					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: PII15-FS					Naslov dokumenta: **Politika upravljanja incidentov in kršitev varnosti osebno določljivih podatkov v finančnem sektorju**							
Različica: 1.0		Datum začetka veljavnosti: 01.01.2025			Lastnik dokumenta:							
X	Politika		Standard		Postopek		Obrazec		Register		Drugo	

Zgodovina revizij				
Številka revizije	**Datum revizije**	**Spremembe**	**Pregledal**	**Lastnik procesa**

Odobritve			
Ime	**Delovno mesto**	**Datum**	**Podpis**

Usklajenost s standardi in predpisi

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Komentar
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Komunikacije PIMS in dokumentirana dokazila o incidentih
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Povezava z operativnim nadzorom, oceno tveganj za zasebnost in obravnavo tveganj
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Spremljanje, vrednotenje, neskladnosti, korektivni ukrepi in izboljševanje
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Načrtovanje upravljanja incidentov in priprava na obdelavo osebno določljivih podatkov
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Odziv na incidente informacijske varnosti, ki vključujejo osebno določljive podatke
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Pravne, zakonske, regulativne in pogodbene zahteve ter varstvo zapisov
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Pogodba obdelovalca z naročnikom in podpora obveznostim naročnika
GDPR	Article 5(2); Article 24	Controller	Supporting	Odgovornost za skladnost in odgovornost upravljavca
GDPR	Article 26	Joint Controller	Supporting	Usklajevanje odgovornosti skupnih

				upravljavcev pri incidentih
GDPR	Article 28	Both	Supporting	Pomoč obdelovalca in pogodbene obveznosti obdelovalca
GDPR	Article 32	Both	Supporting	Varnost obdelave in zmožnost zaznavanja kršitev
GDPR	Article 33	Both	Primary	Obveščanje o kršitvah varnosti osebnih podatkov in dokumentiranje kršitev
GDPR	Article 34	Controller	Primary	Obveščanje prizadetih posameznikov, na katere se nanašajo osebno določljivi podatki, o kršitvah varnosti osebnih podatkov
GDPR	Article 39	Conditional	Supporting	Svetovanje DPO, spremljanje, sodelovanje in podpora kontaktni točki
DORA Regulation (EU) 2022/2554	Article 17	Conditional	Primary	Postopek upravljanja incidentov, povezanih z IKT, za finančne subjekte v obsegu
DORA Regulation (EU) 2022/2554	Article 18	Conditional	Primary	Merila za razvrščanje incidentov, povezanih z IKT, in pomembnih kibernetskih groženj
DORA Regulation (EU) 2022/2554	Article 19	Conditional	Primary	Poročanje o večjih incidentih, povezanih z IKT, in obveščanje o pomembnih kibernetskih grožnjah

DORA Regulation (EU) 2022/2554	Article 20	Conditional	Supporting	Vsebina poročanja, časovni roki, predloge in postopki
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Poročanje o pomembnih incidentih, kjer je to uporabljivo
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Načeli informacijske varnosti in skladnosti zasebnosti
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Odgovornosti pri odzivanju na incidente v zvezi z osebno določljivimi podatki in poročanje o dogodkih
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Načrtovanje incidentov, ocenjevanje, odziv, pridobljene izkušnje in zbiranje dokazil
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Življenjski cikel procesa upravljanja incidentov
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Politika, načrt, ozaveščanje, preizkušanje in pridobljene izkušnje na področju incidentov
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Operacije zaznavanja, obveščanja, triaže, analize, odziva in poročanja
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Pričakovanja glede obveščanja javnega oblačnega obdelovalca in evidence kršitev

1. Področje uporabe

1.1 Ta politika določa zahteve za prepoznavanje, poročanje, triažo, razvrščanje, ocenjevanje, zajezitev, obveščanje, dokumentiranje, zapiranje in izboljševanje na podlagi incidentov v zvezi z osebno določljivimi podatki in kršitev varnosti osebnih podatkov v obsegih PIMS finančnega sektorja.

