					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: PII15					Dokumentum címe: **PII-incidensek és PII-adatsértések kezelésére vonatkozó szabályzat**							
Verzió: 1.0		Hatálybalépés dátuma: 01.01.2025			A dokumentum tulajdonosa:							
X	Szabályzat		Szabvány		Eljárás		Űrlap		Nyilvántartás		Egyéb	

Felülvizsgálati előzmények				
Felülvizsgálat száma	**Felülvizsgálat dátuma**	**Változások**	**Felülvizsgálta**	**A folyamat tulajdonosa**

Jóváhagyások			
Név	**Beosztás**	**Dátum**	**Aláírás**

Vonatkozó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/kontroll/cikk	Applicability	Coverage Type	Megjegyzés
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	PIMS-kommunikáció és dokumentált adatsértési bizonyítékok
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Operatív kontroll, adatvédelmi kockázatértékelés és kockázatkezelési kapcsolódás
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Nyomon követés, értékelés, meg nem felelés, helyesbítő intézkedés és fejlesztés
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Incidenskezelési tervezés és felkészülés a PII-kezeléshez
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	PII-t érintő információbiztonsági incidensekre adott válasz
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Jogi, törvényi, szabályozási és szerződéses követelmények, valamint a nyilvántartások védelme
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Adatfeldolgozói ügyfélmegállapodás és az ügyfélkötelezettségek támogatása
GDPR	Article 5(2); Article 24	Controller	Supporting	Elszámoltathatóság és adatkezelői felelősség
GDPR	Article 26	Joint Controller	Supporting	Közös adatkezelői adatsértési felelősség koordinálása
GDPR	Article 28	Both	Supporting	Adatfeldolgozói segítségnyújtás és adatfeldolgozói

				szerződéses kötelezettségek
GDPR	Article 32	Both	Supporting	Az adatkezelés biztonsága és adatsértés-észlelési képesség
GDPR	Article 33	Both	Primary	Személyesadat-sértés bejelentése és az adatsértés dokumentálása
GDPR	Article 34	Controller	Primary	Személyesadat-sértések közlése az érintett PII-alanyokkal
GDPR	Article 39	Conditional	Supporting	DPO-tanácsadás, nyomon követés, együttműködés és kapcsolattartási pont támogatása
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Információbiztonsági és adatvédelmi megfelelési alapelvek
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	PII-incidensreagálási felelősségek és eseményjelentés
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Incidenstervezés, értékelés, reagálás, tanulságok levonása és bizonyítékgyűjtés
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Az incidenskezelési folyamat életciklusa
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Incidensszabályzat, terv, tudatosság, tesztelés és tanulságok levonása
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Észlelési, értesítési, triázs-, elemzési, reagálási és jelentési műveletek
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Felhő-adatfeldolgozói értesítési és adatsértési nyilvántartási elvárások

NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Jelentős incidensek jelentése, ahol alkalmazandó
DORA Regulation (EU) 2022/2554	Article 17; Article 18; Article 19	Conditional	Supporting	IKT-incidenskezelés, osztályozás és jelentés, ahol alkalmazandó

1. Hatály

1.1 Ez a szabályzat meghatározza a PIMS alkalmazási területén belüli PII-incidensek és PII-adatsértések azonosítására, jelentésére, elsődleges értékelésére, értékelésére, elszigetelésére, bejelentésére, dokumentálására, lezárására és az azokból eredő fejlesztésre vonatkozó követelményeket.

1.2 Ez a szabályzat alkalmazandó:

1.2.1 a szervezetre, amikor PII-adatkezelőként jár el;

1.2.2 a szervezetre, amikor közös adatkezelőként jár el, és az adatsértési felelősségek koordinálása szükséges;

1.2.3 a szervezetre, amikor PII-adatfeldolgozóként jár el;

1.2.4 a szervezetre, amikor al-adatfeldolgozóként jár el;

1.2.5 azokra a rendszerekre, alkalmazásokra, szolgáltatásokra, folyamatokra, beszállítókra, adatfeldolgozókra, al-adatfeldolgozókra és harmadik felekre, amelyek a PIMS alkalmazási területén belül PII-t kezelnek, tárolnak, továbbítanak, támogatnak, ahhoz hozzáférnek, vagy arra egyéb módon hatással vannak.

