

				Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: PII08				Názov dokumentu: Politika ochrany súkromia už od návrhu a štandardne							
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

Právne upozornenie (autorské práva a obmedzenia používania)
(C) 2025 Clarysec LLC. All rights reserved.

Tento dokument je duševným vlastníctvom spoločnosti Clarysec LLC. Žiadna časť tohto dokumentu nesmie byť bez predchádzajúceho výslovného písomného súhlasu kopírovaná, znovu použitá, distribuovaná ani upravovaná na komerčné alebo implementačné účely.

Neoprávnené použitie je prísne zakázané a môže viesť k právnym krokom.

V prípade licencovania kontaktujte: info@clarysec.com

Súlاد s normami a predpismi

Norma / predpis	Kapitola / kontrola / článok	Uplatniteľnosť	Typ pokrytia	Poznámka
ISO/IEC 27701:2025	Clause 6.1.2; Clause 6.1.3	Both	Supporting	Vázba na posúdenie rizík ochrany súkromia a ošetrovanie rizík ochrany súkromia
ISO/IEC 27701:2025	Clause 6.3; Clause 8.1	Both	Primary	Plánované zmeny a prevádzkové riadenie
ISO/IEC 27701:2025	Clause 7.5	Both	Supporting	Zdokumentované dôkazy o návrhu ochrany súkromia
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorovanie a nápravné opatrenia
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.6; Annex A.1.2.9	Controller	Supporting	Účely, spúšťač PIA a záznamy
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3	Controller	Primary	Obmedzenie zberu a spracúvania
ISO/IEC 27701:2025	Annex A.1.4.4; Annex A.1.4.5	Controller	Supporting	Ciele presnosti a minimalizácie
ISO/IEC 27701:2025	Annex A.1.4.6; Annex A.1.4.7	Controller	Supporting	Deidentifikácia, návrh výmazu a dočasné súbory
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Dohoda so zákazníkom, podpora a záznamy sprostredkovateľa
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Supporting	Návrhové schopnosti sprostredkovateľa
ISO/IEC 27701:2025	Annex A.3.27; Annex A.3.29	Both	Supporting	Životný cyklus vývoja a inžinierske princípy
GDPR	Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Supporting	Obmedzenie účelu, minimalizácia a preukázateľná zodpovednosť
GDPR	Article 24	Controller	Supporting	Opatrenia prevádzkovateľa

GDPR	Article 25	Controller	Primary	Ochrana údajov už od návrhu a štandardne
GDPR	Article 28	Both	Supporting	Pokyny a súčinnosť sprostredkovateľa
GDPR	Article 30	Both	Supporting	Záznamy o spracúvaní
GDPR	Article 35	Controller	Supporting	Väzba na spúšťač DPIA
ISO/IEC 29100:2020	Clause 4.7	Both	Supporting	Kontroly ochrany súkromia už od návrhu
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Účel, zber, minimalizácia a obmedzenie použitia
ISO/IEC 29100:2020	Clause 5.7; Clause 5.10; Clause 5.12	Both	Supporting	Presnosť, preukázateľná zodpovednosť a súlad
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8	Both	Primary	Princípy a kontroly ochrany PII

1. Rozsah

1.1 Táto politika stanovuje požiadavky na začlenenie ochrany súkromia už od návrhu a ochrany súkromia v predvolenom nastavení do nových a zmenených činností spracúvania PII, projektov, produktov, služieb, systémov, aplikácií, integrácií, činností obstarávania a zmien obchodných procesov v rozsahu PIMS.

1.2 Táto politika sa vzťahuje na kontexty prevádzkovateľa, spoločného prevádzkovateľa, sprostredkovateľa a ďalšieho sprostredkovateľa. Povinnosti sprostredkovateľa a ďalšieho sprostredkovateľa sa uplatňujú tam, kde organizácia navrhuje, konfiguruje, mení alebo prevádzkuje spracúvanie v mene zákazníka, prevádzkovateľa alebo nadriadeného sprostredkovateľa podľa zdokumentovaných pokynov.

1.3 Táto politika pokrýva:

- 1.3.1 požiadavky ochrany súkromia pri iniciovaní projektu;
- 1.3.2 kontroly návrhu účelu, minimalizácie údajov a predvolených nastavení;
- 1.3.3 preskúmanie návrhu ochrany súkromia pred spustením do produkčného prostredia;
- 1.3.4 preskúmanie návrhu ochrany súkromia vyvolané zmenou;
- 1.3.5 kontroly obstarávania z hľadiska ochrany súkromia už od návrhu;
- 1.3.6 väzbu na riziká ochrany súkromia, preverenie potreby DPIA a dôkazy o nápravných opatreniach.