1.2 **Obvestilo o implementaciji:** Ta politika je nadomestna različica PII15 za finančni sektor. Za isti obseg PIMS, poslovno enoto, produkt, okolje naročnika, regulirano storitev ali dokazno mejo se ne sme izvajati hkrati s PII15. Organizacije morajo za isti obseg izbrati bodisi PII15 bodisi PII15-FS, da se izognejo podvajanju obveznosti upravljanja incidentov, podvajanju registrov in podvajanju dela z revizijskimi dokazili.

1.3 Ta politika se uporablja za:

1.3.1 organizacijo, ki deluje kot upravljavec osebno določljivih podatkov v okviru finančnega sektorja;

1.3.2 organizacijo, ki deluje kot skupni upravljavec, kadar je potrebno usklajevanje odgovornosti za incident ali kršitev;

1.3.3 organizacijo, ki deluje kot obdelovalec osebno določljivih podatkov za naročnike iz finančnega sektorja;

1.3.4 organizacijo, ki deluje kot podobdelovalec za naročnike iz finančnega sektorja ali nadrejene obdelovalce;

1.3.5 sisteme, aplikacije, storitve, procese, dobavitelje, obdelovalce, podobdelovalce in tretje osebe, ki obdelujejo, hranijo, prenašajo, podpirajo, dostopajo do osebno določljivih podatkov ali kako drugače vplivajo nanje znotraj obsega PIMS finančnega sektorja.

1.4 Ta politika uporablja REG10 - register incidentov in kršitev varnosti osebno določljivih podatkov kot primarni dokazni objekt za upravljanje incidentov in kršitev varnosti osebno določljivih podatkov v finančnem sektorju.

1.5 Ta politika uporablja podporne dokazne objekte, kot sledi:

1.5.1 REG01 za obseg PIMS ter kontekst veljavnih zainteresiranih strani, sektorja, naročnikov, pogodb in poročanja.

1.5.2 REG02 za prizadete dejavnosti obdelave, kategorije osebno določljivih podatkov, kategorije posameznikov, na katere se nanašajo osebno določljivi podatki, namene, sisteme in storitve.

1.5.3 REG03 za Izjavo o uporabnosti in posodobitve uporabljivosti kontrol, vključno z nadomestitvijo PII15 s PII15-FS za isti obseg.

1.5.4 REG04 za povezave s tveganji za zasebnost, DPIA, preostalim tveganjem in obravnavo tveganj.

1.5.5 REG08 za dokazila o stičnih točkah za incidente pri obdelovalcih, podobdelovalcih, naročnikih, dobaviteljih in tretjih osebah.

1.5.6 REG09 za povezavo z mednarodnim prenosom, kadar incident vpliva na čezmejno obdelavo.

1.5.7 REG11 za dokazila o usposabljanju, ozaveščanju in usposobljenosti za odzivanje na incidente.

1.5.8 REG12 za dokazila o presoji, neskladnostih, korektivnih ukrepih, pregledu vodstva in izboljševanju.

1.6 Ta politika se za specialistične kontrole opira na povezane politike PIMS:

1.6.1 PII03 ureja popis dejavnosti obdelave in evidence pravnih podlag.

1.6.2 PII04 ureja obvestilo o zasebnosti in kontrole preglednosti zunaj komunikacij, specifičnih za kršitve.

1.6.3 PII06 ureja zahteve za uveljavljanje pravic posameznikov, na katere se nanašajo osebno določljivi podatki, ki nastanejo pred incidentom, med njim ali po njem.

1.6.4 PII07 ureja metodologijo ocene tveganj za zasebnost in DPIA.

1.6.5 PII08 ureja kontrole varstva zasebnosti že pri načrtovanju in privzeto.

1.6.6 PII10 ureja kontrole hrambe, izbrisa in odstranjevanja.

1.6.7 PII12 ureja kontrole razmerij zasebnosti z obdelovalci, podobdelovalci, dobavitelji in tretjimi osebami.

1.6.8 PII13 ureja mehanizme mednarodnega prenosa osebno določljivih podatkov in evidence tveganj prenosa.

1.6.9 PII14 ureja preventivne in odkrivalne kontrole varnosti in dostopa za osebno določljive podatke.

1.6.10 PII16 ureja usposabljanje, ozaveščanje in usposobljenost na področju zasebnosti.

1.6.11 PII17 ureja dokumentirane informacije in upravljanje dokazil.

1.6.12 PII18 ureja spremljanje, notranjo presojo, pregled vodstva, neskladnosti, korektivne ukrepe in nenehno izboljševanje.

