					Sem vložte název registrované právnické osoby							
Číslo dokumentu: PII21					Název dokumentu: **Politika ochrany soukromí pro AI a automatizované rozhodování**							
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 informace a operativní řízení důkazů o zpracování pro AI, profilování a automatizované rozhodování
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorování, neshody a nápravná opatření pro kontroly ochrany soukromí v oblasti AI
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9	Controller	Primary	Účel, právní základ, posouzení dopadu na soukromí a záznamy správce
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Smlouvy se zpracovateli a odpovědnosti společných správců pro zpracování PII související s AI
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4	Controller	Primary	Povinnosti vůči subjektům PII a transparentnost zpracování souvisejícího s AI
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11	Controller	Primary	Námitka, přístup, oprava, výmaz, vyřizování žádostí a povinnosti související s automatizovaným rozhodováním
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5	Controller	Primary	Omezení shromažďování, zpracování a minimalizace pro vstupy, výstupy a odvozená data AI

ISO/IEC 27701:2025	Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5	Conditional	Supporting	Směrování mezinárodního předávání, zpřístupnění a žádostí o zpřístupnění pro PII související s AI
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Processor	Primary	Smlouva se zpracovatelem, dokumentované pokyny, podpora povinností zákazníka a záznamy
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Podpora zpracovatele pro povinnosti vůči subjektům, směrování předávání a vyřizování zpřístupnění
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Ochrana záznamů a protokolování související se zpracováním PII v oblasti AI
GDPR	Article 4(4); Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(d); Article 5(2)	Controller	Primary	Profilování, korektnost, transparentnost, omezení účelu, minimalizace, přesnost a odpovědnost
GDPR	Article 6; Article 9; Article 10	Controller	Primary	Zákonnost, údaje zvláštních kategorií a ochranná opatření pro údaje o odsouzeních v trestních věcech nebo trestných činech
GDPR	Article 12; Article 13; Article 14; Article 15	Controller	Primary	Transparentní informace, přístup a smysluplné informace o automatizovaném rozhodování

GDPR	Article 16; Article 17; Article 18; Article 21; Article 22	Controller	Primary	Oprava, výmaz, omezení, námitka a práva týkající se automatizovaného rozhodování
GDPR	Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Odpovědnost správce, návrh/výchozí nastavení, společní správci, zpracovatelé, záznamy, zabezpečení, DPIA a úkoly DPO
GDPR	Article 44	Conditional	Referenced	Směrování mezinárodního předávání pro zpracování PII související s AI
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7	Both	Primary	Zásady účelu, shromažďování, minimalizace, použití, uchovávání, zpřístupnění, přesnosti a kvality
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Transparentnost, účast jednotlivce, odpovědnost, bezpečnost informací a soulad v oblasti ochrany soukromí
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	Přínos PIA, určení prahových hodnot a příprava posouzení rizik pro soukromí souvisejících s AI
ISO/IEC 29151:2022	Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10	Both	Supporting	Kontroly účelu, shromažďování, minimalizace, použití, uchovávání, zpřístupnění, přesnosti a účasti subjektu

1. Rozsah

1.1 Tato politika stanoví povinné požadavky na ochranu soukromí pro činnosti zpracování využívající AI, profilování, skórování, doporučování, podporu rozhodování a automatizované rozhodování, které používají, odvozují, generují, zpřístupňují nebo jinak zpracovávají PII v rozsahu PIMS.

1.2 Tato politika se vztahuje na:

1.2.1 systémy, aplikace, modely, služby, pracovní postupy, rozhodovací enginy, skórovací nástroje, doporučovací systémy, analytické modely a procesy automatizovaného rozhodování využívající AI, které zpracovávají PII;

1.2.2 profilování, segmentaci, klasifikaci, predikci, odvozování, personalizaci, řazení, posuzování způsobilosti, odhalování podvodů, skórování rizik, rozhodování o přístupu, posuzování související se zaměstnáním, profilování týkající se dětí, marketingovou personalizaci a obdobné zpracování, při němž jsou zapojeny PII;

1.2.3 PII související s AI používané pro trénování, testování, validaci, ladění, monitorování, produkční inferenci, přezkum výstupů, měření výkonnosti, vyšetřování incidentů nebo vyřazení modelu;

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

1.2.5 dodavatele, zpracovatele, dílčí zpracovatele, příjemce při sdílení údajů a trasy mezinárodního předávání související s AI, kteří zpracovávají PII.

