

				Sem vložte název registrované právnické osoby							
Číslo dokumentu: PII08				Název dokumentu: Politika ochrany osobních údajů již od návrhu a ve výchozím nastavení							
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

<p>Právní upozornění (autorská práva a omezení užití) (C) 2025 Clarysec LLC. All rights reserved.</p> <p>Tento dokument je duševním vlastnictvím společnosti Clarysec LLC. Žádná jeho část nesmí být kopírována, znovu použita, distribuována ani upravována pro komerční nebo implementační účely bez výslovného písemného souhlasu.</p> <p>Neoprávněné použití je přísně zakázáno a může vést k právním krokům.</p> <p>V případě licencování kontaktujte: info@clarysec.com</p>

V souladu s normami a právními předpisy

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 6.1.2; Clause 6.1.3	Both	Supporting	Vazba na posouzení rizik pro soukromí a jejich ošetření
ISO/IEC 27701:2025	Clause 6.3; Clause 8.1	Both	Primary	Plánované změny a operativní řízení
ISO/IEC 27701:2025	Clause 7.5	Both	Supporting	Dokumentované důkazy k návrhu z hlediska ochrany soukromí
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.1.2.6; Annex A.1.2.9	Controller	Supporting	Účely, spouštěč PIA a záznamy
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3	Controller	Primary	Omezení shromažďování a zpracování
ISO/IEC 27701:2025	Annex A.1.4.4; Annex A.1.4.5	Controller	Supporting	Cíle přesnosti a minimalizace
ISO/IEC 27701:2025	Annex A.1.4.6; Annex A.1.4.7	Controller	Supporting	Návrh deidentifikace, výmazu a dočasných souborů
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Smlouva se zákazníkem, podpora a záznamy zpracovatele
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Supporting	Návrhové schopnosti zpracovatele
ISO/IEC 27701:2025	Annex A.3.27; Annex A.3.29	Both	Supporting	Životní cyklus vývoje a inženýrské principy
GDPR	Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Supporting	Omezení účelu, minimalizace a odpovědnost
GDPR	Article 24	Controller	Supporting	Opatření správce
GDPR	Article 25	Controller	Primary	Ochrana osobních údajů již od návrhu

				a ve výchozím nastavení
GDPR	Article 28	Both	Supporting	Pokyny a součinnost zpracovatele
GDPR	Article 30	Both	Supporting	Záznamy o zpracování
GDPR	Article 35	Controller	Supporting	Vazba na spouštěč DPIA
ISO/IEC 29100:2020	Clause 4.7	Both	Supporting	Opatření ochrany soukromí již od návrhu
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Účel, shromažďování, minimalizace a omezení použití
ISO/IEC 29100:2020	Clause 5.7; Clause 5.10; Clause 5.12	Both	Supporting	Přesnost, odpovědnost a soulad
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8	Both	Primary	Zásady a opatření ochrany PII

1. Rozsah

1.1 Tato politika stanoví požadavky na začlenění ochrany soukromí již od návrhu a ochrany soukromí ve výchozím nastavení do nových a změněných činností zpracování PII, projektů, produktů, služeb, systémů, aplikací, integrací, činností pořizování a změn podnikových procesů v rámci rozsahu PIMS.

1.2 Tato politika se vztahuje na kontexty správce, společného správce, zpracovatele a dílčího zpracovatele. Povinnosti zpracovatele a dílčího zpracovatele platí tam, kde organizace navrhuje, konfiguruje, mění nebo provozuje zpracování jménem zákazníka, správce nebo nadřazeného zpracovatele podle dokumentovaných pokynů.

1.3 Tato politika zahrnuje:

- 1.3.1 požadavky na ochranu soukromí při zahájení projektu;
- 1.3.2 účel, minimalizaci údajů a návrhová opatření pro výchozí nastavení;
- 1.3.3 přezkum návrhu z hlediska ochrany soukromí před spuštěním do produkčního prostředí;
- 1.3.4 přezkum návrhu z hlediska ochrany soukromí vyvolaný změnou;
- 1.3.5 kontroly ochrany osobních údajů již od návrhu při pořizování;
- 1.3.6 vazbu na rizika pro soukromí, předběžné posouzení nutnosti DPIA a důkazy o nápravných opatřeních.

