					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: PII10					Názov dokumentu: **Politika uchovávania, výmazu a likvidácie 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 7.5; Clause 8.1	Both	Primary	Zdokumentované dôkazy o uchovávaní a prevádzková kontrola
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorovanie, nezhody a nápravné opatrenia
ISO/IEC 27701:2025	Annex A.1.2.8; Annex A.1.2.9	Controller / Joint Controller	Supporting	Spoločná zodpovednosť a záznamy o spracúvaní
ISO/IEC 27701:2025	Annex A.1.3.7; Annex A.1.3.8	Controller	Supporting	Podpora vykonania výmazu
ISO/IEC 27701:2025	Annex A.1.4.6; Annex A.1.4.7; Annex A.1.4.8; Annex A.1.4.9	Controller	Primary	Uchovávanie, výmaz a likvidácia
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Supporting	Pokyny zákazníka a záznamy sprostredkovateľa
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.4.2; Annex A.2.4.3	Processor	Primary	Podpora výmazu a schopnosť likvidácie
ISO/IEC 27701:2025	Annex A.3.20; Annex A.3.21; Annex A.3.24	Both	Supporting	Likvidácia médií a nakladanie so zálohami
GDPR	Article 5(1)(e); Article 5(2)	Controller	Primary	Obmedzenie uchovávania a preukázateľná zodpovednosť
GDPR	Article 17	Controller	Supporting	Podpora vykonania výmazu
GDPR	Article 24	Controller	Supporting	Opatrenia prevádzkovateľa
GDPR	Article 26	Joint Controller	Supporting	Rozdelenie spoločnej zodpovednosti
GDPR	Article 28	Processor	Supporting	Výmaz a vrátenie zo strany sprostredkovateľa

GDPR	Article 30	Both	Supporting	Záznamy o spracúvaní
GDPR	Article 32	Both	Supporting	Bezpečné spracúvanie a podpora likvidácie
ISO/IEC 29100:2020	Clause 5.5; Clause 5.6; Clause 5.10	Both	Supporting	Minimalizácia, obmedzenie uchovávania a preukázateľná zodpovednosť
ISO/IEC 29151:2022	Annex A.7; Annex A.7.2	Both	Supporting	Kontroly uchovávania a výmazu dočasných súborov
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	Both	Primary	Rámec výmazu a dokumentácia
ISO/IEC 27555:2025	Clause 7.2; Clause 7.3; Clause 8.3	Controller	Primary	Lehoty výmazu a pravidlá výmazu
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	Both	Primary	Implementácia a výnimky
ISO/IEC 27555:2025	Clause 10.1; Clause 10.2; Clause 10.3	Both	Primary	Zodpovednosti a riadenie implementácie
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1	Both	Supporting	Integrácia rizík ochrany súkromia
ISO/IEC 27002:2022	Control 7.14; Control 8.10	Both	Supporting	Bezpečná likvidácia a výmaz informácií

1. Rozsah

1.1 Táto politika stanovuje požiadavky organizácie na definovanie, preskúmavanie, vykonávanie a preukazovanie uchovávania, výmazu, anonymizácie, deidentifikácie, vrátenia, prenosu a likvidácie PII.

1.2 Táto politika sa vzťahuje na PII spracúvané v kontextoch prevádzkovateľa, spoločného prevádzkovateľa, sprostredkovateľa a ďalšieho sprostredkovateľa vrátane PII uchovávaných v živých systémoch, archívoch, záložných kópiách, replikách, logoch, staging prostrediach, dočasných súboroch, papierových záznamoch a úložných médiách.

1.3 Táto politika sa vzťahuje na povinnosti uchovávania a výmazu vyplývajúce zo schválených účelov spracúvania, záznamov o právnom základe, pokynov prevádzkovateľa, zmluvných požiadaviek, výsledkov výmazu dotknutej osoby, ukončenia služby, likvidácie úložných médií a zistení z monitorovania PIMS.

