					Sem zadajte názov registrovanej právnickej osoby						
Číslo dokumentu: PII15-FS					Názov dokumentu: **Politika riadenia incidentov týkajúcich sa PII a porušení ochrany osobných údajov vo finančnom sektore**						
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 7.4; Clause 7.5	Both	Supporting	Komunikácia PIMS a zdokumentované dôkazy o incidente
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Prevádzková kontrola a väzba na posúdenie a ošetrenie rizík ochrany súkromia
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorovanie, hodnotenie, nezhoda, nápravné opatrenie a zlepšovanie
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Plánovanie a príprava riadenia incidentov pri spracúvaní PII
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Reakcia na incidenty informačnej bezpečnosti zahŕňajúce PII
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Právne, zákonné, regulačné a zmluvné požiadavky a ochrana záznamov
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Zmluva sprostredkovateľa so zákazníkom a podpora povinností zákazníka
GDPR	Article 5(2); Article 24	Controller	Supporting	Preukázateľná zodpovednosť a zodpovednosť prevádzkovateľa
GDPR	Article 26	Joint Controller	Supporting	Koordinácia zodpovedností spoločných prevádzkovateľov pri incidente
GDPR	Article 28	Both	Supporting	Súčinnosť sprostredkovateľa a zmluvné

				povinnosti sprostredkovateľa
GDPR	Article 32	Both	Supporting	Bezpečnosť spracúvania a schopnosť detegovať porušenia ochrany údajov
GDPR	Article 33	Both	Primary	Oznámenie porušenia ochrany osobných údajov a dokumentácia porušenia
GDPR	Article 34	Controller	Primary	Oznámenie porušení ochrany osobných údajov dotknutým osobám
GDPR	Article 39	Conditional	Supporting	Poradenstvo DPO, monitorovanie, spolupráca a podpora kontaktného miesta
DORA Regulation (EU) 2022/2554	Article 17	Conditional	Primary	Proces riadenia incidentov súvisiacich s ICT pre finančné subjekty v rozsahu pôsobnosti
DORA Regulation (EU) 2022/2554	Article 18	Conditional	Primary	Kritériá klasifikácie incidentov súvisiacich s ICT a významných kybernetických hrozieb
DORA Regulation (EU) 2022/2554	Article 19	Conditional	Primary	Hlásenie závažných incidentov súvisiacich s ICT a oznamovanie významných kybernetických hrozieb
DORA Regulation (EU) 2022/2554	Article 20	Conditional	Supporting	Obsah hlásení, lehoty, šablóny a postupy
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Hlásenie významných

				incidentov, ak sa uplatňuje
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Zásady informačnej bezpečnosti a súladu s ochranou súkromia
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Zodpovednosti pri reakcii na incidenty týkajúce sa PII a hlásenie udalostí
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Plánovanie incidentov, posúdenie, reakcia, poučenia a zber dôkazov
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Životný cyklus procesu riadenia incidentov
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Politika incidentov, plán, povedomie, testovanie a poučenia
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Detekcia, oznamovanie, triáž, analýza, reakcia a prevádzka hlásenia
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Očakávania týkajúce sa oznamovania zo strany sprostredkovateľa verejného cloudu a záznamov o porušení

1. Rozsah

1.1 Táto politika stanovuje požiadavky na identifikáciu, nahlasovanie, triáž, klasifikáciu, posudzovanie, zamedzenie šírenia, oznamovanie, dokumentovanie, uzatváranie a zlepšovanie na základe incidentov týkajúcich sa PII a porušení ochrany osobných údajov v rozsahoch PIMS finančného sektora.

1.2 **Oznámenie k implementácii:** Táto politika je náhradným variantom PII15 pre finančný sektor. Nesmie sa implementovať súbežne s PII15 pre rovnaký rozsah PIMS, organizačnú jednotku, produkt, zákaznícke prostredie, regulovanú službu alebo hranicu dôkazov. Organizácie musia pre rovnaký rozsah vybrať buď PII15, alebo PII15-FS, aby sa predišlo duplicitným povinnostiam riadenia incidentov, duplicitným registrom a duplicitnej práci s auditnými dôkazmi.

