					Sem vložte název registrované právnické osoby							
Číslo dokumentu: PII05					Název dokumentu: **Politika správy souhlasů a preferencí**							
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 pro důkazy o souhlasu
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorování, neshoda, nápravné opatření a zlepšování
ISO/IEC 27701:2025	Annex A.1.2.3	Controller	Supporting	Vazba na právní základ
ISO/IEC 27701:2025	Annex A.1.2.4; Annex A.1.2.5	Controller	Primary	Určení souhlasu, jeho získání a zaznamenání
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Záznamy správce o zpracování
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Supporting	Smlouvy se zpracovatelem, účely zákazníka a záznamy zpracovatele
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Supporting	Podpora zpracovatele při plnění povinností správce vůči subjektům PII
ISO/IEC 27701:2025	Annex A.3.14	Both	Supporting	Ochrana záznamů o zpracování PII
GDPR	Article 4(11)	Controller	Supporting	Kritéria souhlasu
GDPR	Article 5(1)(a); Article 5(2)	Controller	Supporting	Zákonnost, korektnost, transparentnost a odpovědnost
GDPR	Article 6(1)(a); Article 6(4)	Controller	Primary	Souhlas jako právní základ a vazba na změněný účel
GDPR	Article 7	Controller	Primary	Podmínky souhlasu a jeho odvolání
GDPR	Article 8	Conditional	Supporting	Eskalace souhlasu dítěte

GDPR	Article 9(2)(a)	Conditional	Supporting	Výslovný souhlas se zpracováním zvláštních kategorií údajů
GDPR	Article 24	Controller	Supporting	Odpovědnost správce a opatření
GDPR	Article 28	Both	Supporting	Vazba na pokyny a součinnost zpracovatele
GDPR	Article 30	Both	Supporting	Vazba na záznamy o zpracování
ISO/IEC 29100:2020	Clause 5.2; Clause 5.8; Clause 5.12	Both	Supporting	Zásady souhlasu a volby, transparentnosti a souladu
ISO/IEC 29151:2022	Annex A.3	Both	Supporting	Opatření pro souhlas a volbu
ISO/IEC TS 27560:2023	Clause 5.2; Clause 6.2; Clause 6.3; Clause 6.4	Conditional	Supporting	Struktura záznamu a potvrzení o souhlasu, pokud se používají

1. Rozsah

1.1 Tato politika stanoví povinné požadavky na určení, kdy je souhlas vyžadován, na vyžádání souhlasu, zachycení důkazů o souhlasu, správu preferencí, zpracování odvolání souhlasu, vedení záznamů o souhlasu a přezkum mechanismů souhlasu.

1.2 Tato politika se vztahuje na zpracování PII, u něhož je souhlas zvolen nebo vyžadován jako právní základ, u něhož je vyžadován výslovný souhlas, u něhož jsou zachycovány preference souhlasu, nebo u něhož organizace spravuje záznamy o souhlasu jménem správce.

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

1.4 Povinnosti zpracovatele a dílčího zpracovatele se uplatní pouze tehdy, jsou-li záznamy o souhlasu, stavy preferencí nebo pokyny k odvolání souhlasu spravovány podle dokumentovaných pokynů správce nebo zákazníka.

1.5 Tato politika nečiní ze souhlasu výchozí právní základ pro zpracování PII.

1.6 Určení právního základu se nadále řídí PII03 - Politika evidence zpracování PII a právního základu.

2. Účel

2.1 Účelem této politiky je zajistit, aby správa souhlasů a preferencí byla zákonná, transparentní, doložitelná, odvolatelná, technicky vymahatelná a podložená řízenými důkazy.

2.2 Tato politika zajišťuje, že souhlas je vyžadován pouze tam, kde je to vhodné, že záznamy o souhlasu jsou úplné a dohledatelné, že odvolání souhlasu jsou respektována a že důkazy o souhlasu zůstávají dostupné pro účely auditu, šetření a odpovědnosti.

3. Cíle

3.1 Cílem této politiky je:

3.1.1 Zajistit, aby byl souhlas používán pouze tehdy, je-li vhodným právním základem nebo je-li pro danou činnost zpracování vyžadován.

3.1.2 Zajistit, aby žádosti o souhlas byly konkrétní, informované, odlišitelné a propojené s příslušným oznámením o ochraně osobních údajů.

3.1.3 Zajistit, aby záznamy o souhlasu a preferencích byly zachycovány a vedeny v REG05.

3.1.4 Zajistit, aby odvolání souhlasu a změny preferencí byly prováděny ve stanovených provozních lhůtách.

3.1.5 Zajistit, aby záznamy o souhlasu byly propojeny s účely zpracování v REG02 a s verzemi oznámení v REG07.

3.1.6 Zajistit, aby činnosti zpracovatelů a dílčích zpracovatelů podporující souhlas probíhaly podle dokumentovaných pokynů správce nebo zákazníka.

