					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: PII16					Názov dokumentu: **Politika školenia, povedomia a kompetentnosti v oblasti ochrany súkromia**							
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 7.2; Clause 7.3	Both	Primary	Kompetentnosť a povedomie
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Komunikácia a zdokumentované dôkazy
ISO/IEC 27701:2025	Clause 8.1; Clause 9.1; Clause 10.2	Both	Supporting	Prevádzkové riadenie, meranie a zlepšovanie
ISO/IEC 27701:2025	Annex A.3.17	Both	Primary	Povedomie, vzdelávanie a školenie o spracúvaní PII
GDPR	Article 5(2); Article 24; Article 28; Article 32; Article 39	Both	Supporting	Preukázateľná zodpovednosť, riadenie sprostredkovateľov, bezpečnosť a úlohy DPO
ISO/IEC 27001:2022	Clause 7.2; Clause 7.3; Annex A control 6.3	Both	Supporting	Kompetentnosť, povedomie a školenie
ISO/IEC 27002:2022	Control 6.3	Both	Supporting	Usmernenie k povedomiu, vzdelávaniu a školeniu
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Informačná bezpečnosť a súlad v oblasti ochrany súkromia

1. Rozsah

1.1 Táto politika stanovuje požiadavky organizácie na školenie, povedomie a kompetentnosť v oblasti ochrany súkromia v rámci systému riadenia informácií o súkromí.

1.2 Táto politika sa vzťahuje na personál, zmluvných dodávateľov, dočasný personál, relevantné tretie strany, sprostredkovateľov, ďalších sprostredkovateľov a iné zainteresované strany, ktorých práca môže ovplyvniť spracúvanie PII, výkonnosť PIMS, práva dotknutých osôb, riziko ochrany súkromia, informačnú bezpečnosť týkajúcu sa PII, pokyny sprostredkovateľom, incidenty týkajúce sa osobných údajov, zdokumentované informácie alebo dôkazy súladu.

1.3 Táto politika sa vzťahuje na kontexty prevádzkovateľa, spoločného prevádzkovateľa, sprostredkovateľa a ďalšieho sprostredkovateľa.

1.4 Táto politika pokrýva:

1.4.1 identifikáciu cieľových skupín školenia v oblasti ochrany súkromia;

1.4.2 školenie pri nástupe;

1.4.3 ročné opakovacie školenie;

1.4.4 školenie podľa rolí a školenie spustené udalosťou;

1.4.5 dôkazy o absolvovaní školenia;

1.4.6 eskaláciu neabsolvovania;

1.4.7 preskúmanie účinnosti školenia;

1.4.8 dôkazy uistenia o školeniach sprostredkovateľov, ďalších sprostredkovateľov a tretích strán.

1.5 Táto politika nevytvára samostatnú maticu školení, informačný panel školení, register ľudských zdrojov, register kompetentnosti, register disciplinárnych opatrení ani register školení zákazníkov. Pridelenia školení, absolvovania, pripomienky, dôkazy kompetentnosti a dôkazy povedomia sa zaznamenávajú v REG11, pričom výnimky, eskalácie, nezhody, nápravné opatrenia a dôkazy o preskúmaní sa zaznamenávajú v REG12. Dôkazy uistenia o školeniach sprostredkovateľov, ďalších sprostredkovateľov a tretích strán sa v relevantných prípadoch zaznamenávajú v REG08.

1.6 Táto politika neduplikuje:

1.6.1 priradenie zodpovednosti za roly v PII02;

1.6.2 požiadavky na evidenciu spracúvania a právny základ v PII03;

1.6.3 metodiku rizík ochrany súkromia a DPIA v PII07;

1.6.4 kontrolné brány ochrany súkromia už od návrhu v PII08;

1.6.5 riadenie životného cyklu sprostredkovateľov v PII12;

1.6.6 prevádzku bezpečnosti PII a riadenia prístupu v PII14;

1.6.7 pracovný tok incidentov týkajúcich sa PII a porušení ochrany údajov v PII15;

1.6.8 správu zdokumentovaných informácií v PII17;

1.6.9 monitorovanie, vnútorný audit a riadenie zlepšovania v PII18.

