					Sem vložte název registrované právnické osoby						
Číslo dokumentu: PII09					Název dokumentu: **Politika shromažďování, používání, zpřístupňování a sdílení PII**						
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 7.5; Clause 8.1	Both	Primary	Dokumentované provozní opatření
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorování a nápravná opatření
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.9	Controller	Primary	Účel a záznamy o zpracování
ISO/IEC 27701:2025	Annex A.1.2.3	Controller	Referenced	Vazba na právní základ
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Supporting	Odpovědnosti společných správců při sdílení
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5	Controller	Primary	Limity shromažďování, zpracování a minimalizace
ISO/IEC 27701:2025	Annex A.1.5.2; Annex A.1.5.3	Conditional	Referenced	Vazba směrování přenosů
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Záznamy o přenosech a zpřístupněních
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Primary	Pokyny a záznamy zpracovatele
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Referenced	Vazba směrování přenosů u zpracovatele
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Záznamy a žádosti zpracovatele o zpřístupnění
GDPR	Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Primary	Omezení účelu, minimalizace a odpovědnost
GDPR	Article 6	Controller	Referenced	Vazba na právní základ
GDPR	Article 24	Controller	Supporting	Odpovědnost správce
GDPR	Article 26	Joint Controller	Supporting	Ujednání společných správců

GDPR	Article 28	Both	Supporting	Pokyny zpracovateli a limity zpřístupnění
GDPR	Article 30	Both	Supporting	Záznamy o zpracování a příjemcích
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Účel, shromažďování, minimalizace a omezení zpřístupnění
ISO/IEC 29100:2020	Clause 5.10; Clause 5.12	Both	Supporting	Odpovědnost a soulad v oblasti ochrany soukromí
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7	Both	Supporting	Opatření pro účel, shromažďování, minimalizaci, použití a zpřístupnění

1. Rozsah

1.1 Tato politika stanoví požadavky na shromažďování, používání, zpřístupňování a sdílení PII v rozsahu PIMS.

1.2 Tato politika se vztahuje na:

1.2.1 shromažďování PII prostřednictvím přímých, nepřímých, automatizovaných, manuálních, interních, externích kanálů a kanálů třetích stran;

1.2.2 schválené interní používání PII obchodními procesy, systémy a aplikacemi;

1.2.3 sekundární využití PII pro nový nebo významně změněný účel;

1.2.4 externí zpřístupnění PII příjemcům, partnerům, orgánům, zpracovatelům, dílčím zpracovatelům, dodavatelům a jiným třetím stranám;

1.2.5 opakující se ujednání o sdílení údajů a jednorázová zpřístupnění;

1.2.6 kontexty správce, společného správce, zpracovatele a dílčího zpracovatele;

1.2.7 REG02 - evidence činností zpracování PII / ROPA, REG08 - registr zpracovatelů, dílčích zpracovatelů a sdílení údajů, REG09 - registr mezinárodních přenosů a REG12 - registr auditů, neshod, nápravných opatření a zlepšování.