1.6.13 PII23 ureja kontrole oblačnega obdelovalca osebno določljivih podatkov, kadar so obveznosti oblačnega obdelovalca v obsegu.

1.7 Za namene te politike:

1.7.1 "PII incident" pomeni domnevni ali potrjeni dogodek, ki je vplival, je morda vplival ali bi razumno lahko vplival na zaupnost, celovitost, razpoložljivost, zakonito obdelavo ali pooblaščeno ravnanje z osebno določljivimi podatki.

1.7.2 "PII breach" pomeni potrjen incident v zvezi z osebno določljivimi podatki, ki vključuje nepooblaščeno, nezakonito, nenamerno ali nenačrtovano uničenje, izgubo, spremembo, razkritje, dostop, nerazpoložljivost ali kompromitacijo osebno določljivih podatkov.

1.7.3 "Financial-sector PII incident" pomeni incident v zvezi z osebno določljivimi podatki, ki vpliva, lahko vpliva ali je razumno povezan z reguliranimi finančnimi storitvami, naročniki iz finančnega sektorja, finančnimi nasprotnimi strankami, finančnimi transakcijami, finančnimi operacijami ali obdelavo osebno določljivih podatkov v finančnem sektorju.

1.7.4 "Major financial-sector incident" pomeni incident v zvezi z osebno določljivimi podatki v finančnem sektorju ali povezan incident IKT, ki izpolnjuje dokumentirana merila pomembnosti ali poročanja v REG10.

1.7.5 "Significant cyber threat" pomeni kibernetsko grožnjo, evidentirano v REG10, ki bi lahko bistveno vplivala na storitve finančnega sektorja v obsegu, obdelavo osebno določljivih podatkov, naročnike, nasprotne stranke ali operacije.

1.7.6 "Breach assessment" pomeni dokumentirano oceno, ali je incident v zvezi z osebno določljivimi podatki kršitev varnosti osebnih podatkov, kateri osebno določljivi podatki in kateri posamezniki, na katere se nanašajo osebno določljivi podatki, so prizadeti, katera tveganja lahko nastanejo, katera obvestila ali komunikacije so potrebni in kateri sanacijski ukrepi so potrebni.

1.7.7 "Awareness" pomeni trenutek, ko ima organizacija razumno stopnjo gotovosti, da je prišlo do varnostnega incidenta ali incidenta zasebnosti in da so bili osebno določljivi podatki kompromitirani ali bi lahko bili kompromitirani.

1.7.8 "High-impact financial-sector PII incident" pomeni incident v zvezi z osebno določljivimi podatki, ki vključuje obdelavo z visokim tveganjem, posebne vrste ali zelo občutljive osebno

določljive podatke, obsežno količino osebno določljivih podatkov, ranljive posameznike, regulirane naročnike, bistveno motnjo storitve, finančne nasprotne stranke, finančne transakcije, večjurisdikcijski vpliv, kompromitacijo privilegiranega dostopa, javno izpostavljenost, izsiljevalsko programsko opremo, nerazpoložljivost storitve ali pomemben operativni, naročniški, finančni ali ugledni vpliv.

1.7.9 "Material incident change" pomeni nove ali spremenjene informacije, ki vplivajo na obseg incidenta, resnost, kategorije osebno določljivih podatkov, vpliv na posameznike, na katere se nanašajo osebno določljivi podatki, vpliv na storitve, razvrstitev za finančni sektor, odločitev o obveščanju, vpliv na naročnika, temeljni vzrok, zajezitev, obnovitev, korektivni ukrep ali obveznosti zunanjega poročanja.