1.4 Táto politika nenahrádza:

- 1.4.1 PII03 pre evidenciu spracúvania, účely, právny základ a záznamy ROPA;
- 1.4.2 PII04 pre obsah a zverejňovanie oznámenia o ochrane údajov;
- 1.4.3 PII05 pre kontroly súhlasu a preferencií;
- 1.4.4 PII06 pre vybavovanie práv dotknutých osôb;
- 1.4.5 PII07 pre metodiku posúdenia rizík ochrany súkromia a DPIA;
- 1.4.6 PII09 pre kontroly zberu, použitia, sprístupnenia a zdieľania;
- 1.4.7 PII10 pre vykonávanie uchovávania, výmazu a likvidácie;
- 1.4.8 PII11 pre prevádzku presnosti a kvality;
- 1.4.9 PII12 pre správu a riadenie životného cyklu sprostredkovateľov, ďalších sprostredkovateľov a tretích strán;
- 1.4.10 PII13 pre mechanizmy medzinárodného prenosu;
- 1.4.11 PII14 pre prevádzku bezpečnosti PII a riadenia prístupu;
- 1.4.12 PII18 pre monitorovanie, audit, nápravné opatrenia a správu zlepšovania na úrovni celého PIMS.

2. Účel

2.1 Účelom tejto politiky je zabezpečiť, aby požiadavky ochrany súkromia boli identifikované, implementované a podložené dôkazmi pred začatím alebo podstatnou zmenou spracúvania PII a aby boli systémy a procesy štandardne konfigurované tak, aby obmedzovali zber, použitie, vystavenie, závislosť od uchovávania, závislosť od sprístupnenia a identifikovateľnosť PII na rozsah nevyhnutný pre zdokumentovaný účel.

3. Ciele

3.1 Cieľmi tejto politiky sú:

- 3.1.1 začleniť požiadavky ochrany súkromia do rozhodnutí o iniciovaní projektu, návrhu, obstarávaní, zmene a spustení do produkčného prostredia;

- 3.1.2 zabezpečiť, aby návrhy spracúvania PII boli prepojené so zdokumentovanými účelmi a záznamami spracúvania REG02;
- 3.1.3 implementovať minimalizáciu údajov a predvolené nastavenia chrániace súkromie pred začatím spracúvania;
- 3.1.4 zabezpečiť spustenie preverenia rizík ochrany súkromia a potreby DPIA bez duplicity metodiky PII07;
- 3.1.5 zabezpečiť zaznamenanie požiadaviek na návrh pri obstarávaní a vo vzťahu k sprostredkovateľom bez duplicity správy životného cyklu podľa PII12;
- 3.1.6 zabezpečiť eskaláciu nevyriešených problémov návrhu prostredníctvom REG12;
- 3.1.7 udržiavať dôkazy o návrhu pripravené na audit v REG02, REG04, REG08 a REG12.

4. Vyhlásenia politiky

4.1 Iniciovanie projektu a požiadavky ochrany súkromia

- 4.1.1 [Both] Process Owner / Business Owner musí zaznamenať záznam o návrhu ochrany súkromia v REG04 pred iniciovaním akéhokoľvek projektu, produktu, služby, systému, aplikácie, integrácie alebo zmeny obchodného procesu, ktorá zahŕňa PII.
- 4.1.2 [Both] Process Owner / Business Owner musí prepojiť každý záznam o návrhu ochrany súkromia v REG04 s existujúcou alebo návrhovou činnosťou spracúvania v REG02 pred schválením funkčných požiadaviek.
- 4.1.3 [Controller] Privacy Lead / PIMS Manager musí zaznamenať požiadavky prevádzkovateľa na ochranu súkromia už od návrhu v REG04 pred schválením funkčného návrhu prevádzkovateľa.
- 4.1.4 [Processor] Vendor / Procurement Owner musí zaznamenať pokyny zákazníka k návrhu ochrany súkromia a zmluvné obmedzenia návrhu v REG08 pred schválením návrhu služby sprostredkovateľa alebo podstatnej zmeny služby.
- 4.1.5 [Conditional] Data Protection Officer / Privacy Advisor musí zaznamenať poradenstvo v REG04 pred schválením návrhu PII, ktorý je vysoko rizikový, nový, citlivý, automatizovaný, vo veľkom rozsahu alebo podstatne zmenený.
- 4.1.6 [Both] Information Security Lead musí zaznamenať závislosti bezpečnostných kontrol PII, ktoré podporujú návrh ochrany súkromia, v REG04 pred schválením architektúry.