3.1.7 Zajistit, aby mechanismy souhlasu byly monitorovány, přezkoumávány, opravovány a auditovatelné.

4. Ustanovení politiky

4.1 Použitelnost souhlasu a právní základ

4.1.1 [Controller] Process Owner / Business Owner musí v REG02 zaznamenat, zda je souhlas vyžadován nebo zvolen, a to před zahájením jakékoli nové nebo významně změněné činnosti zpracování PII, která se opírá o souhlas.

4.1.2 [Controller] Privacy Lead / PIMS Manager musí v REG02 a REG05 ověřit, že souhlas není zvolen jako výchozí právní základ, než schválí novou nebo významně změněnou činnost zpracování založenou na souhlasu.

4.1.3 [Controller] Data Protection Officer / Privacy Advisor musí před spuštěním přezkoumat právní základ souhlasu v REG04, pokud zpracování zahrnuje zvláštní kategorie PII, služby

zaměřené na děti, vysoce rizikové zpracování nebo nerovnováhu mezi organizací a subjektem PII.

4.1.4 [Joint Controller] Privacy Lead / PIMS Manager musí v REG02 a REG05 dokumentovat stranu odpovědnou za získání, zaznamenání, obnovení a respektování souhlasu před zahájením zpracování společnými správci.

4.1.5 [Processor] Privacy Lead / PIMS Manager musí v REG08 a REG05 zaznamenat pokyny zákazníka k zachycení souhlasu, správě preferencí nebo podpoře odvolání souhlasu před implementací mechanismu souhlasu jménem správce.

4.1.6 [Subprocessor] Vendor / Procurement Owner musí v REG08 zaznamenat povinnosti dílčího zpracovatele související se souhlasem před tím, než je dílčímu zpracovateli povoleno nakládat se záznamy o souhlasu, stavy preferencí nebo pokyny k odvolání souhlasu.

4.2 Žádost o souhlas a jeho zachycení

4.2.1 [Controller] Process Owner / Business Owner musí zajistit, aby každá žádost o souhlas byla specifická pro daný účel a propojená s příslušnou verzí oznámení o ochraně osobních údajů v REG07 před jejím předložením subjektu PII.

4.2.2 [Controller] System Owner / Application Owner musí nastavit mechanismy souhlasu tak, aby vyžadovaly potvrzující úkon před zahájením zpracování tam, kde je vyžadován výslovný souhlas nebo souhlas formou opt-in.

4.2.3 [Controller] Process Owner / Business Owner musí při zachycení souhlasu zaznamenat v REG05 referenci subjektu PII, účel, kategorii PII, znění nebo verzi souhlasu, verzi oznámení o ochraně osobních údajů, kanál zachycení, časové razítko, metodu, stav a příslušnou dobu platnosti.

4.2.4 [Conditional] Privacy Lead / PIMS Manager musí v REG05 zaznamenat logiku ověření věku nebo autorizace a před spuštěním vyvolat přezkum REG04, pokud se souhlas týká zpracování zaměřeného na děti.

4.2.5 [Conditional] Privacy Lead / PIMS Manager musí v REG05 označit souhlas jako výslovný před zahájením zpracování, pokud je pro zvolený účel vyžadován výslovný souhlas.

4.2.6 [Both] System Owner / Application Owner musí zabránit pokračování zpracování, které se opírá o souhlas, dokud REG05 neukazuje aktivní stav souhlasu pro příslušný účel.

[... 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 v REG12 před odchýlením se od schváleného požadavku na zachycení souhlasu, správu preferencí, odvolání souhlasu nebo důkazy.

9.1.2 [All] Privacy Lead / PIMS Manager musí každou výjimku související se souhlasem v REG12 schválit nebo zamítnout před implementací a ke každé schválené výjimce přiřadit datum skončení platnosti a kompenzační opatření.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor musí před schválením přezkoumat výjimku v REG04 nebo REG12, pokud se výjimka týká výslovného souhlasu, zpracování zaměřeného na děti, vysoce rizikového zpracování nebo mechanismu odvolání souhlasu.

9.1.4 [Both] System Owner / Application Owner musí zablokovat produkční vydání nebo deaktivovat dotčený mechanismus souhlasu, pokud výjimka vyžadovaná touto politikou nebyla před spuštěním do produkčního prostředí schválena v REG12.

10. Uplatňování politiky

10.1.1 [All] Privacy Lead / PIMS Manager musí do pěti pracovních dnů od zjištění chybějících, neplatných, nepropojených nebo nespolehlivých důkazů o souhlasu zaznamenat neshodu související se souhlasem v REG12.

