					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: PII17					Názov dokumentu: **Politika riadenia zdokumentovaných informácií a dôkazov PIMS**							
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 6.1.3	Both	Supporting	Zdokumentované informácie SoA
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Zdokumentované informácie PIMS
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Riadenie prevádzkových dôkazov
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Dôkazy z monitorovania
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Auditný dôkaz
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Dôkazy z preskúmania manažmentom
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Dôkazy o nezhodách a nápravných opatreniach
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Záznamy prevádzkovateľa o spracúvaní
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Dôkazy o dohode a pokynoch sprostredkovateľa
ISO/IEC 27701:2025	Annex A.3.14	Both	Primary	Ochrana záznamov
GDPR	Article 5(2)	Controller	Supporting	Dôkazy preukázateľnej zodpovednosti
GDPR	Article 24	Controller	Supporting	Opatrenia a dôkazy prevádzkovateľa
GDPR	Article 28	Both	Supporting	Dokumentácia sprostredkovateľa
GDPR	Article 30	Both	Supporting	Záznamy o spracúvaní
GDPR	Article 32	Both	Supporting	Ochrana dôkazov
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Dôkazy súladu s ochranou súkromia
ISO/IEC 29151:2022	Clause 18.1.4	Both	Supporting	Ochrana záznamov

ISO/IEC 27001:2022	Clause 7.5	Both	Supporting	Riadenie zdokumentovaných informácií
ISO/IEC 27002:2022	Control 5.33	Both	Supporting	Ochrana záznamov
ISO/IEC 27002:2022	Control 5.34	Both	Supporting	Ochrana súkromia a PII

1. Rozsah

1.1 Táto politika stanovuje povinné požiadavky na vytváranie, schvaľovanie, verziovanie, ochranu, uchovávanie, vyhľadávanie, preklad, vyradenie a dokladovanie zdokumentovaných informácií PIMS.

1.2 Táto politika sa vzťahuje na politiky PIMS, registre, zdokumentované schválenia, dôkazové záznamy, auditný dôkaz, záznamy z preskúmania manažmentom, dôkazy o nápravných opatreniach a riadené preklady používané na preukázanie zhody PIMS.

1.3 Táto politika sa vzťahuje na kontexty prevádzkovateľa, spoločného prevádzkovateľa, sprostredkovateľa a ďalšieho sprostredkovateľa.

1.4 Táto politika nevytvára samostatný register riadenia dokumentácie. Dôkazy o riadení zdokumentovaných informácií sa vedú prostredníctvom kanonických dôkazových objektov PIMS REG01 až REG12, pričom REG03 a REG12 sa používajú na dôkazy o uplatniteľnosti kontrol, audite, nezhodách, nápravných opatreniach a zlepšovaní.

2. Účel

2.1 Účelom tejto politiky je zabezpečiť, aby zdokumentované informácie PIMS boli presné, riadené, prístupné oprávneným používateľom, chránené pred neoprávnenou zmenou alebo poskytnutím, uchovávané na účely auditovateľnosti a vyradené, keď sa stanú zastaranými.

2.2 Táto politika podporuje pripravenosť na certifikáciu tým, že zabezpečuje, aby dôkazy potrebné na preukázanie zhody PIMS bolo možné nájsť, overiť, vyhľadať a prepojiť s príslušnými politikami, kontrolami, spracovateľskými činnosťami, rizikami, auditmi a nápravnými opatreniami.

3. Ciele

3.1 Cieľmi tejto politiky je:

3.1.1 definovať požiadavky na riadenie zdokumentovaných informácií PIMS;

3.1.2 udržiavať integritu dôkazov v rozsahu REG01 až REG12;

3.1.3 zabezpečiť sledovateľnosť schvaľovania politík a dôkazov;

3.1.4 zabezpečiť zdokumentovanie evidencie verzií a rozhodnutí o vyradení;

3.1.5 prepojiť dôkazy PIMS s Vyhlásením o uplatniteľnosti a mapovaniami politík;

3.1.6 riadiť prístup k dokumentom PIMS a dôkazovým záznamom;

3.1.7 podporovať riadenie verzií viacjazyčných politík a dôkazov;

3.1.8 umožniť včasné vyhľadanie auditného dôkazu;

3.1.9 predchádzať zbytočnej byrokracii pri riadení dokumentácie;

3.1.10 uchovávať záznamy pripravené na audit na účely certifikácie, uistenia zákazníkov a neustáleho zlepšovania.