1.3 Tato politika nenahrazuje:

1.3.1 PII03 pro evidenci činností zpracování, právní základ a vlastnictví ROPA;

1.3.2 PII04 pro obsah oznámení o ochraně osobních údajů, zveřejnění a správu verzí;

1.3.3 PII05 pro provoz souhlasů a preferencí;

1.3.4 PII06 pro vyřizování žádostí subjektů PII o uplatnění práv;

1.3.5 PII07 pro metodiku DPIA a posouzení rizik pro soukromí;

1.3.6 PII08 pro kontrolní brány ochrany osobních údajů již od návrhu;

1.3.7 PII10 pro provádění uchovávání, mazání a likvidace;

1.3.8 PII11 pro řízení přesnosti a kvality;

1.3.9 PII12 pro řízení životního cyklu zpracovatelů, dílčích zpracovatelů a třetích stran;

1.3.10 PII13 pro výběr mechanismu mezinárodního přenosu a opatření k řízení rizik přenosu;

1.3.11 PII14 pro zabezpečení PII a řízení přístupu;

1.3.12 PII15 pro zvládání incidentů a porušení zabezpečení;

1.3.13 PII18 pro celkové řízení monitorování, auditu, neshod, nápravných opatření a zlepšování v rámci PIMS.

1.4 Pro účely této politiky:

1.4.1 „schválené použití“ znamená použití PII, které je zaznamenáno v REG02 pro konkrétní činnost zpracování, účel, kategorii PII, kategorii subjektu PII, vlastníka společnosti a příslušnou roli PIMS.

1.4.2 „shromažďování“ znamená získávání PII přímo od subjektu PII, nepřímo od jiné strany, automaticky ze systému nebo zařízení nebo prostřednictvím interního či externího zdroje údajů.

1.4.3 „sekundární využití“ znamená použití PII pro účel, který dosud není v REG02 zaznamenán jako schválený účel pro příslušnou činnost zpracování.

1.4.4 „posouzení slučitelnosti“ znamená dokumentované posouzení v REG02 zahrnující původní účel, navrhovaný účel, závislost na právním základu, kategorie PII, očekávání subjektů PII, odůvodnění minimalizace, dopad zpřístupnění nebo přenosu a případné směrování na jiné politiky PIMS.

1.4.5 „externí zpřístupnění“ znamená zpřístupnění PII straně mimo organizaci nebo mimo dokumentovaný řetězec pokynů zákazníka.

1.4.6 „sdílení údajů“ znamená opakující se nebo strukturované ujednání, na jehož základě jsou PII zpřístupněny, přeneseny, zpřístupněny k přístupu, vyměňovány nebo jinak dány k dispozici jiné straně.

1.4.7 „citlivé opakující se sdílení“ znamená opakující se sdílení zahrnující zvláštní kategorie PII, PII týkající se trestných činů, PII dětí, záznamy s vysokým dopadem, rozsáhlé sdílení nebo externí sdílení zahrnující místo přenosu zaznamenané v REG09.

2. Účel

2.1 Účelem této politiky je zajistit, aby PII byly shromažďovány, používány, zpřístupňovány a sdíleny pouze pro dokumentované, schválené, omezené a odpovědně řízené účely.

2.2 Tato politika umožňuje organizaci prokázat, že shromažďování a použití jsou navázány na záznamy o zpracování v REG02, že zpřístupnění a ujednání o sdílení údajů jsou zaznamenána v REG08, že směrování mezinárodních přenosů je navázáno na REG09 a že výjimky a neshody jsou řešeny prostřednictvím REG12.

3. Cíle

3.1 Cílem této politiky je:

3.1.1 omezit shromažďování na PII, které jsou nezbytné pro dokumentované účely;

3.1.2 zajistit, aby interní použití PII bylo schváleno před zahájením zpracování;

3.1.3 vyžadovat posouzení slučitelnosti před sekundárním využitím;

3.1.4 vyžadovat schválení a důkazy před externím zpřístupněním;

3.1.5 udržovat důkazy o sdílení údajů v REG08 bez vytváření samostatného registru sdílení údajů;

3.1.6 směrovat závislosti mezinárodních přenosů do REG09 a PII13 bez zdvojování opatření mechanismu přenosu;

3.1.7 stanovit kadenci přezkumu opakujícího se sdílení;

3.1.8 udržovat důkazy připravené pro audit pro shromažďování, použití, zpřístupnění, sdílení, výjimky a nápravná opatření.

4. Prohlášení politiky

4.1 Omezení shromažďování

4.1.1 [Controller] Process Owner / Business Owner musí před zahájením jakékoli nové činnosti shromažďování nebo významné změny shromažďování zaznamenat v REG02 účel shromažďování, zdroj nebo kanál, kategorie PII, kategorie subjektů PII a minimální datové prvky.