1.3 Táto politika sa vzťahuje na:

1.3.1 organizáciu konajúcu ako prevádzkovateľ PII v kontexte finančného sektora;

1.3.2 organizáciu konajúcu ako spoločný prevádzkovateľ, ak sa vyžaduje koordinácia zodpovedností za incident alebo porušenie ochrany osobných údajov;

1.3.3 organizáciu konajúcu ako sprostredkovateľ PII pre zákazníkov z finančného sektora;

1.3.4 organizáciu konajúcu ako ďalší sprostredkovateľ pre zákazníkov z finančného sektora alebo nadradených sprostredkovateľov;

1.3.5 systémy, aplikácie, služby, procesy, dodávateľov, sprostredkovateľov, ďalších sprostredkovateľov a tretie strany, ktoré spracúvajú, uchovávajú, prenášajú, podporujú, pristupujú k PII alebo inak ovplyvňujú PII v rámci rozsahu PIMS finančného sektora.

1.4 Táto politika používa REG10 - Register incidentov a porušení ochrany osobných údajov ako primárny dôkazový objekt pre riadenie incidentov týkajúcich sa PII a porušení ochrany osobných údajov vo finančnom sektore.

1.5 Táto politika používa podporné dôkazové objekty takto:

1.5.1 REG01 pre rozsah PIMS a kontext príslušných zainteresovaných strán, odvetvia, zákazníkov, zmlúv a hlásení.

1.5.2 REG02 pre dotknuté spracovateľské činnosti, kategórie PII, kategórie dotknutých osôb, účely, systémy a služby.

1.5.3 REG03 pre Vyhlásenie o uplatniteľnosti a aktualizácie uplatniteľnosti kontrol vrátane nahradenia PII15 politikou PII15-FS pre rovnaký rozsah.

1.5.4 REG04 pre väzbu na riziká ochrany súkromia, DPIA, zostatkové riziko a ošetrenie rizík.

1.5.5 REG08 pre dôkazy o incidentnom rozhraní so sprostredkovateľmi, ďalšími sprostredkovateľmi, zákazníkmi, dodávateľmi a tretími stranami.

1.5.6 REG09 pre väzbu na medzinárodný prenos, keď incident ovplyvňuje cezhraničné spracúvanie.

1.5.7 REG11 pre dôkazy o školení, povedomí a kompetencii v oblasti reakcie na incidenty.

1.5.8 REG12 pre dôkazy o audite, nezhode, nápravnom opatrení, preskúmaní manažmentom a zlepšovaní.

1.6 Táto politika sa pri špecializovaných kontrolách opiera o súvisiace politiky PIMS:

1.6.1 PII03 upravuje evidenciu spracúvania a záznamy o právnom základe.

1.6.2 PII04 upravuje oznámenie o ochrane údajov a kontroly transparentnosti mimo komunikácie špecifickej pre porušenie ochrany osobných údajov.

1.6.3 PII06 upravuje žiadosti dotknutých osôb o uplatnenie práv, ktoré vzniknú pred incidentom, počas neho alebo po ňom.

1.6.4 PII07 upravuje metodiku posúdenia rizík ochrany súkromia a DPIA.

1.6.5 PII08 upravuje ochranu súkromia už od návrhu a štandardne.

1.6.6 PII10 upravuje kontroly uchovávania, výmazu a likvidácie.

1.6.7 PII12 upravuje kontroly vzťahov ochrany súkromia so sprostredkovateľmi, ďalšími sprostredkovateľmi, dodávateľmi a tretími stranami.

1.6.8 PII13 upravuje mechanizmy medzinárodného prenosu PII a záznamy o rizikách prenosu.

1.6.9 PII14 upravuje preventívne a detekčné bezpečnostné kontroly a kontroly prístupu k PII.

1.6.10 PII16 upravuje školenie, povedomie a kompetenciu v oblasti ochrany súkromia.

1.6.11 PII17 upravuje zdokumentované informácie a správu dôkazov.

1.6.12 PII18 upravuje monitorovanie, interný audit, preskúmanie manažmentom, nezhodu, nápravné opatrenie a neustále zlepšovanie.

1.6.13 PII23 upravuje kontroly cloudového sprostredkovateľa PII, ak sú povinnosti cloudového sprostredkovateľa v rozsahu.

1.7 Na účely tejto politiky:

1.7.1 „PII incident“ znamená podozrivú alebo potvrdenú udalosť, ktorá ovplyvnila, mohla ovplyvniť alebo by primerane mohla ovplyvniť dôvernosť, integritu, dostupnosť, zákonné spracúvanie alebo oprávnené nakladanie s PII.

