					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: PII21					Názov dokumentu: **Politika ochrany súkromia pri AI a automatizovanom rozhodovaní**							
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	Ustanovenie / kontrola / článok	Uplatniteľnosť	Typ pokrytia	Komentár
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Zdokumentované informácie a prevádzkové riadenie dôkazov o spracúvaní pri AI, profilovaní a automatizovanom rozhodovaní
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorovanie, nezhoda a nápravné opatrenia pre kontroly ochrany súkromia pri AI
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9	Controller	Primary	Účel, právny základ, posúdenie vplyvu na súkromie a záznamy prevádzkovateľa
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Zmluvy so sprostredkovateľmi a zodpovednosti spoločného prevádzkovateľa pri spracúvaní PII súvisiacom s AI
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4	Controller	Primary	Povinnosti voči dotknutým osobám a transparentnosť spracúvania súvisiaceho s AI
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11	Controller	Primary	Námietka, prístup, oprava, výmaz, vybavovanie žiadostí a povinnosti pri automatizovanom rozhodovaní
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5	Controller	Primary	Obmedzenia zberu, spracúvania a minimalizácie pre vstupy, výstupy a odvodené údaje AI
ISO/IEC 27701:2025	Annex A.1.5.2; Annex A.1.5.3;	Conditional	Supporting	Smerovanie medzinárodných prenosov,

	Annex A.1.5.4; Annex A.1.5.5			poskytnutí a žiadostí o poskytnutie údajov pri PII súvisiacich s AI
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Processor	Primary	Dohoda so sprostredkovateľom, zdokumentované pokyny, podpora povinností zákazníka a záznamy
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Podpora sprostredkovateľa pri povinnostiach voči dotknutým osobám, smerovaní prenosov a vybavovaní poskytnutí údajov
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Ochrana záznamov a logovanie súvisiace so spracúvaním PII v kontexte AI
GDPR	Article 4(4); Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(d); Article 5(2)	Controller	Primary	Profilovanie, spravodlivosť, transparentnosť, obmedzenie účelu, minimalizácia, presnosť a preukázateľná zodpovednosť
GDPR	Article 6; Article 9; Article 10	Controller	Primary	Zákonnosť, údaje osobitnej kategórie a ochranné opatrenia pre údaje o odsúdeniach za trestné činy alebo priestupkoch
GDPR	Article 12; Article 13; Article 14; Article 15	Controller	Primary	Transparentné informácie, prístup a zmysluplné informácie o automatizovanom rozhodovaní
GDPR	Article 16; Article 17; Article 18;	Controller	Primary	Oprava, výmaz, obmedzenie, námietka a práva pri

	Article 21; Article 22			automatizovanom rozhodovaní
GDPR	Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Zodpovednosť prevádzkovateľa, ochrana údajov už od návrhu a štandardne, spoloční prevádzkovatelia, sprostredkovatelia, záznamy, bezpečnosť, DPIA a úlohy DPO
GDPR	Article 44	Conditional	Referenced	Smerovanie medzinárodných prenosov pri spracúvaní PII súvisiacom s AI
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7	Both	Primary	Zásady účelu, zberu, minimalizácie, použitia, uchovávania, poskytnutia, presnosti a kvality
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Transparentnosť, účasť jednotlivca, preukázateľná zodpovednosť, informačná bezpečnosť a súlad v oblasti ochrany súkromia
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	Prínos PIA, určenie prahovej hodnoty a príprava na posúdenie rizík ochrany súkromia súvisiace s AI
ISO/IEC 29151:2022	Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10	Both	Supporting	Kontroly účelu, zberu, minimalizácie, použitia, uchovávania, poskytnutia, presnosti a účasti dotknutých osôb

1. Rozsah

1.1 Táto politika stanovuje povinné požiadavky na ochranu súkromia pre činnosti spracúvania s využitím umelej inteligencie, profilovania, skórovania, odporúčaní, podpory rozhodovania a automatizovaného rozhodovania, ktoré používajú, odvodzujú, generujú, poskytujú alebo inak spracúvajú PII v rámci rozsahu PIMS.