4.1.2 [Controller] Privacy Lead / PIMS Manager musí před zahájením shromažďování přezkoumat záznam o shromažďování v REG02, pokud je přidána nová kategorie PII, zdroj, kanál nebo účel.

4.1.3 [Controller] Process Owner / Business Owner musí před shromážděním každého datového prvku PII zaznamenat v REG02 odůvodnění nezbytnosti tohoto prvku.

4.1.4 [Processor] Process Owner / Business Owner musí před shromažďováním PII jménem zákazníka zaznamenat v REG02 odkaz na pokyn zákazníka z REG08.

4.1.5 [Joint Controller] Process Owner / Business Owner musí před zahájením společného shromažďování zaznamenat v REG08 rozdělení odpovědností společných správců za shromažďování.

4.2 Opatření pro schválené interní použití

4.2.1 [Controller] Process Owner / Business Owner musí před zahájením použití zaznamenat v REG02 pravidla schváleného interního použití pro každou činnost zpracování.

4.2.2 [Controller] System Owner / Application Owner musí před produkčním vydáním implementovat pouze taková pole pracovních postupů, reporty nebo exporty pro interní použití, které mají odpovídající pravidlo schváleného použití v REG02.

4.2.3 [Processor] Process Owner / Business Owner musí před použitím zákaznických PII pro jakoukoli činnost zpracovatele nebo dílčího zpracovatele zaznamenat v REG08 soulad s pokyny zákazníka.

4.2.4 [Controller] Privacy Lead / PIMS Manager musí alespoň jednou ročně přezkoumat pravidla schváleného použití v REG02 pro každou aktivní činnost zpracování.

4.2.5 [All] Privacy Lead / PIMS Manager musí do pěti pracovních dnů zaznamenat neshodu v REG12, pokud je zjištěno nedokumentované interní použití PII.

[... 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 schváleného pravidla shromažďování, použití, zpřístupnění nebo sdílení zaznamenat žádost o výjimku v REG12.

9.1.2 [All] Privacy Lead / PIMS Manager musí před aktivací výjimky zaznamenat v REG12 rozhodnutí o schválení nebo zamítnutí.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor musí před schválením výjimky zahrnující neslučitelné sekundární využití, citlivé opakující se sdílení, konflikt s právně závazným zpřístupněním nebo směrování přenosu zaznamenat stanovisko v REG12.

9.1.4 [All] Top Management musí před aktivací jakékoli výjimky s dobou trvání delší než 30 kalendářních dnů nebo s dopadem na více než jednu činnost zpracování zaznamenat schválení v REG12.

9.1.5 [All] Process Owner / Business Owner musí uzavřít výjimku v REG12 k datu skončení platnosti nebo do pěti pracovních dnů po skončení okolnosti zakládající výjimku.

10. Uplatňování politiky

10.1.1 [All] Privacy Lead / PIMS Manager musí do pěti pracovních dnů od zjištění zaznamenat neschválené shromažďování, použití, zpřístupnění nebo sdílení jako neshodu v REG12.

10.1.2 [Controller] Process Owner / Business Owner musí do jednoho pracovního dne pozastavit shromažďování, použití, zpřístupnění nebo sdílení, pokud Privacy Lead / PIMS Manager zaznamená v REG12 absenci schválených důkazů v REG02 nebo REG08.

10.1.3 [Processor] Process Owner / Business Owner musí do jednoho pracovního dne zaznamenat v REG08 a REG12 rozhodnutí o zastavení nebo eskalaci, pokud jsou zákaznické PII použity nebo zpřístupněny mimo dokumentovaný pokyn.

10.1.4 [All] Top Management musí do 30 kalendářních dnů od eskalace přezkoumat nevyřešené neshody s vysokým dopadem týkající se shromažďování, použití, zpřístupnění nebo sdílení v REG12.

10.1.5 [All] Internal Audit / Compliance Reviewer musí do 15 pracovních dnů poté, co Privacy Lead / PIMS Manager označí uzavření, ověřit v REG12 důkazy o uzavření nápravných opatření.

