					Sem vložte název registrované právnické osoby							
Číslo dokumentu: PII07					Název dokumentu: **Politika posuzování rizik pro soukromí a DPIA**							
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 6.1.1	Both	Primary	Rizika a příležitosti PIMS
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 vazba na SoA
ISO/IEC 27701:2025	Clause 6.3	Both	Supporting	Plánované změny PIMS a opětovné posouzení rizik
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumentované informace o rizicích pro soukromí a DPIA
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	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	Supporting	Monitorování a měření rizik pro soukromí
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Přezkoumání rizik pro soukromí vedením
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Neshoda související s riziky a nápravné opatření
ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Primary	Posouzení dopadu na soukromí
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Záznamy o zpracování podporující posouzení rizik
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Smlouva zpracovatele se zákazníkem a podpora při DPIA

ISO/IEC 27701:2025	Annex A.2.2.6	Processor	Supporting	Informace zpracovatele podporující soulad zákazníka
GDPR	Article 5(2)	Controller	Supporting	Důkazy o odpovědnosti
GDPR	Article 24	Controller	Supporting	Odpovědnost správce a opatření
GDPR	Article 25	Controller	Supporting	Ochrana osobních údajů již od návrhu a ve výchozím nastavení
GDPR	Article 28	Both	Supporting	Podpora zpracovatele a pokyny
GDPR	Article 30	Both	Supporting	Záznamy o zpracování podporující DPIA
GDPR	Article 32	Both	Supporting	Bezpečnostní riziko a ochranná opatření
GDPR	Article 35	Controller	Primary	Posouzení vlivu na ochranu osobních údajů
GDPR	Article 36	Controller	Primary	Předchozí konzultace
GDPR	Article 39	Conditional	Supporting	Stanovisko DPO a monitorování, kde je to použitelné
ISO/IEC 29100:2020	Clause 4.7; Clause 5.11; Clause 5.12	Both	Supporting	Opatření ochrany soukromí, bezpečnost informací a soulad v oblasti ochrany soukromí
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Primary	Rozsah PIA, přínosy, spouštěč a příprava
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2	Both	Supporting	Program ochrany PII a identifikace požadavků
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7	Both	Supporting	Integrace organizačního řízení rizik pro soukromí

1. Rozsah

1.1 Tato politika stanoví požadavky na posouzení rizik pro soukromí, předběžné posouzení nutnosti DPIA, provedení úplného posouzení vlivu na ochranu osobních údajů (DPIA), ošetření rizik, přijetí zbytkového rizika, konzultace, přezkum a správu důkazů pro zpracování PII v rozsahu PIMS.

1.2 Tato politika se vztahuje na:

1.2.1 nové a významně změněné činnosti zpracování PII;

1.2.2 kontexty zpracování v roli správce, společného správce, zpracovatele a dílčího zpracovatele;

1.2.3 systémy, aplikace, služby, obchodní procesy, dodavatele, zpracovatele, dílčí zpracovatele, mezinárodní předávání a ujednání o sdílení údajů, které ovlivňují zpracování PII;

1.2.4 důkazy o rizicích pro soukromí a DPIA vedené v REG04 a podpůrné důkazy vedené v REG02, REG03, REG08, REG09, REG10, REG11 a REG12.

1.3 Tato politika nenahrazuje opatření pro evidenci činností zpracování, opatření pro oznámení o ochraně osobních údajů, opatření pro souhlas, opatření pro práva subjektů PII, opatření ochrany osobních údajů již od návrhu, opatření pro dodavatele, opatření pro mezinárodní předávání, opatření pro bezpečnost PII, opatření pro incidenty, opatření pro dokumentované informace ani opatření pro monitorování/audit/zlepšování. Tyto požadavky jsou stanoveny v souvisejících politikách uvedených v kapitole 12.

1.4 Pro účely této politiky znamená posouzení rizik pro soukromí dokumentovanou identifikaci, analýzu, vyhodnocení, ošetření, přezkum a monitorování potenciálních nepříznivých dopadů na soukromí vyplývajících ze zpracování PII.