10.1.2 [Controller] Process Owner / Business Owner musí pozastavit nebo napravit zpracování pro dotčený účel před pokračováním dalšího zpracování založeného na souhlasu, pokud je souhlas vyžadován, ale nelze jej doložit v REG05.

10.1.3 [Both] System Owner / Application Owner musí deaktivovat nebo opravit nevyhovující mechanismus zachycení souhlasu, preferencí nebo odvolání souhlasu ve lhůtě přiřazené v REG12.

10.1.4 [Processor] Vendor / Procurement Owner musí do pěti pracovních dnů od zjištění eskalovat selhání pokynů zákazníka týkající se záznamů o souhlasu, stavů preferencí nebo podpory odvolání souhlasu v REG08 a REG12.

10.1.5 [All] Internal Audit / Compliance Reviewer musí ověřit důkazy o uzavření nápravných opatření souvisejících se souhlasem v REG12 do přiřazeného termínu splnění.

11. Přezkum a údržba

11.1.1 [All] Privacy Lead / PIMS Manager musí tuto politiku každoročně přezkoumat a zaznamenat výsledek přezkumu v REG12.

11.1.2 [All] Privacy Lead / PIMS Manager musí tuto politiku přezkoumat do 30 dnů od významné změny právních předpisů o souhlasu, technologie souhlasu, nástrojů pro správu preferencí, struktury oznámení o ochraně osobních údajů nebo požadavků certifikace PIMS.

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

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

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 Tato politika je podporována následujícími souvisejícími politikami:

12.2 PII01 - Politika systému řízení informací o soukromí

12.3 PII02 - Politika rolí, odpovědností a odpovědnosti v oblasti ochrany soukromí

12.4 PII03 - Politika evidence zpracování PII a právního základu

12.5 PII04 - Politika oznámení o ochraně osobních údajů a transparentnosti

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, používání, zpřístupňování a sdílení PII

12.10 PII10 - Politika uchovávání, výmazu a likvidace PII

12.11 PII11 - Politika přesnosti a kvality PII

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

12.13 PII14 - Politika bezpečnosti PII a řízení přístupu

12.14 PII16 - Politika školení, povědomí a kompetencí v oblasti ochrany soukromí

12.15 PII17 - Politika dokumentovaných informací a správy důkazů PIMS

12.16 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 informace a operativní řízení pro určování použitelnosti souhlasu, zachycování důkazů o souhlasu, správu odvolání souhlasu, verzování záznamů o souhlasu, testování mechanismů a udržování REG05. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.2.6; 4.3.1; 4.3.2; 4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.5.2; 4.5.3; 4.5.4; 7.1.1; 7.1.2; 7.1.3; 7.1.6].

13.2.2 **Clause 9.1; Clause 10.2** - Mapováno na monitorování souhlasu, metriky, auditní vzorkování, zaznamenávání neshod, nápravná opatření a ověřování účinnosti. Addressed by clauses [4.5.5; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 10.1.1; 10.1.2; 10.1.3; 10.1.4; 10.1.5].

13.2.3 **Annex A.1.2.3** - Mapováno na potvrzení, kdy je souhlas vhodným právním základem, a na propojení záznamů o souhlasu se záznamy právního základu v REG02. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.4.2; 4.5.3].

13.2.4 **Annex A.1.2.4; Annex A.1.2.5** - Mapováno na určování, kdy a jak je souhlas získáván, zachycení souhlasu, zaznamenání důkazu, správu výslovného souhlasu, odvolání souhlasu, obnovení souhlasu a stav souhlasu. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.3.1; 4.3.2; 4.3.3; 4.3.6; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5].

13.2.5 **Annex A.1.2.9** - Mapováno na záznamy správce pro zpracování založené na souhlasu, historii souhlasu, vazbu na oznámení, uchovávání důkazů a záznamy o souhlasu připravené pro audit. Addressed by clauses [4.2.3; 4.3.6; 4.5.1; 4.5.3; 7.1.1; 8.1.1; 8.1.3].

13.2.6 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Mapováno na zákaznické smlouvy zpracovatele, sladění s účelem a pokyny zákazníka a záznamy zpracovatele, pokud jsou pro správce prováděny služby podpory souhlasu. Addressed by clauses [4.1.5; 4.1.6; 4.3.4; 4.3.5; 4.5.4; 6.1.4; 7.1.4; 8.1.4; 10.1.4].

13.2.7 **Annex A.2.3.2** - Mapováno na podporu zpracovatele při plnění povinností správce vůči subjektům PII, pokud jsou odvolání souhlasu, změny preferencí nebo důkazy o souhlasu vyřizovány podle pokynu zákazníka. Addressed by clauses [4.3.4; 4.3.5; 4.5.4; 6.1.4; 8.1.4].