1.2 Táto politika sa vzťahuje na:

1.2.1 systémy, aplikácie, modely, služby, pracovné toky, rozhodovacie mechanizmy, skórovacie nástroje, odporúčacie systémy, analytické modely a procesy automatizovaného rozhodovania s podporou AI, ktoré spracúvajú PII;

1.2.2 profilovanie, segmentáciu, klasifikáciu, predikciu, odvodzovanie, personalizáciu, radenie, posudzovanie oprávnenosti, detekciu podvodov, skórovanie rizík, rozhodnutia o prístupe, posudzovanie súvisiace so zamestnaním, profilovanie detí, marketingovú personalizáciu a podobné spracúvanie, pri ktorom sú zapojené PII;

1.2.3 PII súvisiace s AI používané na tréning, testovanie, validáciu, ladenie, monitorovanie, produkčné odvodzovanie, preskúmanie výstupov, meranie výkonnosti, vyšetrovanie incidentov alebo vyradenie modelu;

1.2.4 kontexty prevádzkovateľa, spoločného prevádzkovateľa, sprostredkovateľa a ďalšieho sprostredkovateľa;

1.2.5 dodávateľov, sprostredkovateľov, ďalších sprostredkovateľov, príjemcov zdieľania údajov a trasy medzinárodného prenosu súvisiace s AI, ktorí spracúvajú PII.

1.3 Táto politika nevytvára úplný rámec správy a riadenia AI, systém riadenia AI, inventár AI, inventár modelov, register rizík modelov, register spravodlivosti, register algoritmov, register incidentov AI, výbor pre AI, rolu vlastníka modelu, rolu vlastníka systému AI, pracovný tok právneho poradenstva ani samostatný formulár schvaľovania AI.

1.4 Táto politika nenahrádza:

1.4.1 PII03 pre evidenciu spracúvania, právny základ a vlastníctvo ROPA;

1.4.2 PII04 pre správu oznámení o ochrane údajov;

1.4.3 PII05 pre správu súhlasov a správu preferencií;

1.4.4 PII06 pre pracovný tok práv dotknutých osôb;

1.4.5 PII07 pre metodiku posúdenia rizík ochrany súkromia a DPIA;

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

1.4.7 PII09 pre kontroly zberu, používania, poskytnutia a zdieľania;

1.4.8 PII10 pre vykonávanie uchovávania, výmazu a likvidácie;

1.4.9 PII11 pre kontroly presnosti a kvality;

1.4.10 PII12 pre správu životného cyklu sprostredkovateľov, ďalších sprostredkovateľov a tretích strán;

1.4.11 PII13 pre kontroly medzinárodných prenosov;

1.4.12 PII14 pre bezpečnosť a riadenie prístupu;

1.4.13 PII15 pre riešenie incidentov a porušení ochrany údajov;

1.4.14 PII18 pre monitorovanie, audit a zlepšovanie;

1.4.15 PII19 pre ochranu súkromia zamestnancov;

1.4.16 PII20 pre ochranu súkromia detí;

1.4.17 PII22 pre marketingovú ochranu súkromia a cookies.

2. Účel

2.1 Účelom tejto politiky je zabezpečiť, aby činnosti AI, profilovania a automatizovaného rozhodovania zahŕňajúce PII boli identifikované, zdokumentované, posúdené z hľadiska rizík, transparentné, napadnuteľné, monitorované a riadené prostredníctvom PIMS bez vytvárania duplicitných artefaktov správy špecifických pre AI.

2.2 Táto politika zabezpečuje, aby boli povinnosti ochrany súkromia pri spracúvaní PII súvisiacom s AI preukázané prostredníctvom REG02, REG04, REG06, REG07, REG08, REG09, REG10 a REG12.

3. Ciele

3.1 Cieľmi tejto politiky je:

3.1.1 identifikovať v REG02 spracúvanie s využitím AI, profilovania a automatizovaného rozhodovania zahŕňajúce PII;

3.1.2 zdokumentovať v REG02 účely, právny základ, kategórie PII, zdroje údajov, odvodené údaje, výstupy, príjemcov a účinky rozhodnutí súvisiace s AI;

3.1.3 spúšťať preverenie rizík ochrany súkromia a smerovanie DPIA prostredníctvom REG04;

3.1.4 zabezpečiť, aby boli oznámenia o ochrane údajov a zmysluplné informácie súvisiace s AI zaznamenané v REG07;