1.4 Tato politika nenahrazuje:

- 1.4.1 PII03 pro evidenci činností zpracování, účely, právní základ a záznamy ROPA;
- 1.4.2 PII04 pro obsah oznámení o ochraně osobních údajů a jeho zveřejnění;
- 1.4.3 PII05 pro souhlas a opatření správy preferencí;
- 1.4.4 PII06 pro vyřizování práv subjektů PII;
- 1.4.5 PII07 pro metodiku posouzení rizik pro soukromí a DPIA;
- 1.4.6 PII09 pro opatření shromažďování, použití, zpřístupnění a sdílení;
- 1.4.7 PII10 pro provádění uchovávání, výmazu a likvidace;
- 1.4.8 PII11 pro provoz přesnosti a kvality;
- 1.4.9 PII12 pro správu a řízení životního cyklu zpracovatelů, dílčích zpracovatelů a třetích stran;
- 1.4.10 PII13 pro mechanismy mezinárodních přenosů;
- 1.4.11 PII14 pro provoz zabezpečení PII a řízení přístupu;
- 1.4.12 PII18 pro celoplošné řízení monitorování, auditu, nápravných opatření a zlepšování v PIMS.

2. Účel

2.1 Účelem této politiky je zajistit, aby požadavky na ochranu soukromí byly identifikovány, zavedeny a doloženy dříve, než zpracování PII začne nebo se významně změní, a aby systémy a procesy byly ve výchozím nastavení konfigurovány tak, aby omezovaly shromažďování, použití, expozici, závislost na uchovávání, závislost na zpřístupnění a identifikovatelnost PII na to, co je nezbytné pro dokumentovaný účel.

3. Cíle

3.1 Cílem této politiky je:

- 3.1.1 začlenit požadavky na ochranu soukromí do rozhodnutí o zahájení projektu, návrhu, pořizování, změnách a spuštění do produkčního prostředí;
- 3.1.2 zajistit, aby návrhy zpracování PII byly provázány s dokumentovanými účely a záznamy o zpracování v REG02;

- 3.1.3 zavést minimalizaci údajů a výchozí nastavení chránící soukromí dříve, než zpracování začne;
- 3.1.4 zajistit spuštění předběžného posouzení rizik pro soukromí a předběžného posouzení nutnosti DPIA bez duplikování metodiky PII07;
- 3.1.5 zajistit zaznamenání požadavků na návrh při pořizování a požadavků na návrh zpracovatele bez duplikování správy a řízení životního cyklu podle PII12;
- 3.1.6 zajistit eskalaci nevyřešených návrhových problémů prostřednictvím REG12;
- 3.1.7 udržovat důkazy k návrhu připravené pro audit v REG02, REG04, REG08 a REG12.

4. Prohlášení politiky

4.1 Zahájení projektu a požadavky na ochranu soukromí

- 4.1.1 [Both] Process Owner / Business Owner musí v REG04 zaznamenat záznam k návrhu z hlediska ochrany soukromí před zahájením jakéhokoli projektu, produktu, služby, systému, aplikace, integrace nebo změny podnikového procesu, který zahrnuje PII.
- 4.1.2 [Both] Process Owner / Business Owner musí každý záznam k návrhu z hlediska ochrany soukromí v REG04 propojit se stávající nebo návrhovou činností zpracování v REG02 před schválením funkčních požadavků.
- 4.1.3 [Controller] Privacy Lead / PIMS Manager musí v REG04 zaznamenat požadavky správce na ochranu osobních údajů již od návrhu před schválením funkčního návrhu správce.
- 4.1.4 [Processor] Vendor / Procurement Owner musí v REG08 zaznamenat pokyny zákazníka k návrhu ochrany soukromí a smluvní omezení návrhu před schválením návrhu služby zpracovatele nebo významné změny služby.
- 4.1.5 [Conditional] Data Protection Officer / Privacy Advisor musí v REG04 zaznamenat doporučení před schválením vysoce rizikového, nového, citlivého, automatizovaného, rozsáhlého nebo významně změněného návrhu PII.
- 4.1.6 [Both] Information Security Lead musí v REG04 zaznamenat závislosti bezpečnostních opatření PII, které podporují návrh ochrany soukromí, před schválením architektury.

