					Sem vložte název registrované právnické osoby							
Číslo dokumentu: PII01					Název dokumentu: **Politika systému řízení informací o soukromí**							
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

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 4.1	Both	Primary	Kontext a určení role PIMS
ISO/IEC 27701:2025	Clause 4.2	Both	Primary	Zainteresované strany a požadavky
ISO/IEC 27701:2025	Clause 4.3	Both	Primary	Rozsah PIMS
ISO/IEC 27701:2025	Clause 4.4	Both	Primary	Zavedení a zlepšování PIMS
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Vedení a závazek
ISO/IEC 27701:2025	Clause 5.2	Both	Primary	Politika ochrany soukromí
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	Role a pravomoci
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	Rizika a příležitosti
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Posouzení rizik pro soukromí
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Ošetření rizik pro soukromí a SoA
ISO/IEC 27701:2025	Clause 6.2	Both	Primary	Cíle ochrany soukromí
ISO/IEC 27701:2025	Clause 6.3	Both	Primary	Plánované změny PIMS
ISO/IEC 27701:2025	Clause 7.1	Both	Primary	Zdroje
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Kompetence
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Povědomí
ISO/IEC 27701:2025	Clause 7.4	Both	Primary	Komunikace
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumentované informace
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Operativní plánování a řízení
ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Provozní posouzení rizik pro soukromí

ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Provozní ošetření rizik pro soukromí
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Monitorování a vyhodnocování
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Interní audit
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Přezkoumání vedením
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Neustálé zlepšování
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	Neshoda a nápravné opatření
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9	Controller	Primary	Záznamy správy a řízení na straně správce
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3	Processor	Primary	Smlouva zpracovatele a účely
ISO/IEC 27701:2025	Annex A.3.3	Both	Primary	Vazba na politiku zabezpečení osobně identifikovatelných údajů (PII)
GDPR	Article 5(2)	Controller	Supporting	Důkazy odpovědnosti
GDPR	Article 24	Controller	Supporting	Opatření a politika správce
GDPR	Article 26	Joint Controller	Supporting	Ujednání společných správců
GDPR	Article 28	Both	Supporting	Správa zpracovatelů
GDPR	Article 30	Both	Supporting	Záznamy o zpracování
GDPR	Article 32	Both	Supporting	Zabezpečení zpracování
GDPR	Article 35	Controller	Supporting	Správa DPIA
ISO/IEC 29100:2020	Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12	Both	Supporting	Opatření a zásady ochrany soukromí

ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	Proces a příprava PIA
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2; Annex A.2	Controller	Supporting	Program a politika ochrany osobně identifikovatelných údajů (PII)
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1	Both	Supporting	Integrace organizačních rizik pro soukromí

1. Rozsah

1.1 Tato politika stanoví systém řízení informací o soukromí organizace pro zpracování osobně identifikovatelných údajů (PII) v kontextech správce, společného správce, zpracovatele a dílčího zpracovatele.

1.2 Tato politika se vztahuje na:

1.2.1 rozsah PIMS, kontext, zainteresované strany a organizační hranice;

1.2.2 určení role PIMS pro činnosti zpracování osobně identifikovatelných údajů (PII);

1.2.3 politiku ochrany soukromí, cíle ochrany soukromí, posouzení rizik pro soukromí, ošetření rizik pro soukromí a Prohlášení o použitelnosti PIMS;

1.2.4 správu a řízení PIMS, monitorování, interní audit, přezkoumání vedením, neshodu, nápravné opatření a neustálé zlepšování;

1.2.5 dokumentované informace a důkazy potřebné k prokázání shody PIMS a odpovědnosti.

1.3 Pro účely této politiky znamená významná změna jakoukoli změnu, která ovlivňuje rozsah PIMS, účely zpracování osobně identifikovatelných údajů (PII), kategorie osobně identifikovatelných údajů (PII), kategorie subjektů PII, místa zpracování, rozdělení rolí správce nebo zpracovatele, architekturu systému, ujednání s dodavatelem nebo dílčím zpracovatelem, profil rizik pro soukromí, použitelné právní nebo smluvní povinnosti nebo rozsah certifikace.

2. Účel

2.1 Tato politika definuje povinné požadavky na správu a řízení pro zavedení, implementaci, udržování, monitorování a neustálé zlepšování PIMS.