1.5 Pro účely této politiky znamená DPIA dokumentované posouzení používané pro zpracování správcem, které pravděpodobně povede k vysokému riziku pro subjekty PII a které hodnotí nezbytnost zpracování, přiměřenost, rizika, ochranná opatření, zbytkové riziko, potřeby konzultace a podmínky schválení.

1.6 Pro účely této politiky znamená vysoké zbytkové riziko pro soukromí riziko pro soukromí, které po navrženém nebo zavedeném ošetření rizika zůstává nad schválenou prahovou hodnotou pro přijetí.

1.7 Pro účely této politiky znamená významná změna jakoukoli změnu ovlivňující rozsah PIMS, účel zpracování, právní základ, kategorie PII, kategorie subjektů PII, rozsah zpracování, technologii zpracování, monitorování nebo profilování, automatizované rozhodování, zranitelné subjekty PII, příjemce, zpracovatele, dílčí zpracovatele, mezinárodní předávání, uchovávání, bezpečnostní opatření, rizikový profil, pokyny zákazníka nebo rozsah certifikace.

2. Účel

2.1 Účelem této politiky je zajistit, aby rizika pro soukromí a povinnosti související s DPIA byly identifikovány, posouzeny, ošetřeny, schváleny, přezkoumány a doloženy dříve, než zpracování PII vytvoří nepřijatelné riziko pro subjekty PII nebo pro PIMS.

2.2 Tato politika umožňuje organizaci prokázat správu ochrany soukromí založenou na rizicích, odpovědnost správce za DPIA, podporu zpracovatele při DPIA, dokumentované ošetření rizik, schválení zbytkového rizika, rozhodování o předchozí konzultaci a neustálé zlepšování opatření ochrany soukromí.

3. Cíle

3.1 Cílem této politiky je:

3.1.1 stanovit povinné spouštěče předběžného posouzení rizik pro soukromí;

3.1.2 stanovit, kdy je vyžadováno úplné posouzení vlivu na ochranu osobních údajů (DPIA);

3.1.3 zajistit, aby rozhodnutí správce o DPIA byla dokumentovaná a přezkoumatelná;

3.1.4 zajistit, aby podpora zpracovatele a dílčího zpracovatele při DPIA byla dokumentována, pokud ji vyžaduje pokyn zákazníka nebo smlouva;

3.1.5 zajistit, aby rizika pro soukromí byla posouzena před pokračováním nového nebo významně změněného zpracování PII;

3.1.6 zajistit, aby ošetření rizik pro soukromí byla přidělena, provedena a ověřena;

3.1.7 zajistit, aby vysoká zbytková rizika pro soukromí byla eskalována a schválena před zahájením nebo pokračováním zpracování;

3.1.8 zajistit dokumentaci rozhodnutí o předchozí konzultaci, pokud vysoké zbytkové riziko přetrvává;

3.1.9 zajistit, aby důkazy o rizicích pro soukromí a DPIA byly vedeny v REG04 a propojeny se souvisejícími důkazními objekty;

3.1.10 zabránit vytváření samostatných registrů DPIA, rizik nebo konzultací mimo REG04.

4. Prohlášení politiky

4.1 Předběžné posouzení rizik pro soukromí

4.1.1 [Both] Process Owner / Business Owner MUST zahájit předběžné posouzení rizik pro soukromí v REG04 před zahájením nového nebo významně změněného zpracování PII zaznamenaného v REG02.

4.1.2 [Both] Privacy Lead / PIMS Manager MUST udržovat kritéria pro předběžné posouzení rizik pro soukromí v REG04 před zahájením prvního provozu PIMS a poté každoročně.

4.1.3 [Controller] Process Owner / Business Owner MUST provést předběžné posouzení nutnosti DPIA v REG04 před zahájením zpracování správcem, které splňuje kritéria předběžného posouzení rizik pro soukromí.

4.1.4 [Processor] Vendor / Procurement Owner MUST zaznamenat požadavky zákazníka na podporu při DPIA v REG08 před zahájením zpracování zpracovatelem, pokud smlouva se zákazníkem nebo dokumentovaný pokyn vyžaduje podporu při DPIA.

