					Sem vložte název registrované právnické osoby							
Číslo dokumentu: PII17					Název dokumentu: **Politika správy dokumentovaných informací a důkazů PIMS**							
Verze: 1.0		Datum účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Standard		Postup		Formulář		Registr		Jiné	

Historie revizí				
Číslo revize	**Datum revize**	**Změny**	**Přezkoumal**	**Vlastník procesu**

Schválení			
Jméno	**Funkce**	**Datum**	**Podpis**

V souladu s normami a právními předpisy

Norma / právní předpis	Kapitola / opatření / článek	Použitelnost	Typ pokrytí	Komentář
ISO/IEC 27701:2025	Clause 6.1.3	Both	Supporting	Dokumentované informace k SoA
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumentované informace PIMS
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Řízení provozních důkazů
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Důkazy z monitorování
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Auditní důkazy
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Důkazy z přezkoumání vedením
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Důkazy o neshodách a nápravných opatřeních
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Záznamy správce o zpracování
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Důkazy o smlouvě a pokynech zpracovatele
ISO/IEC 27701:2025	Annex A.3.14	Both	Primary	Ochrana záznamů
GDPR	Article 5(2)	Controller	Supporting	Důkazy o odpovědnosti
GDPR	Article 24	Controller	Supporting	Opatření a důkazy správce
GDPR	Article 28	Both	Supporting	Dokumentace zpracovatele
GDPR	Article 30	Both	Supporting	Záznamy o zpracování
GDPR	Article 32	Both	Supporting	Ochrana důkazů
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Důkazy o souladu v oblasti ochrany soukromí
ISO/IEC 29151:2022	Clause 18.1.4	Both	Supporting	Ochrana záznamů

ISO/IEC 27001:2022	Clause 7.5	Both	Supporting	Řízení dokumentovaných informací
ISO/IEC 27002:2022	Control 5.33	Both	Supporting	Ochrana záznamů
ISO/IEC 27002:2022	Control 5.34	Both	Supporting	Ochrana soukromí a PII

1. Rozsah

1.1 Tato politika stanoví povinné požadavky na vytváření, schvalování, verzování, ochranu, uchovávání, vyhledávání, překlad, stažení a dokládání dokumentovaných informací PIMS.

1.2 Tato politika se vztahuje na politiky PIMS, registry, dokumentovaná schválení, důkazní záznamy, auditní důkazy, záznamy z přezkoumání vedením, důkazy o nápravných opatřeních a řízené překlady používané k prokázání shody PIMS.

1.3 Tato politika se vztahuje na kontexty správce, společného správce, zpracovatele a dílčího zpracovatele.

1.4 Tato politika nevytváří samostatný registr řízení dokumentů. Důkazy o řízení dokumentovaných informací jsou vedeny prostřednictvím kanonických důkazních objektů PIMS REG01 až REG12, přičemž REG03 a REG12 se používají pro důkazy o použitelnosti opatření, auditu, neshodách, nápravných opatřeních a zlepšování.

2. Účel

2.1 Účelem této politiky je zajistit, aby dokumentované informace PIMS byly přesné, řízené, dostupné oprávněným uživatelům, chráněné před neoprávněnou změnou nebo zpřístupněním, uchovávané pro auditovatelnost a stažené, jakmile se stanou zastaralými.

2.2 Tato politika podporuje připravenost na certifikaci tím, že zajišťuje, aby důkazy potřebné k prokázání shody PIMS bylo možné nalézt, ověřit, vyhledat a propojit s příslušnými politikami, opatřeními, činnostmi zpracování, riziky, audity a nápravnými opatřeními.

3. Cíle

3.1 Cílem této politiky je:

3.1.1 stanovit požadavky na řízení dokumentovaných informací PIMS;

3.1.2 udržovat integritu důkazů napříč REG01 až REG12;

3.1.3 zajistit dohledatelnost schválení politik a důkazů;

3.1.4 zajistit dokumentování historie verzí a rozhodnutí o stažení;

3.1.5 propojit důkazy PIMS s Prohlášením o použitelnosti a mapováním politik;

3.1.6 řídit přístup k dokumentům PIMS a důkazním záznamům;

3.1.7 podporovat řízení vícejazyčných verzí politik a důkazů;

3.1.8 umožnit včasné vyhledání auditních důkazů;

3.1.9 předcházet zbytečné byrokracii při řízení dokumentů;

3.1.10 uchovávat záznamy připravené pro audit pro účely certifikace, ujištění zákazníků a neustálého zlepšování.