1.3 Tato politika nevytváří úplný rámec správy a řízení AI, systém řízení AI, evidenci AI, inventář modelů, registr rizik modelů, registr férovosti, registr algoritmů, registr incidentů AI, výbor pro AI, roli vlastníka modelu, roli vlastníka systému AI, pracovní postup právního poradenství ani samostatný schvalovací formulář pro AI.

1.4 Tato politika nenahrazuje:

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

1.4.2 PII04 pro správu oznámení o ochraně osobních údajů;

1.4.3 PII05 pro správu souhlasů a preferencí;

1.4.4 PII06 pro pracovní postup práv subjektu PII;

1.4.5 PII07 pro metodiku posouzení rizik pro soukromí a DPIA;

1.4.6 PII08 pro brány ochrany soukromí již od návrhu a ve výchozím nastavení;

1.4.7 PII09 pro kontroly shromažďování, použití, zpřístupnění a sdílení;

1.4.8 PII10 pro provádění uchovávání, výmazu a likvidace;

1.4.9 PII11 pro kontroly přesnosti a kvality;

1.4.10 PII12 pro správu životního cyklu zpracovatelů, dílčích zpracovatelů a třetích stran;

1.4.11 PII13 pro kontroly mezinárodního předávání;

1.4.12 PII14 pro bezpečnost a řízení přístupu;

1.4.13 PII15 pro zvládání incidentů a porušení zabezpečení;

1.4.14 PII18 pro monitorování, audit a zlepšování;

1.4.15 PII19 pro ochranu soukromí zaměstnanců;

1.4.16 PII20 pro ochranu soukromí dětí;

1.4.17 PII22 pro marketingovou ochranu soukromí a cookies.

2. Účel

2.1 Účelem této politiky je zajistit, aby činnosti AI, profilování a automatizovaného rozhodování zahrnující PII byly identifikovány, dokumentovány, posouzeny z hlediska rizik, transparentní,

napadnutelné, monitorované a řízené prostřednictvím PIMS, aniž by vznikaly duplicitní artefakty správy specifické pro AI.

2.2 Tato politika zajišťuje, aby povinnosti ochrany soukromí pro zpracování PII související s AI byly doloženy prostřednictvím REG02, REG04, REG06, REG07, REG08, REG09, REG10 a REG12.

3. Cíle

3.1 Cílem této politiky je:

3.1.1 identifikovat zpracování využívající AI, profilování a automatizované rozhodování zahrnující PII v REG02;

3.1.2 dokumentovat účely související s AI, právní základ, kategorie PII, zdroje údajů, odvozené údaje, výstupy, příjemce a účinky rozhodnutí v REG02;

3.1.3 spouštět předběžné posouzení rizik pro soukromí a směrování DPIA prostřednictvím REG04;

3.1.4 zajistit, aby oznámení o ochraně osobních údajů a smysluplné informace související s AI byly zaznamenány v REG07;

3.1.5 směrovat žádosti o uplatnění práv, námitky, lidský přezkum a možnost napadnutí prostřednictvím REG06;

3.1.6 řídit zpracovatele, dílčí zpracovatele, dodavatele a ujednání o sdílení údajů související s AI prostřednictvím REG08;

3.1.7 směrovat mezinárodní předávání související s AI prostřednictvím REG09;

3.1.8 eskalovat podezření na incidenty týkající se PII související s AI, zneužití, neoprávněné zpřístupnění a nepříznivé dopady na soukromí prostřednictvím REG10 a REG12;

3.1.9 zaznamenávat monitorování, výjimky, neshody, nápravná opatření a zlepšení v REG12.