4.1.5 [Both] System Owner / Application Owner MUST poskytnout v REG04 důkazy o návrhu systému, přístupu, bezpečnosti, protokolování a tocích dat před schválením posouzení rizik pro soukromí u nových nebo významně změněných systémů zpracovávajících PII.

4.1.6 [Both] Privacy Lead / PIMS Manager MUST zaznamenat výsledek předběžného posouzení a odůvodnění rozhodnutí o úplném posouzení vlivu na ochranu osobních údajů (DPIA) v REG04 před pokračováním činnosti zpracování.

4.2 Spouštěče DPIA a určení požadavku

4.2.1 [Controller] Privacy Lead / PIMS Manager MUST vyžadovat úplné posouzení vlivu na ochranu osobních údajů (DPIA) v REG04 před zahájením zpracování správcem, které pravděpodobně povede k vysokému riziku.

4.2.2 [Controller] Process Owner / Business Owner MUST před zahájením zpracování předat Privacy Lead / PIMS Manager v REG04 zpracování zahrnující velký rozsah, systematické monitorování, profilování, automatizovaná rozhodnutí, zvláštní kategorie PII, údaje o odsouzeních za trestné činy nebo přestupcích, zranitelné subjekty PII, inovativní technologie nebo významně změněné zpracování.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor MUST zaznamenat stanovisko v REG04 před schválením rozhodnutí o požadavku na úplné posouzení vlivu na ochranu osobních údajů (DPIA) pro vysoce rizikové zpracování správcem.

4.2.4 [Both] Process Owner / Business Owner MUST znovu provést předběžné posouzení rizik pro soukromí v REG04 před použitím PII pro nový účel, přidáním nového příjemce, zavedením

nového zpracovatele nebo dílčího zpracovatele, změnou architektury systému nebo zahájením nového mezinárodního předávání.

4.2.5 [Processor] Privacy Lead / PIMS Manager MUST do 10 pracovních dnů od obdržení žádosti zákazníka o podporu při DPIA dokumentovat v REG08, zda je vyžadována podpora zpracovatele při DPIA.

4.2.6 [Subprocessor] Vendor / Procurement Owner MUST dokumentovat požadavky na podporu při DPIA vůči vyšší úrovni v REG08 před zahájením dílčího zpracování, pokud takovou podporu vyžaduje smlouva se zákazníkem nebo zpracovatelem na vyšší úrovni.

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

9. Výjimky

9.1 Výjimky týkající se rizik pro soukromí a DPIA

9.1.1 [All] Process Owner / Business Owner MUST požádat o jakoukoli výjimku z této politiky v REG12 před tím, než dojde k odchylce.

9.1.2 [All] Privacy Lead / PIMS Manager MUST posoudit dopad každé požadované výjimky na soukromí, právní oblast, certifikaci, provoz a subjekty PII v REG04 nebo REG12 do 10 pracovních dnů od žádosti.

9.1.3 [All] Data Protection Officer / Privacy Advisor MUST zaznamenat stanovisko v REG12 před schválením jakékoli výjimky ovlivňující vysoce rizikové zpracování, dokončení úplného posouzení vlivu na ochranu osobních údajů (DPIA), předchozí konzultaci, vysoké zbytkové riziko pro soukromí nebo podporu zákazníka při DPIA.

9.1.4 [All] Top Management MUST schválit výjimky týkající se rizik pro soukromí nebo DPIA, které ovlivňují vysoce rizikové zpracování, rozsah certifikace, předchozí konzultaci nebo nevyřešené vysoké zbytkové riziko pro soukromí, v REG12 před tím, než výjimka nabude účinnosti.

9.1.5 [All] Privacy Lead / PIMS Manager MUST pro každou schválenou výjimku týkající se rizik pro soukromí nebo DPIA stanovit v REG12 před schválením datum ukončení platnosti nepřesahující 90 dnů.

9.1.6 [All] Process Owner / Business Owner MUST uzavřít nebo znovu posoudit každou výjimku týkající se rizik pro soukromí nebo DPIA v REG12 do pěti pracovních dnů od skončení platnosti.