4. Vyhlásenia politiky

4.1 Riadenie zdokumentovaných informácií PIMS

4.1.1 [All] Privacy Lead / PIMS Manager musí viesť index zdokumentovaných informácií PIMS v REG12 pred prvým zverejnením PIMS a následne štvrťročne.

4.1.2 [All] Process Owner / Business Owner musí identifikovať zdokumentované informácie požadované pre každú vlastnenú spracovateľskú činnosť PII v REG02 pred začatím spracovateľskej činnosti a následne každoročne.

4.1.3 [All] Privacy Lead / PIMS Manager musí prepojiť príslušné politiky, kontroly a dôkazové povinnosti PIMS s REG03 pred každým vydaním politiky a do 15 pracovných dní od akejkoľvek podstatnej zmeny uplatniteľnosti kontroly.

4.1.4 [All] Privacy Lead / PIMS Manager musí priradiť úroveň prístupu a klasifikáciu citlivosti dôkazov ku každej kategórii zdokumentovaných informácií PIMS v REG12 pred použitím danej kategórie.

4.2 Vytváranie, schvaľovanie, verziovanie a zverejňovanie

4.2.1 [All] Privacy Lead / PIMS Manager musí pred zverejnením zdokumentovaných informácií PIMS priradiť v REG12 identifikátor dokumentu, vlastníka, číslo verzie, stav schválenia, dátum účinnosti a dátum preskúmania.

4.2.2 [All] Top Management musí schváliť základné politiky PIMS a podstatné zmeny politík v REG12 pred zverejnením.

4.2.3 [All] Privacy Lead / PIMS Manager musí schváliť šablóny dôkazov PIMS alebo vložené časti registrov v REG12 pred prevádzkovým použitím.

4.2.4 [All] Privacy Lead / PIMS Manager musí zaznamenať evidenciu verzií a odôvodnenie zmeny v REG12 pred vydaním aktualizovaných zdokumentovaných informácií PIMS.

4.2.5 [All] Privacy Lead / PIMS Manager musí zaznamenať komunikáciu schválených zmien zdokumentovaných informácií PIMS v REG11 do 30 dní od zverejnenia.

[... 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 pred odchýlením sa od tejto politiky požiadať o výnimku zo zdokumentovaných informácií alebo riadenia dôkazov v REG12.

9.1.2 [All] Privacy Lead / PIMS Manager musí posúdiť každú výnimku zo zdokumentovaných informácií alebo riadenia dôkazov v REG12 do 10 pracovných dní od žiadosti.

9.1.3 [All] Data Protection Officer / Privacy Advisor musí zaznamenať poradenstvo v REG12 pred schválením akejkoľvek výnimky zahŕňajúcej poskytnutie dôkazov obsahujúcich PII, prekladovú nezrovnalosť, konflikt uchovávania alebo obmedzenie auditného dôkazu.

9.1.4 [All] Top Management musí schváliť výnimky zo zdokumentovaných informácií presahujúce 30 dní alebo ovplyvňujúce certifikáciu, vysokorizikové spracúvanie alebo externé uistenie v REG12 pred nadobudnutím účinnosti výnimky.

9.1.5 [All] Privacy Lead / PIMS Manager musí v REG12 stanoviť dátum uplynutia platnosti nepresahujúci 90 dní pre každú schválenú výnimku zo zdokumentovaných informácií alebo riadenia dôkazov.

9.1.6 [All] Privacy Lead / PIMS Manager musí uzavrieť alebo opätovne posúdiť každú výnimku zo zdokumentovaných informácií alebo riadenia dôkazov v REG12 do piatich pracovných dní od uplynutia jej platnosti.

10. Uplatňovanie politiky

10.1.1 [All] Privacy Lead / PIMS Manager musí zaznamenať chýbajúce, nepresné, neriadené, zastarané alebo nevyhľadateľné zdokumentované informácie PIMS ako nezhodu v REG12 do piatich pracovných dní od identifikácie.

10.1.2 [All] Privacy Lead / PIMS Manager musí zabrániť zverejneniu zdokumentovaných informácií PIMS, ak v REG12 chýbajú požadované dôkazy o schválení, verzii, vlastníkovi alebo dátume účinnosti.

