					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: PII15-FS					Naziv dokumenta: **Politika upravljanja incidentima i povredama osobnih podataka u financijskom sektoru**							
Verzija: 1.0		Datum stupanja na snagu: 01.01.2025			Vlasnik dokumenta:							
X	Politika		Standard		Postupak		Obrazac		Registar		Drugo	

Povijest revizija				
Broj revizije	**Datum revizije**	**Promjene**	**Pregledao/la**	**Vlasnik procesa**

Odobrenja			
Ime	**Radno mjesto**	**Datum**	**Potpis**

Usklađeno sa standardima i propisima

Standard / propis	Točka / kontrola / članak	Primjenjivost	Vrsta obuhvata	Napomena
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	PIMS komunikacije i dokumentirani dokazi o incidentima
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Operativna kontrola te povezivanje s procjenom i obradom rizika za privatnost
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Praćenje, vrednovanje, nesukladnost, korektivna radnja i poboljšanje
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Planiranje i priprema upravljanja incidentima za obradu osobnih podataka (PII)
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Odgovor na incidente informacijske sigurnosti koji uključuju osobne podatke (PII)
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Pravni, zakonski, regulatorni i ugovorni zahtjevi te zaštita zapisa
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Sporazum klijenta s izvršiteljem obrade i podrška obvezama klijenta
GDPR	Article 5(2); Article 24	Controller	Supporting	Odgovornost i odgovornost voditelja obrade
GDPR	Article 26	Joint Controller	Supporting	Koordinacija odgovornosti zajedničkih voditelja obrade za incidente
GDPR	Article 28	Both	Supporting	Pomoć izvršitelja obrade i ugovorne

				obveze izvršitelja obrade
GDPR	Article 32	Both	Supporting	Sigurnost obrade i sposobnost otkrivanja povrede
GDPR	Article 33	Both	Primary	Prijava povrede osobnih podataka i dokumentiranje povrede
GDPR	Article 34	Controller	Primary	Obavješćivanje pogođenih ispitanika o povredama osobnih podataka
GDPR	Article 39	Conditional	Supporting	DPO savjeti, praćenje, suradnja i podrška kontaktne točke
DORA Regulation (EU) 2022/2554	Article 17	Conditional	Primary	Proces upravljanja incidentima povezanima s ICT-om za financijske subjekte obuhvaćene opsegom
DORA Regulation (EU) 2022/2554	Article 18	Conditional	Primary	Kriteriji klasifikacije incidenata povezanih s ICT-om i značajnih kibernetičkih prijetnji
DORA Regulation (EU) 2022/2554	Article 19	Conditional	Primary	Izvješćivanje o većim incidentima povezanima s ICT-om i obavješćivanje o značajnim kibernetičkim prijetnjama
DORA Regulation (EU) 2022/2554	Article 20	Conditional	Supporting	Sadržaj izvješća, rokovi, predlošci i postupci
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Izvješćivanje o značajnim incidentima gdje je primjenjivo
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Načela informacijske sigurnosti i

				usklađenosti privatnosti
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Odgovornosti za odgovor na incidente u vezi s osobnim podacima (PII) i prijavljivanje događaja
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Planiranje incidenata, procjena, odgovor, naučene lekcije i prikupljanje dokaza
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Životni ciklus procesa upravljanja incidentima
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Politika, plan, podizanje svijesti, testiranje i naučene lekcije u vezi s incidentima
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Operacije otkrivanja, obavješćivanja, trijaže, analize, odgovora i izvješćivanja
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Očekivanja za obavješćivanje izvršitelja obrade u javnom oblaku i zapise o povredi

1. Opseg

1.1 Ova politika definira zahtjeve za identificiranje, prijavljivanje, trijažu, klasifikaciju, procjenu, ograničavanje, obavješćivanje, dokumentiranje, zatvaranje i poboljšavanje na temelju incidenata u vezi s osobnim podacima i povreda osobnih podataka u PIMS opsezima financijskog sektora.

