					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: PII15-FS					Titolo del documento: **Politica di gestione degli incidenti e delle violazioni dei dati personali nel settore finanziario**							
Versione: 1.0		Data di entrata in vigore: 01.01.2025			Proprietario del documento:							
X	Politica		Standard		Procedura		Modulo		Registro		Altro	

Cronologia delle revisioni				
Numero di revisione	**Data di revisione**	**Modifiche**	**Riesaminato da**	**Proprietario del processo**

Approvazioni			
Nome	**Ruolo**	**Data**	**Firma**

Allineamento a standard e normative applicabili

Standard / Normativa	Clausola / Controllo / Articolo	Applicabilità	Tipo di copertura	Commento
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Comunicazioni PIMS ed evidenze documentate sugli incidenti
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Collegamento con controllo operativo, valutazione del rischio privacy e trattamento del rischio
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitoraggio, valutazione, non conformità, azione correttiva e miglioramento
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Pianificazione e preparazione della gestione degli incidenti per il trattamento dei dati personali
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Risposta agli incidenti di sicurezza delle informazioni che coinvolgono dati personali
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Requisiti legali, statutari, normativi e contrattuali e protezione delle registrazioni
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Accordo con il cliente del responsabile del trattamento e supporto agli obblighi del cliente
GDPR	Article 5(2); Article 24	Controller	Supporting	Responsabilizzazione e responsabilità del titolare del trattamento
GDPR	Article 26	Joint Controller	Supporting	Coordinamento delle responsabilità sugli incidenti tra contitolari del trattamento

GDPR	Article 28	Both	Supporting	Assistenza del responsabile del trattamento e obblighi contrattuali del responsabile del trattamento
GDPR	Article 32	Both	Supporting	Sicurezza del trattamento e capacità di rilevazione delle violazioni
GDPR	Article 33	Both	Primary	Notifica delle violazioni dei dati personali e documentazione delle violazioni
GDPR	Article 34	Controller	Primary	Comunicazione delle violazioni dei dati personali agli interessati coinvolti
GDPR	Article 39	Conditional	Supporting	Consulenza del DPO, monitoraggio, cooperazione e supporto come punto di contatto
DORA Regulation (EU) 2022/2554	Article 17	Conditional	Primary	Processo di gestione degli incidenti connessi all'ICT per le entità finanziarie rientranti nell'ambito di applicazione
DORA Regulation (EU) 2022/2554	Article 18	Conditional	Primary	Criteri di classificazione degli incidenti connessi all'ICT e delle minacce informatiche significative
DORA Regulation (EU) 2022/2554	Article 19	Conditional	Primary	Segnalazione degli incidenti gravi connessi all'ICT e notifica delle minacce informatiche significative
DORA Regulation (EU) 2022/2554	Article 20	Conditional	Supporting	Contenuto delle segnalazioni, termini temporali, modelli e procedure

NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Segnalazione degli incidenti significativi ove applicabile
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Principi di sicurezza delle informazioni e conformità privacy
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Responsabilità di risposta agli incidenti relativi ai dati personali e segnalazione degli eventi
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Pianificazione degli incidenti, valutazione, risposta, lezioni apprese e raccolta delle evidenze
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Ciclo di vita del processo di gestione degli incidenti
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Politica, piano, sensibilizzazione, test e lezioni apprese in materia di incidenti
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Operazioni di rilevazione, notifica, triage, analisi, risposta e segnalazione
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Aspettative di notifica del responsabile del trattamento in cloud pubblico e registrazione delle violazioni

1. Ambito di applicazione

1.1 La presente politica definisce i requisiti per identificare, segnalare, sottoporre a triage, classificare, valutare, contenere, notificare, documentare, chiudere e migliorare la gestione degli incidenti relativi ai dati personali e delle violazioni dei dati personali negli ambiti di applicazione PIMS del settore finanziario.

1.2 **Avviso di attuazione:** La presente politica è una variante sostitutiva di PII15 per il settore finanziario. Non deve essere attuata contemporaneamente a PII15 per lo stesso ambito di applicazione del PIMS, unità aziendale, prodotto, ambiente cliente, servizio regolamentato o perimetro delle evidenze. Le organizzazioni devono selezionare PII15 oppure PII15-FS per lo stesso ambito, al fine di evitare obblighi duplicati di gestione degli incidenti, registri duplicati e attività duplicate sulle evidenze di audit.