4.2 Minimalizácia údajov a návrh ochrany súkromia v predvolenom nastavení

- 4.2.1 [Controller] Process Owner / Business Owner musí zdokumentovať minimálne kategórie PII, kategórie dotknutých osôb, zdroje a účely v REG02 a REG04 pred schválením návrhu zberu alebo importu.
- 4.2.2 [Both] System Owner / Application Owner musí konfigurovať predvolené nastavenia spracúvania na minimálny zber a spracúvanie PII potrebné pre zdokumentovaný účel a zaznamenať dôkazy v REG04 pred spustením do produkčného prostredia.
- 4.2.3 [Controller] Process Owner / Business Owner musí zdokumentovať voliteľné polia PII, voliteľné možnosti spracúvania a predvolene vypnuté nastavenia v REG02 a REG04 pred schválením používateľského rozhrania, formulára alebo pracovného toku.
- 4.2.4 [Both] System Owner / Application Owner musí zdokumentovať predvolené nastavenia vystavenia údajov z hľadiska ochrany súkromia pre zobrazenia, reporty, exporty, rozhrania a automatizované pracovné toky v REG04 pred spustením do produkčného prostredia.
- 4.2.5 [Both] Process Owner / Business Owner musí zdokumentovať uskutočniteľnosť deidentifikácie, pseudonymizácie, agregácie alebo neidentifikovateľného spracúvania v REG04 pred schválením použitia identifikovateľných PII na testovanie, analytiku, reporting alebo sekundárne prevádzkové použitie.

4.2.6 [Both] System Owner / Application Owner musí zdokumentovať nakladanie s dočasnými artefaktmi PII vrátane dočasných súborov, cache, logov alebo staging záznamov v REG04 pred spustením do produkčného prostredia.

4.2.7 [Both] Process Owner / Business Owner musí do piatich pracovných dní od identifikácie závislosti smerovať požiadavky na návrh, ktoré patria do pôsobnosti PII10, PII11, PII13 alebo PII14, na súvisiacu dôkazovú cestu politiky v REG04.

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

9. Výnimky

9.1 Výnimky z návrhu ochrany súkromia

9.1.1 [Both] Process Owner / Business Owner musí požiadať o výnimku z návrhu ochrany súkromia v REG12 pred schválením návrhu alebo zmeny, ktorá nemôže splniť uplatniteľnú požiadavku návrhu ochrany súkromia.

9.1.2 [Both] Privacy Lead / PIMS Manager musí posúdiť dopad, kompenzačné kontroly a uplynutie platnosti každej výnimky z návrhu ochrany súkromia v REG12 do piatich pracovných dní od žiadosti.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor musí zaznamenať poradenstvo v REG12 pred schválením výnimky z návrhu ochrany súkromia, ktorá zahŕňa vysoko rizikové, citlivé, automatizované, rozsiahle, sporné alebo právne významné spracúvanie.

9.1.4 [All] Top Management musí schváliť výnimku z návrhu ochrany súkromia ovplyvňujúcu spracúvanie s vysokým dopadom, rozsah certifikácie, nevyriešené významné riziko alebo zákonnú povinnosť v REG12 pred tým, ako výnimka nadobudne účinnosť.

9.1.5 [Both] Privacy Lead / PIMS Manager musí pre každú schválenú výnimku z návrhu ochrany súkromia pred schválením nastaviť v REG12 dátum uplynutia platnosti nepresahujúci 90 dní.

9.1.6 [Both] Privacy Lead / PIMS Manager musí každú výnimku z návrhu ochrany súkromia uzavrieť alebo prehodnotiť v REG12 do piatich pracovných dní od uplynutia platnosti.

10. Uplatňovanie

10.1 Uplatňovanie a riešenie nezhôd

10.1.1 [Both] Privacy Lead / PIMS Manager musí zaznamenať chýbajúce preskúmanie návrhu ochrany súkromia, chýbajúce dôkazy minimalizácie, nevyriešené zlyhanie predvoleného nastavenia alebo neautorizované spustenie do produkčného prostredia ako nezhodu v REG12 do piatich pracovných dní od identifikácie.