10. Uplatňování politiky

10.1 Uplatňování požadavků na rizika pro soukromí a DPIA

10.1.1 [All] Privacy Lead / PIMS Manager MUST zaznamenat chybějící, nepřesné, neúplné, opožděné nebo neschválené důkazy o rizicích pro soukromí nebo DPIA v REG04 jako neshodu v REG12 do pěti pracovních dnů od identifikace.

10.1.2 [Controller] Process Owner / Business Owner MUST pozastavit nové vysoce rizikové zpracování správcem, pokud před spuštěním chybí požadované důkazy o schválení DPIA v REG04.

10.1.3 [Both] System Owner / Application Owner MUST zablokovat spuštění systémů zpracovávajících PII do produkčního prostředí, pokud před schválením spuštění chybí požadované důkazy o ošetření rizik v REG04.

10.1.4 [Both] Vendor / Procurement Owner MUST zablokovat onboarding dodavatele, zpracovatele, dílčího zpracovatele nebo sdílení údajů, pokud před schválením smlouvy chybí požadované důkazy o rizicích pro soukromí nebo podpoře při DPIA v REG04.

10.1.5 [All] Top Management MUST během přezkoumání vedením přezkoumat nevyřešené významné neshody týkající se rizik pro soukromí nebo DPIA v REG12.

10.1.6 [All] Privacy Lead / PIMS Manager MUST eskalovat opakovaná zmeškání termínů pro předběžné posouzení v REG04, přezkum DPIA nebo ošetření rizik Top Management v REG12 do pěti pracovních dnů po druhém výskytu za období 12 měsíců.

10.1.7 [All] Internal Audit / Compliance Reviewer MUST ověřit účinnost nápravného opatření u neshod týkajících se rizik pro soukromí a DPIA v REG12 při nejbližším plánovaném auditu nebo do 60 dnů od uzavření, podle toho, co nastane dříve.

11. Přezkum a údržba

11.1 Přezkum a údržba politiky

11.1.1 [All] Privacy Lead / PIMS Manager MUST každoročně a do 30 dnů od významné změny požadavků na rizika pro soukromí, DPIA, předchozí konzultaci, podporu zpracovatele nebo certifikaci přezkoumat tuto politiku v REG12.

11.1.2 [All] Privacy Lead / PIMS Manager MUST každoročně přezkoumat v REG12 kritéria předběžného posouzení v REG04, kritéria spouštěčů DPIA, kritéria hodnocení rizik a kritéria přijetí zbytkového rizika.

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

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

11.1.5 [All] Privacy Lead / PIMS Manager MUST aktualizovat REG03 a REG04 do 15 pracovních dnů po schválených změnách politiky, které mění použitelnost opatření, kritéria rizik nebo požadavky na předběžné posouzení nutnosti DPIA.

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

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 za ochranu soukromí

12.4 PII03 - Politika evidence zpracování PII a právního základu

12.5 PII04 - Politika oznámení o ochraně osobních údajů a transparentnosti

12.6 PII05 - Politika správy souhlasů a preferencí

12.7 PII06 - Politika správy práv subjektů PII

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 soukromí zpracovatelů, dílčích zpracovatelů a třetích stran

12.13 PII13 - Politika mezinárodního předávání PII

12.14 PII14 - Politika bezpečnosti 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

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 určuje interní ustanovení, která je implementují nebo podporují.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.1** - Mapováno na identifikaci a plánování opatření pro rizika a příležitosti PIMS s využitím kritérií předběžného posouzení, prahových hodnot rizik, eskalace a vstupů pro přezkoumání vedením. Addressed by clauses [4.1.2; 4.4.5; 4.5.6; 6.1.1; 6.1.2; 8.1.2].

13.2.2 **Clause 6.1.2** - Mapováno na provádění předběžného posouzení rizik pro soukromí, posouzení rizik pro soukromí, hodnocení rizik, opětovného posouzení a vyhodnocení spouštěčů DPIA před pokračováním nového nebo významně změněného zpracování. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.6; 4.2.1; 4.2.4; 4.3.1; 4.3.7; 4.6.1].

13.2.3 **Clause 6.1.3** - Mapováno na plánování ošetření rizik pro soukromí, aktualizace použitelnosti opatření, implementaci ošetření, přijetí zbytkového rizika a vazbu na SoA. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 6.1.5; 7.1.7; 11.1.5].