1.3 La presente politica si applica a:

1.3.1 l'organizzazione che agisce come titolare del trattamento in un contesto di settore finanziario;

1.3.2 l'organizzazione che agisce come contitolare del trattamento quando è richiesto il coordinamento delle responsabilità relative a incidenti o violazioni;

1.3.3 l'organizzazione che agisce come responsabile del trattamento per clienti del settore finanziario;

1.3.4 l'organizzazione che agisce come sub-responsabile per clienti del settore finanziario o responsabili del trattamento a monte;

1.3.5 sistemi, applicazioni, servizi, processi, fornitori, responsabili del trattamento, sub-responsabili e terze parti che trattano, archiviano, trasmettono, supportano, accedono o altrimenti incidono sui dati personali nell'ambito di applicazione del PIMS del settore finanziario.

1.4 La presente politica utilizza REG10 - Registro degli incidenti e delle violazioni dei dati personali come principale oggetto di evidenza per la gestione degli incidenti e delle violazioni dei dati personali nel settore finanziario.

1.5 La presente politica utilizza gli oggetti di evidenza di supporto come segue:

1.5.1 REG01 per l'ambito di applicazione del PIMS e il contesto applicabile relativo a parti interessate, settore, clienti, contratti e segnalazioni.

1.5.2 REG02 per attività di trattamento, categorie di dati personali, categorie di interessati, finalità, sistemi e servizi interessati.

1.5.3 REG03 per la Dichiarazione di Applicabilità e gli aggiornamenti sull'applicabilità dei controlli, inclusa la sostituzione di PII15 con PII15-FS per lo stesso ambito.

1.5.4 REG04 per il collegamento con rischio privacy, DPIA, rischio residuo e trattamento del rischio.

1.5.5 REG08 per le evidenze dell'interfaccia relativa agli incidenti con responsabili del trattamento, sub-responsabili, clienti, fornitori e terze parti.

1.5.6 REG09 per il collegamento con i trasferimenti internazionali quando un incidente interessa trattamenti transfrontalieri.

1.5.7 REG11 per le evidenze relative a formazione, sensibilizzazione e competenza nella risposta agli incidenti.

1.5.8 REG12 per le evidenze relative ad audit, non conformità, azione correttiva, riesame della direzione e miglioramento.

1.6 La presente politica si basa sulle politiche PIMS correlate per i controlli specialistici:

1.6.1 PII03 disciplina l'inventario dei trattamenti e le registrazioni della base giuridica.

1.6.2 PII04 disciplina l'informativa privacy e i controlli di trasparenza al di fuori delle comunicazioni specifiche sulle violazioni.

1.6.3 PII06 disciplina le richieste di esercizio dei diritti degli interessati che sorgono prima, durante o dopo un incidente.

1.6.4 PII07 disciplina la metodologia di valutazione del rischio privacy e DPIA.

1.6.5 PII08 disciplina i controlli di privacy by design e privacy by default.

1.6.6 PII10 disciplina i controlli di conservazione, cancellazione e smaltimento.

1.6.7 PII12 disciplina i controlli dei rapporti privacy con responsabili del trattamento, sub-responsabili, fornitori e terze parti.

1.6.8 PII13 disciplina gli strumenti di trasferimento internazionale dei dati personali e le registrazioni dei rischi di trasferimento.

1.6.9 PII14 disciplina i controlli preventivi e di rilevamento per la sicurezza e l'accesso ai dati personali.

1.6.10 PII16 disciplina formazione, sensibilizzazione e competenza in materia di privacy.

1.6.11 PII17 disciplina le informazioni documentate e la gestione delle evidenze.

1.6.12 PII18 disciplina monitoraggio, audit interno, riesame della direzione, non conformità, azione correttiva e miglioramento continuo.

1.6.13 PII23 disciplina i controlli del responsabile del trattamento dei dati personali in cloud, quando gli obblighi del responsabile del trattamento in cloud rientrano nell'ambito.

1.7 Ai fini della presente politica:

1.7.1 "Incidente relativo ai dati personali" indica un evento sospetto o confermato che ha inciso, può aver inciso o potrebbe ragionevolmente incidere sulla riservatezza, integrità, disponibilità, liceità del trattamento o gestione autorizzata dei dati personali.

1.7.2 "Violazione dei dati personali" indica un incidente confermato relativo ai dati personali che comporta distruzione, perdita, alterazione, divulgazione, accesso, indisponibilità o compromissione dei dati personali non autorizzati, illeciti, accidentali o non intenzionali.