4.2 Minimalizace údajů a návrh ochrany soukromí ve výchozím nastavení

- 4.2.1 [Controller] Process Owner / Business Owner musí v REG02 a REG04 dokumentovat minimální kategorie PII, kategorie subjektů PII, zdroje a účely před schválením návrhu shromažďování nebo importu.
- 4.2.2 [Both] System Owner / Application Owner musí nakonfigurovat výchozí nastavení zpracování na minimální shromažďování a zpracování PII potřebné pro dokumentovaný účel a zaznamenat důkazy v REG04 před spuštěním do produkčního prostředí.
- 4.2.3 [Controller] Process Owner / Business Owner musí v REG02 a REG04 dokumentovat volitelná pole PII, volitelné možnosti zpracování a nastavení vypnutá ve výchozím stavu před schválením uživatelského rozhraní, formuláře nebo pracovního postupu.
- 4.2.4 [Both] System Owner / Application Owner musí v REG04 dokumentovat výchozí nastavení expozice z hlediska ochrany soukromí pro pohledy, reporty, exporty, rozhraní a automatizované pracovní postupy před spuštěním do produkčního prostředí.
- 4.2.5 [Both] Process Owner / Business Owner musí v REG04 dokumentovat proveditelnost deidentifikace, pseudonymizace, agregace nebo neidentifikovatelného zpracování před schválením identifikovatelných PII pro testování, analytiku, reporting nebo sekundární provozní použití.
- 4.2.6 [Both] System Owner / Application Owner musí v REG04 dokumentovat nakládání s dočasnými artefakty PII, včetně dočasných souborů, mezipamětí, logů nebo stagingových záznamů, před spuštěním do produkčního prostředí.

- 4.2.7 [Both] Process Owner / Business Owner musí do pěti pracovních dnů od identifikace závislosti nasměrovat požadavky na návrh spadající do PII10, PII11, PII13 nebo PII14 na související cestu důkazů politiky v REG04.

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

9. Výjimky

9.1 Výjimky z návrhu z hlediska ochrany soukromí

- 9.1.1 [Both] Process Owner / Business Owner musí v REG12 požádat o výjimku z návrhu z hlediska ochrany soukromí před schválením návrhu nebo změny, které nemohou splnit příslušný požadavek na návrh z hlediska ochrany soukromí.
- 9.1.2 [Both] Privacy Lead / PIMS Manager musí v REG12 posoudit dopad, kompenzační opatření a dobu platnosti každé výjimky z návrhu z hlediska ochrany soukromí do pěti pracovních dnů od žádosti.
- 9.1.3 [Conditional] Data Protection Officer / Privacy Advisor musí v REG12 zaznamenat doporučení před schválením výjimky z návrhu z hlediska ochrany soukromí zahrnující vysoce rizikové, citlivé, automatizované, rozsáhlé, sporné nebo právně významné zpracování.
- 9.1.4 [All] Top Management musí v REG12 schválit výjimku z návrhu z hlediska ochrany soukromí ovlivňující zpracování s vysokým dopadem, rozsah certifikace, nevyřešené významné riziko nebo právní povinnost před tím, než výjimka nabude účinnosti.
- 9.1.5 [Both] Privacy Lead / PIMS Manager musí v REG12 nastavit datum ukončení nepřesahující 90 dnů pro každou schválenou výjimku z návrhu z hlediska ochrany soukromí před schválením.
- 9.1.6 [Both] Privacy Lead / PIMS Manager musí každou výjimku z návrhu z hlediska ochrany soukromí v REG12 uzavřít nebo opětovně posoudit do pěti pracovních dnů od konce její platnosti.