1.2 **Obavijest o provedbi:** Ova je politika zamjenska varijanta za financijski sektor za PII15. Ne smije se provoditi istodobno s PII15 za isti PIMS opseg, poslovnu jedinicu, proizvod, okruženje klijenta, reguliranu uslugu ili granicu dokaza. Organizacije moraju odabrati ili PII15 ili PII15-FS za isti opseg kako bi izbjegle dvostruke obveze upravljanja incidentima, dvostruke registre i dvostruki rad na revizijskim dokazima.

1.3 Ova se politika primjenjuje na:

1.3.1 organizaciju koja djeluje kao voditelj obrade u kontekstu financijskog sektora;

1.3.2 organizaciju koja djeluje kao zajednički voditelj obrade kada je potrebna koordinacija odgovornosti za incident ili povredu;

1.3.3 organizaciju koja djeluje kao izvršitelj obrade osobnih podataka (PII) za klijente iz financijskog sektora;

1.3.4 organizaciju koja djeluje kao podizvršitelj obrade za klijente iz financijskog sektora ili nadređene izvršitelje obrade;

1.3.5 sustave, aplikacije, usluge, procese, dobavljače, izvršitelje obrade, podizvršitelje obrade i treće strane koje obrađuju, pohranjuju, prenose, podržavaju, pristupaju ili na drugi način utječu na osobne podatke (PII) unutar PIMS opsega financijskog sektora.

1.4 Ova politika koristi REG10 - Registar incidenata i povreda osobnih podataka kao primarni dokazni objekt za upravljanje incidentima i povredama osobnih podataka u financijskom sektoru.

1.5 Ova politika koristi pripadajuće dokazne objekte kako slijedi:

1.5.1 REG01 za PIMS opseg te primjenjivi kontekst zainteresiranih strana, sektorski kontekst, kontekst klijenata, ugovorni kontekst i kontekst izvješćivanja.

1.5.2 REG02 za pogođene aktivnosti obrade, kategorije osobnih podataka (PII), kategorije ispitanika, svrhe, sustave i usluge.

1.5.3 REG03 za Izjavu o primjenjivosti i ažuriranja primjenjivosti kontrola, uključujući zamjenu PII15 politikom PII15-FS za isti opseg.

1.5.4 REG04 za povezivanje s rizikom za privatnost, DPIA-om, preostalim rizikom i obradom rizika.

1.5.5 REG08 za dokaze o sučelju za incidente s izvršiteljima obrade, podizvršiteljima obrade, klijentima, dobavljačima i trećim stranama.

1.5.6 REG09 za povezanost s međunarodnim prijenosom kada incident utječe na prekograničnu obradu.

1.5.7 REG11 za dokaze o osposobljavanju, podizanju svijesti i kompetencijama za odgovor na incidente.

1.5.8 REG12 za dokaze o reviziji, nesukladnosti, korektivnoj radnji, preispitivanju od strane uprave i poboljšanju.

1.6 Ova se politika oslanja na povezane PIMS politike za specijalističke kontrole:

1.6.1 PII03 uređuje inventar obrade i zapise o pravnoj osnovi.

1.6.2 PII04 uređuje obavijest o privatnosti i kontrole transparentnosti izvan komunikacija specifičnih za povredu.

1.6.3 PII06 uređuje zahtjeve za ostvarivanje prava ispitanika koji nastanu prije, tijekom ili nakon incidenta.

1.6.4 PII07 uređuje metodologiju procjene rizika za privatnost i DPIA-e.

1.6.5 PII08 uređuje kontrole ugrađene zaštite privatnosti i zaštite privatnosti prema zadanim postavkama.

1.6.6 PII10 uređuje kontrole zadržavanja, brisanja i zbrinjavanja.

1.6.7 PII12 uređuje kontrole odnosa privatnosti s izvršiteljima obrade, podizvršiteljima obrade, dobavljačima i trećim stranama.

