					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: PII07					Názov dokumentu: **Politika posúdenia rizík ochrany súkromia a DPIA**							
Verzia: 1.0		Dátum nadobudnutia účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Štandard		Postup		Formulár		Register		Iné	

História revízií				
Číslo revízie	**Dátum revízie**	**Zmeny**	**Preskúmal**	**Vlastník procesu**

Schválenia			
Meno	**Pozícia**	**Dátum**	**Podpis**

Súlad s normami a predpismi

Norma / predpis	Kapitola / kontrola / článok	Uplatniteľnosť	Typ pokrytia	Poznámka
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	Riziká a príležitosti PIMS
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Posúdenie rizík ochrany súkromia
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Ošetrenie rizík ochrany súkromia a väzba na SoA
ISO/IEC 27701:2025	Clause 6.3	Both	Supporting	Plánované zmeny PIMS a opätovné posúdenie rizík
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Zdokumentované informácie o rizikách ochrany súkromia a DPIA
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Prevádzkové plánovanie a riadenie
ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Prevádzkové posúdenie rizík ochrany súkromia
ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Prevádzkové ošetrenie rizík ochrany súkromia
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Monitorovanie a meranie rizík ochrany súkromia
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Preskúmanie rizík ochrany súkromia manažmentom
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Nezhody a nápravné opatrenia súvisiace s rizikami
ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Primary	Posúdenie vplyvu na ochranu súkromia
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Záznamy o spracúvaní podporujúce posúdenie rizík
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Zmluva so zákazníkom sprostredkovateľa

				a súčinnosť pri DPIA
ISO/IEC 27701:2025	Annex A.2.2.6	Processor	Supporting	Informácie sprostredkovateľa podporujúce súlad zákazníka
GDPR	Article 5(2)	Controller	Supporting	Dôkazy preukázateľnej zodpovednosti
GDPR	Article 24	Controller	Supporting	Zodpovednosť prevádzkovateľa a opatrenia
GDPR	Article 25	Controller	Supporting	Ochrana údajov už od návrhu a štandardne
GDPR	Article 28	Both	Supporting	Súčinnosť sprostredkovateľa a pokyny
GDPR	Article 30	Both	Supporting	Záznamy o spracúvaní podporujúce DPIA
GDPR	Article 32	Both	Supporting	Bezpečnostné riziká a ochranné opatrenia
GDPR	Article 35	Controller	Primary	Posúdenie vplyvu na ochranu údajov
GDPR	Article 36	Controller	Primary	Predchádzajúca konzultácia
GDPR	Article 39	Conditional	Supporting	Poradenstvo a monitorovanie DPO, ak sa uplatňuje
ISO/IEC 29100:2020	Clause 4.7; Clause 5.11; Clause 5.12	Both	Supporting	Kontroly ochrany súkromia, informačná bezpečnosť a súlad v oblasti ochrany súkromia
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Primary	Rozsah, prínosy, spúšťač a príprava PIA
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2	Both	Supporting	Program ochrany PII a identifikácia požiadaviek

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	Integrácia riadenia rizík ochrany súkromia v organizácii

1. Rozsah

1.1 Táto politika stanovuje požiadavky na posúdenie rizík ochrany súkromia, preverenie potreby DPIA, vykonanie úplnej DPIA, ošetrenie rizík, akceptáciu zostatkového rizika, konzultáciu, preskúmanie a správu dôkazov pri spracúvaní PII v rozsahu PIMS.

1.2 Táto politika sa vzťahuje na:

1.2.1 nové a podstatne zmenené činnosti spracúvania PII;

1.2.2 kontexty spracúvania v postavení prevádzkovateľa, spoločného prevádzkovateľa, sprostredkovateľa a ďalšieho sprostredkovateľa;

1.2.3 systémy, aplikácie, služby, obchodné procesy, dodávateľov, sprostredkovateľov, ďalších sprostredkovateľov, medzinárodné prenosy a dohody o zdieľaní údajov, ktoré ovplyvňujú spracúvanie PII;

1.2.4 dôkazy o rizikách ochrany súkromia a DPIA vedené v REG04 a podporné dôkazy vedené v REG02, REG03, REG08, REG09, REG10, REG11 a REG12.

