udržiavať kritériá riešenia incidentov týkajúcich sa osobných údajov a porušení ochrany osobných údajov v REG10 aspoň raz ročne a po každej podstatnej zmene rozsahu PIMS, právneho kontextu, zmluvných povinností alebo vysoko rizikového spracúvania.

4.1.2 [All] Incident Response Coordinator MUSÍ zaznamenať každý nahlásený alebo zistený podozrivý incident týkajúci sa osobných údajov do REG10 do jedného pracovného dňa od prijatia alebo skôr, ak môže byť aktivovaná uplatniteľná lehota na oznámenie alebo hlásenie zákazníkovi.

4.1.3 [Both] System Owner / Application Owner MUSÍ zachovať relevantné systémové logy, upozornenia, prístupové záznamy, konfiguračné dôkazy a dôkazy o obnove prepojené s REG10, ak podozrivý incident ovplyvňuje systém alebo aplikáciu spracúvajúcu PII.

4.1.4 [Both] Information Security Lead MUSÍ dokončiť úvodnú technickú triáž každej bezpečnostnej udalosti týkajúcej sa PII do 24 hodín od zistenia a zaznamenať počiatočnú závažnosť, dotknuté aktíva a stav zamedzenia šírenia do REG10.

4.2 Klasifikácia a posúdenie porušenia ochrany osobných údajov

4.2.1 [Both] Incident Response Coordinator MUSÍ klasifikovať každý záznam REG10 ako udalosť netýkajúcu sa PII, podozrivý incident týkajúci sa osobných údajov, potvrdený incident týkajúci sa osobných údajov alebo potvrdené porušenie ochrany osobných údajov do 24 hodín od prijatia, alebo aktualizovať záznam REG10 o dôvod, pre ktorý klasifikácia zostáva otvorená.

4.2.2 [Both] Privacy Lead / PIMS Manager MUSÍ identifikovať dotknutú spracovateľskú činnosť, kategórie PII, kategórie dotknutých osôb, systémy, sprostredkovateľov, ďalších sprostredkovateľov, miesta prenosu a riziká ochrany súkromia v REG02, REG04, REG08, REG09 a REG10 pred finalizáciou rozhodnutia o oznámení porušenia ochrany osobných údajov.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor MUSÍ posúdiť riziko pre dotknuté osoby pri každom potvrdenom alebo dôvodne podozrivom porušení ochrany osobných údajov

a zaznamenať odporúčanie k oznámeniu, odôvodnenie rizika a poradenstvo do REG10 pred prijatím rozhodnutia o externom oznámení.

4.2.4 [Processor] Privacy Lead / PIMS Manager MUSÍ identifikovať dotknutého prevádzkovateľa alebo zákazníka a príslušné zmluvné požiadavky na oznámenie hneď, ako sa organizácia dozvie o porušení ochrany osobných údajov ovplyvňujúcom zákaznícke PII, a MUSÍ zaznamenať výsledok v REG08 a REG10.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager MUSÍ overiť dohodnutú zodpovednosť za porušenie ochrany osobných údajov, hlavnú zodpovednosť za komunikáciu a koordinačné nastavenie pred akýmkoľvek externým oznámením alebo komunikáciou spoločného prevádzkovateľa a MUSÍ zaznamenať rozhodnutie v REG08 a REG10.

4.2.6 [Conditional] Privacy Lead / PIMS Manager MUSÍ pri každom incidente s vysokým dopadom týkajúcom sa osobných údajov vyhodnotiť uplatniteľné právne, odvetvové, finančno-sektorové, kyberneticko-bezpečnostné, zmluvné, zákaznícke a príjemcom služieb určené spúšťače hlásenia a zaznamenať výsledok uplatniteľnosti v REG01, REG08 a REG10.

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

9. Výnimky

9.1.1 [Both] Privacy Lead / PIMS Manager MUSÍ zaznamenať každú výnimku z tejto politiky v REG12 pred implementáciou alebo do 24 hodín po núdzovom opatrení, ak predchádzajúce schválenie nebolo uskutočniteľné.