2. Namen

2.1 Namen te politike je zagotoviti, da se incidenti v zvezi z osebno določljivimi podatki in kršitve varnosti osebnih podatkov v finančnem sektorju obravnavajo dosledno, pravočasno, zakonito, varno in z dokazili, pripravljenimi za revizijo.

2.2 Ta politika podpira odgovornost za skladnost z zahtevo, da se incidenti in kršitve varnosti osebno določljivih podatkov v finančnem sektorju evidentirajo v REG10 ter povežejo s prizadetimi evidencami obdelave, tveganji za zasebnost, razmerji z obdelovalci in podobdelovalci, evidencami prenosov, korektivnimi ukrepi, evidencami usposabljanja, odločitvami o poročanju za finančni sektor in dokazili pregleda vodstva, kadar so sproženi.

2.3 Ta politika zagotavlja, da se obveznosti upravljavca, skupnega upravljavca, obdelovalca in podobdelovalca obravnavajo z ločenimi pravili uporabljivosti, ob ohranjanju enotnega integriranega modela dokazil za incidente in kršitve v finančnem sektorju.

3. Cilji

3.1 Cilji te politike so:

3.1.1 zagotoviti, da se domnevni incidenti v zvezi z osebno določljivimi podatki v finančnem sektorju nemudoma prijavijo in evidentirajo;

3.1.2 zagotoviti, da se incidenti v zvezi z osebno določljivimi podatki v finančnem sektorju triažirajo in razvrstijo z uporabo doslednih meril zasebnosti, varnosti, operativnih in sektorskih meril;

3.1.3 zagotoviti, da ocene kršitev upoštevajo prizadete osebno določljive podatke, posameznike, na katere se nanašajo osebno določljivi podatki, sisteme, storitve, dejavnosti obdelave, obdelovalce, podobdelovalce, prenose, tveganja, naročnike, nasprotne stranke in sanacijske ukrepe;

3.1.4 zagotoviti, da so odločitve upravljavca o obveščanju in komunikaciji s posamezniki, na katere se nanašajo osebno določljivi podatki, dokumentirane;

3.1.5 zagotoviti, da se obvestila obdelovalcev in podobdelovalcev o kršitvah naročnikom ali nadrejenim strankam izvedejo brez nepotrebnega odlašanja in v skladu z veljavnimi dogovori;

3.1.6 zagotoviti, da se sprožilci poročanja za finančni sektor ocenijo, dokumentirajo in spremljajo, kjer je to uporabljivo;

3.1.7 zagotoviti, da se dokazila med obravnavo incidenta ohranijo in zaščitijo;

3.1.8 zagotoviti, da se zajezitev, odstranitev, obnovitev in validacija spremljajo prek REG10;

3.1.9 zagotoviti, da se pomembne kibernetske grožnje in večji incidenti v finančnem sektorju usmerijo v ustrezne odločitvene in poročevalske delovne tokove;

3.1.10 zagotoviti, da pridobljene izkušnje iz incidentov vodijo v korektivne ukrepe, usposabljanje, izboljšanje kontrol in pregled vodstva;

3.1.11 zagotoviti, da so zapisi o incidentih in kršitvah na voljo za presojo, pregled vodstva, zagotovila naročnikom in regulativni pregled, kjer je to uporabljivo;

3.1.12 zagotoviti, da PII15-FS nadomesti PII15 za isti obseg finančnega sektorja in ne podvaja dela z dokazili PII15.

4. Izjave politike

4.1 Aktivacija različice, pripravljenost in sprejem prijav

4.1.1 [Conditional] Privacy Lead / PIMS Manager MUST dokumentirati aktivacijo PII15-FS v REG01 in REG03, preden se ta politika uporabi za obseg PIMS finančnega sektorja.

4.1.2 [Conditional] Privacy Lead / PIMS Manager MUST v REG03 in REG12 dokumentirati, da se PII15 ne izvaja hkrati za isti obseg PIMS finančnega sektorja, preden se PII15-FS odobri.