1.7.2 „PII breach“ znamená potvrdený PII incident zahŕňajúci neoprávnené, nezákonné, náhodné alebo neúmyselné zničenie, stratu, zmenu, zverejnenie, prístup k, nedostupnosť alebo kompromitáciu PII.

1.7.3 „Incident vo finančnom sektore týkajúci sa PII“ znamená PII incident, ktorý ovplyvňuje, môže ovplyvniť alebo primerane súvisí s regulovanými finančnými službami, zákazníkmi finančného sektora, finančnými protistranami, finančnými transakciami, finančnými operáciami alebo spracúvaním PII vo finančnom sektore.

1.7.4 „Závažný incident vo finančnom sektore“ znamená incident vo finančnom sektore týkajúci sa PII alebo súvisiaci incident ICT, ktorý spĺňa zdokumentované kritériá významnosti alebo hlásenia v REG10.

1.7.5 „Významná kybernetická hrozba“ znamená kybernetickú hrozbu zaznamenanú v REG10, ktorá by mohla významne ovplyvniť služby finančného sektora v rozsahu, spracúvanie PII, zákazníkov, protistrany alebo operácie.

1.7.6 „Breach assessment“ znamená zdokumentované vyhodnotenie toho, či PII incident predstavuje PII breach, aké PII a ktoré dotknuté osoby sú ovplyvnené, aké riziká môžu vzniknúť, aké oznámenia alebo komunikácia sú potrebné a aké nápravné opatrenia sú vyžadované.

1.7.7 „Povedomie“ znamená okamih, v ktorom má organizácia primeranú mieru istoty, že nastal bezpečnostný incident alebo incident ochrany súkromia a PII boli alebo mohli byť kompromitované.

1.7.8 „Incident s vysokým dopadom vo finančnom sektore týkajúci sa PII“ znamená PII incident zahŕňajúci vysoko rizikové spracúvanie, osobitné kategórie alebo vysoko citlivé PII, rozsiahle PII, zraniteľné osoby, regulovaných zákazníkov, podstatné prerušenie služby, finančné protistrany, finančné transakcie, dopad vo viacerých jurisdikciách, kompromitáciu privilegovaného prístupu, verejné vystavenie, ransomvér, nedostupnosť služby alebo významný prevádzkový, zákaznícky, finančný alebo reputačný dopad.

1.7.9 „Material incident change“ znamená nové alebo zmenené informácie ovplyvňujúce rozsah incidentu, závažnosť, kategórie PII, dopad na dotknuté osoby, dopad na službu, klasifikáciu vo finančnom sektore, rozhodnutie o oznámení, dopad na zákazníka, koreňovú príčinu, zamedzenie šírenia, obnovu, nápravné opatrenie alebo externé oznamovacie povinnosti.

2. Účel

2.1 Účelom tejto politiky je zabezpečiť, aby sa incidenty týkajúce sa PII a porušenia ochrany osobných údajov v kontexte finančného sektora riešili konzistentne, bezodkladne, zákonne, bezpečne a s dôkazmi pripravenými na audit.

2.2 Táto politika podporuje preukázateľnú zodpovednosť tým, že vyžaduje zaznamenanie incidentov týkajúcich sa PII a porušení ochrany osobných údajov vo finančnom sektore v REG10 a ich prepojenie s dotknutými záznamami o spracúvaní, rizikami ochrany súkromia, vzťahmi so sprostredkovateľmi a ďalšími sprostredkovateľmi, záznamami o prenosoch, nápravnými opatreniami, záznamami o školení, rozhodnutiami o hlásení vo finančnom sektore a dôkazmi o preskúmaní manažmentom, ak sú aktivované.

2.3 Táto politika zabezpečuje, aby sa povinnosti prevádzkovateľa, spoločného prevádzkovateľa, sprostredkovateľa a ďalšieho sprostredkovateľa riešili prostredníctvom odlišných pravidiel uplatniteľnosti pri zachovaní jedného integrovaného dôkazového modelu pre incidenty a porušenia ochrany osobných údajov vo finančnom sektore.