9.1.2 [Both] Top Management MUSÍ pred uzavretím incidentu schváliť každú výnimku, ktorá podstatne ovplyvňuje načasovanie oznámenia porušenia ochrany osobných údajov, verejnú komunikáciu, záväzok voči zákazníkovi, zachovanie dôkazov alebo riziko pre dotknuté osoby, pričom dôkazy o schválení sa uchovávajú v REG10 a REG12.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor MUSÍ pred uzavretím incidentu zdokumentovať poradenstvo ku každému oneskorenému oznámeniu, rozhodnutiu o neoznámení alebo výnimočnému komunikačnému prístupu, pričom poradenstvo sa uchováva v REG10.

9.1.4 [Both] Vendor / Procurement Owner MUSÍ zaznamenať výnimky vyvolané dodávateľom, sprostredkovateľom, ďalším sprostredkovateľom alebo zákazníkom, ktoré ovplyvňujú reakciu na incident, v REG08 a REG12 do piatich pracovných dní od identifikácie výnimky.

10. Uplatňovanie politiky

10.1.1 [All] Process Owner / Business Owner MUSÍ eskalovať nenahlásenie podozrivého incidentu týkajúceho sa osobných údajov, nezachovanie dôkazov, nedodržanie priradených opatrení alebo nespoluprácu pri posúdení porušenia ochrany osobných údajov na Privacy Lead / PIMS Manager do dvoch pracovných dní od zistenia, pričom dôkazy sa uchovávajú v REG12.

10.1.2 [Both] Privacy Lead / PIMS Manager MUSÍ zaznamenať nezhodu v REG12, ak porušenie tejto politiky ovplyvňuje prijatie hlásenia incidentu, triáž, zamedzenie šírenia, oznámenie, integritu dôkazov, komunikáciu alebo nápravné opatrenie.

10.1.3 [Both] Vendor / Procurement Owner MUSÍ iniciovať nápravu dodávateľa alebo sprostredkovateľa prostredníctvom REG08 a REG12 do piatich pracovných dní, ak sprostredkovateľ, ďalší sprostredkovateľ, dodávateľ alebo iná tretia strana nesplní dohodnuté povinnosti týkajúce sa incidentu alebo porušenia ochrany osobných údajov.

10.1.4 [Both] Top Management MUSÍ preskúmať podstatné alebo opakujúce sa nezhody v riadení incidentov pri najbližšom plánovanom preskúmaní manažmentom, pričom rozhodnutia a vyžadované opatrenia sa uchovávajú v REG12.

11. Preskúmanie a údržba

11.1.1 [Both] Privacy Lead / PIMS Manager MUSÍ preskúmať túto politiku aspoň raz ročne a zaznamenať výsledok preskúmania, požadované zmeny a stav schválenia v REG12.

11.1.2 [Both] Incident Response Coordinator MUSÍ iniciovať poincidentné preskúmanie tejto politiky do 30 kalendárnych dní po uzavretí každého incidentu s vysokým dopadom týkajúceho sa osobných údajov alebo potvrdeného porušenia ochrany osobných údajov, pričom dôkazy o preskúmaní sa uchovávajú v REG10 a REG12.

11.1.3 [Conditional] Privacy Lead / PIMS Manager MUSÍ preskúmať túto politiku do 30 kalendárnych dní po tom, ako sa dozvie o podstatnej zmene uplatniteľných právnych, odvetvových, zákazníckych, zmluvných, sprostredkovateľských, s ďalším sprostredkovateľom súvisiacich alebo s prenosom súvisiacich požiadaviek na hlásenie incidentov, pričom dôkazy o preskúmaní sa uchovávajú v REG01, REG08, REG09 a REG12.

11.1.4 [Both] Internal Audit / Compliance Reviewer MUSÍ aspoň raz ročne preskúmať implementáciu tejto politiky prostredníctvom programu vnútorného auditu PIMS, pričom auditné zistenia a nápravné opatrenia sa uchovávajú v REG12.

11.1.5 [Both] Top Management MUSÍ počas plánovaného preskúmania manažmentom preskúmať trendy incidentov, významné porušenia ochrany osobných údajov, výkonnosť oznámení, omeškané nápravné opatrenia a účinnosť politiky, pričom výstupy sa uchovávajú v REG12.