10. Uplatňování politiky

10.1 Uplatňování politiky a řešení neshod

- 10.1.1 [Both] Privacy Lead / PIMS Manager musí v REG12 zaznamenat chybějící přezkum návrhu z hlediska ochrany soukromí, chybějící důkazy o minimalizaci, nevyřešené selhání výchozího nastavení nebo neoprávněné spuštění do produkčního prostředí jako neshodu do pěti pracovních dnů od identifikace.
- 10.1.2 [Both] System Owner / Application Owner musí zabránit spuštění systému zpracovávajícího PII do produkčního prostředí, pokud není dokončen přezkum návrhu z hlediska ochrany soukromí v REG04, a zaznamenat rozhodnutí v REG12 před spuštěním do produkčního prostředí.
- 10.1.3 [Both] Vendor / Procurement Owner musí zabránit onboardingu dodavatele nebo podpisu smlouvy, pokud chybí požadované důkazy k návrhu z hlediska ochrany soukromí v REG08, a zaznamenat rozhodnutí v REG12 před onboardingem nebo podpisem.
- 10.1.4 [Both] Process Owner / Business Owner musí pozastavit použití nového nebo změněného návrhu zpracování PII, dokud není dokončen přezkum REG04, aktualizace REG02 a požadované výjimky REG12.
- 10.1.5 [All] Top Management musí vyžadovat nápravné opatření v REG12 do 10 pracovních dnů v případě opakovaného, dlouhodobého nebo vysoce dopadového selhání návrhu z hlediska ochrany soukromí.
- 10.1.6 [All] Internal Audit / Compliance Reviewer musí ověřit účinnost nápravných opatření u neshod návrhu z hlediska ochrany soukromí v REG12 při příštím plánovaném auditu PIMS nebo do 60 dnů od uzavření podle toho, co nastane dříve.

11. Přezkum a údržba

11.1 Přezkum politiky a návrhových opatření

- 11.1.1 [All] Privacy Lead / PIMS Manager musí tuto politiku každoročně a do 30 dnů od významné právní změny, změny zpracování, technologie, rozsahu certifikace nebo opatření PIMS přezkoumat v REG12.
- 11.1.2 [Both] Process Owner / Business Owner musí každoročně a do 30 dnů od významné změny zpracování přezkoumat aktivní činnosti zpracování v REG02 z hlediska změn závislostí návrhu z hlediska ochrany soukromí.
- 11.1.3 [Both] System Owner / Application Owner musí každoročně a do 30 dnů od významné změny systému přezkoumat důkazy o konfiguraci s ochranou soukromí ve výchozím nastavení v REG04.
- 11.1.4 [Both] Vendor / Procurement Owner musí přezkoumat povinnosti dodavatelů, zpracovatelů, dílčích zpracovatelů a třetích stran týkající se návrhu z hlediska ochrany soukromí v REG08 před obnovením a do 30 dnů od významné změny vztahu.
- 11.1.5 [Conditional] Data Protection Officer / Privacy Advisor musí před schválením přezkoumat dopad významných změn politiky na soukromí v REG12.
- 11.1.6 [All] Top Management musí v REG12 schválit významné změny této politiky před zveřejněním.

12. Související politiky

- 12.1 PII01 - Politika systému řízení informací o soukromí
- 12.2 PII02 - Politika rolí, odpovědností a odpovědnosti za soulad v oblasti 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 PII09 - Politika shromažďování, použití, zpřístupnění a sdílení PII
- 12.9 PII10 - Politika uchovávání, výmazu a likvidace PII
- 12.10 PII11 - Politika přesnosti a kvality PII
- 12.11 PII12 - Politika správy zpracovatelů, dílčích zpracovatelů a třetích stran v oblasti soukromí
- 12.12 PII13 - Politika mezinárodních přenosů PII
- 12.13 PII14 - Politika zabezpečení PII a řízení přístupu
- 12.14 PII17 - Politika dokumentovaných informací a správy důkazů PIMS
- 12.15 PII18 - Politika monitorování, auditu a zlepšování PIMS

13. Referenční normy a rámce

- 13.1 Tato politika je namapována 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 6.1.2; Clause 6.1.3** - Mapováno na předběžné posouzení rizik pro soukromí, vazbu opatření ošetření, analýzu návrhových závislostí, eskalaci a nápravná opatření bez duplikování úplné metodiky posouzení rizik pro soukromí a DPIA. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.5; 5.1.3; 7.1.7].