3. Ciele

3.1 Cieľmi tejto politiky je:

3.1.1 zabezpečiť bezodkladné nahlásenie a zaznamenanie podozrivých incidentov vo finančnom sektore týkajúcich sa PII;

3.1.2 zabezpečiť triáž a klasifikáciu incidentov vo finančnom sektore týkajúcich sa PII podľa konzistentných kritérií ochrany súkromia, bezpečnosti, prevádzky a odvetvia;

3.1.3 zabezpečiť, aby posúdenia porušenia ochrany osobných údajov zohľadňovali dotknuté PII, dotknuté osoby, systémy, služby, spracovateľské činnosti, sprostredkovateľov, ďalších sprostredkovateľov, prenosy, riziká, zákazníkov, protistrany a nápravné opatrenia;

3.1.4 zabezpečiť dokumentovanie rozhodnutí prevádzkovateľa o oznámení a komunikácii s dotknutými osobami;

3.1.5 zabezpečiť, aby oznámenia sprostredkovateľa a ďalšieho sprostredkovateľa zákazníkom alebo nadradeným stranám o porušení ochrany osobných údajov boli vykonané bez zbytočného odkladu a v súlade s príslušnými dohodami;

3.1.6 zabezpečiť vyhodnotenie, zdokumentovanie a sledovanie spúšťačov hlásenia vo finančnom sektore, ak sa uplatňujú;

3.1.7 zabezpečiť zachovanie a ochranu dôkazov počas riešenia incidentu;

3.1.8 zabezpečiť sledovanie zamedzenia šírenia, odstránenia, obnovy a validácie prostredníctvom REG10;

3.1.9 zabezpečiť smerovanie významných kybernetických hrozieb a závažných incidentov vo finančnom sektore do príslušných rozhodovacích a oznamovacích pracovných tokov;

3.1.10 zabezpečiť, aby poučenia z incidentov viedli k nápravným opatreniam, školeniu, zlepšeniu kontrol a preskúmaniu manažmentom;

3.1.11 zabezpečiť dostupnosť záznamov o incidentoch a porušeniach ochrany osobných údajov pre audit, preskúmanie manažmentom, uistenie zákazníkov a regulačné preskúmanie, ak sa uplatňujú;

3.1.12 zabezpečiť, aby PII15-FS nahrádzala PII15 pre rovnaký rozsah finančného sektora a neduplikovala dôkazovú prácu podľa PII15.

4. Vyhlásenia politiky

4.1 Aktivácia variantu, pripravenosť a príjem

4.1.1 [Conditional] Privacy Lead / PIMS Manager MUSÍ zdokumentovať aktiváciu PII15-FS v REG01 a REG03 pred použitím tejto politiky pre rozsah PIMS finančného sektora.

4.1.2 [Conditional] Privacy Lead / PIMS Manager MUSÍ pred schválením PII15-FS zdokumentovať v REG03 a REG12, že PII15 nie je súbežne implementovaná pre rovnaký rozsah PIMS finančného sektora.

4.1.3 [All] Incident Response Coordinator MUSÍ zaznamenať každý nahlásený alebo zistený podozrivý incident vo finančnom sektore týkajúci sa PII v REG10 do jedného pracovného dňa od prijatia alebo skôr, ak môže byť aktivovaná príslušná notifikačná, zákaznícka alebo oznamovacia lehota.

4.1.4 [Conditional] Privacy Lead / PIMS Manager MUSÍ udržiavať kritériá riešenia incidentov týkajúcich sa PII a porušení ochrany osobných údajov vo finančnom sektore v REG10 najmenej raz ročne a po každej podstatnej zmene rozsahu PIMS, právneho kontextu, povinností voči zákazníkom, zmluvných povinností, odvetvového kontextu hlásenia alebo vysoko rizikového spracúvania.

4.1.5 [Both] Information Security Lead MUSÍ potvrdiť požiadavky na zachovanie dôkazov o incidente v REG10 do 24 hodín po tom, ako podozrivý incident ovplyvní systém, službu alebo aplikáciu spracúvajúcu PII.

4.1.6 [Conditional] Vendor / Procurement Owner MUSÍ udržiavať kontakty tretích strán pre incidenty vo finančnom sektore a požiadavky na smerovanie dôkazov v REG08 pred onboardingom a najmenej raz ročne pre sprostredkovateľov, ďalších sprostredkovateľov, dodávateľov a outsourcovaných poskytovateľov hlásenia v rozsahu.

4.2 Klasifikácia a posúdenie porušenia ochrany osobných údajov

4.2.1 [All] Incident Response Coordinator MUSÍ klasifikovať každý záznam v REG10 do 24 hodín od príjmu ako udalosť bez PII, podozrivý PII incident, potvrdený PII incident, potvrdený PII breach, incident vo finančnom sektore týkajúci sa PII, závažný incident vo finančnom sektore, významnú kybernetickú hrozbu alebo záznam čakajúci na klasifikáciu.