2.2 Účelem této politiky je zajistit, aby organizace dokázala prokázat odpovědné, rizikově orientované a důkazy podložené řízení zpracování osobně identifikovatelných údajů (PII) napříč použitelnými rolemi PIMS.

3. Cíle

3.1 Cílem této politiky je:

3.1.1 vymezit rozsah, kontext, hranice a použitelnost rolí PIMS;

3.1.2 přiřadit odpovědnost za správu a řízení PIMS s použitím kanonických rolí PIMS;

3.1.3 stanovit cíle ochrany soukromí a měřitelná očekávání výkonnosti PIMS;

3.1.4 udržovat Prohlášení o použitelnosti PIMS pro vybraná a vyloučená opatření;

3.1.5 začlenit posouzení rizik pro soukromí, ošetření rizik pro soukromí a správu DPIA do provozu PIMS;

3.1.6 zajistit, aby povinnosti správce, společného správce, zpracovatele a dílčího zpracovatele byly identifikovány před zahájením zpracování;

3.1.7 udržovat důkazy připravené k auditu pro připravenost na certifikaci a neustálé zlepšování;

3.1.8 vyhnout se zbytečným rolím, registrům, formulářům a duplicitním provozním opatřením.

4. Prohlášení politiky

4.1 Zavedení, kontext a rozsah PIMS

4.1.1 [Both] Top Management musí schválit rozsah PIMS v REG01 před prvotní implementací PIMS a do 30 dnů od jakékoli významné změny.

4.1.2 [Both] Privacy Lead / PIMS Manager musí každoročně a do 30 dnů od jakékoli významné změny dokumentovat externí a interní kontextové otázky ochrany soukromí v REG01.

4.1.3 [Both] Privacy Lead / PIMS Manager musí každoročně a do 30 dnů od jakékoli významné změny dokumentovat relevantní zainteresované strany a jejich požadavky na PIMS v REG01.

4.1.4 [Both] Privacy Lead / PIMS Manager musí před každým přezkoumáním vedením udržovat souhrn interakcí procesů PIMS v REG01.

4.2 Určení role PIMS

4.2.1 [Both] Process Owner / Business Owner musí před zahájením každé činnosti zpracování osobně identifikovatelných údajů (PII) klasifikovat roli PIMS organizace v REG02.

4.2.2 [Joint Controller] Vendor / Procurement Owner musí před zahájením společného zpracování dokumentovat rozdělení odpovědností společných správců v REG08.

4.2.3 [Processor] Vendor / Procurement Owner musí před onboardingem služby dokumentovat pokyny zákazníka ke zpracování pro činnosti zpracovatele v REG08.

4.2.4 [Subprocessor] Vendor / Procurement Owner musí před zahájením dílčího zpracování dokumentovat pokyny zákazníka v předcházejícím smluvním řetězci a schválená ujednání o dílčím zpracování v REG08.

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

9. Výjimky

9.1 Žádost o výjimku a schválení

9.1.1 [All] Process Owner / Business Owner musí před vznikem odchylky dokumentovat jakoukoli požadovanou výjimku z této politiky v REG12.

9.1.2 [Both] Privacy Lead / PIMS Manager musí před schválením posoudit riziko pro soukromí každé požadované výjimky v REG04.

9.1.3 [Both] Top Management musí před implementací schválit v REG12 výjimky, které překračují přijaté prahové hodnoty rizik pro soukromí.

9.1.4 [Both] Privacy Lead / PIMS Manager musí čtvrtletně přezkoumávat aktivní výjimky PIMS v REG12 až do jejich uzavření.

9.2 Uzavření výjimky

9.2.1 [All] Process Owner / Business Owner musí k datu schválené expirace výjimky dokumentovat důkazy o uzavření výjimky v REG12.

9.2.2 [Both] Internal Audit / Compliance Reviewer musí během nejbližšího plánovaného interního auditu ověřit důkazy o uzavření expirované výjimky v REG12.

10. Uplatňování politiky

10.1 Řešení neshod

10.1.1 [All] Privacy Lead / PIMS Manager musí do pěti pracovních dnů od zjištění zaznamenat podezření na neshody s touto politikou v REG12.