- 13.2.2 **Clause 6.3; Clause 8.1** - Mapováno na plánované změny v oblasti soukromí, zahájení projektu, operativní přezkum návrhu z hlediska ochrany soukromí, řízení spuštění do produkčního prostředí a přezkum významné změny. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.3; 4.3.5; 4.5.1; 4.5.3; 4.5.4; 4.5.6; 7.1.2; 7.1.5; 10.1.2].
- 13.2.3 **Clause 7.5** - Mapováno na dokumentované důkazy k návrhu z hlediska ochrany soukromí uchovávané v REG02, REG04, REG08 a REG12. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.2.3; 4.4.1; 4.4.2; 4.4.3; 5.1.2; 5.1.5; 5.1.6; 5.1.7; 7.1.1; 7.1.3; 7.1.4].
- 13.2.4 **Clause 9.1; Clause 10.2** - Mapováno na metriky návrhu z hlediska ochrany soukromí, vzorkování důkazů, zaznamenávání neshod, nápravná opatření a ověření účinnosti. Addressed by clauses [4.3.6; 4.4.5; 4.5.5; 6.1.1; 6.1.2; 6.1.4; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 10.1.1; 10.1.5; 10.1.6].
- 13.2.5 **Annex A.1.2.2; Annex A.1.2.6; Annex A.1.2.9** - Mapováno na dokumentování účelů zpracování, záznamů o zpracování, vazby návrhu z hlediska ochrany soukromí a spouštěčů předběžného posouzení rizik pro soukromí nebo DPIA pro zpracování správcem. Addressed by clauses [4.1.2; 4.2.1; 4.3.1; 4.4.2; 4.5.2; 5.1.5; 7.1.3; 11.1.2].
- 13.2.6 **Annex A.1.4.2; Annex A.1.4.3** - Mapováno na omezení shromažďování a zpracování PII prostřednictvím minimálních požadavků na údaje založených na účelu, volitelného zpracování vypnutého ve výchozím stavu a minimálních výchozích nastavení zpracování. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.5.4; 7.1.5; 11.1.3].
- 13.2.7 **Annex A.1.4.4; Annex A.1.4.5** - Mapováno na směřování závislostí přesnosti, cíle minimalizace, proveditelnost deidentifikace a důkazy o návrhu pro minimalizaci identifikovatelných PII. Addressed by clauses [4.2.5; 4.2.7; 4.3.2; 4.5.2; 7.1.3; 11.1.2].
- 13.2.8 **Annex A.1.4.6; Annex A.1.4.7** - Mapováno na identifikaci deidentifikace, závislosti na výmazu, dočasných artefaktů PII ve fázi návrhu a směřování do opatření životního cyklu bez duplikování provádění uchovávání nebo likvidace. Addressed by clauses [4.2.5; 4.2.6; 4.2.7; 4.3.3; 4.5.4; 7.1.5; 11.1.3].
- 13.2.9 **Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7** - Mapováno na pokyny zákazníka pro zpracovatele, informace k podpoře zákazníka, záznamy návrhu zpracovatele a zákazníkem schválené změny návrhu služby. Addressed by clauses [4.1.4; 4.4.1; 4.4.3; 4.4.6; 5.1.7; 7.1.4; 11.1.4].
- 13.2.10 **Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4** - Mapováno na návrhové schopnosti zpracovatele pro dočasné soubory, závislost na vrácení nebo likvidaci a závislost na opatřeních přenosu zaznamenané jako důkazy k návrhu bez duplikování provozních postupů výmazu nebo bezpečnostních opatření. Addressed by clauses [4.2.6; 4.2.7; 4.4.3; 4.4.4; 4.4.6; 7.1.4; 7.1.6; 11.1.4].
- 13.2.11 **Annex A.3.27; Annex A.3.29** - Mapováno na požadavky na ochranu soukromí v životním cyklu vývoje, inženýrské principy, kontrolní body ochrany PII a důkazy o konfiguraci s ochranou soukromí ve výchozím nastavení. Addressed by clauses [4.1.6; 4.3.3; 4.3.4; 4.4.4; 4.5.1; 4.5.4; 5.1.4; 5.1.6; 7.1.5; 7.1.6; 10.1.2; 11.1.3].