2. Účel

2.1 Účelom tejto politiky je zabezpečiť, aby osoby, ktorých práca ovplyvňuje spracúvanie PII, rozumeli svojim zodpovednostiam v oblasti ochrany súkromia, absolvovali primerané školenia v stanovených intervaloch, udržiavali kompetentnosť relevantnú pre svoju rolu a vytvárali auditovateľné dôkazy o školení, povedomí a eskalácii.

2.2 Táto politika podporuje jednotnú implementáciu PIMS tým, že používa REG11 ako primárny dôkazový objekt pre školenie a povedomie a REG08, REG10 a REG12 ako podporné dôkazové objekty.

3. Ciele

3.1 Cieľmi tejto politiky je:

3.1.1 definovať cieľové skupiny školenia v oblasti ochrany súkromia;

3.1.2 definovať požiadavky na školenie pri nástupe;

3.1.3 definovať požiadavky na ročné opakovacie školenie;

3.1.4 definovať požiadavky na školenie v oblasti ochrany súkromia podľa rolí;

3.1.5 zaznamenávať dôkazy o absolvovaní v REG11;

3.1.6 eskalovať neabsolvovanie prostredníctvom REG12;

3.1.7 v relevantných prípadoch udržiavať dôkazy uistenia o školeniach sprostredkovateľov, ďalších sprostredkovateľov a tretích strán v REG08;

3.1.8 preskúmavať účinnosť školení bez vytvárania nadmerných metrík alebo duplicitných registrov;

3.1.9 zabezpečiť, aby obsah školení zostal zosúladený s aktuálnymi politikami PIMS a podstatnými povinnosťami v oblasti ochrany súkromia.

4. Vyhlásenia politiky

4.1 Cieľová skupina a pridelenie školenia

4.1.1 [All] Privacy Lead / PIMS Manager musí v REG11 definovať kategórie cieľových skupín školenia PIMS pred začiatkom každého ročného školiaceho cyklu.

4.1.2 [All] Process Owner / Business Owner musí v REG11 identifikovať personál, ktorého povinnosti zahŕňajú spracúvanie PII, pred nástupom, priradením roly alebo podstatnou zmenou pracovných povinností.

4.1.3 [Conditional] System Owner / Application Owner musí v REG11 identifikovať používateľov vyžadujúcich školenie v oblasti ochrany súkromia pre systémy PII, privilegovaný prístup alebo administráciu pred povolením alebo podstatnou zmenou prístupu.

4.1.4 [Joint Controller] Privacy Lead / PIMS Manager musí v REG11 alebo REG08 zaznamenať rozdelenie zodpovedností spoločných prevádzkovateľov za školenie pred začatím alebo podstatnou zmenou spoločnej spracovateľskej činnosti.

4.1.5 [Conditional] Data Protection Officer / Privacy Advisor musí v REG11 identifikovať potreby rozšíreného školenia v oblasti ochrany súkromia pred priradením školenia rolám, ktoré vykonávajú vysokorizikové spracúvanie, spracúvanie osobitných kategórií PII, vybavovanie práv dotknutých osôb, DPIA, medzinárodné prenosy alebo posúdenie porušenia ochrany osobných údajov.

4.1.6 [All] Privacy Lead / PIMS Manager musí v REG11 zaznamenať priradenú cieľovú skupinu školenia, typ školenia, požadovaný dátum absolvovania a vlastníka dôkazov pred začiatkom každého ročného školiaceho cyklu.

4.2 Interval školenia pri nástupe a ročného školenia

4.2.1 [All] Privacy Lead / PIMS Manager musí v REG11 priradiť základné školenie povedomia o ochrane súkromia do 10 pracovných dní od nástupu personálu s prístupom k PII alebo so zodpovednosťami v PIMS.