4. Prohlášení politiky

4.1 Identifikace AI, profilování a automatizovaného rozhodování

4.1.1 [Controller] Při návrhu nového nebo významně změněného systému, aplikace, modelu, pracovního postupu, služby nebo obchodního procesu musí Process Owner / Business Owner určit, zda používá AI, profilování, skórování, doporučování, podporu rozhodování nebo automatizované rozhodování zahrnující PII, a toto určení zaznamenat v REG02.

4.1.2 [Controller] Před zahájením zpracování PII souvisejícího s AI musí Process Owner / Business Owner dokumentovat účel zpracování, kategorie PII, kategorie subjektů PII, zdroje údajů, kategorie vyvozených nebo odvozených údajů, kategorie výstupů, kategorie příjemců, právní základ a vazbu na uchovávání v REG02.

4.1.3 [Controller] Před použitím profilování, skórování, doporučování, podpory rozhodování nebo automatizovaného rozhodování v produkčním prostředí musí Process Owner / Business Owner dokumentovat kontext rozhodnutí, očekávaný účinek na subjekty PII, zapojení člověka a trasu pro uplatnění práv v REG02 a REG04.

4.1.4 [Joint Controller] Před prováděním zpracování PII souvisejícího s AI se společným správcem musí Privacy Lead / PIMS Manager dokumentovat odpovědnost za vymezení účelu, oznámení, vyřizování práv, podporu DPIA, správu zpracovatelů a eskalaci incidentů v REG08.

4.1.5 [Processor] Před zpracováním PII prostřednictvím služby související s AI pro zákazníka musí Process Owner / Business Owner potvrdit, že pokyny zákazníka, povolené účely, zakázaná použití, nakládání s výstupy a povinnosti součinnosti jsou dokumentovány v REG08.

4.1.6 [Both] Před aktivací zpracování PII souvisejícího s AI musí Privacy Lead / PIMS Manager potvrdit, že zpracování je propojeno s příslušnými kanonickými důkazními objekty a že mimo REG02, REG04, REG06, REG07, REG08, REG09, REG10 nebo REG12 není vytvořen žádný samostatný registr specifický pro AI.

4.2 Posouzení rizik pro soukromí a směrování DPIA

4.2.1 [Controller] Před spuštěním nebo významnou změnou zpracování PII souvisejícího s AI musí Privacy Lead / PIMS Manager dokončit předběžné posouzení rizik pro soukromí a zaznamenat rozhodnutí o DPIA v REG04.

4.2.2 [Conditional] Pokud zpracování související s AI zahrnuje profilování, automatizovaná rozhodnutí, rozsáhlé hodnocení, údaje zvláštních kategorií, údaje o trestných činech, zranitelné subjekty PII, posuzování zaměstnanců, děti, monitorování chování, lokalizační údaje, biometrické údaje, skórování s významným dopadem nebo významné účinky, musí Data Protection Officer / Privacy Advisor přezkoumat riziko pro soukromí a zaznamenat doporučení v REG04.

4.2.3 [Controller] Před spuštěním zpracování PII souvisejícího s AI do produkčního prostředí musí Process Owner / Business Owner dokumentovat opatření ošetření rizik, stav zbytkového rizika a důkazy připravenosti ke spuštění v REG04 nebo REG12.

4.2.4 [Controller] Před opětovným použitím PII pro trénování, testování, validaci, ladění, monitorování nebo zlepšování modelu AI pro nový nebo významně změněný účel musí Process Owner / Business Owner dokončit přezkum ochrany soukromí a zaznamenat rozhodnutí v REG02 a REG04.

4.2.5 [Conditional] Pokud po plánovaném ošetření zůstává zbytkové riziko pro soukromí vysoké, musí Top Management schválit, zamítnout nebo vyžadovat další ošetření před produkčním použitím a zaznamenat rozhodnutí v REG04 a REG12.