3.1.5 smerovať žiadosti o práva, námietky, ľudské preskúmanie a napadnuteľnosť prostredníctvom REG06;

3.1.6 riadiť sprostredkovateľov, ďalších sprostredkovateľov, dodávateľov a dohody o zdieľaní údajov súvisiace s AI prostredníctvom REG08;

3.1.7 smerovať medzinárodné prenosy súvisiace s AI prostredníctvom REG09;

3.1.8 eskalovať podozrenia na incidenty PII, zneužitie, neoprávnené poskytnutie a nepriaznivé výsledky ochrany súkromia súvisiace s AI prostredníctvom REG10 a REG12;

3.1.9 zaznamenávať monitorovanie, výnimky, nezhody, nápravné opatrenia a zlepšenia v REG12.

4. Vyhlásenia politiky

4.1 Identifikácia AI, profilovania a automatizovaného rozhodovania

4.1.1 [Controller] Keď sa navrhuje nový alebo podstatne zmenený systém, aplikácia, model, pracovný tok, služba alebo obchodný proces, Process Owner / Business Owner musí určiť, či používa AI, profilovanie, skórovanie, odporúčania, podporu rozhodovania alebo automatizované rozhodovanie zahŕňajúce PII, a zaznamenať toto určenie v REG02.

4.1.2 [Controller] Pred začatím spracúvania PII súvisiaceho s AI musí Process Owner / Business Owner zdokumentovať v REG02 účel spracúvania, kategórie PII, kategórie dotknutých osôb, zdroje údajov, kategórie odvodených alebo vytvorených údajov, kategórie výstupov, kategórie príjemcov, právny základ a väzbu na uchovávanie.

4.1.3 [Controller] Pred použitím profilovania, skórovania, odporúčaní, podpory rozhodovania alebo automatizovaného rozhodovania v produkcii musí Process Owner / Business Owner zdokumentovať kontext rozhodnutia, očakávaný účinok na dotknuté osoby, ľudskú účasť a trasu uplatnenia práv v REG02 a REG04.

4.1.4 [Joint Controller] Pred vykonaním spracúvania PII súvisiaceho s AI so spoločným prevádzkovateľom musí Privacy Lead / PIMS Manager zdokumentovať zodpovednosť za vymedzenie účelu, oznámenie, vybavovanie práv, podporu DPIA, správu sprostredkovateľov a eskaláciu incidentov v REG08.

4.1.5 [Processor] Pred spracúvaním PII prostredníctvom služby súvisiacej s AI pre zákazníka musí Process Owner / Business Owner potvrdiť, že pokyny zákazníka, povolené účely,

zakázané použitia, nakladanie s výstupmi a povinnosti súčinnosti sú zdokumentované v REG08.

4.1.6 [Both] Pred aktiváciou spracúvania PII súvisiaceho s AI musí Privacy Lead / PIMS Manager potvrdiť, že spracúvanie je prepojené s príslušnými kanonickými dôkazovými objektmi a že mimo REG02, REG04, REG06, REG07, REG08, REG09, REG10 alebo REG12 sa nevytvára žiadny samostatný register špecifický pre AI.

4.2 Posúdenie rizík ochrany súkromia a smerovanie DPIA

4.2.1 [Controller] Pred spustením alebo podstatnou zmenou spracúvania PII súvisiaceho s AI musí Privacy Lead / PIMS Manager dokončiť preverenie rizík ochrany súkromia a zaznamenať rozhodnutie o DPIA v REG04.

4.2.2 [Conditional] Keď spracúvanie súvisiace s AI zahŕňa profilovanie, automatizované rozhodnutia, rozsiahle hodnotenie, údaje osobitnej kategórie, údaje o trestných činoch, zraniteľné dotknuté osoby, posudzovanie zamestnancov, deti, behaviorálne monitorovanie, lokalizačné údaje, biometrické údaje, skórovanie s vysokým dopadom alebo významné účinky, Data Protection Officer / Privacy Advisor musí preskúmať riziko ochrany súkromia a zaznamenať odporúčanie v REG04.

4.2.3 [Controller] Pred produkčným spustením spracúvania PII súvisiaceho s AI musí Process Owner / Business Owner zdokumentovať opatrenia na ošetrenie rizík, stav zvyškového rizika a dôkazy pripravenosti na spustenie do produkčného prostredia v REG04 alebo REG12.