1.4 Táto politika nedefinuje výber právneho základu, obsah oznámenia o ochrane údajov, úplné vybavovanie práv dotknutých osôb, riadenie životného cyklu sprostredkovateľov, mechanizmy medzinárodného prenosu, architektúru bezpečnostných kontrol, pracovný tok reakcie na incidenty ani metodiku auditu PIMS. Tieto kontroly sú upravené v súvisiacich politikách.

1.5 Na účely tejto politiky podstatná zmena znamená akúkoľvek zmenu účelu spracúvania, kategórie PII, kategórie dotknutých osôb, umiestnenia systémového úložiska, právneho predpisu alebo zmluvy týkajúcej sa uchovávania, pokynu zákazníka, architektúry zálohovania, prístupu k archivácii, spôsobu likvidácie, usporiadania so sprostredkovateľom alebo ďalším sprostredkovateľom, pracovného toku výmazu alebo rozsahu certifikácie PIMS, ktorá ovplyvňuje uchovávanie, výmaz alebo likvidáciu.

2. Účel

2.1 Účelom tejto politiky je zabezpečiť, aby sa PII uchovávali iba na schválené účely a počas schválených lehôt, aby sa vymazali alebo inak zlikvidovali, keď už nie sú potrebné, a aby boli podložené dôkazmi pripravenými na audit.

2.2 Táto politika umožňuje organizácii preukázať obmedzenie uchovávania, zodpovedné riadenie uchovávania, kontrolované vykonávanie výmazu, bezpečnú likvidáciu, zosúladenie pokynov sprostredkovateľa, riadenie výnimiek a neustále zlepšovanie bez vytvárania samostatného registra výmazov.

3. Ciele

3.1 Ciele tejto politiky sú:

3.1.1 definovať vlastníctvo pravidiel uchovávania a požadované metadáta uchovávania;

3.1.2 zabezpečiť, aby boli pravidlá uchovávania zaznamenané v PII Processing Inventory / ROPA;

3.1.3 zabezpečiť, aby boli úkony výmazu zo strany sprostredkovateľov a ďalších sprostredkovateľov založené na pokyne zákazníka alebo zmluve;

3.1.4 zabezpečiť, aby sa PII po uplynutí lehoty vymazali, vrátili, preniesli, anonymizovali, deidentifikovali alebo zlikvidovali pomocou schválených metód;

3.1.5 rozlišovať živé systémy, archívy, zálohy, repliky, logy, staging oblasti a dočasné súbory;

3.1.6 zabezpečiť, aby boli dôkazy o výmaze a likvidácii uchovávané v kanonických dôkazových objektoch PIMS;

3.1.7 zabezpečiť, aby boli výnimky z uchovávania časovo obmedzené, schválené a preskúmavané;

3.1.8 integrovať monitorovanie uchovávania a výmazu s nezhodami, nápravnými opatreniami a zlepšovaním.

4. Vyhlásenia politiky

4.1 Priradenie pravidla uchovávania

4.1.1 [Controller] Process Owner / Business Owner MUSÍ priradiť zdokumentované pravidlo uchovávania ku každej spracovateľskej činnosti prevádzkovateľa v REG02 pred začiatkom spracovateľskej činnosti.

4.1.2 [Joint Controller] Process Owner / Business Owner MUSÍ zaznamenať rozdelenie zodpovedností za uchovávanie a výmaz spoločných prevádzkovateľov v REG02 a REG08 pred začiatkom alebo zmenou spoločného spracúvania.

4.1.3 [Processor] Vendor / Procurement Owner MUSÍ zaznamenať pokyny zákazníka týkajúce sa uchovávania, vrátenia, prenosu alebo výmazu pri činnostiach sprostredkovateľa v REG08 pred začiatkom alebo zmenou spracúvania sprostredkovateľom.

4.1.4 [Subprocessor] Vendor / Procurement Owner MUSÍ zaznamenať požiadavky prenesené na ďalšieho sprostredkovateľa týkajúce sa uchovávania, vrátenia, prenosu alebo výmazu v REG08 pred onboardingom ďalšieho sprostredkovateľa alebo zmenou pokynu.