1.7.3 "Incidente relativo ai dati personali nel settore finanziario" indica un incidente relativo ai dati personali che incide, può incidere o è ragionevolmente connesso a servizi finanziari regolamentati, clienti del settore finanziario, controparti finanziarie, transazioni finanziarie, operazioni finanziarie o trattamento dei dati personali nel settore finanziario.

1.7.4 "Incidente grave del settore finanziario" indica un incidente relativo ai dati personali nel settore finanziario o un incidente ICT correlato che soddisfa i criteri documentati di rilevanza o segnalazione in REG10.

1.7.5 "Minaccia informatica significativa" indica una minaccia informatica registrata in REG10 che potrebbe incidere in modo rilevante sui servizi del settore finanziario inclusi nell'ambito, sul trattamento dei dati personali, sui clienti, sulle controparti o sulle operazioni.

1.7.6 "Valutazione della violazione" indica la valutazione documentata volta a determinare se un incidente relativo ai dati personali costituisce una violazione dei dati personali, quali dati personali e interessati sono coinvolti, quali rischi possono sorgere, quali notifiche o comunicazioni sono richieste e quali azioni correttive sono necessarie.

1.7.7 "Consapevolezza" indica il momento in cui l'organizzazione ha un ragionevole grado di certezza che si sia verificato un incidente di sicurezza o privacy e che i dati personali siano stati o possano essere stati compromessi.

1.7.8 "Incidente relativo ai dati personali ad alto impatto nel settore finanziario" indica un incidente relativo ai dati personali che coinvolge trattamenti ad alto rischio, categorie particolari di dati o dati personali altamente sensibili, dati personali su larga scala, persone vulnerabili,

clienti regolamentati, interruzioni rilevanti del servizio, controparti finanziarie, transazioni finanziarie, impatti multi-giurisdizionali, compromissione di accessi privilegiati, esposizione pubblica, ransomware, indisponibilità del servizio o impatti operativi, sui clienti, finanziari o reputazionali significativi.

1.7.9 "Modifica sostanziale dell'incidente" indica informazioni nuove o modificate che incidono su ambito dell'incidente, gravità, categorie di dati personali, impatto sugli interessati, impatto sul servizio, classificazione per il settore finanziario, decisione di notifica, impatto sui clienti, causa radice, contenimento, ripristino, azione correttiva o obblighi di segnalazione esterna.

2. Finalità

2.1 La finalità della presente politica è garantire che gli incidenti relativi ai dati personali e le violazioni dei dati personali nei contesti del settore finanziario siano gestiti in modo coerente, tempestivo, lecito, sicuro e con evidenze idonee per l'audit.

2.2 La presente politica sostiene la responsabilizzazione imponendo che gli incidenti e le violazioni dei dati personali nel settore finanziario siano registrati in REG10 e collegati, ove attivati, alle registrazioni dei trattamenti interessati, ai rischi privacy, ai rapporti con responsabili del trattamento e sub-responsabili, alle registrazioni dei trasferimenti, alle azioni correttive, alle registrazioni della formazione, alle decisioni di segnalazione per il settore finanziario e alle evidenze del riesame della direzione.

2.3 La presente politica garantisce che gli obblighi di titolare del trattamento, contitolare del trattamento, responsabile del trattamento e sub-responsabile siano gestiti mediante regole di applicabilità distinte, mantenendo al contempo un modello integrato unico di evidenze per incidenti e violazioni nel settore finanziario.

3. Obiettivi

3.1 Gli obiettivi della presente politica sono:

3.1.1 garantire che gli incidenti sospetti relativi ai dati personali nel settore finanziario siano segnalati e registrati tempestivamente;

3.1.2 garantire che gli incidenti relativi ai dati personali nel settore finanziario siano sottoposti a triage e classificati utilizzando criteri coerenti in materia di privacy, sicurezza, operatività e settore;

3.1.3 garantire che le valutazioni delle violazioni considerino dati personali, interessati, sistemi, servizi, attività di trattamento, responsabili del trattamento, sub-responsabili, trasferimenti, rischi, clienti, controparti e azioni di rimedio interessati;

3.1.4 garantire che le decisioni di notifica del titolare del trattamento e di comunicazione agli interessati siano documentate;