1.6.8 PII13 uređuje mehanizme međunarodnog prijenosa osobnih podataka (PII) i zapise o riziku prijenosa.

1.6.9 PII14 uređuje preventivne i detektivne kontrole sigurnosti osobnih podataka (PII) i pristupa.

1.6.10 PII16 uređuje osposobljavanje, podizanje svijesti i kompetencije u području privatnosti.

1.6.11 PII17 uređuje dokumentirane informacije i upravljanje dokazima.

1.6.12 PII18 uređuje praćenje, unutarnju reviziju, preispitivanje od strane uprave, nesukladnost, korektivnu radnju i kontinuirano poboljšanje.

1.6.13 PII23 uređuje kontrole izvršitelja obrade osobnih podataka (PII) u oblaku kada su obveze izvršitelja obrade u oblaku obuhvaćene opsegom.

1.7 Za potrebe ove politike:

1.7.1 „Incident u vezi s osobnim podacima" znači sumnjivi ili potvrđeni događaj koji je utjecao, mogao utjecati ili bi razumno mogao utjecati na povjerljivost, cjelovitost, dostupnost, zakonitu obradu ili ovlašteno postupanje s osobnim podacima (PII).

1.7.2 „Povreda osobnih podataka" znači potvrđeni incident u vezi s osobnim podacima koji uključuje neovlašteno, nezakonito, slučajno ili nenamjerno uništenje, gubitak, izmjenu, otkrivanje, pristup, nedostupnost ili kompromitaciju osobnih podataka (PII).

1.7.3 „Incident u vezi s osobnim podacima u financijskom sektoru" znači incident u vezi s osobnim podacima koji utječe, može utjecati ili je razumno povezan s reguliranim financijskim uslugama, klijentima iz financijskog sektora, financijskim drugim ugovornim stranama, financijskim transakcijama, financijskim operacijama ili obradom osobnih podataka (PII) u financijskom sektoru.

1.7.4 „Veliki incident u financijskom sektoru" znači incident u vezi s osobnim podacima u financijskom sektoru ili povezani ICT incident koji ispunjava dokumentirane kriterije značajnosti ili izvješćivanja u REG10.

1.7.5 „Značajna kibernetička prijetnja" znači kibernetička prijetnja evidentirana u REG10 koja bi mogla značajno utjecati na financijske usluge obuhvaćene opsegom, obradu osobnih podataka (PII), klijente, druge ugovorne strane ili operacije.

1.7.6 „Procjena povrede" znači dokumentirano vrednovanje je li incident u vezi s osobnim podacima povreda osobnih podataka, koji su osobni podaci (PII) i ispitanici pogođeni, koji rizici mogu nastati, koje su prijave ili obavijesti potrebne i koje su korektivne mjere potrebne.

1.7.7 „Svjesnost" znači trenutak u kojem organizacija ima razuman stupanj sigurnosti da se sigurnosni incident ili incident privatnosti dogodio i da su osobni podaci (PII) bili ili mogli biti kompromitirani.

1.7.8 „Incident visokog utjecaja u vezi s osobnim podacima u financijskom sektoru" znači incident u vezi s osobnim podacima koji uključuje obradu visokog rizika, posebne kategorije osobnih podataka ili izrazito osjetljive osobne podatke, osobne podatke velikog opsega, ranjive pojedince, regulirane klijente, značajan prekid usluge, financijske druge ugovorne strane, financijske transakcije, učinak u više jurisdikcija, kompromitaciju privilegiranog pristupa, javnu izloženost, ransomware, nedostupnost usluge ili značajan operativni, korisnički, financijski ili reputacijski utjecaj.

1.7.9 „Značajna promjena u vezi s incidentom” znači nove ili izmijenjene informacije koje utječu na opseg incidenta, ozbiljnost, kategorije osobnih podataka (PII), utjecaj na ispitanike, utjecaj na uslugu, klasifikaciju za financijski sektor, odluku o obavješćivanju, utjecaj na klijenta, temeljni uzrok, ograničavanje, oporavak, korektivnu radnju ili vanjske obveze izvješćivanja.