10.1.3 [All] Process Owner / Business Owner musí zabrániť predloženiu dôkazov o spracúvaní na audit, ak v REG02 chýbajú požadované dôkazy o vlastníkovi, dátume, stave alebo schválení.

10.1.4 [All] System Owner / Application Owner musí odobrať neoprávnený prístup k repozitárom zdokumentovaných informácií PIMS a zaznamenať odobratie v REG12 do jedného pracovného dňa od identifikácie.

10.1.5 [All] Internal Audit / Compliance Reviewer musí overiť účinnosť nápravného opatrenia pri nezhodách v zdokumentovaných informáciách v REG12 pri najbližšom plánovanom audite alebo do 60 dní od uzavretia, podľa toho, čo nastane skôr.

11. Preskúmanie a údržba

11.1.1 [All] Privacy Lead / PIMS Manager musí túto politiku preskúmať každoročne a do 30 dní od podstatnej zmeny požiadaviek na zdokumentované informácie PIMS.

11.1.2 [All] Privacy Lead / PIMS Manager musí túto politiku preskúmať do 30 dní po významnom auditnom zistení, certifikačnej nezhode, zmene platformy repozitára alebo zmene procesu viacjazyčného zverejňovania.

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 zverejnením.

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

12. Súvisiace politiky

12.1 Túto politiku podporujú tieto súvisiace politiky:

12.2 PII01 - Politika systému manažérstva ochrany 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 oznámenia o ochrane údajov a transparentnosti

12.6 PII05 - Politika správy súhlasov a preferencií

12.7 PII06 - Politika riadenia práv dotknutých osôb

12.8 PII07 - Politika posúdenia rizík ochrany súkromia a DPIA

12.9 PII08 - Politika ochrany súkromia už od návrhu a štandardne

12.10 PII09 - Politika zhromažďovania, používania, poskytnutia a zdieľania PII

12.11 PII10 - Politika uchovávania, vymazania a likvidácie PII

12.12 PII11 - Politika presnosti a kvality PII

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

12.14 PII13 - Politika medzinárodného prenosu PII

12.15 PII14 - Politika bezpečnosti a riadenia prístupu k PII

12.16 PII15 - Politika riadenia incidentov a porušení ochrany PII

12.17 PII16 - Politika školenia, povedomia a kompetentnosti v oblasti ochrany súkromia

12.18 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 body, ktoré ich implementujú alebo podporujú.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.3** - Mapované na udržiavanie Vyhlásenia o uplatniteľnosti PIMS, záznamov o uplatniteľnosti kontrol a väzby medzi politikou a dôkazmi. Addressed by clauses [4.1.3; 4.3.3; 6.1.3; 7.1.2].

13.2.2 **Clause 7.5** - Mapované na identifikáciu zdokumentovaných informácií, schvaľovanie, riadenie verzií, prístup, vyhľadávanie, uchovávanie, vyradenie, väzbu prekladových verzií a metadáta uchovávania. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.5; 4.4.1; 4.4.2; 4.4.4; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.1; 4.6.2; 4.6.3; 4.6.4].

13.2.3 **Clause 8.1** - Mapované na prevádzkové plánovanie a dôkazy o riadení pre záznamy o spracúvaní, šablóny dôkazov, kvalitu prevádzkových dôkazov a externe poskytnuté dôkazy. Addressed by clauses [4.1.2; 4.2.3; 4.3.2; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1** - Mapované na udržiavanie zdokumentovaných dôkazov o meraní, výkonnosti vyhľadávania, medzerách v dôkazoch, nesúladoch prekladov a dokončení preskúmania prístupu k repozitáru. Addressed by clauses [8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6].

13.2.5 **Clause 9.2** - Mapované na vyhľadávanie auditného dôkazu, auditné vzorkovanie, sledovateľnosť auditného dôkazu a auditné zistenia súvisiace s riadením zdokumentovaných informácií. Addressed by clauses [4.3.4; 4.4.4; 6.1.3; 8.1.3; 10.1.5].

13.2.6 **Clause 9.3** - Mapované na dôkazy z preskúmania manažmentom, zohľadnenie riadenia zdokumentovaných informácií pri preskúmaní manažmentom a preskúmanie výkonnosti riadenia dôkazov zo strany Top Management. Addressed by clauses [6.1.2; 8.1.1; 8.1.2; 11.1.4].