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

9. Výjimky

9.1 [All] Před odchýlením se od požadavku na ochranu soukromí souvisejícího s AI v této politice musí žádající Process Owner / Business Owner předložit odůvodnění výjimky a důkazy o kompenzačních opatřeních v REG12.

9.2 [Conditional] Pokud výjimka ovlivňuje profilování, automatizované rozhodování, lidský přezkum, možnost napadnutí, transparentnost, výsledek DPIA, skórování s významným dopadem, zpracování týkající se dětí, zpracování týkající se zaměstnanců, omezení zpracovatele nebo mezinárodní předávání, musí Data Protection Officer / Privacy Advisor výjimku přezkoumat a zaznamenat doporučení v REG04 nebo REG12.

9.3 [Conditional] Pokud výjimka vytváří nebo zachovává vysoké zbytkové riziko pro soukromí, musí Top Management výjimku schválit nebo zamítnout a zaznamenat rozhodnutí v REG04 a REG12.

9.4 [All] Před vypršením schválené výjimky ochrany soukromí související s AI musí Privacy Lead / PIMS Manager přezkoumat stav uzavření, obnovení nebo nápravného opatření a zaznamenat výsledek v REG12.

10. Prosazování požadavků politiky

10.1 [All] Pokud je zjištěno nedodržení této politiky, musí Privacy Lead / PIMS Manager zaznamenat neshodu a nápravné opatření v REG12.

10.2 [Both] Pokud existuje podezření na neoprávněné zpracování, zpřístupnění nebo přístup k PII související s AI, zneužití modelu, selhání práv nebo nepříznivý dopad na soukromí, musí Incident Response Coordinator zahájit eskalaci incidentu a zaznamenat důkazy v REG10 a REG12.

10.3 [Both] Pokud zpracovatel, dílčí zpracovatel, dodavatel nebo příjemce při sdílení údajů nesplní povinnosti ochrany soukromí související s AI, musí Vendor / Procurement Owner zaznamenat nápravné, eskalační nebo ukončovací opatření v REG08 a REG12.

10.4 [All] Pokud dojde k opakovaným nebo systémovým neshodám v oblasti ochrany soukromí souvisejícím s AI, musí Top Management přezkoumat problém a zaznamenat opatření vedení v REG12.

11. Přezkum a údržba

11.1 [All] Alespoň jednou ročně musí Privacy Lead / PIMS Manager přezkoumat tuto politiku z hlediska trvalé vhodnosti a zaznamenat výsledek přezkumu v REG12.

11.2 [Conditional] Pokud se významně změní právní předpisy, služby, modely, zdroje údajů, postupy profilování, logika automatizovaného rozhodování, ujednání s dodavateli, trasy předávání nebo rizika pro soukromí, musí Privacy Lead / PIMS Manager přezkoumat dotčené kontroly ochrany soukromí související s AI a zaznamenat výsledek v REG02, REG04 nebo REG12.

11.3 [Controller] Alespoň jednou ročně a po významných změnách uživatelské cesty souvisejících s AI musí Process Owner / Business Owner přezkoumat důkazy o transparentnosti, smysluplných informacích, lidském přezkumu a trase pro uplatnění práv a zaznamenat přezkum v REG06 a REG07.

11.4 [All] Po uzavření nápravných opatření v oblasti ochrany soukromí souvisejících s AI musí Internal Audit / Compliance Reviewer ověřit účinnost a zaznamenat důkazy o ověření v REG12.