2. Svrha

2.1 Svrha je ove politike osigurati da se incidentima i povredama osobnih podataka u kontekstu financijskog sektora postupa dosljedno, pravodobno, zakonito, sigurno i uz dokaze spremne za reviziju.

2.2 Ova politika podržava odgovornost zahtijevajući da se incidenti i povrede osobnih podataka u financijskom sektoru evidentiraju u REG10 i povežu s pogođenim zapisima obrade, rizicima za privatnost, odnosima s izvršiteljima obrade i podizvršiteljima obrade, zapisima o prijenosu, korektivnim radnjama, zapisima o osposobljavanju, odlukama o izvješćivanju za financijski sektor i dokazima za preispitivanje od strane uprave kada su ti elementi pokrenuti.

2.3 Ova politika osigurava da se obveze voditelja obrade, zajedničkog voditelja obrade, izvršitelja obrade i podizvršitelja obrade obrađuju kroz odvojena pravila primjenjivosti, uz održavanje jednog integriranog modela dokaza za incidente i povrede u financijskom sektoru.

3. Ciljevi

3.1 Ciljevi ove politike su:

3.1.1 osigurati da se sumnjivi incidenti u vezi s osobnim podacima u financijskom sektoru prijave i evidentiraju pravodobno;

3.1.2 osigurati da se incidenti u vezi s osobnim podacima u financijskom sektoru trijažiraju i klasificiraju prema dosljednim kriterijima privatnosti, sigurnosti, operativnim i sektorskim kriterijima;

3.1.3 osigurati da procjene povrede uzimaju u obzir pogođene osobne podatke (PII), ispitanike, sustave, usluge, aktivnosti obrade, izvršitelje obrade, podizvršitelje obrade, prijenose, rizike, klijente, druge ugovorne strane i korektivne mjere;

3.1.4 osigurati dokumentiranje odluka o prijavi voditelja obrade i obavješćivanju ispitanika;

3.1.5 osigurati da se obavijesti izvršitelja obrade i podizvršitelja obrade o povredi klijentima ili nadređenim stranama daju bez nepotrebnog odgađanja i u skladu s primjenjivim sporazumima;

3.1.6 osigurati da se okidači izvješćivanja za financijski sektor procijene, dokumentiraju i prate gdje je primjenjivo;

3.1.7 osigurati da se dokazi očuvaju i zaštite tijekom postupanja s incidentom;

3.1.8 osigurati da se ograničavanje, uklanjanje prijetnje, oporavak i provjera prate putem REG10;

3.1.9 osigurati da se značajne kibernetičke prijetnje i veliki incidenti u financijskom sektoru usmjere u odgovarajuće tijekove rada za odlučivanje i izvješćivanje;

3.1.10 osigurati da naučene lekcije iz incidenata rezultiraju korektivnom radnjom, osposobljavanjem, poboljšanjem kontrola i preispitivanjem od strane uprave;

3.1.11 osigurati da su zapisi o incidentima i povredama dostupni za reviziju, preispitivanje od strane uprave, dokazivanje prema klijentima i regulatorni pregled gdje je primjenjivo;

3.1.12 osigurati da PII15-FS zamjenjuje PII15 za isti opseg financijskog sektora i da ne duplicira rad na dokazima iz PII15.

4. Izjave politike

4.1 Aktivacija varijante, spremnost i zaprimanje

4.1.1 [Conditional] Privacy Lead / PIMS Manager MUST dokumentirati aktivaciju PII15-FS u REG01 i REG03 prije nego što se ova politika koristi za PIMS opseg financijskog sektora.

4.1.2 [Conditional] Privacy Lead / PIMS Manager MUST dokumentirati u REG03 i REG12 da se PII15 ne provodi istodobno za isti PIMS opseg financijskog sektora prije odobrenja PII15-FS.