4. Prohlášení politiky

4.1 Řízení dokumentovaných informací PIMS

4.1.1 [All] Privacy Lead / PIMS Manager musí vést index dokumentovaných informací PIMS v REG12 před prvním zveřejněním PIMS a poté čtvrtletně.

4.1.2 [All] Process Owner / Business Owner musí identifikovat dokumentované informace požadované pro každou jím vlastněnou činnost zpracování PII v REG02 před zahájením činnosti zpracování a poté každoročně.

4.1.3 [All] Privacy Lead / PIMS Manager musí propojit příslušné politiky PIMS, opatření a důkazní povinnosti s REG03 před každým vydáním politiky a do 15 pracovních dnů od jakékoli významné změny použitelnosti opatření.

4.1.4 [All] Privacy Lead / PIMS Manager musí přiřadit každé kategorii dokumentovaných informací PIMS úroveň přístupu a klasifikaci citlivosti důkazů v REG12 před použitím dané kategorie.

4.2 Vytváření, schvalování, verzování a zveřejňování

4.2.1 [All] Privacy Lead / PIMS Manager musí před zveřejněním dokumentovaných informací PIMS přiřadit v REG12 identifikátor dokumentu, vlastníka, číslo verze, stav schválení, datum účinnosti a datum přezkumu.

4.2.2 [All] Top Management musí před zveřejněním schválit v REG12 základní politiky PIMS a významné změny politik.

4.2.3 [All] Privacy Lead / PIMS Manager musí před provozním použitím schválit v REG12 šablony důkazů PIMS nebo vložené části registrů.

4.2.4 [All] Privacy Lead / PIMS Manager musí před vydáním aktualizovaných dokumentovaných informací PIMS zaznamenat v REG12 historii verzí a odůvodnění změny.

4.2.5 [All] Privacy Lead / PIMS Manager musí zaznamenat komunikaci schválených změn dokumentovaných informací PIMS v REG11 do 30 dnů od zveřejnění.

[... Oddíly 4.3–8 nejsou součástí tohoto náhledu. Pro přístup k úplnému obsahu zakupte celý dokument. ...]

9. Výjimky

9.1.1 [All] Process Owner / Business Owner musí před odchýlením se od této politiky požádat v REG12 o výjimky z řízení dokumentovaných informací nebo důkazů.

9.1.2 [All] Privacy Lead / PIMS Manager musí každou výjimku z řízení dokumentovaných informací nebo důkazů posoudit v REG12 do 10 pracovních dnů od žádosti.

9.1.3 [All] Data Protection Officer / Privacy Advisor musí před schválením jakékoli výjimky zahrnující zpřístupnění důkazů obsahujících PII, nesrovnalost v překladu, konflikt uchovávání nebo omezení auditních důkazů zaznamenat doporučení v REG12.

9.1.4 [All] Top Management musí před nabytím účinnosti výjimky schválit v REG12 výjimky z dokumentovaných informací přesahující 30 dnů nebo ovlivňující certifikaci, vysoce rizikové zpracování nebo externí ujištění.

9.1.5 [All] Privacy Lead / PIMS Manager musí pro každou schválenou výjimku z řízení dokumentovaných informací nebo důkazů stanovit v REG12 datum skončení platnosti nepřesahující 90 dnů.

9.1.6 [All] Privacy Lead / PIMS Manager musí každou výjimku z řízení dokumentovaných informací nebo důkazů uzavřít nebo znovu posoudit v REG12 do pěti pracovních dnů od skončení její platnosti.

10. Uplatňování požadavků

10.1.1 [All] Privacy Lead / PIMS Manager musí do pěti pracovních dnů od identifikace zaznamenat chybějící, nepřesné, neřízené, zastaralé nebo nevyhledatelné dokumentované informace PIMS jako neshodu v REG12.