4.1.5 [Both] Privacy Lead / PIMS Manager MUSÍ pred schválením pravidla overiť, že každé schválené pravidlo uchovávania v REG02 obsahuje lehotu uchovávania, počiatočný spúšťač, vlastníka, odôvodnenie, konečný spôsob naloženia a dátum ďalšieho preskúmania.

4.1.6 [Both] Data Protection Officer / Privacy Advisor MUSÍ pred schválením akéhokoľvek pravidla uchovávania zahŕňajúceho právny konflikt, vysokorizikové spracúvanie, PII osobitnej kategórie alebo uchovávanie nad rámec pôvodného účelu spracúvania zaznamenať stanovisko v REG02 alebo REG12.

4.2 Preskúmanie a obmedzenie uchovávania

4.2.1 [Both] Process Owner / Business Owner MUSÍ preskúmať pridelené pravidlá uchovávania v REG02 najmenej raz ročne a do 30 dní od podstatnej zmeny.

4.2.2 [Both] Privacy Lead / PIMS Manager MUSÍ schváliť alebo zamietnuť nové alebo zmenené pravidlá uchovávania v REG02 do 10 pracovných dní od predloženia.

4.2.3 [Both] System Owner / Application Owner MUSÍ potvrdiť technickú alebo manuálnu metódu uplatňovania každého pravidla uchovávania v REG02 pred spustením do produkčného prostredia a počas každého ročného preskúmania uchovávania.

4.2.4 [Controller] Process Owner / Business Owner MUSÍ obmedziť aktívne používanie PII uchovávaných iba z právnych, zmluvných, auditných dôvodov alebo z dôvodov sporu v REG02 do piatich pracovných dní od identifikácie podmienky obmedzenia.

4.2.5 [Both] Privacy Lead / PIMS Manager MUSÍ zaznamenať nevyriešené riziko nadmerného uchovávania alebo oneskorené preskúmanie uchovávania v REG12 do piatich pracovných dní od identifikácie.

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

9. Výnimky

9.1.1 [All] Process Owner / Business Owner MUSÍ predložiť každú žiadosť o uchovávanie PII nad rámec schváleného pravidla uchovávania REG02 v REG12 pred aktiváciou výnimky.

9.1.2 [All] Privacy Lead / PIMS Manager MUSÍ schváliť alebo zamietnuť žiadosti o výnimku z uchovávania v REG12 pred aktiváciou výnimky.

9.1.3 [All] Data Protection Officer / Privacy Advisor MUSÍ pred schválením akejkoľvek výnimky zahŕňajúcej právny konflikt, odmietnutie výmazu, vysokorizikové PII, externé zdieľanie alebo dopad na certifikáciu zaznamenať stanovisko v REG12.

9.1.4 [All] Top Management MUSÍ schváliť výnimky z uchovávania presahujúce 90 dní, ovplyvňujúce vysokorizikové spracúvanie alebo ovplyvňujúce externé uistenie v REG12 pred aktiváciou výnimky.

9.1.5 [All] Privacy Lead / PIMS Manager MUSÍ pre každú schválenú výnimku z uchovávania, výmazu alebo likvidácie priradiť vlastníka, dátum uplynutia platnosti, kompenzačnú kontrolu a frekvenciu preskúmania v REG12.

9.1.6 [All] Privacy Lead / PIMS Manager MUSÍ najmenej mesačne preskúmať každú otvorenú výnimku v REG12 až do jej uzavretia.

9.1.7 [All] Process Owner / Business Owner MUSÍ uzavrieť alebo obnoviť každú výnimku v REG12 pred dátumom uplynutia jej platnosti.

10. Uplatňovanie politiky

10.1.1 [All] Privacy Lead / PIMS Manager MUSÍ zaznamenať nezhodu v REG12 do piatich pracovných dní od identifikácie chýbajúcich metadát uchovávania, oneskoreného preskúmania uchovávania, nepodporeného uchovávania, zmeškaného úkonu konečného spôsobu naloženia alebo chýbajúcich dôkazov.

10.1.2 [All] System Owner / Application Owner MUSÍ pozastaviť nové produkčné používanie spracovateľskej činnosti v REG12, ak pred spustením do produkčného prostredia chýbajú požadované technické kontroly uchovávania.