10.1.2 [All] Process Owner / Business Owner musí po schválení neshody implementovat schválená nápravná opatření v REG12 do přiřazeného termínu splnění.

10.1.3 [All] Top Management musí při každém přezkoumání vedením přezkoumat nevyřešené závažné neshody PIMS v REG12.

10.1.4 [All] Internal Audit / Compliance Reviewer musí do 30 dnů od nahlášeného uzavření ověřit účinnost nápravného opatření v REG12.

10.2 Eskalace

10.2.1 [All] Privacy Lead / PIMS Manager musí do pěti pracovních dnů po termínu splnění eskalovat závažná nápravná opatření po termínu na Top Management v REG12.

10.2.2 [All] Top Management musí do 15 pracovních dnů od eskalace zaznamenat rozhodnutí o závažných nápravných opatřeních po termínu v REG12.

11. Přezkum a údržba

11.1 Přezkum politiky

11.1.1 [All] Privacy Lead / PIMS Manager musí každoročně a do 30 dnů od jakékoli významné změny právního, organizačního, zpracovatelského, technologického nebo certifikačního rozsahu přezkoumat tuto politiku v REG12.

11.1.2 [All] Data Protection Officer / Privacy Advisor musí před schválením politiky poskytnout dokumentované poradenství v REG12, pokud se významně změní povinnosti v oblasti ochrany soukromí.

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

11.1.4 [All] Privacy Lead / PIMS Manager musí do 15 pracovních dnů po schválených změnách politiky, které mění rozsah PIMS nebo použitelnost opatření, aktualizovat REG01 a REG03.

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

12. Související politiky

12.1 Tuto politiku podporují následující související politiky:

12.2 PII02 - Politika rolí, povinností a odpovědnosti v oblasti ochrany soukromí

12.3 PII03 - Politika evidence zpracování PII a právního základu

12.4 PII07 - Politika posouzení rizik pro soukromí a DPIA

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

12.6 PII12 - Politika zpracovatelů, dílčích zpracovatelů a sdílení dat

12.7 PII14 - Politika zabezpečení PII a řízení přístupu

12.8 PII15 - Politika řízení incidentů a porušení zabezpečení PII

12.9 PII16 - Politika školení, povědomí a kompetence v oblasti ochrany soukromí

12.10 PII17 - Politika dokumentovaných informací PIMS a správy důkazů

12.11 PII18 - Politika monitorování, auditu a zlepšování PIMS

13. Referenční normy a rámce

13.1 Tato politika je mapována 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 4.1** - Mapováno na určování organizačního kontextu, kontextových otázek ochrany soukromí a použitelnosti role správce nebo zpracovatele pro činnosti PIMS. Addressed by clauses [4.1.2; 4.2.1; 6.1.3].

13.2.2 **Clause 4.2** - Mapováno na identifikaci zainteresovaných stran, subjektů PII, zákazníků, dozorových orgánů, zpracovatelů, dílčích zpracovatelů a jejich relevantních požadavků na PIMS. Addressed by clauses [4.1.3; 7.2.1; 11.1.1].

13.2.3 **Clause 4.3** - Mapováno na definování, schvalování, udržování a změny dokumentovaného rozsahu PIMS. Addressed by clauses [4.1.1; 6.1.3; 11.1.4].

13.2.4 **Clause 4.4** - Mapováno na zavedení, implementaci, udržování a zlepšování procesů PIMS a jejich vzájemných interakcí. Addressed by clauses [4.1.4; 7.1.1; 7.2.1].

13.2.5 **Clause 5.1** - Mapováno na schvalování ze strany Top Management, zdroje, přezkum správy a řízení a vedení v oblasti účinnosti a zlepšování PIMS. Addressed by clauses [4.3.1; 5.1.1; 6.1.1; 8.1.4; 10.1.3].

13.2.6 **Clause 5.2** - Mapováno na udržování této politiky ochrany soukromí jako schválené dokumentované informace a komunikaci změn politiky. Addressed by clauses [4.3.1; 11.1.1; 11.1.3; 11.1.5].

