					Sem vložte název registrované právnické osoby						
Číslo dokumentu: PII02					Název dokumentu: **Politika rolí, odpovědností a odpovědnosti za ochranu 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

Norma / právní předpis	Kapitola / opatření / článek	Použitelnost	Typ pokrytí	Komentář
ISO/IEC 27701:2025	Clause 4.1	Both	Primary	Kontext rolí PIMS
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Vedení a odpovědnost
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	Role, odpovědnosti a pravomoci PIMS
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Kompetence pro role
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Povědomí o rolích
ISO/IEC 27701:2025	Clause 7.4	Both	Supporting	Komunikace rolí
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumentované informace k rolím
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Vlastnictví operativního řízení
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Nezávislá auditní role
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Přezkoumání odpovědnosti vedením
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Neshoda a nápravné opatření související s rolí
ISO/IEC 27701:2025	Annex A.1.2.7	Controller	Supporting	Odpovědnost za smlouvu se zpracovatelem
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Primary	Role a odpovědnosti společných správců
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Záznamy odpovědnosti
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Primary	Dohody se zákazníky a pokyny u zpracovatele
ISO/IEC 27701:2025	Annex A.2.2.3	Processor	Supporting	Soulad účelu zpracovatele
GDPR	Article 5(2)	Controller	Supporting	Důkazy o odpovědnosti

GDPR	Article 24	Controller	Supporting	Odpovědnost správce a opatření
GDPR	Article 26	Joint Controller	Supporting	Ujednání společných správců
GDPR	Article 28	Both	Supporting	Správa zpracovatelů a pokyny
GDPR	Article 30	Both	Supporting	Záznamy o zpracování a důkazy o odpovědnosti
GDPR	Article 37	Conditional	Referenced	Určení DPO, kde je použitelné
GDPR	Article 38	Conditional	Supporting	Postavení a nezávislost DPO, kde je použitelné
GDPR	Article 39	Conditional	Supporting	Úkoly DPO, kde jsou použitelné
ISO/IEC 29100:2020	Clause 4.1; Clause 4.2	Both	Supporting	Aktéři a role rámce ochrany soukromí
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Odpovědnost za soulad v oblasti ochrany soukromí
ISO/IEC 29151:2022	Clause 6.1.2; Clause 6.1.3	Both	Supporting	Role ochrany PII a oddělení povinností
ISO/IEC 27002:2022	Control 5.2	Both	Supporting	Role a odpovědnosti v oblasti bezpečnosti informací
ISO/IEC 27002:2022	Control 5.3	Both	Supporting	Oddělení povinností

1. Rozsah

1.1 Tato politika definuje model rolí PIMS, strukturu odpovědnosti, pravidla přiřazování odpovědností, pravidla pro kombinování rolí, očekávání týkající se eskalace a požadavky na důkazy pro správu ochrany soukromí.

1.2 Tato politika se vztahuje na personál, funkce, systémy, dodavatele, zpracovatele, dílčí zpracovatele a vztahy společných správců, které se účastní zpracování PII v rozsahu PIMS nebo jej ovlivňují.

1.3 Tato politika se použije v kontextech správce, společného správce, zpracovatele a dílčího zpracovatele.

1.4 Tato politika nevytváří nové organizační pracovní pozice. Definuje kanonické role PIMS, které mohou být přiřazeny stávajícím osobám nebo funkcím za předpokladu, že jsou dokumentovány požadavky na přiřazení role, kompetenci, nezávislost a střet zájmů.

2. Účel

2.1 Účelem této politiky je zajistit, aby odpovědnosti v PIMS byly jasně přiřazeny, pochopeny, komunikovány, doloženy, přezkoumávány a zlepšovány.

2.2 Tato politika umožňuje organizaci prokázat odpovědnost za správu ochrany soukromí, vlastnictví zpracování PII, určení role správce a zpracovatele, rozdělení odpovědností společných správců, nakládání s pokyny pro zpracovatele, odpovědnost dodavatelů v oblasti ochrany soukromí, nezávislý přezkum a eskalaci podle rolí.

3. Cíle

3.1 Cíli této politiky jsou:

3.1.1 definovat kanonické role PIMS používané napříč souborem politik PIMS;

3.1.2 zajistit, aby každá významná odpovědnost PIMS měla přiřazenou odpovědnou roli;

3.1.3 podporovat odpovědnost správce, společného správce, zpracovatele a dílčího zpracovatele;

3.1.4 umožnit praktické kombinování rolí pro malé a střední organizace při současném řízení střetů zájmů;

3.1.5 zachovat nezávislý přezkum prováděný Internal Audit / Compliance Reviewer;

3.1.6 zajistit, aby přiřazení rolí a změny rolí byly zaznamenávány v kanonických důkazních objektech;

3.1.7 zajistit, aby nositelé rolí PIMS obdrželi odpovídající komunikaci a povědomí;

3.1.8 zajistit, aby mezery, střety a neshody související s rolemi byly eskalovány a napraveny.