4.1.3 [All] Incident Response Coordinator MUST evidentirati svaki prijavljeni ili otkriveni sumnjivi incident u vezi s osobnim podacima u financijskom sektoru u REG10 u roku od jednog radnog dana od zaprimanja, ili ranije kada se može pokrenuti primjenjivi rok za obavješćivanje, klijenta ili izvješćivanje.

4.1.4 [Conditional] Privacy Lead / PIMS Manager MUST održavati kriterije za postupanje s incidentima i povredama osobnih podataka u financijskom sektoru u REG10 najmanje jednom godišnje i nakon svake značajne promjene PIMS opsega, pravnog konteksta, obveza prema klijentima, ugovornih obveza, sektorskog konteksta izvješćivanja ili obrade visokog rizika.

4.1.5 [Both] Information Security Lead MUST potvrditi zahtjeve za očuvanje dokaza o incidentu u REG10 u roku od 24 sata nakon što sumnjivi incident utječe na sustav, uslugu ili aplikaciju koja obrađuje osobne podatke (PII).

4.1.6 [Conditional] Vendor / Procurement Owner MUST održavati zahtjeve za kontakte u vezi s incidentima trećih strana u financijskom sektoru i usmjeravanje dokaza u REG08 prije uvođenja te najmanje jednom godišnje za izvršitelje obrade, podizvršitelje obrade, dobavljače i vanjske pružatelje izvješćivanja obuhvaćene opsegom.

4.2 Klasifikacija i procjena povrede

4.2.1 [All] Incident Response Coordinator MUST klasificirati svaki unos u REG10 u roku od 24 sata od zaprimanja kao događaj koji nije povezan s osobnim podacima (PII), sumnjivi incident u vezi s osobnim podacima, potvrđeni incident u vezi s osobnim podacima, potvrđenu povredu osobnih podataka, incident u vezi s osobnim podacima u financijskom sektoru, veliki incident u financijskom sektoru, značajnu kibernetičku prijetnju ili unos na čekanju klasifikacije.

4.2.2 [Conditional] Information Security Lead MUST procijeniti pogođene usluge, klijente, druge ugovorne strane, transakcije, vrijeme nedostupnosti usluge, geografsku rasprostranjenost, gubitak podataka, kritičnost usluge i ekonomski utjecaj u REG10 kada incident u vezi s osobnim podacima može utjecati na financijske usluge ili operacije.

4.2.3 [Both] Privacy Lead / PIMS Manager MUST identificirati pogođenu aktivnost obrade, kategorije osobnih podataka (PII), kategorije ispitanika, sustave, izvršitelje obrade, podizvršitelje obrade, lokacije prijenosa i rizike za privatnost u REG02, REG04, REG08, REG09 i REG10 prije finalizacije odluke o prijavi povrede.

4.2.4 [Controller] Data Protection Officer / Privacy Advisor MUST procijeniti rizik za pogođene ispitanike za svaku potvrđenu ili razumno sumnjivu povredu osobnih podataka te zabilježiti preporuku o obavješćivanju, obrazloženje rizika i savjet u REG10 prije donošenja odluke o vanjskom obavješćivanju.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager MUST evidentirati raspodjelu odgovornosti zajedničkih voditelja obrade za incident u REG08 i REG10 u roku od 24 sata nakon utvrđivanja zajedničke odgovornosti za sumnjivu ili potvrđenu povredu osobnih podataka.

4.2.6 [Processor] Privacy Lead / PIMS Manager MUST procijeniti upute klijenta, ugovorne obveze obavješćivanja i obveze suradnje u REG08 i REG10 u roku od 24 sata nakon što sumnjiva ili potvrđena povreda osobnih podataka utječe na obradu koja se obavlja u svojstvu izvršitelja obrade.

4.2.7 [Subprocessor] Vendor / Procurement Owner MUST identificirati nadređeni lanac obavješćivanja i potrebno usmjeravanje dokaza u REG08 i REG10 u roku od 24 sata nakon što sumnjivi ili potvrđeni incident u vezi s osobnim podacima utječe na obradu koja se obavlja u svojstvu podizvršitelja obrade.

[... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ...]

9. Iznimke

9.1.1 [All] Privacy Lead / PIMS Manager MUST evidentirati svaku iznimku od ove politike u REG12 prije provedbe ili u roku od 24 sata nakon hitne radnje kada prethodno odobrenje nije bilo izvedivo.

9.1.2 [Conditional] Top Management MUST odobriti svaku iznimku koja značajno utječe na rok prijave povrede, rok izvješćivanja za financijski sektor, javnu komunikaciju, obvezu prema klijentu, očuvanje dokaza ili rizik za ispitanike prije zatvaranja incidenta, pri čemu se dokazi odobrenja zadržavaju u REG10 i REG12.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor MUST dokumentirati savjet za svako odgođeno obavješćivanje, odluku o neobavješćivanju, iznimku izvješćivanja ili izniman pristup komunikaciji prije zatvaranja incidenta, pri čemu se savjet zadržava u REG10.

9.1.4 [Both] Vendor / Procurement Owner MUST evidentirati iznimke dobavljača, izvršitelja obrade, podizvršitelja obrade, klijenata ili vanjskih pružatelja koje utječu na odgovor na incidente u financijskom sektoru u REG08 i REG12 u roku od pet radnih dana nakon utvrđivanja iznimke.

9.1.5 [All] Privacy Lead / PIMS Manager MUST pregledavati otvorene iznimke od ove politike najmanje jednom mjesečno do zatvaranja, pri čemu se status pregleda zadržava u REG12.

10. Provedba i poštivanje

10.1.1 [All] Process Owner / Business Owner MUST eskalirati neuspjeh prijave sumnjivog incidenta u vezi s osobnim podacima u financijskom sektoru, očuvanja dokaza, praćenja dodijeljenih radnji ili suradnje u procjeni povrede prema Privacy Lead / PIMS Manager u roku od dva radna dana nakon otkrivanja, pri čemu se dokazi zadržavaju u REG12.

10.1.2 [Both] Incident Response Coordinator MUST eskalirati zakašnjelo prijavljivanje, propuštenu klasifikaciju, nedostajuće dokaze, propuštenu eskalaciju ili dospjelu radnju ograničavanja prema Privacy Lead / PIMS Manager u roku od jednog radnog dana nakon utvrđivanja problema, pri čemu se dokazi zadržavaju u REG10 i REG12.

10.1.3 [Both] Privacy Lead / PIMS Manager MUST evidentirati nesukladnost u REG12 kada kršenje ove politike utječe na zaprimanje incidenta, trijažu, ograničavanje, obavješćivanje, izvješćivanje, cjelovitost dokaza, komunikaciju ili korektivnu radnju.

10.1.4 [Both] Vendor / Procurement Owner MUST pokrenuti otklanjanje kod dobavljača, izvršitelja obrade, podizvršitelja obrade ili vanjskog pružatelja putem REG08 i REG12 u roku od pet radnih dana kada treća strana ne ispuni dogovorene obveze u vezi s incidentom, povredom, dokazima ili izvješćivanjem.

10.1.5 [Conditional] Top Management MUST pregledati značajne ili ponavljajuće nesukladnosti s PII15-FS na sljedećem planiranom preispitivanju od strane uprave, pri čemu se odluke i potrebne radnje zadržavaju u REG12.

10.1.6 [All] Privacy Lead / PIMS Manager MUST pokrenuti korektivno osposobljavanje u REG11 u roku od 30 kalendarskih dana kada nesukladnost s politikom uključuje svijest o ulozi, zakašnjelo prijavljivanje, neuspjeh eskalacije, neuspjeh postupanja s dokazima ili neuspjeh komunikacije.

11. Pregled i održavanje

11.1.1 [Conditional] Privacy Lead / PIMS Manager MUST pregledati ovu politiku najmanje jednom godišnje i evidentirati ishod pregleda, potrebne promjene i status odobrenja u REG12.