10.1.2 [Both] System Owner / Application Owner musí zabrániť spusteniu systému spracúvajúceho PII do produkčného prostredia, ak preskúmanie návrhu ochrany súkromia v REG04 nie je dokončené, a zaznamenať rozhodnutie v REG12 pred spustením do produkčného prostredia.

10.1.3 [Both] Vendor / Procurement Owner musí zabrániť onboardingu dodávateľa alebo podpisu zmluvy, ak chýbajú požadované dôkazy návrhu ochrany súkromia v REG08, a zaznamenať rozhodnutie v REG12 pred onboardingom alebo podpisom.

10.1.4 [Both] Process Owner / Business Owner musí pozastaviť používanie nového alebo zmeneného návrhu spracúvania PII, kým nie sú dokončené preskúmanie REG04, aktualizácie REG02 a požadované výnimky REG12.

10.1.5 [All] Top Management musí vyžadovať nápravné opatrenie v REG12 do 10 pracovných dní pri opakovanom, dlhodobom alebo vysoko dopadovom zlyhaní návrhu ochrany súkromia.

- 10.1.6 [All] Internal Audit / Compliance Reviewer musí overiť účinnosť nápravných opatrení pri nezhodách návrhu ochrany súkromia v REG12 pri najbližšom plánovanom audite PIMS alebo do 60 dní od uzavretia, podľa toho, čo nastane skôr.

11. Preskúmanie a údržba

11.1 Preskúmanie politiky a kontrol návrhu

- 11.1.1 [All] Privacy Lead / PIMS Manager musí túto politiku preskúmať v REG12 každoročne a do 30 dní od podstatnej zmeny právnych požiadaviek, spracúvania, technológie, rozsahu certifikácie alebo kontroly PIMS.
- 11.1.2 [Both] Process Owner / Business Owner musí preskúmať aktívne činnosti spracúvania v REG02 z hľadiska zmien závislostí návrhu ochrany súkromia každoročne a do 30 dní od podstatnej zmeny spracúvania.
- 11.1.3 [Both] System Owner / Application Owner musí preskúmať dôkazy o konfigurácii ochrany súkromia v predvolenom nastavení v REG04 každoročne a do 30 dní od podstatnej zmeny systému.
- 11.1.4 [Both] Vendor / Procurement Owner musí preskúmať povinnosti dodávateľov, sprostredkovateľov, ďalších sprostredkovateľov a tretích strán týkajúce sa návrhu ochrany súkromia v REG08 pred obnovením a do 30 dní od podstatnej zmeny vzťahu.
- 11.1.5 [Conditional] Data Protection Officer / Privacy Advisor musí preskúmať dopad podstatných zmien politiky na ochranu súkromia v REG12 pred schválením.
- 11.1.6 [All] Top Management musí schváliť podstatné zmeny tejto politiky v REG12 pred zverejnením.

12. Súvisiace politiky

- 12.1 PII01 - Politika systému riadenia informácií o súkromí
- 12.2 PII02 - Politika rolí, zodpovedností a preukázateľnej zodpovednosti v oblasti ochrany súkromia
- 12.3 PII03 - Politika evidencie spracúvania PII a právneho základu
- 12.4 PII04 - Politika oznámenia o ochrane údajov a transparentnosti
- 12.5 PII05 - Politika správy súhlasov a preferencií
- 12.6 PII06 - Politika riadenia práv dotknutých osôb
- 12.7 PII07 - Politika posúdenia rizík ochrany súkromia a DPIA
- 12.8 PII09 - Politika zberu, použitia, prístupnosti a zdieľania PII
- 12.9 PII10 - Politika uchovávanía, výmazu a likvidácie PII
- 12.10 PII11 - Politika presnosti a kvality PII
- 12.11 PII12 - Politika riadenia ochrany súkromia sprostredkovateľov, ďalších sprostredkovateľov a tretích strán
- 12.12 PII13 - Politika medzinárodného prenosu PII
- 12.13 PII14 - Politika bezpečnosti PII a riadenia prístupu
- 12.14 PII17 - Politika zdokumentovaných informácií a správy dôkazov PIMS
- 12.15 PII18 - Politika monitorovania, auditu a zlepšovania PIMS