4. Prohlášení politiky

4.1 Model rolí a přiřazení PIMS

4.1.1 [All] Top Management musí schválit kanonický model rolí PIMS v REG01 před počáteční implementací PIMS a poté každoročně.

4.1.2 [All] Privacy Lead / PIMS Manager musí udržovat jmenovitá přiřazení rolí PIMS v REG01 před implementací PIMS a do 10 pracovních dnů od personálních nebo organizačních změn.

4.1.3 [All] Privacy Lead / PIMS Manager musí dokumentovat rozsah odpovědnosti a úroveň pravomocí pro každou přiřazenou roli PIMS v REG01 před tím, než přiřazení nabude účinnosti.

4.1.4 [All] Process Owner / Business Owner musí přiřadit odpovědného vlastníka činnosti zpracování pro každou činnost zpracování PII v REG02 před zahájením činnosti zpracování.

4.1.5 [All] System Owner / Application Owner musí dokumentovat odpovědného vlastníka systému pro každý systém zpracovávající PII v REG02 před spuštěním systému do produkčního prostředí.

4.1.6 [All] Vendor / Procurement Owner musí dokumentovat vlastníka vztahu pro každého zpracovatele, dílčího zpracovatele, sdílení údajů s třetí stranou nebo vztah společných správců v REG08 před onboardingem nebo schválením dohody.

4.2 Kombinování rolí, oddělení a nezávislost

4.2.1 [All] Privacy Lead / PIMS Manager musí dokumentovat každou kombinaci rolí PIMS v REG01 před tím, než kombinace rolí nabude účinnosti.

4.2.2 [All] Top Management musí v REG01 před přiřazením schválit kombinace rolí zahrnující Privacy Lead / PIMS Manager, Data Protection Officer / Privacy Advisor, Information Security Lead, Incident Response Coordinator nebo Internal Audit / Compliance Reviewer.

4.2.3 [All] Internal Audit / Compliance Reviewer musí dokumentovat nezávislost na procesu PIMS, který je přezkoumáván, v REG12 před zahájením každého auditu PIMS nebo přezkumu souladu.

4.2.4 [All] Privacy Lead / PIMS Manager musí zaznamenat kompenzační opatření pro nevyhnutelné konflikty oddělení povinností v REG12 před schválením kombinace rolí.

4.2.5 [All] Data Protection Officer / Privacy Advisor musí zaznamenat obavy týkající se nezávislosti role nebo střetu zájmů v REG12 do pěti pracovních dnů od jejich identifikace.

[... 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 požádat o výjimku z odpovědnosti role v REG12 před provozováním činnosti zpracování PII bez požadované přiřazené role.

9.1.2 [All] Privacy Lead / PIMS Manager musí posoudit dopad a zmírnění každé výjimky z odpovědnosti role v REG12 do 10 pracovních dnů od žádosti.

9.1.3 [All] Top Management musí schválit výjimky z odpovědnosti role přesahující 30 dnů nebo ovlivňující vysoce rizikové zpracování v REG12 před tím, než výjimka nabude účinnosti.

9.1.4 [All] Privacy Lead / PIMS Manager musí před schválením stanovit datum skončení platnosti nepřesahující 90 dnů v REG12 pro každou schválenou výjimku z odpovědnosti role.

9.1.5 [All] Privacy Lead / PIMS Manager musí uzavřít nebo znovu posoudit každou výjimku z odpovědnosti role v REG12 do pěti pracovních dnů od skončení platnosti.

10. Uplatňování politiky

10.1.1 [All] Privacy Lead / PIMS Manager musí zaznamenat chybějící, nepřesná nebo zastaralá přiřazení rolí PIMS jako neshody v REG12 do pěti pracovních dnů od identifikace.

10.1.2 [All] Top Management musí vyžadovat nápravné opatření v REG12 do 15 pracovních dnů u opakovaných nebo dlouhodobých selhání odpovědnosti.

10.1.3 [All] Process Owner / Business Owner musí zabránit spuštění nového nebo změněného zpracování PII do produkčního prostředí, pokud požadované důkazy o rolích a odpovědnosti chybí v REG02 nebo REG08.

10.1.4 [All] Internal Audit / Compliance Reviewer musí ověřit účinnost nápravných opatření u neshod týkajících se odpovědnosti rolí v REG12 při nejbližším plánovaném auditu nebo do 60 dnů od uzavření, podle toho, co nastane dříve.