12. Súvisiace politiky

12.1 Táto politika sa má čítať spolu s:

12.2 PII01 - Politika systému riadenia informácií o ochrane súkromia

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 PII04 - Politika oznámení o ochrane údajov a transparentnosti

12.6 PII06 - Politika riadenia práv dotknutých osôb

12.7 PII07 - Politika posúdenia rizík ochrany súkromia a DPIA

12.8 PII08 - Politika ochrany súkromia už od návrhu a štandardne

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 PII16 - Politika školenia, povedomia a spôsobilosti v oblasti ochrany súkromia

12.14 PII17 - Politika zdokumentovaných informácií a správy dôkazov PIMS

12.15 PII18 - Politika monitorovania, auditu a zlepšovania PIMS

13. Referenčné normy a rámce

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.7; 4.5.1; 4.5.3; 4.5.4; 5.2.2; 6.2.2; 7.1.1; 7.1.7; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.2.2; 4.3.4; 4.6.3; 6.3.1; 7.1.4; 11.1.2].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 6.4.1; 6.5.1; 8.1.1; 8.1.4; 10.1.2; 11.1.4; 11.1.5].

13.4 ISO/IEC 27701:2025 - Annex A.3.11. Addressed by clauses [4.1.1; 4.1.2; 4.2.6; 4.4.1; 5.1.1; 5.4.1; 7.1.1; 7.1.2; 7.1.6].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.4; 4.2.1; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.3; 4.4.4; 4.5.1; 4.5.4; 6.3.1].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.2.6; 4.4.6; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.4; 6.2.2; 9.1.2; 11.1.3].

13.7 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.6. Addressed by clauses [4.2.4; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5; 10.1.3].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.2; 4.4.1; 4.5.1; 4.5.3; 4.5.4; 4.6.2; 5.2.1; 6.3.1; 8.1.3; 11.1.5].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.1; 4.4.3; 5.3.1; 6.2.2; 11.1.3].

13.10 GDPR - Article 28. Addressed by clauses [4.2.4; 4.3.5; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5; 10.1.3].

13.11 GDPR - Article 32. Addressed by clauses [4.1.3; 4.1.4; 4.3.2; 4.3.3; 4.5.2; 4.6.3; 5.5.1; 7.1.4; 8.1.2; 11.1.2].

13.12 GDPR - Article 33. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.1; 4.5.4; 8.1.3; 9.1.3].

13.13 GDPR - Article 34. Addressed by clauses [4.2.3; 4.2.5; 4.4.2; 4.4.3; 4.4.7; 4.5.4; 8.1.3; 9.1.3].

13.14 GDPR - Article 39. Addressed by clauses [4.2.3; 4.4.2; 5.3.1; 6.2.2; 9.1.3; 11.1.3].

13.15 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.2.2; 4.3.2; 4.3.3; 4.5.3; 4.6.2; 4.6.3; 5.2.2; 6.4.1; 8.1.4; 11.1.4].

13.16 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.2.3; 4.4.1; 4.4.3; 4.6.5; 7.1.3; 7.1.6].

13.17 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.5.1; 4.5.2; 4.6.1; 4.6.2; 7.1.2; 7.1.6].

13.18 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.2; 4.6.1; 5.4.1; 7.1.6; 11.1.2].

13.19 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.1; 4.6.1; 4.6.5; 5.1.1; 7.1.1; 7.1.3; 7.1.6; 8.1.6; 11.1.1; 11.1.2].

13.20 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.4.1; 4.4.4; 4.5.1; 5.4.2; 6.1.2; 8.1.2].

13.21 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.4; 4.3.5; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5].

13.22 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.2.6; 4.4.6; 4.4.7; 5.3.1; 6.2.2; 8.1.3; 11.1.3].

13.23 DORA Regulation (EU) 2022/2554 - Article 17; Article 18; Article 19. Addressed by clauses [4.2.1; 4.2.6; 4.4.6; 4.4.7; 5.1.2; 6.2.1; 8.1.3; 11.1.3; 11.1.5].