1.3 Ez a szabályzat a REG10 - PII-incidens- és adatsértési nyilvántartást használja a PII-incidens- és adatsértés-kezelés elsődleges bizonyítékobjektumaként.

1.4 Ez a szabályzat a támogató bizonyítékobjektumokat az alábbiak szerint használja:

1.4.1 REG01 a PIMS alkalmazási területéhez, az alkalmazandó érdekelt felekhez, valamint a jogi, szerződéses, ágazati és ügyféljelentési kontextushoz.

1.4.2 REG02 az érintett adatkezelési tevékenységekhez, PII-kategóriákhoz, PII-alanyi kategóriákhoz, célokhoz és rendszerekhez.

1.4.3 REG03 az alkalmazhatósági nyilatkozathoz és a kontrollalkalmazhatósági frissítésekhez.

1.4.4 REG04 az adatvédelmi kockázathoz, DPIA-hoz és maradványkockázati kapcsolódáshoz.

1.4.5 REG08 az adatfeldolgozói, al-adatfeldolgozói, ügyfél-, beszállítói és harmadik féllel kapcsolatos incidensinterfész-bizonyítékokhoz.

1.4.6 REG09 a nemzetközi adattovábbítási kapcsolódáshoz, ha egy incidens határokon átnyúló adatkezelést érint.

1.4.7 REG11 a képzésre, tudatosságra és incidensreagálási kompetenciára vonatkozó bizonyítékokhoz.

1.4.8 REG12 az audit-, meg nem felelési, helyesbítő intézkedési és fejlesztési bizonyítékokhoz.

1.5 Ez a szabályzat a kapcsolódó PIMS-szabályzatokra támaszkodik a speciális kontrollok tekintetében:

1.5.1 A PII03 szabályozza az adatkezelési tevékenységek nyilvántartását és a jogalap-nyilvántartásokat.

1.5.2 A PII04 szabályozza az adatvédelmi tájékoztatókat és az átláthatósági kontrollokat az adatsértés-specifikus kommunikáción kívül.

1.5.3 A PII06 szabályozza azokat a PII-alanyi joggyakorlási kérelmeket, amelyek egy incidens előtt, alatt vagy után merülnek fel.

1.5.4 A PII07 szabályozza az adatvédelmi kockázatértékelési és DPIA-módszertant.

1.5.5 A PII08 szabályozza a beépített és alapértelmezett adatvédelmi kontrollokat.

1.5.6 A PII10 szabályozza a megőrzési, törlési és megsemmisítési kontrollokat.

1.5.7 A PII12 szabályozza az adatfeldolgozói, al-adatfeldolgozói, beszállítói és harmadik féllel fennálló adatvédelmi kapcsolatok kontrolljait.

1.5.8 A PII13 szabályozza a nemzetközi PII-továbbítási mechanizmusokat és az adattovábbítási kockázati nyilvántartásokat.

1.5.9 A PII14 szabályozza a megelőző és észlelő PII-biztonsági és hozzáférési kontrollokat.

1.5.10 A PII16 szabályozza az adatvédelmi képzést, tudatosságot és kompetenciát.

1.5.11 A PII17 szabályozza a dokumentált információk és bizonyítékok kezelését.

1.5.12 A PII18 szabályozza a nyomon követést, belső auditot, vezetőségi felülvizsgálatot, meg nem felelést, helyesbítő intézkedést és folyamatos fejlesztést.