11. Přezkum a údržba

11.1.1 [All] Privacy Lead / PIMS Manager musí tuto politiku přezkoumat každoročně a do 30 dnů od významné změny modelu rolí PIMS.

11.1.2 [All] Data Protection Officer / Privacy Advisor musí před schválením přezkoumat navrhované změny této politiky z hlediska dopadu na role v oblasti ochrany soukromí v REG12.

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

11.1.4 [All] Privacy Lead / PIMS Manager musí aktualizovat REG01 a REG11 do 15 pracovních dnů po schválených změnách rolí, odpovědností nebo komunikačních požadavků PIMS.

12. Související politiky

12.1 Tato politika je podporována následujícími souvisejícími politikami:

12.2 PII01 - Politika systému řízení informací o 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 řízení ochrany soukromí u zpracovatelů, dílčích zpracovatelů a třetích stran

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 kompetencí 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 určení kontextu rolí PIMS, použitelnosti správce a zpracovatele, vlastnictví zpracování a záznamů odpovědnosti za vztahy. Addressed by clauses [4.3.5; 5.1.5; 5.1.7; 7.1.2].

13.2.2 **Clause 5.1** - Mapováno na schválení ze strany Top Management, dohled nad odpovědností, každoroční přezkoumání vedením, metriky odpovědnosti a nápravná opatření při selhání rolí. Addressed by clauses [4.1.1; 4.2.2; 5.1.1; 6.1.1; 8.1.6; 10.1.2; 11.1.3].

13.2.3 **Clause 5.3** - Mapováno na přiřazování, dokumentování, komunikaci a údržbu rolí, odpovědností a pravomocí PIMS, vlastnictví systémů, vlastnictví zpracování, vlastnictví vztahů s dodavateli, vlastnictví eskalace incidentů a odpovědnost za nezávislý přezkum. Addressed by clauses [4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.4.2; 4.4.3; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.4 **Clause 7.2** - Mapováno na důkazy o kompetenci a povědomí specifických pro roli u přiřazených odpovědností PIMS. Addressed by clauses [7.1.4; 8.1.5].

13.2.5 **Clause 7.3** - Mapováno na povědomí o přiřazených odpovědnostech PIMS, důkazy o potvrzení a každoroční vykazování povědomí o rolích. Addressed by clauses [4.5.1; 4.5.2; 7.1.4; 8.1.5].

13.2.6 **Clause 7.4** - Mapováno na komunikaci přiřazení rolí, změn rolí, eskalací a informací o předání rolí. Addressed by clauses [4.5.1; 4.5.4; 6.1.5; 7.1.6].

13.2.7 **Clause 7.5** - Mapováno na dokumentované informace pro přiřazení rolí PIMS, rozsahy odpovědností, úrovně pravomocí, každoroční uchovávání důkazů a údržbu matice rolí. Addressed by clauses [4.1.2; 4.1.3; 4.5.3; 7.1.1; 11.1.4].

13.2.8 **Clause 8.1** - Mapováno na vlastnictví operativních opatření pro činnosti zpracování, systémy, dodavatele, zpracovatele, dílčí zpracovatele, vztahy společných správců a kontroly

spuštění do produkčního prostředí. Addressed by clauses [4.1.4; 4.1.5; 4.1.6; 7.1.2; 7.1.3; 7.1.5; 10.1.3].

13.2.9 **Clause 9.2** - Mapováno na nezávislý audit a přezkum souladu u důkazů o přiřazení rolí, důkazů o kombinování rolí, důkazů o nezávislosti, zjištění a uzavření nápravných opatření. Addressed by clauses [4.2.3; 5.1.9; 6.1.4; 8.1.4; 10.1.4].

13.2.10 **Clause 9.3** - Mapováno na přezkoumání úplnosti přiřazení rolí PIMS, střetů rolí, výjimek, metrik odpovědnosti a výstupů přezkumu odpovědnosti vedením. Addressed by clauses [5.1.1; 6.1.1; 8.1.6; 11.1.1].

13.2.11 **Clause 10.2** - Mapováno na eskalaci, zaznamenávání neshod, nápravná opatření, uzavření výjimek a ověření účinnosti u otázek odpovědnosti rolí. Addressed by clauses [4.2.5; 4.4.5; 6.1.5; 9.1.5; 10.1.1; 10.1.2; 10.1.4].

13.2.12 **Annex A.1.2.7** - Mapováno na přiřazení a dokumentování odpovědnosti za smlouvu se zpracovatelem a eskalaci odpovědnosti třetí strany před schválením nebo obnovením smlouvy. Addressed by clauses [4.1.6; 4.4.4; 5.1.7; 7.1.3].