4.2.2 [All] Process Owner / Business Owner musí zabezpečiť, aby priradený personál absolvoval školenie o ochrane súkromia pri nástupe v REG11 pred schválením prístupu k PII bez dohľadu alebo do 30 dní od nástupu, podľa toho, čo nastane skôr.

4.2.3 [All] Privacy Lead / PIMS Manager musí v REG11 priradiť ročné opakovacie školenie v oblasti ochrany súkromia najmenej raz za 12 mesiacov.

4.2.4 [All] Process Owner / Business Owner musí v REG11 potvrdiť stav absolvovania ročného opakovacieho školenia pre priradený personál do zverejneného ročného termínu.

4.2.5 [Conditional] Privacy Lead / PIMS Manager musí v REG11 priradiť cielené opakovacie školenie do 30 dní po podstatnej zmene politiky ochrany súkromia, podstatnej zmene procesu PIMS, auditnom zistení, opakovanom zlyhaní školenia alebo relevantnom ponaučení z incidentu týkajúceho sa PII.

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

9. Výnimky

9.1.1 [All] Process Owner / Business Owner musí v REG12 zaznamenať žiadosť o výnimku zo školenia v oblasti ochrany súkromia pred predĺžením požadovaného termínu absolvovania.

9.1.2 [All] Privacy Lead / PIMS Manager musí v REG12 schváliť alebo zamietnuť žiadosti o výnimku zo školenia v oblasti ochrany súkromia pred tým, ako výnimka nadobudne účinnosť.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor musí pred schválením poskytnúť poradenstvo k výnimkám zo školenia v REG12, ak výnimka ovplyvňuje vysokorizikové spracúvanie, osobitné kategórie PII, vybavovanie práv, riešenie incidentov, medzinárodné prenosy alebo dôkazy pre certifikáciu.

9.1.4 [Conditional] Top Management musí v REG12 schváliť výnimky zo školenia v oblasti ochrany súkromia pred aktiváciou, keď výnimka ovplyvňuje opakované neabsolvovanie, privilegovaný prístup k PII, spracúvanie PII s vysokým dopadom alebo dôkazy predkladané regulačným orgánom.

9.1.5 [All] Privacy Lead / PIMS Manager musí v REG12 definovať vlastníka výnimky, dátum uplynutia platnosti, kompenzačné opatrenie a dátum preskúmania pred schválením akejkoľvek výnimky zo školenia v oblasti ochrany súkromia.

9.1.6 [All] Process Owner / Business Owner musí v REG12 uzavrieť alebo obnoviť schválené výnimky zo školenia v oblasti ochrany súkromia pred dátumom uplynutia platnosti výnimky.

10. Uplatňovanie politiky

10.1.1 [All] Privacy Lead / PIMS Manager musí v REG12 zaznamenať nezhodu týkajúcu sa školenia do piatich pracovných dní, keď dôkazy o povinnom školení v oblasti ochrany súkromia chýbajú, sú neúplné, omeškané alebo nie sú sledovateľné k REG11.

10.1.2 [All] Process Owner / Business Owner musí zabezpečiť, aby bolo omeškané povinné školenie v oblasti ochrany súkromia absolvované alebo eskalované v REG11 alebo REG12 do 10 pracovných dní po zaznamenaní stavu omeškania.

10.1.3 [Conditional] System Owner / Application Owner musí v REG12 obmedziť nový prístup k PII s vysokým dopadom, keď požadované školenie pri nástupe alebo školenie podľa rolí v oblasti ochrany súkromia zostáva po eskalácii neabsolvované.

10.1.4 [Processor] Vendor / Procurement Owner musí eskalovať chýbajúce dôkazy uistenia o školeniach sprostredkovateľov, ďalších sprostredkovateľov alebo externej pracovnej sily v REG08 a REG12 do piatich pracovných dní po identifikácii.