11. Přezkum a údržba

11.1.1 [All] Privacy Lead / PIMS Manager musí tuto politiku alespoň jednou ročně přezkoumat a rozhodnutí zaznamenat v REG12.

11.1.2 [All] Privacy Lead / PIMS Manager musí tuto politiku přezkoumat do 30 kalendářních dnů od významné změny rozsahu PIMS, účelů zpracování, modelu sdílení, směrování přenosů nebo použitelné povinnosti a výsledek zaznamenat v REG12.

11.1.3 [All] Process Owner / Business Owner musí alespoň jednou ročně a do 30 kalendářních dnů od významné změny zpracování znovu potvrdit aktivní záznamy REG02 a REG08.

11.1.4 [All] Internal Audit / Compliance Reviewer musí zahrnout opatření PII09 do každoročního auditního vzorkování a pokrytí zaznamenat v REG12.

11.1.5 [All] Privacy Lead / PIMS Manager musí do deseti pracovních dnů aktualizovat v REG12 odkazy na související politiky, pokud změna PII03, PII08, PII10, PII12, PII13, PII14 nebo PII18 změní provozní hranici této politiky.

12. Související politiky

12.1 Tuto politiku je vhodné číst společně s:

12.1.1 PII01 - Politika systému řízení informací o soukromí

12.1.2 PII02 - Politika rolí, odpovědností a odpovědnosti za soukromí

12.1.3 PII03 - Politika evidence činností zpracování PII a právních základů

12.1.4 PII04 - Politika oznámení o ochraně osobních údajů a transparentnosti

12.1.5 PII05 - Politika řízení souhlasů a preferencí

12.1.6 PII06 - Politika řízení práv subjektů PII

12.1.7 PII07 - Politika posouzení rizik pro soukromí a DPIA

12.1.8 PII08 - Politika ochrany osobních údajů již od návrhu a ve výchozím nastavení

12.1.9 PII10 - Politika uchovávání, mazání a likvidace PII

12.1.10 PII11 - Politika přesnosti a kvality PII

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

12.1.12 PII13 - Politika mezinárodních přenosů PII

12.1.13 PII14 - Politika zabezpečení PII a řízení přístupu

12.1.14 PII15 - Politika řízení incidentů a porušení zabezpečení PII

12.1.15 PII17 - Politika dokumentovaných informací a správy důkazů PIMS

12.1.16 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 7.5; Clause 8.1** - Mapováno na dokumentované provozní záznamy a řízení důkazů o shromažďování, schváleném použití, sekundárním využití, zpřístupnění, sdílení a směrování přenosů. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.3; 4.3.5; 4.4.1; 4.4.2; 4.5.1; 7.1.1; 7.1.4].

13.2.2 **Clause 9.1; Clause 10.2** - Mapováno na monitorování, měření, přezkum, řešení výjimek, neshody a nápravná opatření pro opatření týkající se shromažďování, použití, zpřístupnění a sdílení. Addressed by clauses [4.2.4; 4.2.5; 6.1.1; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 9.1.1; 10.1.1; 10.1.5; 11.1.4].

13.2.3 **Annex A.1.2.2; Annex A.1.2.9** - Mapováno na dokumentované účely správce, záznamy schváleného použití a důkazy o zpracování v REG02. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.4; 4.3.1; 4.3.2; 4.3.4; 4.5.5].

13.2.4 **Annex A.1.2.3** - Mapováno na vazbu právního základu pro shromažďování, použití a směrování sekundárního využití bez nahrazení PII03. Addressed by clauses [4.3.4; 6.1.2; 7.1.1].

13.2.5 **Annex A.1.2.8** - Mapováno na důkazy v REG08 o odpovědnostech společných správců za shromažďování a sdílení. Addressed by clauses [4.1.5; 4.4.4; 6.1.4].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5** - Mapováno na omezení shromažďování, omezení zpracování a odůvodnění minimalizace před shromážděním nebo použitím PII. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.3.1; 4.3.2; 7.1.2].