13.2.13 **Annex A.1.2.8** - Mapováno na dokumentování rozdělení odpovědností společných správců a důkazů o odpovědnosti za vztah před zahájením zpracování společnými správci. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.2.14 **Annex A.1.2.9** - Mapováno na udržování záznamů odpovědnosti pro vlastnictví zpracování správcem, klasifikaci rolí a vlastnictví důkazů. Addressed by clauses [4.3.1; 4.3.5; 4.5.3; 8.1.1].

13.2.15 **Annex A.2.2.2** - Mapováno na odpovědnost za zákaznickou dohodu zpracovatele, vlastnictví pokynů zákazníka a důkazy o vztahu se zpracovatelem. Addressed by clauses [4.3.3; 5.1.7; 7.1.3; 8.1.3].

13.2.16 **Annex A.2.2.3** - Mapováno na sladění účelu a pokynů zpracovatele prostřednictvím vlastnictví pokynů zákazníka a ověření rolí správce/zpracovatele. Addressed by clauses [4.3.3; 4.3.5; 5.1.7].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapováno na důkazy o odpovědnosti pro přiřazení rolí, vlastnictví zpracování, přezkumy rolí, neshody a auditní zjištění. Addressed by clauses [4.5.3; 6.1.2; 8.1.1; 10.1.1].

13.3.2 **Article 24** - Mapováno na odpovědnost správce, odpovědné vlastnictví zpracování, dohled ze strany Top Management, každoroční přezkum a opatření odpovědnosti. Addressed by clauses [4.1.1; 4.3.1; 5.1.1; 6.1.1; 8.1.6].

13.3.3 **Article 26** - Mapováno na dokumentování rozdělení odpovědností společných správců a důkazů o odpovědnosti za vztah před zahájením zpracování společnými správci. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.3.4 **Article 28** - Mapováno na rozdělení odpovědností zpracovatele a dílčího zpracovatele, vlastnictví pokynů zákazníka, odpovědnost za smlouvu a eskalační cesty třetích stran. Addressed by clauses [4.3.3; 4.3.4; 4.4.4; 5.1.7; 7.1.3].

13.3.5 **Article 30** - Mapováno na záznamy o zpracování, vlastnictví zpracování, klasifikaci rolí PIMS a ověření rolí správce/zpracovatele. Addressed by clauses [4.1.4; 4.3.1; 4.3.5; 8.1.1].

13.3.6 **Article 37** - Mapováno na dokumentování role Data Protection Officer / Privacy Advisor tam, kde je určení použitelné nebo dobrovolně provedeno. Addressed by clauses [4.1.2; 4.1.3; 5.1.3; 11.1.2].

13.3.7 **Article 38** - Mapováno na postavení, nezávislost, zapojení a řešení střetu zájmů u Data Protection Officer / Privacy Advisor, kde je použitelné. Addressed by clauses [4.2.5; 5.1.3; 6.1.3; 11.1.2].

13.3.8 **Article 39** - Mapováno na poradenství v oblasti ochrany soukromí, pozorování z monitorování, poradní přezkum a přezkum dopadů na soukromí související s rolemi prováděný Data Protection Officer / Privacy Advisor, kde je použitelné. Addressed by clauses [4.4.1; 5.1.3; 6.1.3; 11.1.2].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.1; Clause 4.2** - Mapováno na aktéry rámce ochrany soukromí a rozdělení rolí pro subjekty PII, správce PII, zpracovatele PII, třetí strany a klasifikaci rolí PIMS. Addressed by clauses [4.1.4; 4.1.6; 4.3.5; 5.1.5; 5.1.7].

13.4.2 **Clause 5.12** - Mapováno na odpovědnost za soulad v oblasti ochrany soukromí, důkazy rolí, přezkum, auditní zjištění a ověření nápravných opatření. Addressed by clauses [4.5.3; 6.1.2; 8.1.4; 10.1.4].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 6.1.2; Clause 6.1.3** - Mapováno na definici rolí ochrany PII, dokumentování rolí, komunikaci rolí, koordinaci bezpečnosti a ochrany soukromí a oddělení povinností pro ochranu PII. Addressed by clauses [4.1.1; 4.2.1; 4.2.3; 4.2.4; 4.4.2; 5.1.4; 7.1.4].

13.6 ISO/IEC 27002:2022

13.6.1 Control 5.2 - Mapováno na definování, přidělování, dokumentování, komunikaci a údržbu odpovědností PIMS a bezpečnosti informací. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.4.2; 4.5.1; 5.1.4; 7.1.1].

13.6.2 Control 5.3 - Mapováno na oddělení povinností, schvalování kombinování rolí, nezávislý přezkum, opatření ke konfliktům a ověření nápravných opatření u střetů rolí. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 9.1.2; 10.1.4].