4.2.2 [Conditional] Information Security Lead MUSÍ v REG10 posúdiť dotknuté služby, klientov, protistrany, transakcie, výpadok služby, geografický rozsah, stratu údajov, kritickosť služby a ekonomický dopad, ak PII incident môže ovplyvniť služby alebo operácie finančného sektora.

4.2.3 [Both] Privacy Lead / PIMS Manager MUSÍ identifikovať dotknutú spracovateľskú činnosť, kategórie PII, kategórie dotknutých osôb, systémy, sprostredkovateľov, ďalších sprostredkovateľov, miesta prenosu a riziká ochrany súkromia v REG02, REG04, REG08, REG09 a REG10 pred finalizáciou rozhodnutia o oznámení porušenia ochrany osobných údajov.

4.2.4 [Controller] Data Protection Officer / Privacy Advisor MUSÍ posúdiť riziko pre dotknuté osoby pri každom potvrdenom alebo dôvodne predpokladanom PII breach a zaznamenať odporúčanie k oznámeniu, odôvodnenie rizika a poradenstvo v REG10 pred prijatím rozhodnutia o externom oznámení.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager MUSÍ zaznamenať rozdelenie zodpovedností spoločných prevádzkovateľov pri incidente v REG08 a REG10 do 24 hodín po identifikovaní spoločnej zodpovednosti za podozrivý alebo potvrdený PII breach.

4.2.6 [Processor] Privacy Lead / PIMS Manager MUSÍ posúdiť pokyny zákazníka, zmluvné oznamovacie povinnosti a povinnosti spolupráce v REG08 a REG10 do 24 hodín po tom, ako podozrivý alebo potvrdený PII breach ovplyvní spracúvanie vykonávané v postavení sprostredkovateľa.

4.2.7 [Subprocessor] Vendor / Procurement Owner MUSÍ identifikovať nadradený oznamovací reťazec a požadované smerovanie dôkazov v REG08 a REG10 do 24 hodín po tom, ako podozrivý alebo potvrdený PII incident ovplyvní spracúvanie vykonávané v postavení ďalšieho sprostredkovateľa.

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

9. Výnimky

9.1.1 [All] Privacy Lead / PIMS Manager MUSÍ zaznamenať každú výnimku z tejto politiky v REG12 pred implementáciou alebo do 24 hodín po núdzovom opatrení, ak predchádzajúce schválenie nebolo uskutočniteľné.

9.1.2 [Conditional] Top Management MUSÍ pred uzavretím incidentu schváliť každú výnimku, ktorá podstatne ovplyvňuje načasovanie oznámenia porušenia ochrany osobných údajov, načasovanie hlásenia vo finančnom sektore, verejnú komunikáciu, záväzok voči zákazníkovi, zachovanie dôkazov alebo riziko pre dotknuté osoby, pričom dôkazy o schválení sa uchovajú v REG10 a REG12.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor MUSÍ pred uzavretím incidentu zdokumentovať poradenstvo ku každému oneskorenému oznámeniu, rozhodnutiu neoznámiť, výnimke z hlásenia alebo výnimočnému komunikačnému prístupu, pričom poradenstvo sa uchová v REG10.

9.1.4 [Both] Vendor / Procurement Owner MUSÍ do piatich pracovných dní po identifikovaní výnimky zaznamenať v REG08 a REG12 výnimky dodávateľa, sprostredkovateľa, ďalšieho sprostredkovateľa, zákazníka alebo outsourcovaného poskytovateľa, ktoré ovplyvňujú reakciu na incident vo finančnom sektore.

9.1.5 [All] Privacy Lead / PIMS Manager MUSÍ najmenej mesačne až do uzavretia preskúmavať otvorené výnimky z tejto politiky, pričom stav preskúmania sa uchová v REG12.

10. Uplatňovanie politiky

10.1.1 [All] Process Owner / Business Owner MUSÍ do dvoch pracovných dní po zistení eskalovať neohlásenie podozrivého incidentu vo finančnom sektore týkajúceho sa PII, nezachovanie dôkazov, nedodržanie pridelených opatrení alebo nespoluprácu pri posúdení porušenia ochrany osobných údajov na Privacy Lead / PIMS Manager, pričom dôkazy sa uchovajú v REG12.