4.2.4 [Controller] Pred opätovným použitím PII na tréning, testovanie, validáciu, ladenie, monitorovanie alebo zlepšovanie modelu na nový alebo podstatne zmenený účel musí Process Owner / Business Owner dokončiť preskúmanie ochrany súkromia a zaznamenať rozhodnutie v REG02 a REG04.

4.2.5 [Conditional] Keď po plánovanom ošetrení zostáva vysoké zvyškové riziko ochrany súkromia, Top Management musí pred produkčným použitím schváliť, zamietnuť alebo vyžadovať ďalšie ošetrenie a zaznamenať rozhodnutie v REG04 a REG12.

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

9. Výnimky

9.1 [All] Pred odchýlením sa od požiadavky ochrany súkromia súvisiacej s AI v tejto politike musí žiadajúci Process Owner / Business Owner predložiť odôvodnenie výnimky a dôkazy o kompenzačnej kontrole v REG12.

9.2 [Conditional] Keď výnimka ovplyvňuje profilovanie, automatizované rozhodovanie, ľudské preskúmanie, napadnuteľnosť, transparentnosť, výsledok DPIA, skórovanie s vysokým dopadom, spracúvanie súvisiace s deťmi, spracúvanie súvisiace so zamestnancami, obmedzenia sprostredkovateľov alebo medzinárodné prenosy, Data Protection Officer / Privacy Advisor musí preskúmať výnimku a zaznamenať odporúčanie v REG04 alebo REG12.

9.3 [Conditional] Keď výnimka vytvára alebo zachováva vysoké zvyškové riziko ochrany súkromia, Top Management musí výnimku schváliť alebo zamietnuť a zaznamenať rozhodnutie v REG04 a REG12.

9.4 [All] Pred uplynutím platnosti schválenej výnimky ochrany súkromia súvisiacej s AI musí Privacy Lead / PIMS Manager preskúmať stav uzavretia, obnovenia alebo nápravného opatrenia a zaznamenať výsledok v REG12.

10. Uplatňovanie politiky

10.1 [All] Keď sa zistí nedodržanie tejto politiky, Privacy Lead / PIMS Manager musí zaznamenať nezhodu a nápravné opatrenie v REG12.

10.2 [Both] Keď vznikne podozrenie na neoprávnené spracúvanie PII, poskytnutie, prístup, zneužitie modelu, zlyhanie práv alebo nepriaznivý výsledok ochrany súkromia súvisiace s AI, Incident Response Coordinator musí iniciovať eskaláciu incidentu a zaznamenať dôkazy v REG10 a REG12.

10.3 [Both] Keď sprostredkovateľ, ďalší sprostredkovateľ, dodávateľ alebo príjemca zdieľania údajov nesplní povinnosti ochrany súkromia súvisiace s AI, Vendor / Procurement Owner musí zaznamenať nápravu, eskaláciu alebo ukončenie v REG08 a REG12.

10.4 [All] Keď sa vyskytnú opakované alebo systémové nezhody ochrany súkromia súvisiace s AI, Top Management musí preskúmať otázku a zaznamenať opatrenie manažmentu v REG12.

11. Preskúmanie a údržba

11.1 [All] Aspoň raz ročne musí Privacy Lead / PIMS Manager preskúmať túto politiku z hľadiska jej trvalej vhodnosti a zaznamenať výsledok preskúmania v REG12.

11.2 [Conditional] Keď sa podstatne zmenia zákony, služby, modely, zdroje údajov, postupy profilovania, logika automatizovaného rozhodovania, dodávateľské vzťahy, trasy prenosu alebo riziká ochrany súkromia, Privacy Lead / PIMS Manager musí preskúmať dotknuté kontroly ochrany súkromia súvisiace s AI a zaznamenať výsledok v REG02, REG04 alebo REG12.

11.3 [Controller] Aspoň raz ročne a po podstatných zmenách používateľskej cesty súvisiacej s AI musí Process Owner / Business Owner preskúmať dôkazy transparentnosti, zmysluplných informácií, ľudského preskúmania a trás uplatnenia práv a zaznamenať preskúmanie v REG06 a REG07.

11.4 [All] Po uzavretí nápravných opatrení ochrany súkromia súvisiacich s AI musí Internal Audit / Compliance Reviewer overiť účinnosť a zaznamenať dôkazy overenia v REG12.