3.1.5 garantire che le notifiche di violazione da parte di responsabili del trattamento e sub-responsabili ai clienti o ai soggetti a monte siano effettuate senza ingiustificato ritardo e in conformità agli accordi applicabili;

3.1.6 garantire che i presupposti di segnalazione per il settore finanziario siano valutati, documentati e tracciati ove applicabile;

3.1.7 garantire che le evidenze siano preservate e protette durante la gestione degli incidenti;

3.1.8 garantire che contenimento, eradicazione, ripristino e convalida siano tracciati tramite REG10;

3.1.9 garantire che le minacce informatiche significative e gli incidenti gravi del settore finanziario siano instradati verso i flussi decisionali e di segnalazione appropriati;

3.1.10 garantire che le lezioni apprese dagli incidenti producano azioni correttive, formazione, miglioramento dei controlli e riesame della direzione;

3.1.11 garantire che le registrazioni degli incidenti e delle violazioni siano disponibili per audit, riesame della direzione, assurance dei clienti e riesame normativo ove applicabile;

3.1.12 garantire che PII15-FS sostituisca PII15 per lo stesso ambito del settore finanziario e non duplichi le attività sulle evidenze di PII15.

4. Dichiarazioni di politica

4.1 Attivazione della variante, preparazione e presa in carico

4.1.1 [Conditional] Il Privacy Lead / PIMS Manager deve documentare l'attivazione di PII15-FS in REG01 e REG03 prima che la presente politica sia utilizzata per un ambito di applicazione del PIMS nel settore finanziario.

4.1.2 [Conditional] Il Privacy Lead / PIMS Manager deve documentare in REG03 e REG12 che PII15 non è attuata contemporaneamente per lo stesso ambito di applicazione del PIMS nel settore finanziario prima dell'approvazione di PII15-FS.

4.1.3 [All] L'Incident Response Coordinator deve registrare ogni incidente sospetto relativo ai dati personali nel settore finanziario segnalato o rilevato in REG10 entro un giorno lavorativo dalla ricezione, o prima quando possa essere attivata una tempistica applicabile di notifica, cliente o segnalazione.

4.1.4 [Conditional] Il Privacy Lead / PIMS Manager deve mantenere in REG10 i criteri di gestione degli incidenti e delle violazioni dei dati personali nel settore finanziario almeno annualmente e dopo ogni modifica sostanziale all'ambito di applicazione del PIMS, al contesto legale, agli obblighi verso i clienti, agli obblighi contrattuali, al contesto di segnalazione settoriale o ai trattamenti ad alto rischio.

4.1.5 [Both] L'Information Security Lead deve confermare in REG10 i requisiti di preservazione delle evidenze dell'incidente entro 24 ore da quando un incidente sospetto interessa un sistema, servizio o applicazione che tratta dati personali.

4.1.6 [Conditional] Il Vendor / Procurement Owner deve mantenere in REG08 i requisiti di contatto per incidenti di terze parti del settore finanziario e di instradamento delle evidenze prima dell'onboarding e almeno annualmente per responsabili del trattamento, sub-responsabili, fornitori e prestatori esterni di servizi di segnalazione inclusi nell'ambito.

4.2 Classificazione e valutazione della violazione

4.2.1 [All] L'Incident Response Coordinator deve classificare ogni voce REG10 entro 24 ore dalla presa in carico come evento non relativo a dati personali, incidente sospetto relativo ai dati personali, incidente confermato relativo ai dati personali, violazione confermata dei dati personali, incidente relativo ai dati personali nel settore finanziario, incidente grave del settore finanziario, minaccia informatica significativa o voce in attesa di classificazione.

4.2.2 [Conditional] L'Information Security Lead deve valutare in REG10 servizi, clienti, controparti, transazioni, indisponibilità del servizio, diffusione geografica, perdita di dati, criticità del servizio e impatto economico interessati quando un incidente relativo ai dati personali può incidere sui servizi o sulle operazioni del settore finanziario.

4.2.3 [Both] Il Privacy Lead / PIMS Manager deve identificare l'attività di trattamento, le categorie di dati personali, le categorie di interessati, i sistemi, i responsabili del trattamento, i sub-responsabili, le località di trasferimento e i rischi privacy interessati in REG02, REG04, REG08, REG09 e REG10 prima che la decisione di notifica della violazione sia finalizzata.