11.1.2 [Conditional] Incident Response Coordinator MUST pokrenuti pregled ove politike nakon incidenta u roku od 30 kalendarskih dana nakon zatvaranja svakog incidenta visokog utjecaja u vezi s osobnim podacima u financijskom sektoru, potvrđene povrede osobnih podataka,

velikog incidenta u financijskom sektoru ili značajne kibernetičke prijetnje, pri čemu se dokazi pregleda zadržavaju u REG10 i REG12.

11.1.3 [Conditional] Privacy Lead / PIMS Manager MUST pregledati ovu politiku u roku od 30 kalendarskih dana nakon saznanja o značajnoj promjeni pravnih, sektorskih, klijentskih, ugovornih, izvršiteljskih, podizvršiteljskih, predložaka izvješćivanja, rokova izvješćivanja ili zahtjeva izvješćivanja o incidentima povezanih s prijenosom, pri čemu se dokazi pregleda zadržavaju u REG01, REG08, REG09 i REG12.

11.1.4 [Both] Internal Audit / Compliance Reviewer MUST pregledati provedbu ove politike najmanje jednom godišnje kroz program unutarnje revizije PIMS-a, pri čemu se revizijski nalazi i korektivne radnje zadržavaju u REG12.

11.1.5 [Conditional] Top Management MUST pregledati trendove incidenata, značajne povrede, učinkovitost izvješćivanja, dospjele korektivne radnje i djelotvornost politike tijekom planiranog preispitivanja od strane uprave, pri čemu se izlazni rezultati zadržavaju u REG12.

11.1.6 [Conditional] Privacy Lead / PIMS Manager MUST pregledati zamjenski odnos između PII15-FS i PII15 najmanje jednom godišnje i nakon svake promjene opsega PIMS-a kako bi se potvrdilo da se obje politike ne provode za isti opseg financijskog sektora, pri čemu se dokazi pregleda zadržavaju u REG03 i REG12.

12. Povezane politike

12.1 Ovu politiku treba čitati zajedno sa sljedećim dokumentima:

12.2 PII01 - Politika sustava upravljanja informacijama o privatnosti

12.3 PII02 - Politika uloga, odgovornosti i odgovornosti za privatnost

12.4 PII03 - Politika inventara obrade osobnih podataka i pravne osnove

12.5 PII04 - Politika obavijesti o privatnosti i transparentnosti

12.6 PII06 - Politika upravljanja pravima ispitanika

12.7 PII07 - Politika procjene rizika za privatnost i DPIA-e

12.8 PII08 - Politika ugrađene zaštite privatnosti i zaštite privatnosti prema zadanim postavkama

12.9 PII10 - Politika zadržavanja, brisanja i zbrinjavanja osobnih podataka

12.10 PII12 - Politika upravljanja privatnošću izvršitelja obrade, podizvršitelja obrade i trećih strana

12.11 PII13 - Politika međunarodnog prijenosa osobnih podataka

12.12 PII14 - Politika sigurnosti i kontrole pristupa osobnim podacima

12.13 PII16 - Politika osposobljavanja, podizanja svijesti i kompetencija u području privatnosti

12.14 PII17 - Politika dokumentiranih informacija i upravljanja dokazima PIMS-a

12.15 PII18 - Politika praćenja, revizije i poboljšanja PIMS-a

12.16 PII23 - Politika izvršitelja obrade osobnih podataka u oblaku, gdje su obveze izvršitelja obrade u oblaku u financijskom sektoru obuhvaćene opsegom

12.17 PII15 - Politika upravljanja incidentima i povredama osobnih podataka osnovna je politika za incidente i povrede. PII15-FS je zamjenska varijanta za financijski sektor za PII15. PII15 i PII15-FS ne smiju se provoditi istodobno za isti PIMS opseg, poslovnu jedinicu, proizvod, okruženje klijenta, reguliranu uslugu ili granicu dokaza.

13. Referentni standardi i 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].