4.1.3 [All] Incident Response Coordinator MUST vsak prijavljeni ali zaznani domnevni incident v zvezi z osebno določljivimi podatki v finančnem sektorju evidentirati v REG10 v enem delovnem dnevu od prejema ali prej, kadar se lahko sproži veljavni rok za obveščanje, naročnika ali poročanje.

4.1.4 [Conditional] Privacy Lead / PIMS Manager MUST vzdrževati merila za obravnavo incidentov in kršitev varnosti osebno določljivih podatkov v finančnem sektorju v REG10 najmanj letno in po vsaki bistveni spremembi obsega PIMS, pravnega konteksta, obveznosti do naročnikov, pogodbenih obveznosti, sektorskega konteksta poročanja ali obdelave z visokim tveganjem.

4.1.5 [Both] Information Security Lead MUST potrditi zahteve za ohranitev dokazil o incidentu v REG10 v 24 urah po tem, ko domnevni incident vpliva na sistem, storitev ali aplikacijo, ki obdeluje osebno določljive podatke.

4.1.6 [Conditional] Vendor / Procurement Owner MUST vzdrževati zahteve glede kontaktov za incidente tretjih oseb v finančnem sektorju in usmerjanja dokazil v REG08 pred uvajanjem ter najmanj letno za obdelovalce, podobdelovalce, dobavitelje in zunanje izvajalce poročanja v obsegu.

4.2 Razvrščanje in ocena kršitve

4.2.1 [All] Incident Response Coordinator MUST vsak vnos REG10 v 24 urah po sprejemu razvrstiti kot dogodek brez osebno določljivih podatkov, domnevni incident v zvezi z osebno določljivimi podatki, potrjeni incident v zvezi z osebno določljivimi podatki, potrjeno kršitev varnosti osebnih podatkov, incident v zvezi z osebno določljivimi podatki v finančnem sektorju, večji incident v finančnem sektorju, pomembno kibernetsko grožnjo ali vnos z razvrstitvijo v teku.

4.2.2 [Conditional] Information Security Lead MUST v REG10 oceniti prizadete storitve, stranke, nasprotne stranke, transakcije, izpad storitve, geografsko razširjenost, izgubo podatkov, kritičnost storitve in ekonomski vpliv, kadar lahko incident v zvezi z osebno določljivimi podatki vpliva na storitve ali operacije finančnega sektorja.

4.2.3 [Both] Privacy Lead / PIMS Manager MUST pred dokončno odločitvijo o obveščanju o kršitvi v REG02, REG04, REG08, REG09 in REG10 opredeliti prizadeto dejavnost obdelave, kategorije osebno določljivih podatkov, kategorije posameznikov, na katere se nanašajo osebno določljivi podatki, sisteme, obdelovalce, podobdelovalce, lokacije prenosov in tveganja za zasebnost.

4.2.4 [Controller] Data Protection Officer / Privacy Advisor MUST za vsako potrjeno ali razumno domnevno kršitev varnosti osebnih podatkov oceniti tveganje za prizadete posameznike, na katere se nanašajo osebno določljivi podatki, ter v REG10 evidentirati priporočilo glede obveščanja, utemeljitev tveganja in nasvet, preden je sprejeta odločitev o zunanjem obveščanju.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager MUST v REG08 in REG10 evidentirati razdelitev odgovornosti skupnih upravljavcev pri incidentu v 24 urah po ugotovitvi deljene odgovornosti za domnevno ali potrjeno kršitev varnosti osebnih podatkov.

4.2.6 [Processor] Privacy Lead / PIMS Manager MUST v REG08 in REG10 oceniti navodila naročnika, pogodbene obveznosti obveščanja in obveznosti sodelovanja v 24 urah po tem, ko domnevna ali potrjena kršitev varnosti osebnih podatkov vpliva na obdelavo, izvedeno v vlogi obdelovalca.

4.2.7 [Subprocessor] Vendor / Procurement Owner MUST v REG08 in REG10 opredeliti nadrejeno verigo obveščanja in zahtevano usmerjanje dokazil v 24 urah po tem, ko domnevni ali potrjeni incident v zvezi z osebno določljivimi podatki vpliva na obdelavo, izvedeno v vlogi podobdelovalca.