4.2.4 [Controller] Il Data Protection Officer / Privacy Advisor deve valutare il rischio per gli interessati coinvolti per ogni violazione dei dati personali confermata o ragionevolmente sospetta e registrare in REG10 la raccomandazione di notifica, la motivazione del rischio e il parere prima che sia assunta la decisione di notifica esterna.

4.2.5 [Joint Controller] Il Privacy Lead / PIMS Manager deve registrare in REG08 e REG10 la ripartizione delle responsabilità dell'incidente tra contitolari del trattamento entro 24 ore dall'identificazione di una responsabilità condivisa per una violazione dei dati personali sospetta o confermata.

4.2.6 [Processor] Il Privacy Lead / PIMS Manager deve valutare in REG08 e REG10 le istruzioni del cliente, gli obblighi contrattuali di notifica e gli obblighi di cooperazione entro 24 ore da quando una violazione dei dati personali sospetta o confermata interessa il trattamento svolto in qualità di responsabile del trattamento.

4.2.7 [Subprocessor] Il Vendor / Procurement Owner deve identificare in REG08 e REG10 la catena di notifica a monte e l'instradamento richiesto delle evidenze entro 24 ore da quando un incidente relativo ai dati personali sospetto o confermato interessa il trattamento svolto in qualità di sub-responsabile.

[... Le sezioni 4.3–8 non sono incluse in questa anteprima. Acquistare il documento completo per accedere all'intero contenuto. ...]

9. Eccezioni

9.1.1 [All] Il Privacy Lead / PIMS Manager deve registrare qualsiasi eccezione alla presente politica in REG12 prima dell'attuazione, oppure entro 24 ore dall'azione di emergenza quando l'approvazione preventiva non era praticabile.

9.1.2 [Conditional] Top Management deve approvare qualsiasi eccezione che incida in modo sostanziale sulla tempistica di notifica della violazione, sulla tempistica di segnalazione per il settore finanziario, sulla comunicazione pubblica, sugli impegni verso i clienti, sulla preservazione delle evidenze o sul rischio per gli interessati prima della chiusura dell'incidente, conservando le evidenze di approvazione in REG10 e REG12.

9.1.3 [Conditional] Il Data Protection Officer / Privacy Advisor deve documentare il parere per qualsiasi notifica ritardata, decisione di mancata notifica, eccezione di segnalazione o approccio di comunicazione eccezionale prima della chiusura dell'incidente, conservando il parere in REG10.

9.1.4 [Both] Il Vendor / Procurement Owner deve registrare in REG08 e REG12 entro cinque giorni lavorativi dall'identificazione dell'eccezione le eccezioni di fornitori, responsabili del trattamento, sub-responsabili, clienti o prestatori esterni che incidono sulla risposta agli incidenti del settore finanziario.

9.1.5 [All] Il Privacy Lead / PIMS Manager deve riesaminare almeno mensilmente le eccezioni aperte alla presente politica fino alla chiusura, conservando lo stato del riesame in REG12.

10. Applicazione

10.1.1 [All] Il Process Owner / Business Owner deve inoltrare in escalation al Privacy Lead / PIMS Manager la mancata segnalazione di un incidente sospetto relativo ai dati personali nel settore finanziario, la mancata preservazione delle evidenze, il mancato rispetto delle azioni assegnate o la mancata cooperazione con la valutazione della violazione entro due giorni lavorativi dalla scoperta, conservando le evidenze in REG12.

10.1.2 [Both] L'Incident Response Coordinator deve inoltrare in escalation al Privacy Lead / PIMS Manager segnalazioni tardive, classificazioni mancate, evidenze mancanti, escalation mancate o azioni di contenimento scadute entro un giorno lavorativo dall'identificazione del problema, conservando le evidenze in REG10 e REG12.

10.1.3 [Both] Il Privacy Lead / PIMS Manager deve registrare una non conformità REG12 quando una violazione della presente politica incide su presa in carico dell'incidente, triage, contenimento, notifica, segnalazione, integrità delle evidenze, comunicazione o azione correttiva.

10.1.4 [Both] Il Vendor / Procurement Owner deve avviare tramite REG08 e REG12 azioni di rimedio per fornitori, responsabili del trattamento, sub-responsabili o prestatori esterni entro cinque giorni lavorativi quando una terza parte non rispetta gli obblighi concordati relativi a incidente, violazione, evidenze o segnalazione.

10.1.5 [Conditional] Top Management deve riesaminare le non conformità PII15-FS sostanziali o ricorrenti al successivo riesame della direzione programmato, conservando decisioni e azioni richieste in REG12.