13.2.7 **Clause 5.3** - Mapováno na přiřazování a komunikaci rolí, odpovědností a pravomocí PIMS. Addressed by clauses [5.1.1; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.8 **Clause 6.1.1** - Mapováno na plánování opatření pro rizika a příležitosti PIMS s využitím kontextu, požadavků zainteresovaných stran, cílů a vstupů pro zlepšování. Addressed by clauses [4.1.2; 4.1.3; 4.4.1; 6.1.1; 8.1.1].

13.2.9 **Clause 6.1.2** - Mapováno na požadavek provést posouzení rizik pro soukromí před novým nebo významně změněným zpracováním a udržovat důkazy o rizicích pro soukromí. Addressed by clauses [4.4.1; 5.1.3; 8.2.4; 9.1.2].

13.2.10 **Clause 6.1.3** - Mapováno na ošetření rizik pro soukromí, výběr opatření, vazbu na program bezpečnosti informací a udržování Prohlášení o použitelnosti. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.3; 7.1.4; 8.2.2].

13.2.11 **Clause 6.2** - Mapováno na stanovení, měření, monitorování, komunikaci a aktualizaci cílů PIMS. Addressed by clauses [4.3.1; 4.3.2; 8.1.2; 8.1.4].

13.2.12 **Clause 6.3** - Mapováno na plánované změny PIMS a řízení změn ovlivňujících rozsah, role, opatření a dokumentované informace. Addressed by clauses [4.1.1; 6.1.3; 7.1.1; 11.1.4].

13.2.13 **Clause 7.1** - Mapováno na určování a poskytování zdrojů pro zavedení, provoz, údržbu a zlepšování PIMS. Addressed by clauses [5.1.1; 6.1.1; 7.1.1].

13.2.14 **Clause 7.2** - Mapováno na očekávání kompetencí a důkazy podporující odpovědnosti PIMS a výkon rolí. Addressed by clauses [5.1.3; 5.1.8; 11.1.5].

13.2.15 **Clause 7.3** - Mapováno na povědomí o politice ochrany soukromí, přínos k účinnosti PIMS a důsledky neshody. Addressed by clauses [11.1.5; 10.1.1; 10.2.1].

13.2.16 **Clause 7.4** - Mapováno na interní a externí komunikace relevantní pro správu a řízení PIMS, změny politiky a eskalaci. Addressed by clauses [6.2.1; 10.2.1; 11.1.5].

13.2.17 **Clause 7.5** - Mapováno na vytváření, udržování a řízení dokumentovaných informací, připravenost důkazů a uchovávání. Addressed by clauses [4.5.1; 4.5.3; 7.1.6; 11.1.4].

13.2.18 **Clause 8.1** - Mapováno na plánování, implementaci a řízení provozních procesů PIMS a externě poskytovaných procesů. Addressed by clauses [4.4.4; 7.1.3; 7.1.5; 7.2.1].

13.2.19 **Clause 8.2** - Mapováno na provádění posouzení rizik pro soukromí v plánovaných intervalech a při navržení nebo výskytu významných změn. Addressed by clauses [4.4.1; 8.2.4; 9.1.2].

13.2.20 **Clause 8.3** - Mapováno na implementaci plánů ošetření rizik pro soukromí a uchovávání důkazů o výsledcích ošetření. Addressed by clauses [4.4.3; 7.1.3; 8.2.2].

13.2.21 **Clause 9.1** - Mapováno na monitorování, měření, analýzu, vyhodnocování, metriky a vykazování účinnosti PIMS. Addressed by clauses [8.1.1; 8.1.2; 8.1.4; 8.2.1; 8.2.2; 8.2.3; 8.2.4].

13.2.22 **Clause 9.2** - Mapováno na plánování interního auditu, vzorkování důkazů, výsledky auditu a nezávislý přezkum. Addressed by clauses [5.1.9; 6.2.1; 8.1.3; 9.2.2].

13.2.23 **Clause 9.3** - Mapováno na vstupy pro přezkoumání vedením, přezkum výkonnosti, výstupy přezkoumání vedením a rozhodnutí o zlepšování. Addressed by clauses [6.1.1; 6.1.2; 8.1.4; 10.1.3].

13.2.24 **Clause 10.1** - Mapováno na neustálé zlepšování prostřednictvím přezkoumání vedením, metrik, sledování nápravných opatření a údržby politiky. Addressed by clauses [6.1.1; 6.2.2; 10.1.4; 11.1.1].