10.1.2 [All] Privacy Lead / PIMS Manager musí zabránit zveřejnění dokumentovaných informací PIMS, pokud v REG12 chybí požadované důkazy o schválení, verzi, vlastníkovi nebo datu účinnosti.

10.1.3 [All] Process Owner / Business Owner musí zabránit předložení důkazů o zpracování k auditu, pokud v REG02 chybí požadované důkazy o vlastníkovi, datu, stavu nebo schválení.

10.1.4 [All] System Owner / Application Owner musí odebrat neoprávněný přístup k repozitářům dokumentovaných informací PIMS a zaznamenat odebrání v REG12 do jednoho pracovního dne od identifikace.

10.1.5 [All] Internal Audit / Compliance Reviewer musí při nejbližším plánovaném auditu nebo do 60 dnů od uzavření, podle toho, co nastane dříve, ověřit v REG12 účinnost nápravných opatření k neshodám v dokumentovaných informacích.

11. Přezkum a údržba

11.1.1 [All] Privacy Lead / PIMS Manager musí tuto politiku přezkoumat každoročně a do 30 dnů od významné změny požadavků na dokumentované informace PIMS.

11.1.2 [All] Privacy Lead / PIMS Manager musí tuto politiku přezkoumat do 30 dnů po závažném zjištění auditu, certifikační neshodě, změně platformy repozitáře nebo změně procesu vícejazyčného zveřejňování.

11.1.3 [All] Data Protection Officer / Privacy Advisor musí před schválením přezkoumat v REG12 změny této politiky významné z hlediska ochrany soukromí.

11.1.4 [All] Top Management musí před zveřejněním schválit v REG12 významné změny této politiky.

11.1.5 [All] Privacy Lead / PIMS Manager musí zaznamenat komunikaci schválených změn této politiky v REG11 do 30 dnů od zveřejnění.

12. Související politiky

12.1 Tato politika je podporována následujícími souvisejícími politikami:

12.2 PII01 - Politika systému řízení informací o soukromí

12.3 PII02 - Politika rolí, odpovědností a odpovědnosti za ochranu soukromí

12.4 PII03 - Politika evidence zpracování PII a právního základu

12.5 PII04 - Politika oznámení o ochraně osobních údajů a transparentnosti

12.6 PII05 - Politika správy souhlasů a preferencí

12.7 PII06 - Politika správy práv subjektů PII

12.8 PII07 - Politika posouzení rizik pro soukromí a DPIA

12.9 PII08 - Politika ochrany soukromí již od návrhu a ve výchozím nastavení

12.10 PII09 - Politika shromažďování, používání, zpřístupňování a sdílení PII

12.11 PII10 - Politika uchovávání, výmazu a likvidace PII

12.12 PII11 - Politika přesnosti a kvality PII

12.13 PII12 - Politika řízení ochrany soukromí u zpracovatelů, dílčích zpracovatelů a třetích stran

12.14 PII13 - Politika mezinárodního předávání PII

12.15 PII14 - Politika zabezpečení PII a řízení přístupu

12.16 PII15 - Politika řízení incidentů a porušení zabezpečení PII

12.17 PII16 - Politika školení, povědomí a způsobilosti v oblasti ochrany soukromí

12.18 PII18 - Politika monitorování, auditu a zlepšování PIMS

13. Referenční normy a rámce

13.1 Tato politika je namapována na následující normy a právní předpisy. Mapování vysvětluje, jak politika podporuje citované požadavky, a identifikuje interní ustanovení, která je implementují nebo podporují.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.3** - Namapováno na vedení Prohlášení o použitelnosti PIMS, záznamů o použitelnosti opatření a vazeb mezi politikami a důkazy. Addressed by clauses [4.1.3; 4.3.3; 6.1.3; 7.1.2].