13.2.4 **Clause 6.3** - Mapováno na plánované změny PIMS a zpracování, které spouštějí opětovné posouzení rizik pro soukromí a přezkum DPIA. Addressed by clauses [4.2.4; 4.6.1; 11.1.1].

13.2.5 **Clause 7.5** - Mapováno na řízené dokumentované informace pro předběžné posouzení rizik pro soukromí, důkazy DPIA, ošetření rizik, přijetí zbytkového rizika, rozhodnutí o předchozí konzultaci, výjimky, neshody a důkazy o přezkumu politiky. Addressed by clauses [4.1.6; 4.3.7; 4.4.1; 4.5.1; 5.1.2; 7.1.1; 9.1.1; 10.1.1; 11.1.1].

13.2.6 **Clause 8.1** - Mapováno na provozování opatření pro rizika pro soukromí a DPIA před spuštěním do produkčního prostředí, onboardingem, schválením zpracování, uzavřením ošetření a propojením s nápravným opatřením. Addressed by clauses [4.1.1; 4.1.5; 7.1.2; 7.1.3; 7.1.4; 7.1.5; 7.1.6; 7.1.7; 7.1.8].

13.2.7 **Clause 8.2** - Mapováno na provozní posouzení rizik pro soukromí u nových, změněných, systémových, dodavatelských, transferových a incidenty vyvolaných změn zpracování. Addressed by clauses [4.1.1; 4.2.4; 4.3.1; 4.3.5; 4.5.5; 4.6.1].

13.2.8 **Clause 8.3** - Mapováno na provozní ošetření rizik pro soukromí, přiřazení ošetření, implementaci ošetření, eskalaci ošetření po termínu a ověření účinnosti. Addressed by clauses [4.4.1; 4.4.3; 4.4.4; 4.4.6; 4.4.7; 8.1.3; 10.1.7].

13.2.9 **Clause 9.1** - Mapováno na monitorování a měření pokrytí předběžným posouzením, stavu DPIA, otevřených rizik, opatření k ošetření po termínu, opatření dodavatelů, opatření k ošetření bezpečnosti, opatření opětovného posouzení po incidentech a zjištění auditu. Addressed by clauses [4.6.3; 4.6.4; 4.6.5; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 8.1.8].

13.2.10 **Clause 9.3** - Mapováno na přezkoumání vysokých zbytkových rizik pro soukromí, opatření k ošetření po termínu, stavu úplných posouzení vlivu na ochranu osobních údajů (DPIA), rozhodnutí o předchozí konzultaci a významných výjimek z rizik pro soukromí vedením. Addressed by clauses [4.6.6; 6.1.1; 6.1.2; 6.1.3; 10.1.5].

13.2.11 **Clause 10.2** - Mapováno na neshody týkající se rizik pro soukromí a DPIA, výjimky, otevření nápravných opatření, eskalaci a ověření účinnosti. Addressed by clauses [4.4.6; 9.1.1; 9.1.2; 9.1.4; 9.1.6; 10.1.1; 10.1.5; 10.1.6; 10.1.7].

13.2.12 **Annex A.1.2.6** - Mapováno na posouzení potřeby a případnou implementaci posouzení dopadu na soukromí pro nové nebo změněné zpracování správcem. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.2.13 **Annex A.1.2.9** - Mapováno na záznamy o zpracování podporující vstupy pro posouzení rizik pro soukromí a DPIA, včetně účelu, kategorií, systémů, příjemců, předávání a dodavatelů. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.2.14 **Annex A.2.2.2** - Mapováno na smlouvy zpracovatele se zákazníky a povinnosti podpory zákazníka při DPIA. Addressed by clauses [4.1.4; 4.2.5; 4.5.4; 5.1.7; 7.1.6].