13.2.7 **Clause 10.2** - Mapované na nezhody v zdokumentovaných informáciách, nápravné opatrenia, riadenie výnimiek, uzavretie a overenie účinnosti. Addressed by clauses [4.3.4; 6.1.4; 9.1.1; 9.1.2; 9.1.4; 9.1.5; 9.1.6; 10.1.1; 10.1.5].

13.2.8 **Annex A.1.2.9** - Mapované na záznamy prevádzkovateľa o spracúvaní, záznamy preukázateľnej zodpovednosti, kvalitu dôkazov o spracúvaní a uchovávanie dôkazov podporujúcich povinnosti prevádzkovateľa. Addressed by clauses [4.1.2; 4.3.2; 4.5.1; 7.1.3].

13.2.9 **Annex A.2.2.2** - Mapované na dohodu so sprostredkovateľom, pokyn zákazníka, externe poskytnuté dôkazy a riadenie dôkazov o vzťahu so sprostredkovateľom. Addressed by clauses [5.1.7; 7.1.4].

13.2.10 **Annex A.3.14** - Mapované na ochranu záznamov PIMS pred stratou, neoprávnenou zmenou, neoprávneným prístupom, neoprávneným poskytnutím a nesprávnou likvidáciou. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.2; 4.5.4; 4.5.5; 10.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapované na dôkazy preukázateľnej zodpovednosti, sledovateľnosť dôkazov, vyhľadávanie dôkazov, záznamy o nezhodách a záznamy pripravené na audit preukazujúce súlad. Addressed by clauses [4.1.1; 4.3.2; 4.3.3; 4.4.4; 4.5.4; 6.1.3; 8.1.3; 10.1.1].

13.3.2 **Article 24** - Mapované na dôkazy o správe a riadení prevádzkovateľa, záznamy o schválení, riadenie politík, opatrenia preukázateľnej zodpovednosti, zdokumentované preskúmanie a dohľad zo strany Top Management. Addressed by clauses [4.2.2; 4.3.3; 6.1.2; 9.1.4; 11.1.4].

13.3.3 **Article 28** - Mapované na dokumentáciu sprostredkovateľov a ďalších sprostredkovateľov, dôkazy o pokynoch zákazníkov, externe poskytnuté dôkazy o procesoch a riadenie poskytnutia dôkazov. Addressed by clauses [4.4.5; 5.1.7; 7.1.4].

13.3.4 **Article 30** - Mapované na dôkazy záznamov o spracúvaní, požiadavky na kvalitu dôkazov, odkazy na spracovateľské činnosti a metadáta vlastníka/stavu dôkazov o spracúvaní. Addressed by clauses [4.1.2; 4.3.2; 7.1.3; 10.1.3].

13.3.5 **Article 32** - Mapované na ochranu repozitárov dôkazov, obmedzenia prístupu, schvaľovanie prístupov, preskúmanie ochrany repozitárov a odobratie neoprávneného prístupu. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Mapované na dôkazy súladu s ochranou súkromia, vyhľadávanie auditného dôkazu, sledovateľnosť dôkazov, podporu nezávislého preskúmania a dôkazy o nápravných opatreniach. Addressed by clauses [4.3.3; 4.4.4; 4.6.3; 6.1.3; 8.1.3; 10.1.5].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.1.4** - Mapované na ochranu záznamov súvisiacich s PII, uchovávanie záznamov a kontroly prístupu k repozitárom dôkazov a ich vymazania. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.5.2; 4.5.5; 10.1.4].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 7.5** - Mapované na identifikáciu zdokumentovaných informácií, schvaľovanie, dostupnosť, ochranu, riadenie verzií, uchovávanie, naloženie a riadenie externe požadovaných zdokumentovaných informácií. Addressed by clauses [4.1.1; 4.2.1; 4.2.4; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.6.4].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.33 - Mapované na ochranu záznamov PIMS pred stratou, zničením, falšovaním, neoprávneným prístupom, neoprávneným poskytnutím a nesprávnou likvidáciou. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.7.2 Control 5.34 - Mapované na ochranu súkromia a PII v zdokumentovaných informáciách, repozitároch dôkazov, poskytnutiach a záznamoch s riadeným prístupom. Addressed by clauses [4.1.4; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 6.1.5].