13.2.2 **Clause 7.5** - Namapováno na identifikaci dokumentovaných informací, schvalování, řízení verzí, přístup, vyhledávání, uchování, stažení, vazbu překladové verze a metadata uchovávání. 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** - Namapováno na důkazy o operativním plánování a řízení pro záznamy o zpracování, šablony důkazů, kvalitu provozních důkazů a externě poskytnuté důkazy. Addressed by clauses [4.1.2; 4.2.3; 4.3.2; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1** - Namapováno na vedení dokumentovaných důkazů o měření, výkonnosti vyhledávání, mezerách v důkazech, nesouladech překladů a dokončení přezkumu přístupů k repozitáři. 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** - Namapováno na vyhledávání auditních důkazů, auditní vzorkování, dohledatelnost auditních důkazů a zjištění auditu související s řízením dokumentovaných informací. Addressed by clauses [4.3.4; 4.4.4; 6.1.3; 8.1.3; 10.1.5].

13.2.6 **Clause 9.3** - Namapováno na důkazy z přezkoumání vedením, zohlednění řízení dokumentovaných informací při přezkoumání vedením a přezkum výkonnosti řízení důkazů, který provádí Top Management. Addressed by clauses [6.1.2; 8.1.1; 8.1.2; 11.1.4].

13.2.7 **Clause 10.2** - Namapováno na neshody v dokumentovaných informacích, nápravná opatření, řešení výjimek, uzavření a ověření 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** - Namapováno na záznamy správce o zpracování, záznamy odpovědnosti, kvalitu důkazů o zpracování a uchovávání důkazů podporujících povinnosti správce. Addressed by clauses [4.1.2; 4.3.2; 4.5.1; 7.1.3].

13.2.9 **Annex A.2.2.2** - Namapováno na smlouvu zpracovatele, pokyn zákazníka, externě poskytnuté důkazy a řízení důkazů o vztahu se zpracovatelem. Addressed by clauses [5.1.7; 7.1.4].

13.2.10 **Annex A.3.14** - Namapováno na ochranu záznamů PIMS před ztrátou, neoprávněnou změnou, neoprávněným přístupem, neoprávněným vydáním a nesprávnou likvidací. 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)** - Namapováno na důkazy o odpovědnosti, dohledatelnost důkazů, vyhledávání důkazů, záznamy neshod a záznamy připravené pro audit dokládající soulad. 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** - Namapováno na důkazy o správě a řízení správce, záznamy o schválení, řízení politik, opatření odpovědnosti, dokumentovaný přezkum a dohled ze 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** - Namapováno na dokumentaci zpracovatelů a dílčích zpracovatelů, důkazy o pokynech zákazníka, externě poskytnuté procesní důkazy a řízení zpřístupnění důkazů. Addressed by clauses [4.4.5; 5.1.7; 7.1.4].

13.3.4 **Article 30** - Namapováno na důkazy o záznamech zpracování, požadavky na kvalitu důkazů, odkazy na činnosti zpracování a metadata vlastníka/stavu důkazů o zpracování. Addressed by clauses [4.1.2; 4.3.2; 7.1.3; 10.1.3].

13.3.5 **Article 32** - Namapováno na ochranu repozitářů důkazů, omezení přístupu, schvalování přístupu, přezkum ochrany repozitáře a odebrání neoprávněného přístupu. 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** - Namapováno na důkazy o souladu v oblasti ochrany soukromí, vyhledávání auditních důkazů, dohledatelnost důkazů, podporu nezávislého přezkumu a důkazy o nápravných opatřeních. 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** - Namapováno na ochranu záznamů souvisejících s PII, uchování záznamů a řízení přístupu k repozitáři důkazů a výmazu. 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** - Namapováno na identifikaci dokumentovaných informací, schvalování, dostupnost, ochranu, řízení verzí, uchovávání, vypořádání a řízení externě požadovaných dokumentovaných informací. 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 - Namapováno na ochranu záznamů PIMS před ztrátou, zničením, falšováním, neoprávněným přístupem, neoprávněným vydáním a nesprávnou likvidací. 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 - Namapováno na ochranu soukromí a PII v dokumentovaných informacích, repozitářích důkazů, zpřístupněních a záznamech s řízeným přístupem. Addressed by clauses [4.1.4; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 6.1.5].