1.6 E szabályzat alkalmazásában:

1.6.1 „PII-incidens” olyan gyanított vagy megerősített esemény, amely érintette, érinthette, vagy észszerűen érintheti a PII bizalmasságát, sértetlenségét, rendelkezésre állását, jogszerű kezelését vagy engedélyezett kezelését.

1.6.2 „PII-adatsértés” olyan megerősített PII-incidens, amely a PII jogosulatlan, jogellenes, véletlen vagy nem szándékos megsemmisítésével, elvesztésével, megváltoztatásával, közlésével, az ahhoz való hozzáféréssel, annak elérhetetlenné válásával vagy kompromittálódásával jár.

1.6.3 „Adatsértési értékelés” annak dokumentált értékelése, hogy egy PII-incidens PII-adatsértésnek minősül-e, milyen PII és mely PII-alanyok érintettek, milyen kockázatok merülhetnek fel, milyen bejelentések vagy közlések szükségesek, és milyen helyreállító intézkedésre van szükség.

1.6.4 „Tudomásszerzés” az a pont, amikor a szervezet észszerű bizonyossággal rendelkezik arról, hogy biztonsági vagy adatvédelmi incidens történt, és a PII kompromittálódott vagy kompromittálódhatott.

1.6.5 „Nagy hatású PII-incidens” olyan PII-incidens, amely magas kockázatú adatkezeléssel, különleges kategóriájú vagy fokozottan érzékeny PII-vel, nagy mennyiségű PII-vel, sérülékeny személyekkel, szabályozott ügyfelekkel, több joghatóságot érintő hatással, lényeges ügyfélhatással, emelt jogosultságú hozzáférés kompromittálódásával, nyilvános kitettséggel, zsarolóvírussal, szolgáltatás-elérhetetlenséggel vagy jelentős működési vagy reputációs hatással jár.

1.6.6 „Lényeges incidensváltozás” olyan új vagy megváltozott információ, amely érinti az incidens hatókörét, súlyosságát, a PII-kategóriákat, a PII-alanyokra gyakorolt hatást, a bejelentési döntést, az ügyfélhatást, a gyökérokot, az elszigetelést, a helyreállítást, a helyesbítő intézkedést vagy a külső jelentéstételi kötelezettségeket.

2. Cél

2.1 E szabályzat célja annak biztosítása, hogy a PII-incidenseket és adatsértéseket következetesen, haladéktalanul, jogszerűen, biztonságosan és auditra alkalmas bizonyítékokkal kezeljék.

2.2 Ez a szabályzat támogatja az elszámoltathatóságot azzal, hogy előírja a PII-incidensek és adatsértések REG10-ben történő rögzítését, valamint azok összekapcsolását az érintett adatkezelési nyilvántartásokkal, adatvédelmi kockázatokkal, adatfeldolgozói és al-adatfeldolgozói kapcsolatokkal, adattovábbítási nyilvántartásokkal, helyesbítő intézkedésekkel és képzési nyilvántartásokkal, ahol ezek alkalmazandók.

2.3 Ez a szabályzat biztosítja, hogy az adatkezelői, közös adatkezelői, adatfeldolgozói és al-adatfeldolgozói kötelezettségeket elkülönített alkalmazhatósági szabályok szerint kezeljék, miközben egy integrált incidens- és adatsértési bizonyítékmodellt tartanak fenn.

3. Célkitűzések

3.1 E szabályzat célkitűzései a következők:

3.1.1 annak biztosítása, hogy a gyanított PII-incidenseket haladéktalanul jelentsék és rögzítsék;

3.1.2 annak biztosítása, hogy a PII-incidenseket következetes szempontok alapján triázsolják és osztályozzák;

3.1.3 annak biztosítása, hogy az adatsértési értékelések figyelembe vegyék az érintett PII-t, PII-alanyokat, rendszereket, adatkezelési tevékenységeket, adatfeldolgozókat, al-adatfeldolgozókat, adattovábbításokat, kockázatokat és helyreállító intézkedéseket;