10.1.6 [All] Il Privacy Lead / PIMS Manager deve attivare la formazione correttiva in REG11 entro 30 giorni di calendario quando una non conformità alla politica coinvolge consapevolezza del ruolo, segnalazione tardiva, mancata escalation, mancata gestione delle evidenze o mancata comunicazione.

11. Riesame e manutenzione

11.1.1 [Conditional] Il Privacy Lead / PIMS Manager deve riesaminare la presente politica almeno annualmente e registrare in REG12 l'esito del riesame, le modifiche richieste e lo stato di approvazione.

11.1.2 [Conditional] L'Incident Response Coordinator deve attivare un riesame post-incidente della presente politica entro 30 giorni di calendario dalla chiusura di qualsiasi incidente relativo ai dati personali ad alto impatto nel settore finanziario, violazione confermata dei dati personali, incidente grave del settore finanziario o minaccia informatica significativa, conservando le evidenze del riesame in REG10 e REG12.

11.1.3 [Conditional] Il Privacy Lead / PIMS Manager deve riesaminare la presente politica entro 30 giorni di calendario da quando viene a conoscenza di una modifica sostanziale dei requisiti di segnalazione degli incidenti legali, settoriali, del cliente, contrattuali, del responsabile del trattamento, del sub-responsabile, del modello di segnalazione, della tempistica di segnalazione o relativi ai trasferimenti, conservando le evidenze del riesame in REG01, REG08, REG09 e REG12.

11.1.4 [Both] L'Internal Audit / Compliance Reviewer deve riesaminare l'attuazione della presente politica almeno annualmente tramite il programma di audit interno PIMS, conservando in REG12 le risultanze di audit e le azioni correttive.

11.1.5 [Conditional] Top Management deve riesaminare tendenze degli incidenti, violazioni significative, prestazioni di segnalazione, azioni correttive scadute ed efficacia della politica durante il riesame della direzione programmato, conservando gli output in REG12.

11.1.6 [Conditional] Il Privacy Lead / PIMS Manager deve riesaminare almeno annualmente e dopo ogni modifica dell'ambito di applicazione del PIMS il rapporto di sostituzione tra PII15-FS e PII15, per verificare che entrambe le politiche non siano attuate per lo stesso ambito del settore finanziario, conservando le evidenze del riesame in REG03 e REG12.

12. Politiche correlate

12.1 La presente politica deve essere letta congiuntamente a:

12.1.1 PII01 - Politica del Sistema di gestione delle informazioni sulla privacy

12.1.2 PII02 - Politica su ruoli, responsabilità e responsabilizzazione privacy

12.1.3 PII03 - Politica sull'inventario dei trattamenti dei dati personali e sulla base giuridica

12.1.4 PII04 - Politica su informativa privacy e trasparenza

12.1.5 PII06 - Politica di gestione dei diritti degli interessati

12.1.6 PII07 - Politica di valutazione del rischio privacy e DPIA

12.1.7 PII08 - Politica di privacy by design e privacy by default

12.1.8 PII10 - Politica di conservazione, cancellazione e smaltimento dei dati personali

12.1.9 PII12 - Politica di gestione privacy di responsabili del trattamento, sub-responsabili e terze parti

12.1.10 PII13 - Politica sui trasferimenti internazionali di dati personali

12.1.11 PII14 - Politica di sicurezza e controllo degli accessi ai dati personali

12.1.12 PII16 - Politica su formazione, sensibilizzazione e competenza in materia di privacy

12.1.13 PII17 - Politica di gestione delle informazioni documentate e delle evidenze PIMS

12.1.14 PII18 - Politica di monitoraggio, audit e miglioramento PIMS

12.1.15 PII23 - Politica per il responsabile del trattamento dei dati personali in cloud, quando gli obblighi del responsabile del trattamento in cloud del settore finanziario rientrano nell'ambito

12.2 PII15 - Politica di gestione degli incidenti e delle violazioni dei dati personali è la politica di baseline per incidenti e violazioni. PII15-FS è una variante sostitutiva di PII15 per il settore finanziario. PII15 e PII15-FS non devono essere attuate contemporaneamente per lo stesso ambito di applicazione del PIMS, unità aziendale, prodotto, ambiente cliente, servizio regolamentato o perimetro delle evidenze.

13. Standard e quadri di riferimento

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].