1.3 Táto politika nenahrádza kontroly evidencie spracúvania, kontroly oznámení o ochrane údajov, kontroly súhlasu, kontroly práv dotknutých osôb, kontroly ochrany súkromia už od návrhu, kontroly dodávateľov, kontroly medzinárodných prenosov, kontroly bezpečnosti PII, kontroly incidentov, kontroly zdokumentovaných informácií ani kontroly monitorovania/auditu/zlepšovania. Tieto požiadavky sú stanovené v súvisiacich politikách uvedených v časti 12.

1.4 Na účely tejto politiky posúdenie rizík ochrany súkromia znamená zdokumentovanú identifikáciu, analýzu, hodnotenie, ošetrenie, preskúmanie a monitorovanie možných nepriaznivých vplyvov na ochranu súkromia vyplývajúcich zo spracúvania PII.

1.5 Na účely tejto politiky DPIA znamená zdokumentované posúdenie používané pri spracúvaní prevádzkovateľom, ktoré pravdepodobne povedie k vysokému riziku pre dotknuté osoby a ktoré hodnotí nevyhnutnosť spracúvania, primeranosť, riziká, ochranné opatrenia, zostatkové riziko, potreby konzultácie a podmienky schválenia.

1.6 Na účely tejto politiky vysoké zvyškové riziko ochrany súkromia znamená riziko ochrany súkromia, ktoré po navrhnutom alebo zavedenom ošetrení rizika zostáva nad schválenou prahovou hodnotou akceptácie.

1.7 Na účely tejto politiky podstatná zmena znamená akúkoľvek zmenu ovplyvňujúcu rozsah PIMS, účel spracúvania, právny základ, kategórie PII, kategórie dotknutých osôb, rozsah spracúvania, technológiu spracúvania, monitorovanie alebo profilovanie, automatizované rozhodovanie, zraniteľné dotknuté osoby, príjemcov, sprostredkovateľov, ďalších sprostredkovateľov, medzinárodné prenosy, uchovávanie, bezpečnostné kontroly, rizikový profil, pokyny zákazníka alebo rozsah certifikácie.

2. Účel

2.1 Účelom tejto politiky je zabezpečiť, aby boli riziká ochrany súkromia a povinnosti týkajúce sa DPIA identifikované, posúdené, ošetrené, schválené, preskúmané a doložené dôkazmi skôr, než spracúvanie PII vytvorí neprijateľné riziko pre dotknuté osoby alebo pre PIMS.

2.2 Táto politika umožňuje organizácii preukázať riadenie ochrany súkromia založené na riziku, preukázateľnú zodpovednosť prevádzkovateľa za DPIA, súčinnosť sprostredkovateľa pri DPIA, zdokumentované ošetrenie rizík, schválenie zostatkového rizika, rozhodovanie o predchádzajúcej konzultácii a neustále zlepšovanie kontrol ochrany súkromia.

3. Ciele

3.1 Cieľmi tejto politiky je:

3.1.1 stanoviť povinné spúšťače preverenia rizík ochrany súkromia;

3.1.2 stanoviť, kedy sa vyžaduje úplná DPIA;

3.1.3 zabezpečiť, aby rozhodnutia prevádzkovateľa o DPIA boli zdokumentované a preskúmateľné;

3.1.4 zabezpečiť, aby bola súčinnosť sprostredkovateľa a ďalšieho sprostredkovateľa pri DPIA zdokumentovaná, ak ju vyžaduje pokyn zákazníka alebo zmluva;

3.1.5 zabezpečiť, aby boli riziká ochrany súkromia posúdené pred začatím nového alebo podstatne zmeneného spracúvania PII;

3.1.6 zabezpečiť, aby boli ošetrenia rizík ochrany súkromia pridelené, zavedené a overené;

3.1.7 zabezpečiť, aby boli vysoké zvyškové riziká ochrany súkromia eskalované a schválené pred začatím alebo pokračovaním spracúvania;

3.1.8 zabezpečiť, aby boli rozhodnutia o predchádzajúcej konzultácii zdokumentované, ak pretrváva vysoké zvyškové riziko;

3.1.9 zabezpečiť, aby boli dôkazy o rizikách ochrany súkromia a DPIA vedené v REG04 a prepojené so súvisiacimi dôkazovými objektmi;

3.1.10 zabrániť vytváraniu samostatných registrov DPIA, rizík alebo konzultácií mimo REG04.

4. Vyhlásenia politiky

4.1 Preverenie rizík ochrany súkromia

4.1.1 [Both] Process Owner / Business Owner MUSÍ začať preverenie rizík ochrany súkromia v REG04 pred začatím nového alebo podstatne zmeneného spracúvania PII zaznamenaného v REG02.