3.1.4 annak biztosítása, hogy az adatkezelői bejelentési és a PII-alanyok felé történő közlési döntéseket dokumentálják;

3.1.5 annak biztosítása, hogy az adatfeldolgozói és al-adatfeldolgozói adatsértési értesítések az ügyfelek vagy upstream felek felé indokolatlan késedelem nélkül és az alkalmazandó megállapodásoknak megfelelően megtörténjenek;

3.1.6 annak biztosítása, hogy az incidenskezelés során a bizonyítékokat megőrizzék és védjék;

3.1.7 annak biztosítása, hogy az elszigetelést, eltávolítást, helyreállítást és ellenőrzést a REG10-en keresztül kövessék nyomon;

3.1.8 annak biztosítása, hogy adott esetben értékeljék a szabályozott, szerződéses, ügyfél- és ágazati jelentési kiváltó okokat;

3.1.9 annak biztosítása, hogy az incidensekből levont tanulságok helyesbítő intézkedéseket és folyamatos fejlesztést eredményezzenek;

3.1.10 annak biztosítása, hogy az incidens- és adatsértési nyilvántartások adott esetben rendelkezésre álljanak audit, vezetőségi felülvizsgálat, ügyfélbizonyosság és szabályozási felülvizsgálat céljából.

4. Szabályzati rendelkezések

4.1 Incidensfelkészültség és incidensfelvétel

4.1.1 [Both] The Privacy Lead / PIMS Manager köteles a PII-incidensek és adatsértések kezelési kritériumait a REG10-ben legalább évente, valamint a PIMS alkalmazási területét, a jogi környezetet, a szerződéses kötelezettségeket vagy a magas kockázatú adatkezelést érintő bármely lényeges változás után fenntartani.

4.1.2 [All] The Incident Response Coordinator köteles minden bejelentett vagy észlelt gyanított PII-incidenst a beérkezéstől számított egy munkanapon belül, vagy ennél korábban, ha alkalmazandó bejelentési vagy ügyféljelentési határidő indulhat, a REG10-ben rögzíteni.

4.1.3 [Both] The System Owner / Application Owner köteles megőrizni a releváns rendszernaplókat, riasztásokat, hozzáférési nyilvántartásokat, konfigurációs bizonyítékokat és helyreállítási bizonyítékokat a REG10-hez kapcsolva, ha a gyanított incidens PII-t kezelő rendszert vagy alkalmazást érint.

4.1.4 [Both] The Information Security Lead köteles a PII-t érintő bármely biztonsági esemény kezdeti technikai triázsát az észleléstől számított 24 órán belül elvégezni, és a kezdeti súlyosságot, az érintett vagyonelemeket és az elszigetelési állapotot a REG10-ben rögzíteni.

4.2 Osztályozás és adatsértési értékelés

4.2.1 [Both] The Incident Response Coordinator köteles minden REG10-bejegyzést nem PII-eseményként, gyanított PII-incidensként, megerősített PII-incidensként vagy megerősített PII-adatsértésként osztályozni a bejelentésbefogadástól számított 24 órán belül, vagy a REG10-bejegyzést frissíteni azzal az indokkal, hogy az osztályozás miért marad függőben.

4.2.2 [Both] The Privacy Lead / PIMS Manager köteles az érintett adatkezelési tevékenységet, PII-kategóriákat, PII-alanyi kategóriákat, rendszereket, adatfeldolgozókat, al-adatfeldolgozókat, adattovábbítási helyszíneket és adatvédelmi kockázatokat a REG02-ben, REG04-ben, REG08-ban, REG09-ben és REG10-ben azonosítani, mielőtt az adatsértési bejelentésről szóló döntés véglegessé válik.

4.2.3 [Controller] The Data Protection Officer / Privacy Advisor köteles minden megerősített vagy észszerűen feltételezett PII-adatsértés esetén értékelni az érintett PII-alanyokat fenyegető kockázatot, és a bejelentési javaslatot, a kockázati indokolást és a tanácsot a REG10-ben rögzíteni, mielőtt a külső bejelentési döntés megszületik.

