					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: PII15-FS					Dokumenttitel: **Richtlinie zum Management von PII-Vorfällen und Verletzungen des Schutzes personenbezogener Daten im Finanzsektor**							
Version: 1.0		Datum des Inkrafttretens: 01.01.2025			Dokumentenverantwortlicher:							
X	Richtlinie		Standard		Verfahren		Formular		Register		Sonstiges	

Änderungshistorie				
Änderungsnummer	**Änderungsdatum**	**Änderungen**	**Geprüft von**	**Prozessverantwortlicher**

Genehmigungen			
Name	**Position**	**Datum**	**Unterschrift**

Ausgerichtet an Standards und Vorschriften

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	PIMS-Kommunikation und dokumentierte Vorfallsnachweise
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Operative Steuerung sowie Verknüpfung mit Datenschutz-Risikobeurteilung und -behandlung
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Überwachung, Bewertung, Nichtkonformität, Korrekturmaßnahmen und Verbesserung
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Planung und Vorbereitung des Vorfallmanagements für die Verarbeitung personenbezogener Daten
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Reaktion auf Informationssicherheitsvorfälle, die personenbezogene Daten betreffen
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen sowie Schutz von Aufzeichnungen
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Unterstützung für Kundenvereinbarung des Auftragsverarbeiters und Kundenpflichten
GDPR	Article 5(2); Article 24	Controller	Supporting	Rechenschaftspflicht und Verantwortung des Verantwortlichen
GDPR	Article 26	Joint Controller	Supporting	Koordination der Verantwortlichkeiten gemeinsam Verantwortlicher bei Vorfällen
GDPR	Article 28	Both	Supporting	Unterstützung durch Auftragsverarbeiter und vertragliche Pflichten des Auftragsverarbeiters
GDPR	Article 32	Both	Supporting	Sicherheit der Verarbeitung und Fähigkeit zur Erkennung von Verletzungen

GDPR	Article 33	Both	Primary	Meldung von Verletzungen des Schutzes personenbezogener Daten und Dokumentation der Verletzung
GDPR	Article 34	Controller	Primary	Benachrichtigung betroffener Personen über Verletzungen des Schutzes personenbezogener Daten
GDPR	Article 39	Conditional	Supporting	Beratung, Überwachung, Zusammenarbeit und Kontaktstellenunterstützung durch den DPO
DORA Regulation (EU) 2022/2554	Article 17	Conditional	Primary	Managementprozess für IKT-bezogene Vorfälle bei in den Anwendungsbereich fallenden Finanzunternehmen
DORA Regulation (EU) 2022/2554	Article 18	Conditional	Primary	Klassifizierungskriterien für IKT-bezogene Vorfälle und erhebliche Cyberbedrohungen
DORA Regulation (EU) 2022/2554	Article 19	Conditional	Primary	Meldung schwerwiegender IKT-bezogener Vorfälle und Mitteilung erheblicher Cyberbedrohungen
DORA Regulation (EU) 2022/2554	Article 20	Conditional	Supporting	Meldeinhalte, Fristen, Vorlagen und Verfahren
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Meldung erheblicher Vorfälle, soweit anwendbar
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Grundsätze der Informationssicherheit und der Einhaltung datenschutzrechtlicher Anforderungen
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Verantwortlichkeiten für die Reaktion auf PII-Vorfälle und Ereignismeldung
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Vorfallsplanung, Bewertung, Reaktion, gewonnene Erkenntnisse und Beweissicherung
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Lebenszyklus des Vorfallmanagementprozesses

ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Vorfallsrichtlinie, Plan, Sensibilisierung, Tests und gewonnene Erkenntnisse
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Erkennung, Benachrichtigung, Triage, Analyse, Reaktion und Berichtsaktivitäten
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Erwartungen an die Benachrichtigung und Verletzungsaufzeichnungen bei Auftragsverarbeitern in der Public Cloud

1. Geltungsbereich

1.1 Diese Richtlinie legt die Anforderungen für die Identifizierung, Meldung, Triage, Klassifizierung, Bewertung, Eindämmung, Benachrichtigung, Dokumentation, den Abschluss und die Verbesserung im Zusammenhang mit Datenschutzvorfällen und Verletzungen des Schutzes personenbezogener Daten in PIMS-Geltungsbereichen des Finanzsektors fest.