13.2.15 **Annex A.2.2.6** - Mapováno na poskytování informací zpracovatelem potřebných pro soulad zákazníka, včetně podpory při DPIA a důkazů o podpoře zákazníka. Addressed by clauses [4.2.5; 4.2.6; 4.5.4; 8.1.5].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapováno na důkazy o odpovědnosti pro předběžné posouzení nutnosti DPIA, rozhodnutí o úplném posouzení vlivu na ochranu osobních údajů (DPIA), ošetření rizik, přijetí zbytkového rizika, rozhodnutí o předchozí konzultaci, výjimky, zjištění auditu a nápravná opatření. Addressed by clauses [4.1.6; 4.3.7; 4.4.5; 4.5.1; 4.6.4; 10.1.1; 10.1.7].

13.3.2 **Article 24** - Mapováno na odpovědnost správce za přiměřená opatření k rizikům pro soukromí, přezkum vysokého zbytkového rizika, schválení vedením a údržbu politiky. Addressed by clauses [4.4.5; 4.5.3; 6.1.2; 10.1.5; 11.1.4].

13.3.3 **Article 25** - Mapováno na důkazy o ochraně osobních údajů již od návrhu a ochraně soukromí ve výchozím nastavení používané při posouzení rizik a před schválením spuštění do produkčního prostředí. Addressed by clauses [4.1.5; 4.3.4; 7.1.5].

13.3.4 **Article 28** - Mapováno na podporu zpracovatele a dílčího zpracovatele při DPIA, zpracování pokynů zákazníka a důkazy o ošetření dodavatelských rizik. Addressed by clauses [4.1.4; 4.2.5; 4.2.6; 4.4.4; 4.5.4; 7.1.6; 8.1.5].

13.3.5 **Article 30** - Mapováno na záznamy o zpracování podporující vstupy pro posouzení rizik pro soukromí a DPIA. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.3.6 **Article 32** - Mapováno na vstupy bezpečnostních rizik PII, výběr ochranných opatření, ošetření bezpečnostních rizik a aktualizace stavu bezpečnostních opatření. Addressed by clauses [4.1.5; 4.3.3; 4.4.2; 8.1.6].

13.3.7 **Article 35** - Mapováno na předběžné posouzení nutnosti DPIA, určení požadavku na úplné posouzení vlivu na ochranu osobních údajů (DPIA), obsah DPIA, stanovisko DPO, přezkum a blokování vysoce rizikového zpracování bez požadovaného schválení DPIA. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.3.6; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.3.8 **Article 36** - Mapováno na rozhodování o předchozí konzultaci, stanovisko DPO, schválení Top Management a opatření k pokračování, pozastavení, přepracování návrhu nebo konzultaci, pokud přetrvává vysoké zbytkové riziko. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 6.1.2].

13.3.9 **Article 39** - Mapováno na poradenství a monitorování Data Protection Officer / Privacy Advisor, kde je použitelné, pro rozhodnutí o DPIA, vysoce rizikové zpracování, předchozí konzultaci a změny politiky. Addressed by clauses [4.2.3; 4.3.6; 4.5.2; 5.1.3; 6.1.3; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.11; Clause 5.12** - Mapováno na identifikaci opatření ochrany soukromí, bezpečnostní ochranná opatření, soulad v oblasti ochrany soukromí, důkazy o rizicích pro soukromí, monitorování a přezkum. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.7; 4.6.3; 4.6.5; 8.1.6; 10.1.7].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Mapováno na rozsah procesu PIA, přínosy, určení spouštěčů, přípravu, vstupy pro posouzení, důkazy od zainteresovaných stran a strukturu zprávy DPIA vedenou v REG04. Addressed by clauses [4.1.1; 4.1.3; 4.1.6; 4.2.1; 4.3.1; 4.3.2; 4.3.7; 7.1.1].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2** - Mapováno na požadavky programu ochrany PII, identifikaci požadavků na ochranu PII, výběr opatření založený na rizicích a vazbu na ošetření rizik pro soukromí. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 6.1.5].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7** - Mapováno na zásady organizačního řízení rizik pro soukromí, vedení, integraci, posouzení rizik, ošetření rizik, monitorování a přezkum a zaznamenávání a vykazování. Addressed by clauses [4.1.2; 4.3.1; 4.3.7; 4.4.1; 4.4.5; 4.6.3; 4.6.4; 5.1.1; 6.1.1; 6.1.2; 8.1.1; 8.1.3].