[... Razdelki 4.3–8 niso vključeni v ta predogled. Kupite celoten dokument za dostop do celotne vsebine. ...]

9. Izjeme

9.1.1 [All] Privacy Lead / PIMS Manager MUST vsako izjemo od te politike evidentirati v REG12 pred implementacijo ali v 24 urah po nujnem ukrepu, kadar predhodna odobritev ni bila izvedljiva.

9.1.2 [Conditional] Top Management MUST pred zaprtjem incidenta odobriti vsako izjemo, ki bistveno vpliva na roke obveščanja o kršitvi, roke poročanja za finančni sektor, javno komunikacijo, zavezo naročniku, ohranitev dokazil ali tveganje za posameznike, na katere se nanašajo osebno določljivi podatki, pri čemer se dokazilo o odobritvi hrani v REG10 in REG12.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor MUST pred zaprtjem incidenta dokumentirati nasvet za vsako zamujeno obvestilo, odločitev o neobveščanju, izjemo pri poročanju ali izjemen pristop h komunikaciji, pri čemer se nasvet hrani v REG10.

9.1.4 [Both] Vendor / Procurement Owner MUST v REG08 in REG12 v petih delovnih dneh po ugotovitvi izjeme evidentirati izjeme dobaviteljev, obdelovalcev, podobdelovalcev, naročnikov ali zunanjih izvajalcev, ki vplivajo na odzivanje na incidente v finančnem sektorju.

9.1.5 [All] Privacy Lead / PIMS Manager MUST odprte izjeme od te politike pregledovati najmanj mesečno do zaprtja, pri čemer se status pregleda hrani v REG12.

10. Uveljavljanje

10.1.1 [All] Process Owner / Business Owner MUST neporočanje o domnevnem incidentu v zvezi z osebno določljivimi podatki v finančnem sektorju, neohranitev dokazil, neupoštevanje dodeljenih ukrepov ali nesodelovanje pri oceni kršitve eskalirati Privacy Lead / PIMS Manager v dveh delovnih dneh po odkritju, pri čemer se dokazila hranijo v REG12.

10.1.2 [Both] Incident Response Coordinator MUST pozno poročanje, zamujeno razvrstitev, manjkajoča dokazila, zamujeno eskalacijo ali zapadli ukrep zajezitve eskalirati Privacy Lead / PIMS Manager v enem delovnem dnevu po ugotovitvi težave, pri čemer se dokazila hranijo v REG10 in REG12.

10.1.3 [Both] Privacy Lead / PIMS Manager MUST evidentirati neskladnost REG12, kadar kršitev te politike vpliva na sprejem incidenta, triažo, zajezitev, obveščanje, poročanje, celovitost dokazil, komunikacijo ali korektivni ukrep.

10.1.4 [Both] Vendor / Procurement Owner MUST v petih delovnih dneh začeti odpravo pri dobavitelju, obdelovalcu, podobdelovalcu ali zunanjem izvajalcu prek REG08 in REG12, kadar tretja oseba ne izpolni dogovorjenih obveznosti glede incidentov, kršitev, dokazil ali poročanja.

10.1.5 [Conditional] Top Management MUST bistvene ali ponavljajoče se neskladnosti PII15-FS pregledati na naslednjem načrtovanem pregledu vodstva, pri čemer se odločitve in zahtevani ukrepi hranijo v REG12.

10.1.6 [All] Privacy Lead / PIMS Manager MUST v REG11 sprožiti sanacijsko usposabljanje v 30 koledarskih dneh, kadar neskladnost s politiko vključuje ozaveščenost o vlogah, pozno poročanje, neuspešno eskalacijo, napako pri ravnanju z dokazili ali komunikacijsko napako.

11. Pregled in vzdrževanje

11.1.1 [Conditional] Privacy Lead / PIMS Manager MUST to politiko pregledati najmanj letno ter v REG12 evidentirati izid pregleda, zahtevane spremembe in status odobritve.