1.2 **Implementierungshinweis:** Diese Richtlinie ist eine Ersatzvariante für PII15 im Finanzsektor. Sie DARF NICHT gleichzeitig mit PII15 für denselben PIMS-Geltungsbereich, dieselbe Geschäftseinheit, dasselbe Produkt, dieselbe Kundenumgebung, denselben regulierten Dienst oder dieselbe Nachweisgrenze umgesetzt werden. Organisationen müssen für denselben Geltungsbereich entweder PII15 oder PII15-FS auswählen, um doppelte Pflichten zum Vorfallmanagement, doppelte Register und doppelte Arbeiten an Auditnachweisen zu vermeiden.

1.3 Diese Richtlinie gilt für:

1.3.1 die Organisation, die in einem Finanzsektorkontext als Verantwortlicher handelt;

1.3.2 die Organisation, die als gemeinsam Verantwortlicher handelt, wenn eine Koordination der Verantwortung für Vorfälle oder Verletzungen erforderlich ist;

1.3.3 die Organisation, die als Auftragsverarbeiter für Kunden des Finanzsektors handelt;

1.3.4 die Organisation, die als Unterauftragsverarbeiter für Kunden des Finanzsektors oder vorgelagerte Auftragsverarbeiter handelt;

1.3.5 Systeme, Anwendungen, Dienste, Prozesse, Lieferanten, Auftragsverarbeiter, Unterauftragsverarbeiter und Dritte, die personenbezogene Daten innerhalb des PIMS-Geltungsbereichs des Finanzsektors verarbeiten, speichern, übermitteln, unterstützen, darauf zugreifen oder sie anderweitig beeinflussen.

1.4 Diese Richtlinie verwendet REG10 - Register für PII-Vorfälle und Verletzungen des Schutzes personenbezogener Daten als primäres Nachweisobjekt für das Management von PII-Vorfällen und Verletzungen des Schutzes personenbezogener Daten im Finanzsektor.

1.5 Diese Richtlinie verwendet unterstützende Nachweisobjekte wie folgt:

1.5.1 REG01 für PIMS-Geltungsbereich, anwendbaren Kontext interessierter Parteien, sektoralen Kontext, Kundenkontext, vertraglichen Kontext und Meldekontext.

1.5.2 REG02 für betroffene Verarbeitungstätigkeiten, Kategorien personenbezogener Daten, Kategorien betroffener Personen, Zwecke, Systeme und Dienste.

1.5.3 REG03 für die Erklärung zur Anwendbarkeit und Aktualisierungen der Anwendbarkeit von Kontrollen, einschließlich der Ersetzung von PII15 durch PII15-FS für denselben Geltungsbereich.

1.5.4 REG04 für die Verknüpfung mit Datenschutzrisiken, DPIA, Restrisiko und Risikobehandlung.

1.5.5 REG08 für Nachweise zu Vorfall-Schnittstellen mit Auftragsverarbeitern, Unterauftragsverarbeitern, Kunden, Lieferanten und Dritten.

1.5.6 REG09 für die Verknüpfung internationaler Übermittlungen, wenn ein Vorfall grenzüberschreitende Verarbeitung betrifft.

1.5.7 REG11 für Nachweise zu Schulung, Sensibilisierung und Kompetenz in der Reaktion auf Vorfälle.

1.5.8 REG12 für Nachweise zu Audit, Nichtkonformität, Korrekturmaßnahmen, Managementbewertung und Verbesserung.

1.6 Diese Richtlinie stützt sich für Spezialkontrollen auf verwandte PIMS-Richtlinien:

1.6.1 PII03 regelt das Verzeichnis der Verarbeitungstätigkeiten und Aufzeichnungen zu Rechtsgrundlagen.

1.6.2 PII04 regelt Datenschutzhinweise und Transparenzkontrollen außerhalb verletzungsspezifischer Kommunikation.

1.6.3 PII06 regelt Anfragen zu Rechten betroffener Personen, die vor, während oder nach einem Vorfall entstehen.

1.6.4 PII07 regelt die Methodik der Datenschutz-Risikobeurteilung und DPIA.

1.6.5 PII08 regelt Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen.

1.6.6 PII10 regelt Kontrollen zur Aufbewahrung, Löschung und Entsorgung.

1.6.7 PII12 regelt Datenschutzkontrollen in Beziehungen zu Auftragsverarbeitern, Unterauftragsverarbeitern, Lieferanten und Dritten.