4.1.2 [Both] Privacy Lead / PIMS Manager MUSÍ udržiavať kritériá preverenia rizík ochrany súkromia v REG04 pred úvodnou prevádzkou PIMS a následne raz ročne.

4.1.3 [Controller] Process Owner / Business Owner MUSÍ dokončiť preverenie potreby DPIA v REG04 pred začatím spracúvania prevádzkovateľom, ktoré spĺňa kritériá preverenia rizík ochrany súkromia.

4.1.4 [Processor] Vendor / Procurement Owner MUSÍ zaznamenať požiadavky zákazníka na súčinnosť pri DPIA v REG08 pred začatím spracúvania sprostredkovateľom, ak zmluva so zákazníkom alebo zdokumentovaný pokyn vyžaduje podporu pri DPIA.

4.1.5 [Both] System Owner / Application Owner MUSÍ pred schválením posúdenia rizík ochrany súkromia pre nové alebo podstatne zmenené systémy spracúvajúce PII poskytnúť v REG04 dôkazy o návrhu systému, prístupe, bezpečnosti, logovaní a tokoch údajov.

4.1.6 [Both] Privacy Lead / PIMS Manager MUSÍ pred pokračovaním spracovateľskej činnosti zaznamenať v REG04 výsledok preverenia a odôvodnenie rozhodnutia o úplnej DPIA.

4.2 Spúšťače DPIA a určenie požiadavky

4.2.1 [Controller] Privacy Lead / PIMS Manager MUSÍ vyžadovať úplnú DPIA v REG04 pred začatím spracúvania prevádzkovateľom, ktoré pravdepodobne povedie k vysokému riziku.

4.2.2 [Controller] Process Owner / Business Owner MUSÍ pred začatím spracúvania postúpiť Privacy Lead / PIMS Manager v REG04 spracúvanie zahŕňajúce veľký rozsah, systematické monitorovanie, profilovanie, automatizované rozhodnutia, osobitné kategórie PII, údaje o odsúdeniach za trestné činy alebo trestných činoch, zraniteľné dotknuté osoby, inovatívnu technológiu alebo podstatne zmenené spracúvanie.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor MUSÍ zaznamenať poradenstvo v REG04 pred schválením rozhodnutia o požiadavke na úplnú DPIA pri vysokorizikovom spracúvaní prevádzkovateľom.

4.2.4 [Both] Process Owner / Business Owner MUSÍ opätovne preveriť riziko ochrany súkromia v REG04 pred použitím PII na nový účel, pridaním nového príjemcu, zavedením nového

sprostredkovateľa alebo ďalšieho sprostredkovateľa, zmenou systémovej architektúry alebo začatím nového medzinárodného prenosu.

4.2.5 [Processor] Privacy Lead / PIMS Manager MUSÍ do 10 pracovných dní od prijatia žiadosti zákazníka o súčinnosť pri DPIA zdokumentovať v REG08, či sa vyžaduje podpora sprostredkovateľa pri DPIA.

4.2.6 [Subprocessor] Vendor / Procurement Owner MUSÍ pred začatím ďalšieho sprostredkovania zdokumentovať v REG08 požiadavky na súčinnosť pri DPIA vo vzťahu k predchádzajúcemu článku reťazca, ak takúto súčinnosť vyžaduje zmluva s upstream zákazníkom alebo sprostredkovateľom.

[... Sekcie 4.3–8 nie sú súčasťou tohto náhľadu. Pre prístup k úplnému obsahu si zakúpte celý dokument. ...]

9. Výnimky

9.1 Výnimky týkajúce sa rizík ochrany súkromia a DPIA

9.1.1 [All] Process Owner / Business Owner MUSÍ požiadať o akúkoľvek výnimku z tejto politiky v REG12 pred tým, ako dôjde k odchýlke.

9.1.2 [All] Privacy Lead / PIMS Manager MUSÍ do 10 pracovných dní od žiadosti posúdiť v REG04 alebo REG12 dopad každej požadovanej výnimky na ochranu súkromia, právne požiadavky, certifikáciu, prevádzku a dotknuté osoby.