10.1.5 [Conditional] Incident Response Coordinator musí do jedného pracovného dňa prepojiť opatrenia na uplatňovanie politiky súvisiace so školeniami s REG10, keď zlyhanie školenia prispelo k podozrivému alebo potvrdenému incidentu týkajúcemu sa PII.

10.1.6 [All] Internal Audit / Compliance Reviewer musí overiť dôkazy o uzavretí nápravných opatrení týkajúcich sa školení v REG12 pri najbližšom plánovanom audite alebo do 60 dní od uzavretia, podľa toho, čo nastane skôr.

11. Preskúmanie a údržba

11.1.1 [All] Privacy Lead / PIMS Manager musí najmenej raz ročne preskúmať túto politiku a obsah školení a zaznamenať výsledok preskúmania v REG11 alebo REG12.

11.1.2 [All] Privacy Lead / PIMS Manager musí preskúmať túto politiku do 30 dní po podstatnej zmene rozsahu PIMS, právnych predpisov o ochrane súkromia, spracovateľských činností, modelu rolí, ponaučení z incidentov, auditných zistení alebo výsledkov účinnosti školení.

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

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

11.1.5 [All] Privacy Lead / PIMS Manager musí do 30 dní po schválenej podstatnej zmene politiky aktualizovať obsah školení a dôkazy o pridelení v REG11.

12. Súvisiace politiky

12.1 Táto politika sa má čítať spolu s:

12.2 PII01 - Politika systému riadenia 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 oznámenia o ochrane údajov a transparentnosti;

12.6 PII05 - Politika správy súhlasov a preferencií;

12.7 PII06 - Politika riadenia práv dotknutých osôb;

12.8 PII07 - Politika posúdenia rizík ochrany súkromia a DPIA;

12.9 PII08 - Politika ochrany súkromia už od návrhu a štandardne;

12.10 PII09 - Politika zhromažďovania, používania, poskytovania a zdieľania PII;

12.11 PII10 - Politika uchovávania, výmazu a likvidácie PII;

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

12.13 PII13 - Politika medzinárodného prenosu PII;

12.14 PII14 - Politika bezpečnosti PII a riadenia prístupu;

12.15 PII15 - Politika riadenia incidentov a porušení ochrany PII;

12.16 PII17 - Politika riadenia zdokumentovaných informácií a dôkazov PIMS;

12.17 PII18 - Politika monitorovania, auditu a zlepšovania PIMS.

13. Referenčné normy a rámce

13.1 ISO/IEC 27701:2025 - Clause 7.2; Clause 7.3; Clause 7.4. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 7.1.1; 7.1.2; 7.1.3; 11.1.1; 11.1.5].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.4; 4.6.5; 6.1.1; 6.1.2; 6.1.3; 6.1.5; 7.1.7; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 9.1.1; 9.1.2; 9.1.5; 10.1.1; 10.1.2; 10.1.6; 11.1.1; 11.1.2; 11.1.4].

13.3 ISO/IEC 27701:2025 - Annex A.3.17. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 11.1.5].

13.4 GDPR - Article 5(2); Article 24; Article 28; Article 32; Article 39. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.4.4; 4.5.3; 4.5.4; 4.5.5; 5.1.1; 5.1.3; 5.1.7; 6.1.2; 6.1.3; 6.1.4; 7.1.4; 7.1.5; 9.1.3; 9.1.4; 10.1.3; 10.1.4; 10.1.5; 11.1.3].

13.5 ISO/IEC 27001:2022 - Clause 7.2; Clause 7.3; Annex A control 6.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.3; 4.3.1; 4.3.5; 4.4.1; 4.4.3; 4.5.1; 4.5.2; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 6.1.1; 7.1.1; 7.1.2; 8.1.1; 8.1.2; 8.1.3; 11.1.1].

13.6 ISO/IEC 27002:2022 - Control 6.3. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 10.1.2].

13.7 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.5.5; 4.6.4; 4.6.5; 5.1.3; 6.1.2; 6.1.3; 6.1.5; 8.1.5; 9.1.3; 10.1.1; 10.1.6; 11.1.2].