10.1.3 [All] Process Owner / Business Owner MUSÍ do piatich pracovných dní zastaviť neschválené aktívne používanie PII uchovávaných iba z právnych, zmluvných, auditných dôvodov alebo z dôvodov sporu a zaznamenať úkon v REG02 alebo REG12.

10.1.4 [Processor] Vendor / Procurement Owner MUSÍ eskalovať oneskorené zákazníkom riadené úkony konečného spôsobu naloženia v REG08 a REG12 do piatich pracovných dní od zmeškanej zmluvnej lehoty.

10.1.5 [Subprocessor] Vendor / Procurement Owner MUSÍ eskalovať chýbajúce dôkazy o konečnom spôsobe naloženia zo strany ďalšieho sprostredkovateľa v REG08 a REG12 do piatich pracovných dní od zmeškanej zmluvnej lehoty na predloženie dôkazov.

10.1.6 [All] Internal Audit / Compliance Reviewer MUSÍ overiť účinnosť nápravných opatrení pri nezhodách týkajúcich sa uchovávania, výmazu a likvidácie v REG12 pri najbližšom plánovanom audite alebo do 60 dní od uzavretia, podľa toho, čo nastane skôr.

10.1.7 [Conditional] Incident Response Coordinator MUSÍ iniciovať riešenie v REG10, keď nezhoda týkajúca sa uchovávania, výmazu alebo likvidácie naznačuje podozrenie na incident PII.

11. Preskúmanie a údržba

11.1.1 [All] Privacy Lead / PIMS Manager MUSÍ každoročne preskúmať túto politiku a zaznamenať výsledok preskúmania v REG12.

11.1.2 [All] Privacy Lead / PIMS Manager MUSÍ preskúmať túto politiku do 30 dní od podstatnej zmeny právnych predpisov týkajúcich sa uchovávania, účelu spracúvania, pokynu sprostredkovateľa, systémovej architektúry, architektúry zálohovania, prístupu k archivácii, pracovného toku výmazu, procesu likvidácie alebo požiadaviek na certifikáciu PIMS.

11.1.3 [All] Data Protection Officer / Privacy Advisor MUSÍ pred schválením preskúmať zmeny tejto politiky významné z hľadiska ochrany súkromia v REG12.

11.1.4 [All] Top Management MUSÍ schváliť podstatné zmeny tejto politiky v REG12 pred jej zverejnením.

11.1.5 [All] Privacy Lead / PIMS Manager MUSÍ zaznamenať komunikáciu schválených zmien politiky v REG11 do 30 dní od zverejnenia.

12. Súvisiace politiky

12.1 Túto politiku podporujú tieto súvisiace politiky:

12.2 PII01 - Politika systému riadenia 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 PII04 - Politika oznámenia o ochrane údajov a transparentnosti

12.6 PII06 - Politika riadenia práv dotknutých osôb

12.7 PII08 - Politika ochrany súkromia už od návrhu a štandardne

12.8 PII09 - Politika zhromažďovania, používania, poskytovania a zdieľania PII

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

12.10 PII14 - Politika bezpečnosti PII a riadenia prístupu

12.11 PII15 - Politika riadenia incidentov PII a porušení ochrany údajov

12.12 PII17 - Politika zdokumentovaných informácií a riadenia dôkazov PIMS

12.13 PII18 - Politika monitorovania, auditu a zlepšovania PIMS

13. Referenčné normy a rámce

13.1 Táto politika je mapovaná na nasledujúce 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

13.2.1 **Clause 7.5; Clause 8.1** - Mapované na zdokumentované dôkazy o uchovávaní, prevádzkové plánovanie, metadáta uchovávania, dôkazy o implementácii a záznamy o vykonaní životného cyklu. Addressed by clauses [4.1.5; 4.2.3; 4.3.5; 4.4.1; 7.1.1; 7.1.3; 7.1.4; 7.1.5; 7.1.6].