9.1.3 [All] Data Protection Officer / Privacy Advisor MUSÍ pred schválením akejkoľvek výnimky ovplyvňujúcej vysokorizikové spracúvanie, dokončenie úplnej DPIA, predchádzajúcu konzultáciu, vysoké zvyškové riziko ochrany súkromia alebo súčinnosť zákazníka pri DPIA zaznamenať poradenstvo v REG12.

9.1.4 [All] Top Management MUSÍ pred nadobudnutím účinnosti výnimky schváliť v REG12 výnimky týkajúce sa rizík ochrany súkromia alebo DPIA, ktoré ovplyvňujú vysokorizikové spracúvanie, rozsah certifikácie, predchádzajúcu konzultáciu alebo nevyriešené vysoké zvyškové riziko ochrany súkromia.

9.1.5 [All] Privacy Lead / PIMS Manager MUSÍ pred schválením nastaviť v REG12 dátum skončenia platnosti nepresahujúci 90 dní pre každú schválenú výnimku týkajúcu sa rizík ochrany súkromia alebo DPIA.

9.1.6 [All] Process Owner / Business Owner MUSÍ do piatich pracovných dní od skončenia platnosti uzavrieť alebo opätovne posúdiť každú výnimku týkajúcu sa rizík ochrany súkromia alebo DPIA v REG12.

10. Uplatňovanie politiky

10.1 Uplatňovanie požiadaviek na riziká ochrany súkromia a DPIA

10.1.1 [All] Privacy Lead / PIMS Manager MUSÍ do piatich pracovných dní od identifikácie zaznamenať chýbajúce, nepresné, neúplné, oneskorené alebo neschválené dôkazy o rizikách ochrany súkromia alebo DPIA v REG04 ako nezhodu v REG12.

10.1.2 [Controller] Process Owner / Business Owner MUSÍ pozastaviť nové vysokorizikové spracúvanie prevádzkovateľom, ak pred spustením chýbajú požadované dôkazy o schválení DPIA v REG04.

10.1.3 [Both] System Owner / Application Owner MUSÍ zablokovať spustenie systémov spracúvajúcich PII do produkčného prostredia, ak pred schválením spustenia chýbajú požadované dôkazy o ošetrení rizík v REG04.

10.1.4 [Both] Vendor / Procurement Owner MUSÍ zablokovať onboarding dodávateľa, sprostredkovateľa, ďalšieho sprostredkovateľa alebo zdieľania údajov, ak pred schválením

zmluvy chýbajú požadované dôkazy o rizikách ochrany súkromia alebo súčinnosti pri DPIA v REG04.

10.1.5 [All] Top Management MUSÍ počas preskúmania manažmentom preskúmať nevyriešené významné nezhody týkajúce sa rizík ochrany súkromia alebo DPIA v REG12.

10.1.6 [All] Privacy Lead / PIMS Manager MUSÍ do piatich pracovných dní po druhom výskyte v 12-mesačnom období eskalovať opakované zmeškanie lehôt preverenia v REG04, preskúmania DPIA alebo ošetrenia rizika na Top Management v REG12.

10.1.7 [All] Internal Audit / Compliance Reviewer MUSÍ overiť účinnosť nápravných opatrení pri nezhodách týkajúcich sa rizík ochrany súkromia a DPIA v REG12 pri najbližšom plánovanom audite alebo do 60 dní od uzavretia podľa toho, čo nastane skôr.

11. Preskúmanie a údržba

11.1 Preskúmanie a údržba politiky

11.1.1 [All] Privacy Lead / PIMS Manager MUSÍ preskúmať túto politiku v REG12 raz ročne a do 30 dní od podstatnej zmeny požiadaviek na riziká ochrany súkromia, DPIA, predchádzajúcu konzultáciu, súčinnosť sprostredkovateľa alebo certifikáciu.

11.1.2 [All] Privacy Lead / PIMS Manager MUSÍ raz ročne preskúmať v REG12 kritériá preverenia v REG04, kritériá spúšťačov DPIA, kritériá hodnotenia rizík a kritériá akceptácie zostatkového rizika.

11.1.3 [All] Data Protection Officer / Privacy Advisor MUSÍ pred schválením preskúmať zmeny tejto politiky významné z hľadiska ochrany súkromia v REG12.

11.1.4 [All] Top Management MUSÍ pred zverejnením schváliť podstatné zmeny tejto politiky v REG12.