10.1.2 [Both] Incident Response Coordinator MUSÍ do jedného pracovného dňa po identifikovaní problému eskalovať oneskorené hlásenie, zmeškanú klasifikáciu, chýbajúce dôkazy, zmeškanú eskaláciu alebo oneskorené opatrenie na zamedzenie šírenia na Privacy Lead / PIMS Manager, pričom dôkazy sa uchovajú v REG10 a REG12.

10.1.3 [Both] Privacy Lead / PIMS Manager MUSÍ zaznamenať nezhodu v REG12, ak porušenie tejto politiky ovplyvňuje príjem incidentu, triáž, zamedzenie šírenia, oznámenie, hlásenie, integritu dôkazov, komunikáciu alebo nápravné opatrenie.

10.1.4 [Both] Vendor / Procurement Owner MUSÍ do piatich pracovných dní iniciovať nápravu dodávateľa, sprostredkovateľa, ďalšieho sprostredkovateľa alebo outsourcovaného poskytovateľa prostredníctvom REG08 a REG12, ak tretia strana nesplní dohodnuté povinnosti týkajúce sa incidentu, porušenia ochrany osobných údajov, dôkazov alebo hlásenia.

10.1.5 [Conditional] Top Management MUSÍ preskúmať podstatné alebo opakujúce sa nezhody s PII15-FS pri najbližšom plánovanom preskúmaní manažmentom, pričom rozhodnutia a požadované opatrenia sa uchovajú v REG12.

10.1.6 [All] Privacy Lead / PIMS Manager MUSÍ do 30 kalendárnych dní aktivovať nápravné školenie v REG11, ak nezhoda s politikou zahŕňa povedomie o role, oneskorené hlásenie, zlyhanie eskalácie, zlyhanie nakladania s dôkazmi alebo zlyhanie komunikácie.

11. Preskúmanie a údržba

11.1.1 [Conditional] Privacy Lead / PIMS Manager MUSÍ preskúmať túto politiku najmenej raz ročne a zaznamenať výsledok preskúmania, požadované zmeny a stav schválenia v REG12.

11.1.2 [Conditional] Incident Response Coordinator MUSÍ do 30 kalendárnych dní po uzavretí každého incidentu s vysokým dopadom vo finančnom sektore týkajúceho sa PII, potvrdeného PII breach, závažného incidentu vo finančnom sektore alebo významnej kybernetickej hrozby iniciovať poincidentné preskúmanie tejto politiky, pričom dôkazy o preskúmaní sa uchovajú v REG10 a REG12.

11.1.3 [Conditional] Privacy Lead / PIMS Manager MUSÍ preskúmať túto politiku do 30 kalendárnych dní po tom, ako sa dozvie o podstatnej zmene právnych, odvetvových, zákazníckych, zmluvných požiadaviek, požiadaviek sprostredkovateľa, ďalšieho sprostredkovateľa, šablóny hlásenia, lehoty hlásenia alebo požiadaviek na hlásenie incidentov súvisiacich s prenosom, pričom dôkazy o preskúmaní sa uchovajú v REG01, REG08, REG09 a REG12.

11.1.4 [Both] Internal Audit / Compliance Reviewer MUSÍ najmenej raz ročne preskúmať implementáciu tejto politiky prostredníctvom programu interného auditu PIMS, pričom auditné zistenia a nápravné opatrenia sa uchovajú v REG12.

11.1.5 [Conditional] Top Management MUSÍ počas plánovaného preskúmania manažmentom preskúmať trendy incidentov, významné porušenia ochrany osobných údajov, výkonnosť hlásenia, oneskorené nápravné opatrenia a účinnosť politiky, pričom výstupy sa uchovajú v REG12.

11.1.6 [Conditional] Privacy Lead / PIMS Manager MUSÍ najmenej raz ročne a po každej zmene rozsahu PIMS preskúmať náhradný vzťah medzi PII15-FS a PII15 s cieľom overiť, že obe politiky nie sú implementované pre rovnaký rozsah finančného sektora, pričom dôkazy o preskúmaní sa uchovajú v REG03 a REG12.