11.1.2 [Conditional] Incident Response Coordinator MUST sprožiti pregled te politike po incidentu v 30 koledarskih dneh po zaprtju vsakega incidenta v zvezi z osebno določljivimi podatki v finančnem sektorju z velikim vplivom, potrjene kršitve varnosti osebnih podatkov, večjega incidenta v finančnem sektorju ali pomembne kibernetske grožnje, pri čemer se dokazila o pregledu hranijo v REG10 in REG12.

11.1.3 [Conditional] Privacy Lead / PIMS Manager MUST to politiko pregledati v 30 koledarskih dneh po seznanitvi z bistveno spremembo pravnih, sektorskih, naročniških, pogodbenih, obdelovalskih, podobdelovalskih zahtev, zahtev glede predlog za poročanje, rokov poročanja ali zahtev poročanja o incidentih, povezanih s prenosi, pri čemer se dokazila o pregledu hranijo v REG01, REG08, REG09 in REG12.

11.1.4 [Both] Internal Audit / Compliance Reviewer MUST izvajanje te politike pregledati najmanj letno skozi program notranjih presoj PIMS, pri čemer se ugotovitve presoje in korektivni ukrepi hranijo v REG12.

11.1.5 [Conditional] Top Management MUST med načrtovanim pregledom vodstva pregledati trende incidentov, pomembne kršitve, uspešnost poročanja, zapadle korektivne ukrepe in učinkovitost politike, pri čemer se izhodi hranijo v REG12.

11.1.6 [Conditional] Privacy Lead / PIMS Manager MUST nadomestitveno razmerje med PII15-FS in PII15 pregledati najmanj letno in po vsaki spremembi obsega PIMS, da preveri, da se obe politiki ne izvajata za isti obseg finančnega sektorja, pri čemer se dokazila o pregledu hranijo v REG03 in REG12.

12. Povezane politike

12.1 To politiko je treba brati skupaj z:

12.1.1 PII01 - Politika sistema upravljanja informacij o zasebnosti

12.1.2 PII02 - Politika vlog, odgovornosti in odgovornosti za skladnost na področju zasebnosti

12.1.3 PII03 - Politika popisa dejavnosti obdelave osebno določljivih podatkov in pravne podlage

12.1.4 PII04 - Politika obvestila o zasebnosti in preglednosti

12.1.5 PII06 - Politika upravljanja pravic posameznikov, na katere se nanašajo osebno določljivi podatki

12.1.6 PII07 - Politika ocene tveganj za zasebnost in DPIA

12.1.7 PII08 - Politika varstva zasebnosti že pri načrtovanju in privzeto

12.1.8 PII10 - Politika hrambe, izbrisa in odstranjevanja osebno določljivih podatkov

12.1.9 PII12 - Politika upravljanja zasebnosti obdelovalcev, podobdelovalcev in tretjih oseb

12.1.10 PII13 - Politika mednarodnega prenosa osebno določljivih podatkov

12.1.11 PII14 - Politika varnosti in nadzora dostopa do osebno določljivih podatkov

12.1.12 PII16 - Politika usposabljanja, ozaveščanja in usposobljenosti na področju zasebnosti

12.1.13 PII17 - Politika dokumentiranih informacij in upravljanja dokazil PIMS

12.1.14 PII18 - Politika spremljanja, presoje in izboljševanja PIMS

12.1.15 PII23 - Politika oblačnega obdelovalca osebno določljivih podatkov, kadar so obveznosti oblačnega obdelovalca v finančnem sektorju v obsegu

12.2 PII15 - Politika upravljanja incidentov in kršitev varnosti osebno določljivih podatkov je osnovna politika incidentov in kršitev. PII15-FS je nadomestna različica PII15 za finančni sektor. PII15 in PII15-FS se ne smeta izvajati hkrati za isti obseg PIMS, poslovno enoto, produkt, okolje naročnika, regulirano storitev ali dokazno mejo.

13. Referenčni standardi in okviri

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].