11.1.5 [All] Privacy Lead / PIMS Manager MUSÍ do 15 pracovných dní po schválených zmenách politiky, ktoré menia uplatniteľnosť kontrol, kritériá rizík alebo požiadavky preverenia DPIA, aktualizovať REG03 a REG04.

11.1.6 [All] Privacy Lead / PIMS Manager MUSÍ do 30 dní od zverejnenia zaznamenať komunikáciu schválených zmien tejto politiky v REG11.

12. Súvisiace politiky

12.1 Túto politiku podporujú tieto súvisiace politiky:

12.2 PII01 - Politika systému manažérstva informácií o súkromí

12.3 PII02 - Politika rolí, zodpovedností a preukázateľnej zodpovednosti v oblasti ochrany súkromia

12.4 PII03 - Politika evidencie spracúvania PII a právneho základu

12.5 PII04 - Politika oznámení o ochrane údajov a transparentnosti

12.6 PII05 - Politika správy súhlasov a preferencií

12.7 PII06 - Politika riadenia práv dotknutých osôb

12.8 PII08 - Politika ochrany súkromia už od návrhu a v predvolenom nastavení

12.9 PII09 - Politika zhromažďovania, používania, sprístupňovania a zdieľania PII

12.10 PII10 - Politika uchovávania, vymazania a likvidácie PII

12.11 PII11 - Politika presnosti a kvality PII

12.12 PII12 - Politika riadenia ochrany súkromia u sprostredkovateľov, ďalších sprostredkovateľov a tretích strán

12.13 PII13 - Politika medzinárodných prenosov PII

12.14 PII14 - Politika bezpečnosti PII a riadenia prístupu

12.15 PII15 - Politika riadenia incidentov a porušení ochrany PII

12.16 PII17 - Politika zdokumentovaných informácií a správy dôkazov PIMS

12.17 PII18 - Politika monitorovania, auditu a zlepšovania PIMS

13. Referenčné normy a rámce

13.1 Táto politika je mapovaná na tieto normy a predpisy. Mapovanie vysvetľuje, ako politika podporuje citované požiadavky, a identifikuje interné ustanovenia, ktoré ich implementujú alebo podporujú.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.1** - Mapované na identifikáciu a plánovanie opatrení pre riziká a príležitosti ochrany súkromia s použitím kritérií preverenia, prahových hodnôt rizika, eskalácie a vstupov pre preskúmanie manažmentom. 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** - Mapované na vykonávanie preverenia rizík ochrany súkromia, posúdenia rizík ochrany súkromia, hodnotenia rizík, opätovného posúdenia a vyhodnotenia spúšťačov DPIA pred pokračovaním nového alebo podstatne zmeneného spracúvania. 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** - Mapované na plánovanie ošetrenia rizík ochrany súkromia, aktualizácie uplatniteľnosti kontrol, implementáciu ošetrenia, akceptáciu zostatkového rizika a väzbu 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** - Mapované na plánované zmeny PIMS a spracúvania, ktoré spúšťajú opätovné posúdenie rizík ochrany súkromia a preskúmanie DPIA. Addressed by clauses [4.2.4; 4.6.1; 11.1.1].

13.2.5 **Clause 7.5** - Mapované na riadené zdokumentované informácie pre preverenie rizík ochrany súkromia, dôkazy DPIA, ošetrenie rizík, akceptáciu zostatkového rizika, rozhodnutia o predchádzajúcej konzultácii, výnimky, nezhody a dôkazy o preskúmaní 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** - Mapované na prevádzkovanie kontrol rizík ochrany súkromia a DPIA pred spustením do produkčného prostredia, onboardingom, schválením spracúvania, uzavretím ošetrenia a prepojením na nápravné opatrenia. 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** - Mapované na prevádzkové posúdenie rizík ochrany súkromia pri nových, zmenených, systémových, dodávateľských, prenosových a incidentmi vyvolaných zmenách spracúvania. 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** - Mapované na prevádzkové ošetrenie rizík ochrany súkromia, pridelenie ošetrenia, implementáciu ošetrenia, eskaláciu ošetrenia po lehote a overenie 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** - Mapované na monitorovanie a meranie pokrytia preverenia, stavu DPIA, otvorených rizík, opatrení na ošetrenie po lehote, opatrení dodávateľov, opatrení na ošetrenie bezpečnosti, opatrení opätovného posúdenia po incidente a auditných zistení. 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** - Mapované na preskúmanie manažmentom vysokých zvyškových rizík ochrany súkromia, opatrení na ošetrenie po lehote, stavu úplných DPIA, rozhodnutí o predchádzajúcej konzultácii a významných výnimiek týkajúcich sa rizík ochrany súkromia. Addressed by clauses [4.6.6; 6.1.1; 6.1.2; 6.1.3; 10.1.5].