12. Súvisiace politiky

12.1 PII01 - Politika systému riadenia informácií o súkromí

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

12.3 PII03 - Politika evidencie spracúvania PII a právneho základu

12.4 PII04 - Politika oznámení o ochrane údajov a transparentnosti

12.5 PII05 - Politika správy súhlasov a preferencií

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 PII09 - Politika zberu, používania, poskytnutia a zdieľania PII

12.10 PII10 - Politika uchovávania, výmazu a likvidácie PII

12.11 PII11 - Politika presnosti a kvality PII

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

12.13 PII13 - Politika medzinárodného prenosu PII

12.14 PII14 - Politika bezpečnosti PII a riadenia prístupu

12.15 PII15 - Politika riadenia incidentov a porušení ochrany PII

12.16 PII17 - Politika zdokumentovaných informácií a správy dôkazov PIMS

12.17 PII18 - Politika monitorovania, auditu a zlepšovania PIMS

12.18 PII19 - Politika ochrany súkromia zamestnancov

12.19 PII20 - Politika ochrany súkromia detí

12.20 PII22 - Politika marketingovej ochrany súkromia a cookies

13. Referenčné normy a rámce

13.1 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.6; 4.8.1; 6.1; 7.1; 7.5; 11.1].

13.2 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.6.2; 4.6.5; 4.8.2; 6.5; 8.1; 8.2; 8.3; 8.4; 8.5; 10.1; 11.4].

13.3 ISO/IEC 27701:2025 - Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.2.3; 4.2.4; 4.8.1; 7.1; 7.2].

13.4 ISO/IEC 27701:2025 - Annex A.1.2.7; Annex A.1.2.8. Addressed by clauses [4.1.4; 4.7.1; 4.7.2; 4.7.3; 5.7; 6.3; 7.6].

13.5 ISO/IEC 27701:2025 - Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 7.3; 11.3].

13.6 ISO/IEC 27701:2025 - Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11. Addressed by clauses [4.1.3; 4.3.2; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 7.4; 11.3].

13.7 ISO/IEC 27701:2025 - Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5. Addressed by clauses [4.2.4; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 7.1; 7.5].

13.8 ISO/IEC 27701:2025 - Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5. Addressed by clauses [4.7.3; 4.7.4; 4.7.5; 7.7].

13.9 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7. Addressed by clauses [4.1.5; 4.3.5; 4.5.5; 4.7.1; 4.7.2; 5.7; 6.3; 7.6].

13.10 ISO/IEC 27701:2025 - Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.3.5; 4.5.5; 4.7.1; 4.7.2; 4.7.4; 4.7.5; 7.6; 7.7].

13.11 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.25. Addressed by clauses [4.4.4; 4.6.1; 4.6.3; 4.8.1; 5.4; 7.5; 7.8; 10.2].

13.12 GDPR - Article 4(4); Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(d); Article 5(2). Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.1; 4.4.1; 4.4.2; 4.4.5; 4.8.1; 8.1].

13.13 GDPR - Article 6; Article 9; Article 10. Addressed by clauses [4.1.2; 4.2.4; 4.4.3; 4.7.3; 7.1].

13.14 GDPR - Article 12; Article 13; Article 14; Article 15. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.5.2; 4.5.3; 7.3; 11.3].

13.15 GDPR - Article 16; Article 17; Article 18; Article 21; Article 22. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 7.4].

13.16 GDPR - Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.2.2; 4.2.5; 4.4.4; 4.7.1; 4.8.2; 5.3; 6.2; 6.4; 7.2].

13.17 GDPR - Article 44. Addressed by clauses [4.7.4; 7.7; 8.4].

13.18 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7. Addressed by clauses [4.1.2; 4.2.4; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.7.5].

13.19 ISO/IEC 29100:2020 - Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.3.1; 4.3.2; 4.5.1; 4.5.2; 4.6.3; 4.8.1; 4.8.2; 8.5; 10.1].

13.20 ISO/IEC 29134:2020 - Clause 5.1; Clause 6.2; Clause 6.3. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.6.4; 6.4; 7.2; 9.2].

13.21 ISO/IEC 29151:2022 - Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10. Addressed by clauses [4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.2; 4.5.4; 4.7.5].