4.2.4 [Processor] The Privacy Lead / PIMS Manager köteles az érintett adatkezelőt vagy ügyfelet és az alkalmazandó szerződéses értesítési követelményeket azonosítani, amint a szervezet tudomást szerez az ügyfél PII-jét érintő PII-adatsértésről, és köteles az eredményt a REG08-ban és REG10-ben rögzíteni.

4.2.5 [Joint Controller] The Privacy Lead / PIMS Manager köteles bármely külső bejelentés vagy közös adatkezelő általi közlés előtt ellenőrizni a megállapodott adatsértési felelősséget, a vezető kommunikációs felelősséget és a koordinációs megállapodást, és köteles a döntést a REG08-ban és REG10-ben rögzíteni.

4.2.6 [Conditional] The Privacy Lead / PIMS Manager köteles minden nagy hatású PII-incidens esetében értékelni az alkalmazandó jogi, ágazati, pénzügyi szektorbeli, kiberbiztonsági, szerződéses, ügyfél- és szolgáltatásigénybevevői jelentési kiváltó okokat, és az alkalmazhatósági eredményt a REG01-ben, REG08-ban és REG10-ben rögzíteni.

[... A 4.3–8. szakaszok nem szerepelnek ebben az előnézetben. A teljes tartalom eléréséhez vásárolja meg a teljes dokumentumot. ...]

9. Kivételek

9.1.1 [Both] The Privacy Lead / PIMS Manager köteles e szabályzat alóli bármely kivételt a végrehajtás előtt, vagy sürgősségi intézkedés esetén, ha az előzetes jóváhagyás nem volt megvalósítható, az intézkedést követő 24 órán belül a REG12-ben rögzíteni.

9.1.2 [Both] Top Management köteles minden olyan kivételt jóváhagyni az incidens lezárása előtt, amely lényegesen érinti az adatsértési bejelentés időzítését, a nyilvános kommunikációt, az ügyfélvállalást, a bizonyítékok megőrzését vagy a PII-alany kockázatát, a jóváhagyási bizonyítékok REG10-ben és REG12-ben történő megőrzésével.

9.1.3 [Conditional] The Data Protection Officer / Privacy Advisor köteles minden késedelmes bejelentéshez, bejelentés mellőzéséről szóló döntéshez vagy kivételes kommunikációs megközelítéshez tanácsot dokumentálni az incidens lezárása előtt, a tanács REG10-ben történő megőrzésével.

9.1.4 [Both] The Vendor / Procurement Owner köteles a beszállító, adatfeldolgozó, al-adatfeldolgozó vagy ügyfél által vezérelt, az incidensreagálást érintő kivételeket a kivétel azonosításától számított öt munkanapon belül a REG08-ban és REG12-ben rögzíteni.

10. Betartatás

10.1.1 [All] The Process Owner / Business Owner köteles a gyanított PII-incidens jelentésének elmulasztását, a bizonyítékok megőrzésének elmulasztását, a kijelölt intézkedések követésének elmulasztását vagy az adatsértési értékeléssel való együttműködés elmulasztását a felfedezéstől számított két munkanapon belül eszkalálni a Privacy Lead / PIMS Manager felé, a bizonyítékok REG12-ben történő megőrzésével.

10.1.2 [Both] The Privacy Lead / PIMS Manager köteles REG12 meg nem felelést rögzíteni, ha e szabályzat megsértése érinti az incidensbefogadást, triázst, elszigetelést, bejelentést, bizonyítékok sértetlenségét, kommunikációt vagy helyesbítő intézkedést.

10.1.3 [Both] The Vendor / Procurement Owner köteles beszállítói vagy adatfeldolgozói helyreállítást kezdeményezni a REG08-on és REG12-n keresztül öt munkanapon belül, ha egy adatfeldolgozó, al-adatfeldolgozó, beszállító vagy más harmadik fél nem teljesíti a megállapodott incidens- vagy adatsértési kötelezettségeket.