13.2.11 **Clause 10.2** - Mapované na nezhody, výnimky, otvorenie nápravných opatrení, eskaláciu a overenie účinnosti týkajúce sa rizík ochrany súkromia a DPIA. 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** - Mapované na posúdenie potreby a prípadnú implementáciu posúdenia vplyvu na ochranu súkromia pri novom alebo zmenenom spracúvaní prevádzkovateľom. 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** - Mapované na záznamy o spracúvaní podporujúce vstupy posúdenia rizík ochrany súkromia a DPIA vrátane účelu, kategórií, systémov, príjemcov, prenosov a dodávateľov. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.2.14 **Annex A.2.2.2** - Mapované na zmluvy sprostredkovateľa so zákazníkmi a povinnosti súčinnosti so zákazníkom pri 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** - Mapované na poskytovanie informácií sprostredkovateľom potrebných na súlad zákazníka vrátane súčinnosti pri DPIA a dôkazov o podpore 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)** - Mapované na dôkazy preukázateľnej zodpovednosti za preverenie DPIA, rozhodnutia o úplnej DPIA, ošetrenie rizík, akceptáciu zostatkového rizika, rozhodnutia o predchádzajúcej konzultácii, výnimky, auditné zistenia a nápravné opatrenia. 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** - Mapované na zodpovednosť prevádzkovateľa za primerané opatrenia pri rizikách ochrany súkromia, preskúmanie vysokého zvyškového rizika, schválenie manažmentom 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** - Mapované na dôkazy ochrany súkromia už od návrhu a ochrany súkromia v predvolenom nastavení používané pri posúdení rizík a pred schválením spustenia do produkčného prostredia. Addressed by clauses [4.1.5; 4.3.4; 7.1.5].

13.3.4 **Article 28** - Mapované na súčinnosť sprostredkovateľa a ďalšieho sprostredkovateľa pri DPIA, spracovanie pokynov zákazníka a dôkazy o ošetrení rizík dodávateľa. 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** - Mapované na záznamy o spracúvaní podporujúce vstupy posúdenia rizík ochrany súkromia a DPIA. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.3.6 **Article 32** - Mapované na vstupy bezpečnostných rizík PII, výber ochranných opatrení, ošetrenie bezpečnostných rizík a aktualizácie stavu bezpečnostných kontrol. Addressed by clauses [4.1.5; 4.3.3; 4.4.2; 8.1.6].

13.3.7 **Article 35** - Mapované na preverenie potreby DPIA, určenie požiadavky na úplnú DPIA, obsah DPIA, poradenstvo DPO, preskúmanie a blokovanie vysokorizikového spracúvania bez požadovaného schválenia 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** - Mapované na rozhodovanie o predchádzajúcej konzultácii, poradenstvo DPO, schválenie Top Management a opatrenia na pokračovanie, pozastavenie, prepracovanie návrhu alebo konzultáciu, ak pretrváva vysoké zvyškové riziko. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 6.1.2].

13.3.9 **Article 39** - Mapované na poradenstvo a monitorovanie zo strany Data Protection Officer / Privacy Advisor, ak sa uplatňuje, pri rozhodnutiach o DPIA, vysokorizikovom spracúvaní, predchádzajúcej konzultácii a zmenách 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** - Mapované na identifikáciu kontrol ochrany súkromia, bezpečnostné ochranné opatrenia, súlad v oblasti ochrany súkromia, dôkazy o

rizikách ochrany súkromia, monitorovanie a preskúmanie. 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** - Mapované na rozsah procesu PIA, prínosy, určenie spúšťača, prípravu, vstupy posúdenia, dôkazy zainteresovaných strán a štruktúru správy DPIA vedenú 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** - Mapované na požiadavky programu ochrany PII, identifikáciu požiadaviek na ochranu PII, výber kontrol na základe rizika a väzbu na ošetrenie rizík ochrany súkromia. 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** - Mapované na organizačné zásady rizík ochrany súkromia, vedenie, integráciu, posúdenie rizík, ošetrenie rizík, monitorovanie a preskúmanie a zaznamenávanie a vykazovanie. 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].