13.2.2 **Clause 9.1; Clause 10.2** - Mapované na monitorovanie, metriky, preskúmanie oneskorených úkonov, nezhody a nápravné opatrenia pre kontroly uchovávania, výmazu a likvidácie. Addressed by clauses [4.2.5; 6.1.1; 6.1.2; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 10.1.1; 10.1.6].

13.2.3 **Annex A.1.2.8; Annex A.1.2.9** - Mapované na dôkazy o zodpovednosti spoločných prevádzkovateľov a záznamy prevádzkovateľa o spracúvaní obsahujúce metadáta uchovávania a konečného spôsobu naloženia. Addressed by clauses [4.1.1; 4.1.2; 4.1.5; 4.2.1; 6.1.4; 7.1.2].

13.2.4 **Annex A.1.3.7; Annex A.1.3.8** - Mapované na podporu vykonania výmazu, smerovanie posúdenia výmazu a prepojenie dôkazov tretích strán, ak výsledky výmazu vyžadujú úkon. Addressed by clauses [4.3.2; 4.3.5; 7.1.8; 10.1.7].

13.2.5 **Annex A.1.4.6; Annex A.1.4.7; Annex A.1.4.8; Annex A.1.4.9** - Mapované na výmaz alebo deidentifikáciu na konci spracúvania, nakladanie s dočasnými súbormi, obmedzenie uchovávania a zdokumentované kontroly konečného spôsobu naloženia. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.3; 4.2.4; 4.3.1; 4.3.5; 4.3.6; 4.4.2; 4.4.5; 4.5.1; 4.5.2; 4.5.3].

13.2.6 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Mapované na zákaznícke zmluvy sprostredkovateľa, zdokumentované účely zákazníka a záznamy sprostredkovateľa o spracúvaní. Addressed by clauses [4.1.3; 4.1.4; 4.3.3; 4.3.4; 6.1.5; 6.1.6; 7.1.7].

13.2.7 **Annex A.2.3.2; Annex A.2.4.2; Annex A.2.4.3** - Mapované na podporu sprostredkovateľa pri povinnostiach zákazníka, nakladanie s dočasnými súbormi a schopnosť vrátenia, prenosu

alebo konečného spôsobu naloženia. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 4.4.4; 4.4.5; 6.1.5; 7.1.7; 10.1.4; 10.1.5].

13.2.8 **Annex A.3.20; Annex A.3.21; Annex A.3.24** - Mapované na nakladanie so životným cyklom úložných médií, kontroly opätovného použitia alebo uvoľnenia zariadení a nakladanie so zálohami pre PII. Addressed by clauses [4.3.6; 4.3.7; 4.4.1; 4.4.3; 4.4.4; 4.4.6; 5.1.4].

13.3 GDPR

13.3.1 **Article 5(1)(e); Article 5(2)** - Mapované na obmedzenie uchovávania, preukázateľnú zodpovednosť za uchovávanie, schválené metadáta uchovávania, dôkazy a preskúmanie. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.2; 4.2.4; 4.3.1; 4.3.5; 6.1.1; 8.1.1; 8.1.2; 10.1.1].

13.3.2 **Article 17** - Mapované na smerovanie schváleného výsledku výmazu, dôkazy o vykonaní a eskaláciu incidentu, ak zlyhania kontroly výmazu naznačujú podozrenie na incident PII. Addressed by clauses [4.3.2; 4.3.5; 7.1.8; 10.1.7].

13.3.3 **Article 24** - Mapované na správu prevádzkovateľa, opatrenia preukázateľnej zodpovednosti, preskúmania, výnimky, nápravné opatrenia a údržbu politiky. Addressed by clauses [4.1.6; 6.1.2; 6.1.3; 9.1.2; 9.1.3; 9.1.4; 11.1.1; 11.1.2; 11.1.4].

13.3.4 **Article 26** - Mapované na rozdelenie zodpovednosti spoločných prevádzkovateľov za uchovávanie a výmaz. Addressed by clauses [4.1.2; 6.1.4].