13. Referenčné normy a rámce

- 13.1 Táto politika je namapovaná na nasledujúce 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 6.1.2; Clause 6.1.3** - Namapované na preverenie rizík ochrany súkromia, väzbu na opatrenia ošetrenia, analýzu závislostí návrhu, eskaláciu a nápravné opatrenia bez duplicity celej metodiky rizík ochrany súkromia 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** - Namapované na plánované zmeny ochrany súkromia, iniciovanie projektu, prevádzkové preskúmanie návrhu ochrany súkromia, kontrolu spustenia do produkčného prostredia a preskúmanie podstatnej zmeny. 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** - Namapované na zdokumentované dôkazy návrhu ochrany súkromia 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** - Namapované na metriky návrhu ochrany súkromia, vzorkovanie dôkazov, zaznamenávanie nezhôd, nápravné opatrenia a overovanie 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** - Namapované na dokumentovanie účelov spracúvania, záznamov spracúvania, väzby návrhu ochrany súkromia a spúšťačov preverenia rizík ochrany súkromia alebo potreby DPIA pri spracúvaní prevádzkovateľa. 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** - Namapované na obmedzenie zberu a spracúvania PII prostredníctvom minimálnych požiadaviek na údaje založených na účele, predvolene vypnutého voliteľného spracúvania a minimálnych predvolených nastavení spracúvania. 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** - Namapované na smerovanie závislostí presnosti, ciele minimalizácie, uskutočniteľnosť deidentifikácie a dôkazy návrhu na minimalizáciu identifikovateľných 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** - Namapované na identifikáciu deidentifikácie, závislosti od výmazu, dočasných artefaktov PII a smerovania na kontroly životného cyklu vo fáze návrhu bez duplicity vykonávania uchovávanie alebo likvidácie. 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** - Namapované na pokyny zákazníka pre sprostredkovateľa, informácie na podporu zákazníka, záznamy návrhu sprostredkovateľa a zákazníkom autorizované zmeny 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** - Namapované na návrhové schopnosti sprostredkovateľa pre dočasné súbory, závislosť od vrátenia alebo likvidácie a závislosť od kontrol prenosu zaznamenané ako dôkazy návrhu bez duplicity postupov prevádzkového výmazu alebo bezpečnostných kontrol. 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** - Namapované na požiadavky ochrany súkromia v životnom cykle vývoja, inžinierske princípy, kontrolné body ochrany PII a dôkazy konfigurácie ochrany súkromia v predvolenom 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)** - Namapované na obmedzenie účelu, návrh minimálneho rozsahu PII, väzbu na záznamy spracúvania, predvolenú minimalizáciu, dôkazy

- a preukázateľnú zodpovednosť. 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** - Namapované na opatrenia prevádzkovateľa, preskúmanie správy, schvaľovanie výnimiek, nápravné opatrenia a údržbu politiky pri implementácii ochrany súkromia už 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** - Namapované na iniciovanie projektu, požiadavky ochrany súkromia vo fáze návrhu, nastavenia ochrany súkromia v predvolenom nastavení, minimalizáciu, kontroly návrhu pri obstarávaní, preskúmanie pred spustením do produkčného prostredia a preskúmanie vyvolané zmenou. 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** - Namapované na pokyny sprostredkovateľa, podporu návrhu sprostredkovateľa, dôkazy návrhu ochrany súkromia dodávateľa a zákazníkom autorizované zmeny 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** - Namapované na väzbu záznamov spracúvania, aktualizácie REG02, závislosti návrhu činností spracúvania a dôkazy záznamov spracúvania. 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** - Namapované na spúšťače preverenia rizík ochrany súkromia a potreby DPIA vo fáze návrhu, poradenstvo pri vysokom riziku a kontroly po implementácii bez duplicity 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** - Namapované na identifikáciu kontrol ochrany súkromia vo fáze návrhu, väzbu na riziká ochrany súkromia a dôkazy návrhu o implementácii kontrol. 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** - Namapované na špecifikáciu účelu, obmedzenie zberu, minimalizáciu údajov, obmedzené použitie a predvolené nastavenia spracúvania. 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** - Namapované na smerovanie závislostí presnosti, dôkazy preukázateľnej zodpovednosti, monitorovanie návrhu ochrany súkromia, audit a nápravné opatrenia. 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** - Namapované na legitímnosť účelu, obmedzenie zberu, minimalizáciu údajov, obmedzenie použitia a sprístupnenia, závislosť od uchovávaní, nakladanie s dočasnými súbormi a kontroly návrhu závislostí presnosti. 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].