1.6.8 PII13 regelt Mechanismen für internationale Übermittlungen personenbezogener Daten und Aufzeichnungen zu Übermittlungsrisiken.

1.6.9 PII14 regelt präventive und aufdeckende PII-Sicherheits- und Zugriffskontrollen.

1.6.10 PII16 regelt Datenschutzschulung, Sensibilisierung und Kompetenz.

1.6.11 PII17 regelt dokumentierte Informationen und Nachweismanagement.

1.6.12 PII18 regelt Überwachung, internes Audit, Managementbewertung, Nichtkonformität, Korrekturmaßnahmen und kontinuierliche Verbesserung.

1.6.13 PII23 regelt Kontrollen für Cloud-PII-Auftragsverarbeiter, soweit Pflichten von Cloud-Auftragsverarbeitern im Geltungsbereich liegen.

1.7 Für diese Richtlinie gilt:

1.7.1 „Datenschutzvorfall“ bezeichnet ein vermutetes oder bestätigtes Ereignis, das die Vertraulichkeit, Integrität, Verfügbarkeit, rechtmäßige Verarbeitung oder autorisierte Handhabung personenbezogener Daten beeinträchtigt hat, beeinträchtigt haben kann oder vernünftigerweise beeinträchtigen könnte.

1.7.2 „Verletzung des Schutzes personenbezogener Daten“ bezeichnet einen bestätigten Datenschutzvorfall, der eine unbefugte, rechtswidrige, versehentliche oder unbeabsichtigte Vernichtung, den Verlust, die Veränderung, Offenlegung, den Zugriff, die Nichtverfügbarkeit oder die Kompromittierung personenbezogener Daten umfasst.

1.7.3 „Datenschutzvorfall im Finanzsektor“ bezeichnet einen Datenschutzvorfall, der regulierte Finanzdienstleistungen, Kunden des Finanzsektors, finanzielle Gegenparteien, Finanztransaktionen, Finanzgeschäfte oder die Verarbeitung personenbezogener Daten im Finanzsektor betrifft, betreffen kann oder in angemessenem Zusammenhang damit steht.

1.7.4 „Schwerwiegender Vorfall im Finanzsektor“ bezeichnet einen Datenschutzvorfall im Finanzsektor oder einen damit verbundenen IKT-Vorfall, der die in REG10 dokumentierten Wesentlichkeits- oder Meldekriterien erfüllt.

1.7.5 „Erhebliche Cyberbedrohung“ bezeichnet eine in REG10 erfasste Cyberbedrohung, die in den Geltungsbereich fallende Finanzsektordienste, die Verarbeitung personenbezogener Daten, Kunden, Gegenparteien oder Betriebsabläufe wesentlich beeinträchtigen könnte.

1.7.6 „Bewertung der Datenschutzverletzung“ bezeichnet die dokumentierte Bewertung, ob ein Datenschutzvorfall eine Verletzung des Schutzes personenbezogener Daten ist, welche personenbezogenen Daten und betroffenen Personen betroffen sind, welche Risiken entstehen können, welche Meldungen oder Benachrichtigungen erforderlich sind und welche Abhilfemaßnahmen erforderlich sind.

1.7.7 „Kenntnis“ bezeichnet den Zeitpunkt, zu dem die Organisation mit hinreichender Sicherheit davon ausgehen kann, dass ein Sicherheits- oder Datenschutzvorfall eingetreten ist und personenbezogene Daten kompromittiert wurden oder kompromittiert worden sein könnten.

1.7.8 „Datenschutzvorfall mit hoher Tragweite im Finanzsektor“ bezeichnet einen Datenschutzvorfall, der Hochrisikoverarbeitung, besondere Kategorien oder hochsensible personenbezogene Daten, umfangreiche personenbezogene Daten, schutzbedürftige Personen, regulierte Kunden, wesentliche Serviceunterbrechung, finanzielle Gegenparteien, Finanztransaktionen, Auswirkungen in mehreren Rechtsordnungen, Kompromittierung privilegierten Zugriffs, öffentliche Exponierung, Ransomware, Nichtverfügbarkeit von Diensten oder erhebliche operative, kundenbezogene, finanzielle oder reputationsbezogene Auswirkungen umfasst.