12. Související politiky

12.1 PII01 - Politika systému řízení informací o soukromí

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

12.3 PII03 - Politika evidence zpracování PII a právního základu

12.4 PII04 - Politika oznámení o ochraně osobních údajů a transparentnosti

12.5 PII05 - Politika správy souhlasů a preferencí

12.6 PII06 - Politika správy práv subjektů PII

12.7 PII07 - Politika posouzení rizik pro soukromí a DPIA

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

12.9 PII09 - Politika shromažďování, použití, zpřístupnění a sdílení PII

12.10 PII10 - Politika uchovávání, výmazu a likvidace PII

12.11 PII11 - Politika přesnosti a kvality PII

12.12 PII12 - Politika správy zpracovatelů, dílčích zpracovatelů a třetích stran v oblasti ochrany soukromí

12.13 PII13 - Politika mezinárodního předávání PII

12.14 PII14 - Politika zabezpečení PII a řízení přístupu

12.15 PII15 - Politika řízení incidentů a porušení zabezpečení PII

12.16 PII17 - Politika dokumentovaných informací a správy důkazů PIMS

12.17 PII18 - Politika monitorování, auditu a zlepšování PIMS

12.18 PII19 - Politika ochrany soukromí zaměstnanců

12.19 PII20 - Politika ochrany soukromí dětí

12.20 PII22 - Politika marketingové ochrany soukromí a cookies

13. Referenční normy a rámce

13.1 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.6; 4.8.1; 6.1; 7.1; 7.5; 11.1].

13.2 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.6.2; 4.6.5; 4.8.2; 6.5; 8.1; 8.2; 8.3; 8.4; 8.5; 10.1; 11.4].

13.3 ISO/IEC 27701:2025 - Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.2.3; 4.2.4; 4.8.1; 7.1; 7.2].

13.4 ISO/IEC 27701:2025 - Annex A.1.2.7; Annex A.1.2.8. Addressed by clauses [4.1.4; 4.7.1; 4.7.2; 4.7.3; 5.7; 6.3; 7.6].

13.5 ISO/IEC 27701:2025 - Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 7.3; 11.3].

13.6 ISO/IEC 27701:2025 - Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11. Addressed by clauses [4.1.3; 4.3.2; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 7.4; 11.3].

13.7 ISO/IEC 27701:2025 - Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5. Addressed by clauses [4.2.4; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 7.1; 7.5].

13.8 ISO/IEC 27701:2025 - Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5. Addressed by clauses [4.7.3; 4.7.4; 4.7.5; 7.7].

13.9 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7. Addressed by clauses [4.1.5; 4.3.5; 4.5.5; 4.7.1; 4.7.2; 5.7; 6.3; 7.6].

13.10 ISO/IEC 27701:2025 - Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.3.5; 4.5.5; 4.7.1; 4.7.2; 4.7.4; 4.7.5; 7.6; 7.7].

13.11 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.25. Addressed by clauses [4.4.4; 4.6.1; 4.6.3; 4.8.1; 5.4; 7.5; 7.8; 10.2].

13.12 GDPR - Article 4(4); Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(d); Article 5(2). Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.1; 4.4.1; 4.4.2; 4.4.5; 4.8.1; 8.1].

13.13 GDPR - Article 6; Article 9; Article 10. Addressed by clauses [4.1.2; 4.2.4; 4.4.3; 4.7.3; 7.1].

13.14 GDPR - Article 12; Article 13; Article 14; Article 15. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.5.2; 4.5.3; 7.3; 11.3].

13.15 GDPR - Article 16; Article 17; Article 18; Article 21; Article 22. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 7.4].

13.16 GDPR - Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.2.2; 4.2.5; 4.4.4; 4.7.1; 4.8.2; 5.3; 6.2; 6.4; 7.2].

13.17 GDPR - Article 44. Addressed by clauses [4.7.4; 7.7; 8.4].

13.18 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7. Addressed by clauses [4.1.2; 4.2.4; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.7.5].

13.19 ISO/IEC 29100:2020 - Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.3.1; 4.3.2; 4.5.1; 4.5.2; 4.6.3; 4.8.1; 4.8.2; 8.5; 10.1].

13.20 ISO/IEC 29134:2020 - Clause 5.1; Clause 6.2; Clause 6.3. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.6.4; 6.4; 7.2; 9.2].

13.21 ISO/IEC 29151:2022 - Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10. Addressed by clauses [4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.2; 4.5.4; 4.7.5].