13.2.25 **Clause 10.2** - Mapováno na řešení neshod, nápravná opatření, eskalaci, uzavírání a ověřování účinnosti. Addressed by clauses [4.5.2; 6.2.2; 6.2.3; 10.1.1; 10.1.2; 10.1.4; 10.2.1; 10.2.2].

13.2.26 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9** - Mapováno na záznamy účelů zpracování na straně správce, vazbu na právní základ, určení potřeby DPIA, rozdělení odpovědností společných správců a záznamy důkazů o zpracování. Addressed by clauses [4.2.1; 4.2.2; 4.4.2; 4.5.1; 7.1.2; 8.2.1].

13.2.27 **Annex A.2.2.2; Annex A.2.2.3** - Mapováno na zákaznické smlouvy zpracovatele, dokumentované pokyny zákazníka a omezení účelů zpracovatele. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.2.28 **Annex A.3.3** - Mapováno na vazbu na politiku zabezpečení osobně identifikovatelných údajů (PII), vlastnictví základního souboru bezpečnostních opatření pro osobně identifikovatelné údaje (PII) a stav opatření bezpečnosti informací v Prohlášení o použitelnosti PIMS. Addressed by clauses [4.3.4; 5.1.4; 7.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapováno na důkazy odpovědnosti, schválení politiky, klasifikaci role při zpracování, použitelnost opatření, monitorování, audit a záznamy nápravných opatření. Addressed by clauses [4.3.1; 4.5.1; 4.5.2; 6.1.1; 8.1.3].

13.3.2 **Article 24** - Mapováno na opatření správy a řízení správce, schválení politiky, cíle PIMS, přezkum účinnosti a dokumentované důkazy odpovědnosti správce. Addressed by clauses [4.3.1; 4.3.2; 6.1.1; 8.1.4; 11.1.1].

13.3.3 **Article 26** - Mapováno na určení a dokumentování rozdělení odpovědností společných správců před zahájením společného zpracování. Addressed by clauses [4.2.2; 5.1.7; 7.1.5].

13.3.4 **Article 28** - Mapováno na záznamy správy a řízení zpracovatelů a dílčích zpracovatelů, pokyny zákazníka ke zpracování a řízení externě poskytovaných procesů. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.3.5 **Article 30** - Mapováno na záznamy o činnostech zpracování, klasifikaci rolí, záznamy odpovědnosti za zpracování a důkazy uchovávané pro auditovatelnost. Addressed by clauses [4.2.1; 5.1.5; 7.1.2; 8.2.1].

13.3.6 **Article 32** - Mapováno na správu a řízení základního souboru bezpečnostních opatření pro osobně identifikovatelné údaje (PII), vlastnictví bezpečnostních opatření, stav implementace bezpečnosti a potvrzení provozních opatření. Addressed by clauses [4.3.4; 4.4.4; 5.1.4; 7.1.4].

13.3.7 **Article 35** - Mapováno na určení potřeby DPIA a posouzení rizik pro soukromí před pokračováním vysoce rizikového nebo významně změněného zpracování správcem. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12** - Mapováno na identifikaci opatření ochrany soukromí, zásady ochrany soukromí, bezpečnost informací, soulad v oblasti ochrany soukromí, audit, důkazy a rizikově orientovanou správu ochrany soukromí. Addressed by clauses [4.3.3; 4.3.4; 4.4.1; 4.5.1; 8.1.3; 10.1.4].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Mapováno na správu a řízení PIA, určení spouštěče DPIA, přípravu PIA, kritéria rizik pro soukromí a dokumentované důkazy posouzení rizik pro soukromí. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4; 9.1.2].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2; Annex A.2** - Mapováno na požadavky programu ochrany osobně identifikovatelných údajů (PII), identifikaci požadavků na ochranu osobně identifikovatelných

údajů (PII), výběr opatření na základě rizik pro soukromí a směřování politiky ochrany osobně identifikovatelných údajů (PII). Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.4].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1** - Mapováno na zásady organizačních rizik pro soukromí, závazek vedení, integraci rizik pro soukromí do správy a řízení PIMS a porozumění roli organizace při zpracování osobně identifikovatelných údajů (PII). Addressed by clauses [4.1.2; 4.2.1; 4.4.1; 4.4.3; 6.1.1].