13.3.5 **Article 28** - Mapované na zosúladenie pokynov sprostredkovateľov a ďalších sprostredkovateľov, vrátenie, prenos, konečný spôsob naloženia, dôkazy a eskaláciu. Addressed by clauses [4.1.3; 4.1.4; 4.3.3; 4.3.4; 6.1.5; 6.1.6; 7.1.7; 10.1.4; 10.1.5].

13.3.6 **Article 30** - Mapované na metadáta uchovávania a konečného spôsobu naloženia v záznamoch o spracúvaní pre činnosti prevádzkovateľa a sprostredkovateľa. Addressed by clauses [4.1.1; 4.1.3; 4.1.5; 4.2.1; 4.4.1; 7.1.2].

13.3.7 **Article 32** - Mapované na bezpečné prevádzkové nakladanie s uchovávanými PII, technické uplatňovanie, kontrolu úložných médií, nakladanie so zálohami a eskaláciu incidentov. Addressed by clauses [4.2.3; 4.3.6; 4.4.3; 4.4.4; 4.4.6; 7.1.3; 7.1.4; 7.1.8].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.5; Clause 5.6; Clause 5.10** - Mapované na minimalizáciu údajov, obmedzenie používania a uchovávania, konečný spôsob naloženia, keď údaje už nie sú potrebné, obmedzenie uchovávaných PII a dôkazy preukázateľnej zodpovednosti. Addressed by clauses [4.1.5; 4.2.1; 4.2.4; 4.3.1; 4.4.2; 4.5.1; 4.5.2; 6.1.1; 8.1.1; 10.1.1].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.7; Annex A.7.2** - Mapované na časovo obmedzené uchovávanie, konečný spôsob naloženia, automatizované alebo manuálne uplatňovanie a nakladanie s dočasnými súbormi. Addressed by clauses [4.2.3; 4.3.1; 4.4.5; 7.1.3; 7.1.4; 7.1.5; 7.1.6].

13.6 ISO/IEC 27555:2025

13.6.1 **Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8** - Mapované na riadenie rámca výmazu, zoskupovanie PII, lehoty uchovávania a výmazu, rozlíšenie archívov a záloh, štruktúru pravidiel výmazu a požiadavky na zdokumentované postupy. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.3; 4.4.1; 4.4.2; 4.4.3; 7.1.1; 7.1.2].

13.6.2 **Clause 7.2; Clause 7.3; Clause 8.3** - Mapované na špecifikáciu pravidelných lehôt výmazu, identifikáciu štandardných lehôt výmazu a priradenie pravidiel výmazu k spracovateľským činnostiam PII. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.2; 7.1.1; 7.1.2].

13.6.3 **Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7** - Mapované na implementačné požiadavky pre systémy, manuálne procesy, celopodnikové

aspekty, sprostredkovateľov, nakladanie pri obnove a riadenie výnimiek. Addressed by clauses [4.3.1; 4.3.3; 4.3.4; 4.4.1; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 7.1.3; 7.1.4; 7.1.5; 7.1.6; 9.1.1; 9.1.5; 9.1.6].

13.6.4 **Clause 10.1; Clause 10.2; Clause 10.3** - Mapované na priradenie rolí, dokumentáciu, prevádzkové začlenenie, audit a riadenie implementácie pre uchovávanie, výmaz a likvidáciu. Addressed by clauses [5.1.2; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.9; 6.1.7; 7.1.3; 7.1.4; 11.1.1; 11.1.2].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1** - Mapované na riadenie ochrany súkromia založené na rizikách, povedomie vedenia, integráciu rizík ochrany súkromia do PIMS a rizikový kontext súvisiaci s uchovávaním. Addressed by clauses [4.1.6; 4.2.5; 4.5.4; 6.1.2; 6.1.3; 9.1.3; 9.1.4].

13.8 ISO/IEC 27002:2022

13.8.1 Control 7.14; Control 8.10 - Mapované na výmaz informácií, kontrolované dokončenie životného cyklu, uvoľnenie úložných médií a dôkazy o konečnom spôsobe naloženia. Addressed by clauses [4.3.1; 4.3.5; 4.3.6; 4.3.7; 4.4.4; 4.4.5; 7.1.3; 7.1.4; 10.1.2].