12. Súvisiace politiky

12.1 Táto politika sa má čítať spolu s:

12.1.1 PII01 - Politika systému riadenia informácií o súkromí

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

12.1.3 PII03 - Politika evidencie spracúvania PII a právneho základu

12.1.4 PII04 - Politika oznámenia o ochrane údajov a transparentnosti

12.1.5 PII06 - Politika riadenia práv dotknutých osôb

12.1.6 PII07 - Politika posúdenia rizík ochrany súkromia a DPIA

12.1.7 PII08 - Politika ochrany súkromia už od návrhu a štandardne

12.1.8 PII10 - Politika uchovávania, výmazu a likvidácie PII

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

12.1.10 PII13 - Politika medzinárodného prenosu PII

12.1.11 PII14 - Politika bezpečnosti PII a riadenia prístupu

12.1.12 PII16 - Politika školenia, povedomia a kompetencie v oblasti ochrany súkromia

12.1.13 PII17 - Politika zdokumentovaných informácií a správy dôkazov PIMS

12.1.14 PII18 - Politika monitorovania, auditu a zlepšovania PIMS

12.1.15 PII23 - Politika cloudového sprostredkovateľa PII, ak sú povinnosti cloudového sprostredkovateľa vo finančnom sektore v rozsahu

12.2 PII15 - Politika riadenia incidentov týkajúcich sa PII a porušení ochrany osobných údajov je základnou politikou incidentov a porušení ochrany osobných údajov. PII15-FS je náhradný variant PII15 pre finančný sektor. PII15 a PII15-FS sa nesmú implementovať súbežne pre rovnaký rozsah PIMS, organizačnú jednotku, produkt, zákaznícke prostredie, regulovanú službu alebo hranicu dôkazov.

13. Referenčné normy a rámce

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.8; 4.5.1; 4.5.4; 4.5.5; 5.2.2; 7.1.1; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.1.3; 4.2.3; 4.3.1; 4.3.4; 4.3.5; 4.7.3; 6.1.4; 7.1.4].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.7.1; 4.7.2; 4.7.6; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 9.1.1; 10.1.1; 11.1.4; 11.1.5].

13.4 ISO/IEC 27701:2025 - Annex A.3.11. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 5.1.1; 6.1.1; 7.1.2; 7.1.6; 7.1.7].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.6.1; 4.6.2].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 4.5.7; 9.1.2; 11.1.3].

13.7 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.6. Addressed by clauses [4.2.6; 4.2.7; 4.3.6; 4.4.4; 4.4.5; 4.4.10; 4.5.6; 5.7.1; 7.1.3; 8.1.5; 10.1.4].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.5.1; 4.7.2; 5.2.1; 6.1.1; 8.1.2; 11.1.6].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.6; 4.5.1].

13.10 GDPR - Article 28. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3; 10.1.4].

13.11 GDPR - Article 32. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.2; 4.7.3; 7.1.4].

13.12 GDPR - Article 33. Addressed by clauses [4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.5.4; 8.1.2].

13.13 GDPR - Article 34. Addressed by clauses [4.4.3; 4.5.4].

13.14 GDPR - Article 39. Addressed by clauses [4.2.4; 4.4.3; 5.3.1; 6.1.4; 9.1.3].

13.15 DORA Regulation (EU) 2022/2554 - Article 17. Addressed by clauses [4.1.3; 4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.3; 4.3.4; 4.3.6; 4.4.7; 4.5.1; 4.7.1; 5.4.1; 6.1.2; 7.1.7].

13.16 DORA Regulation (EU) 2022/2554 - Article 18. Addressed by clauses [4.2.1; 4.2.2; 4.6.1; 4.6.2; 4.6.3; 8.1.3].

13.17 DORA Regulation (EU) 2022/2554 - Article 19. Addressed by clauses [4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.5; 8.1.3].

13.18 DORA Regulation (EU) 2022/2554 - Article 20. Addressed by clauses [4.4.8; 4.5.5; 6.1.4; 7.1.2; 8.1.3; 11.1.3].

13.19 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.4.7; 4.4.8; 4.5.5; 6.1.4; 8.1.3; 11.1.3].

13.20 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.4.3; 4.5.1; 4.5.3; 4.7.2; 5.2.1; 8.1.2].

13.21 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.7.1].

13.22 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.4; 4.3.6; 4.5.2; 4.7.1; 4.7.2; 7.1.7; 10.1.2].

13.23 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.4; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.7.1; 7.1.7].

13.24 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.4; 4.1.6; 4.7.1; 4.7.5; 7.1.6; 7.1.7; 10.1.6].

13.25 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.1; 4.7.1].

13.26 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3].