13.2.7 **Annex A.1.5.2; Annex A.1.5.3** - Mapováno na vazbu směrování přenosů prostřednictvím REG09 bez nahrazení opatření mechanismu přenosu podle PII13. Addressed by clauses [4.5.1; 4.5.2; 7.1.4].

13.2.8 **Annex A.1.5.4; Annex A.1.5.5** - Mapováno na záznamy o přenosech, zpřístupněních a opakujících se ujednáních o sdílení údajů v REG08. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.5.1; 4.5.3; 4.5.4; 4.5.5].

13.2.9 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Mapováno na soulad zpracovatele s pokyny zákazníka a záznamy zpracovatele o limitech shromažďování, použití a sekundárního využití. Addressed by clauses [4.1.4; 4.2.3; 4.3.6; 7.1.3; 10.1.3].

13.2.10 **Annex A.2.5.2; Annex A.2.5.3** - Mapováno na vazbu směrování přenosů u zpracovatele prostřednictvím REG09 bez nahrazení opatření mechanismu přenosu podle PII13. Addressed by clauses [4.5.1; 4.5.2; 7.1.4].

13.2.11 **Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Mapováno na záznamy zpracovatele o zpřístupnění, stav oznámení žádosti o zpřístupnění a důkazy autorizace zpřístupnění v REG08. Addressed by clauses [4.4.5; 4.4.6; 4.4.7; 10.1.3].

13.3 GDPR

13.3.1 **Article 5(1)(b); Article 5(1)(c); Article 5(2)** - Mapováno na důkazy o omezení účelu, minimalizaci údajů a odpovědnosti pro shromažďování, použití, sekundární využití, zpřístupnění a sdílení. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.5.3; 8.1.3; 10.1.1].

13.3.2 Article 6 - Mapováno na vazbu právního základu a směrování nového nebo neslučitelného sekundárního využití bez nahrazení PII03. Addressed by clauses [4.3.4; 6.1.2; 7.1.1].

13.3.3 **Article 24** - Mapováno na správu, schvalování, přezkum a opatření odpovědnosti správce pro shromažďování, použití, zpřístupnění a sdílení. Addressed by clauses [4.1.2; 4.2.4; 4.3.2; 4.3.3; 4.3.5; 4.4.1; 6.1.1; 9.1.2; 10.1.4; 11.1.1].

13.3.4 **Article 26** - Mapováno na důkazy o odpovědnostech společných správců za shromažďování a sdílení. Addressed by clauses [4.1.5; 4.4.4; 6.1.4].

13.3.5 **Article 28** - Mapováno na soulad pokynů zpracovatele a dílčího zpracovatele, autorizaci zákazníka a limity zpřístupnění. Addressed by clauses [4.1.4; 4.2.3; 4.3.6; 4.4.5; 4.4.6; 4.4.7; 7.1.3; 10.1.3].

13.3.6 **Article 30** - Mapováno na záznamy o zpracování, příjemcích, zpřístupnění a sdílení v REG02 a REG08. Addressed by clauses [4.1.1; 4.2.1; 4.4.2; 4.4.3; 4.5.1; 4.5.5; 8.1.1; 8.1.2].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Mapováno na specifikaci účelu, omezení shromažďování, minimalizaci údajů, omezení použití a omezení zpřístupnění. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.5.3].

13.4.2 **Clause 5.10; Clause 5.12** - Mapováno na odpovědnost, důkazy o souladu, přezkum, správu výjimek, auditní vzorkování a nápravná opatření. Addressed by clauses [4.2.4; 4.2.5; 5.1.2; 6.1.1; 8.1.1; 9.1.1; 10.1.1; 11.1.4].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7** - Mapováno na účel, omezení shromažďování, minimalizaci, omezení použití, omezení zpřístupnění a podporu záznamů o zpřístupnění. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.4.6; 4.5.3].