13.2.8 **Annex A.3.14** - Mapováno na ochranu záznamů o souhlasu a preferencích před neoprávněnou změnou a na zachování důkazů auditní stopy. Addressed by clauses [4.5.2; 5.1.6; 7.1.2; 10.1.5].

13.3 GDPR

13.3.1 **Article 4(11)** - Mapováno na kritéria souhlasu vyžadující, aby souhlas byl konkrétní, informovaný, potvrzující tam, kde je to vyžadováno, a propojený s příslušným účelem a verzí oznámení. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.5].

13.3.2 **Article 5(1)(a); Article 5(2)** - Mapováno na zákonnost, korektnost, transparentnost, důkazy o odpovědnosti, auditní vzorkování, nápravná opatření a důkaz o zpracování založeném na souhlasu. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.5.3; 4.5.5; 8.1.1; 8.1.5; 10.1.1; 10.1.5].

13.3.3 **Article 6(1)(a); Article 6(4)** - Mapováno na souhlas jako právní základ pro konkrétní účely a na opětovné posouzení nebo obnovený souhlas při významné změně účelu nebo podmínek zpracování. Addressed by clauses [4.1.1; 4.1.2; 4.4.1; 4.4.2; 4.5.3].

13.3.4 Article 7 - Mapováno na doložitelnost, odlišitelné žádosti o souhlas, odvolání souhlasu, snadnost odvolání, platnost souhlasu a uchovávanou historii souhlasu. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.3.6; 4.4.4; 4.4.5; 10.1.2].

13.3.5 Article 8 - Mapováno na eskalaci souhlasu u služeb zaměřených na děti, logiku ověření věku nebo autorizace a přezkum rizik pro soukromí před spuštěním. Addressed by clauses [4.1.3; 4.2.4; 9.1.3].

13.3.6 **Article 9(2)(a)** - Mapováno na nakládání s výslovným souhlasem, pokud je výslovný souhlas zvolen pro zpracování zvláštních kategorií údajů. Addressed by clauses [4.1.3; 4.2.5; 9.1.3].

13.3.7 **Article 24** - Mapováno na opatření správy u správce, přezkum, schvalování, výjimky, nápravná opatření a dohled vedení nad opatřeními pro souhlas. Addressed by clauses [5.1.1; 5.1.2; 6.1.1; 6.1.2; 6.1.3; 9.1.1; 9.1.2; 11.1.1; 11.1.4].

13.3.8 **Article 28** - Mapováno na vyřizování pokynů zpracovatele, důkazy o podpoře souhlasu, podporu odvolání souhlasu, povinnosti dílčího zpracovatele a eskalaci pokynů zákazníka. Addressed by clauses [4.1.5; 4.1.6; 4.3.4; 4.3.5; 4.5.4; 6.1.4; 7.1.4; 10.1.4].

13.3.9 **Article 30** - Mapováno na propojení záznamů o souhlasu s účely zpracování, záznamy správce, podpůrnými záznamy zpracovatele a dohledatelností REG02/REG05. Addressed by clauses [4.1.1; 4.5.3; 4.5.4; 7.1.1; 8.1.1].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.2; Clause 5.8; Clause 5.12** - Mapováno na souhlas a volbu, transparentnost a vazbu na oznámení, odvolání souhlasu, odpovědnost a důkazy o souladu v oblasti ochrany soukromí. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.5.3; 4.5.5; 8.1.1; 10.1.1].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3** - Mapováno na opatření pro souhlas a volbu vyžadující smysluplný, informovaný a jednoznačný souhlas, změnu preferencí a včasné změny zpracování po změně nebo odvolání souhlasu. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.4.5].

13.6 ISO/IEC TS 27560:2023

13.6.1 **Clause 5.2; Clause 6.2; Clause 6.3; Clause 6.4** - Mapováno na koncepty záznamu a potvrzení o souhlasu, vedení záznamů o souhlasu, strukturu záznamu o souhlasu, stav souhlasu, vazbu na verzi oznámení, strukturu potvrzení a výklad potvrzení o souhlasu, pokud jsou takové záznamy nebo potvrzení používány. Addressed by clauses [4.2.3; 4.3.2; 4.3.6; 4.4.3; 4.4.4; 4.5.2; 4.5.3; 7.1.6].

13.7 Interní požadavky

13.7.1 Interní požadavek - Ustanovení definující REG05 jako autoritativní důkazní objekt, schvalování nestandardních důkazů, blokování provozního vydání, školení, údržbu politiky a komunikaci podporují konzistentnost implementace, ale nejsou přímo mapována na jedno externí ustanovení. Addressed by clauses [4.5.1; 5.1.2; 7.1.5; 9.1.4; 11.1.2; 11.1.3; 11.1.5].