10.1.4 [Both] Top Management köteles a lényeges vagy ismétlődő incidenskezelési meg nem feleléseket a következő ütemezett vezetőségi felülvizsgálat során áttekinteni, a döntések és szükséges intézkedések REG12-ben történő megőrzésével.

11. Felülvizsgálat és karbantartás

11.1.1 [Both] The Privacy Lead / PIMS Manager köteles ezt a szabályzatot legalább évente felülvizsgálni, és köteles a felülvizsgálat eredményét, a szükséges módosításokat és a jóváhagyási állapotot a REG12-ben rögzíteni.

11.1.2 [Both] The Incident Response Coordinator köteles minden nagy hatású PII-incidens vagy megerősített PII-adatsértés lezárását követő 30 naptári napon belül kezdeményezni e szabályzat incidens utáni felülvizsgálatát, a felülvizsgálati bizonyítékok REG10-ben és REG12-ben történő megőrzésével.

11.1.3 [Conditional] The Privacy Lead / PIMS Manager köteles ezt a szabályzatot az alkalmazandó jogi, ágazati, ügyfél-, szerződéses, adatfeldolgozói, al-adatfeldolgozói vagy adattovábbítással kapcsolatos incidensjelentési követelmények lényeges változásáról való tudomásszerzéstől számított 30 naptári napon belül felülvizsgálni, a felülvizsgálati bizonyítékok REG01-ben, REG08-ban, REG09-ben és REG12-ben történő megőrzésével.

11.1.4 [Both] The Internal Audit / Compliance Reviewer köteles e szabályzat végrehajtását legalább évente felülvizsgálni a PIMS belső auditprogramján keresztül, az auditmegállapítások és helyesbítő intézkedések REG12-ben történő megőrzésével.

11.1.5 [Both] Top Management köteles az incidenstrendeket, jelentős adatsértéseket, bejelentési teljesítményt, lejárt határidejű helyesbítő intézkedéseket és a szabályzat eredményességét az ütemezett vezetőségi felülvizsgálat során áttekinteni, a kimenetek REG12-ben történő megőrzésével.

12. Kapcsolódó szabályzatok

12.1 Ezt a szabályzatot az alábbiakkal együtt kell értelmezni:

12.1.1 PII01 - Adatvédelmi információirányítási rendszer szabályzat

12.1.2 PII02 - Adatvédelmi szerepkörök, felelősségek és elszámoltathatóság szabályzat

12.1.3 PII03 - PII adatkezelési tevékenységek nyilvántartása és jogalap szabályzat

12.1.4 PII04 - Adatvédelmi tájékoztató és átláthatósági szabályzat

12.1.5 PII06 - PII-alanyi jogok kezelésére vonatkozó szabályzat

12.1.6 PII07 - Adatvédelmi kockázatértékelési és DPIA szabályzat

12.1.7 PII08 - Beépített és alapértelmezett adatvédelmi szabályzat

12.1.8 PII10 - PII megőrzési, törlési és megsemmisítési szabályzat

12.1.9 PII12 - Adatfeldolgozói, al-adatfeldolgozói és harmadik féllel fennálló adatvédelmi kapcsolatok kezelésére vonatkozó szabályzat

12.1.10 PII13 - Nemzetközi PII-továbbítási szabályzat

12.1.11 PII14 - PII-biztonsági és hozzáférés-szabályozási szabályzat

12.1.12 PII16 - Adatvédelmi képzésre, tudatosságra és kompetenciára vonatkozó szabályzat

12.1.13 PII17 - PIMS dokumentált információk és bizonyítékok kezelésére vonatkozó szabályzat

12.1.14 PII18 - PIMS nyomon követési, audit- és fejlesztési szabályzat

13. Hivatkozott szabványok és keretrendszerek

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].