13.3 **GDPR**

- 13.3.1 **Article 5(1)(b); Article 5(1)(c); Article 5(2)** - Mapováno na omezení účelu, návrh minimálního rozsahu PII, vazbu na záznamy o zpracování, minimalizaci ve výchozím nastavení, důkazy a odpovědnost. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.4.2; 4.5.2; 5.1.5; 8.1.1; 10.1.1].
- 13.3.2 **Article 24** - Mapováno na opatření správce, přezkum správy, schvalování výjimek, nápravná opatření a údržbu politiky pro implementaci ochrany osobních údajů již od návrhu. Addressed by clauses [4.1.3; 4.5.6; 5.1.1; 6.1.2; 9.1.2; 9.1.4; 10.1.5; 11.1.6].

- 13.3.3 **Article 25** - Mapováno na zahájení projektu, požadavky na ochranu soukromí ve fázi návrhu, výchozí nastavení chránící soukromí, minimalizaci, kontroly návrhu při pořizování, přezkum před spuštěním do produkčního prostředí a přezkum vyvolaný změnou. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.5; 4.4.1; 4.5.1; 4.5.3; 4.5.4; 10.1.2].
- 13.3.4 **Article 28** - Mapováno na pokyny zpracovateli, podporu návrhu zpracovatele, důkazy návrhu z hlediska ochrany soukromí u dodavatele a zákazníkem schválené změny návrhu. Addressed by clauses [4.1.4; 4.4.1; 4.4.3; 4.4.5; 4.4.6; 5.1.7; 7.1.4; 10.1.3; 11.1.4].
- 13.3.5 **Article 30** - Mapováno na vazbu na záznamy o zpracování, aktualizace REG02, návrhové závislosti činnosti zpracování a důkazy v záznamech o zpracování. Addressed by clauses [4.1.2; 4.2.1; 4.4.2; 4.5.2; 5.1.5; 7.1.3; 11.1.2].
- 13.3.6 **Article 35** - Mapováno na spouštěče předběžného posouzení rizik pro soukromí a předběžného posouzení nutnosti DPIA ve fázi návrhu, doporučení k vysokému riziku a poimplementační kontroly bez duplikování metodiky DPIA. Addressed by clauses [4.1.5; 4.3.1; 4.3.6; 5.1.3; 6.1.3; 9.1.3].

13.4 ISO/IEC 29100:2020

- 13.4.1 **Clause 4.7** - Mapováno na identifikaci opatření ochrany soukromí ve fázi návrhu, vazbu na rizika pro soukromí a důkazy návrhu pro implementaci opatření. Addressed by clauses [4.1.1; 4.1.3; 4.1.5; 4.3.1; 4.3.2; 4.3.3; 4.3.5; 4.5.1].
- 13.4.2 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Mapováno na specifikaci účelu, omezení shromažďování, minimalizaci údajů, omezené použití a výchozí nastavení zpracování. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.4.2; 4.5.2].
- 13.4.3 **Clause 5.7; Clause 5.10; Clause 5.12** - Mapováno na směřování závislostí přesnosti, důkazy o odpovědnosti, monitorování návrhu z hlediska ochrany soukromí, audit a nápravná opatření. Addressed by clauses [4.2.7; 4.3.6; 4.5.5; 6.1.1; 6.1.4; 8.1.1; 8.1.2; 10.1.1; 10.1.6].

13.5 ISO/IEC 29151:2022

- 13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8** - Mapováno na legitimitu účelu, omezení shromažďování, minimalizaci údajů, omezení použití a zpřístupnění, závislost na uchování, nakládání s dočasnými soubory a návrhová opatření pro závislost přesnosti. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.4.2; 4.5.2; 4.5.4; 7.1.3; 7.1.5].