1.7.9 „Wesentliche Änderung des Vorfalls“ bezeichnet neue oder geänderte Informationen, die den Umfang des Vorfalls, den Schweregrad, Kategorien personenbezogener Daten, Auswirkungen auf betroffene Personen, Serviceauswirkungen, Finanzsektor-Klassifizierung, Meldeentscheidung, Kundenauswirkungen, Ursache, Eindämmung, Wiederherstellung, Korrekturmaßnahmen oder externe Berichtspflichten betreffen.

2. Zweck

2.1 Zweck dieser Richtlinie ist sicherzustellen, dass Datenschutzvorfälle und Verletzungen des Schutzes personenbezogener Daten in Finanzsektorkontexten konsistent, unverzüglich, rechtmäßig, sicher und mit auditbereiten Nachweisen behandelt werden.

2.2 Diese Richtlinie unterstützt die Rechenschaftspflicht, indem sie verlangt, dass Datenschutzvorfälle und Verletzungen des Schutzes personenbezogener Daten im Finanzsektor in REG10 erfasst und, soweit ausgelöst, mit betroffenen Verarbeitungsaufzeichnungen, Datenschutzrisiken, Beziehungen zu Auftragsverarbeitern und Unterauftragsverarbeitern, Übermittlungsaufzeichnungen, Korrekturmaßnahmen, Schulungsaufzeichnungen, Finanzsektor-Meldeentscheidungen und Nachweisen zur Managementbewertung verknüpft werden.

2.3 Diese Richtlinie stellt sicher, dass Pflichten von Verantwortlichen, gemeinsam Verantwortlichen, Auftragsverarbeitern und Unterauftragsverarbeitern durch unterschiedliche Anwendbarkeitsregeln behandelt werden, während ein integriertes Nachweismodell für Vorfälle und Verletzungen im Finanzsektor beibehalten wird.

3. Ziele

3.1 Die Ziele dieser Richtlinie sind:

3.1.1 sicherzustellen, dass vermutete Datenschutzvorfälle im Finanzsektor unverzüglich gemeldet und erfasst werden;

3.1.2 sicherzustellen, dass Datenschutzvorfälle im Finanzsektor anhand konsistenter Kriterien zu Datenschutz, Sicherheit, Betrieb und Sektor triagiert und klassifiziert werden;

3.1.3 sicherzustellen, dass Bewertungen von Datenschutzverletzungen betroffene personenbezogene Daten, betroffene Personen, Systeme, Dienste, Verarbeitungstätigkeiten, Auftragsverarbeiter, Unterauftragsverarbeiter, Übermittlungen, Risiken, Kunden, Gegenparteien und Abhilfemaßnahmen berücksichtigen;

3.1.4 sicherzustellen, dass Entscheidungen zur Meldung durch Verantwortliche und zur Benachrichtigung betroffener Personen dokumentiert werden;

3.1.5 sicherzustellen, dass Meldungen von Verletzungen durch Auftragsverarbeiter und Unterauftragsverarbeiter an Kunden oder vorgelagerte Parteien ohne unangemessene Verzögerung und gemäß anwendbaren Vereinbarungen erfolgen;

3.1.6 sicherzustellen, dass Auslöser für Meldungen im Finanzsektor bewertet, dokumentiert und nachverfolgt werden, soweit anwendbar;

3.1.7 sicherzustellen, dass Nachweise während der Vorfallsbearbeitung gesichert und geschützt werden;

3.1.8 sicherzustellen, dass Eindämmung, Beseitigung, Wiederherstellung und Validierung über REG10 nachverfolgt werden;

3.1.9 sicherzustellen, dass erhebliche Cyberbedrohungen und schwerwiegende Vorfälle im Finanzsektor in geeignete Entscheidungs- und Melde-Workflows gesteuert werden;

3.1.10 sicherzustellen, dass aus Vorfällen gewonnene Erkenntnisse zu Korrekturmaßnahmen, Schulungen, Kontrollverbesserungen und Managementbewertung führen;

3.1.11 sicherzustellen, dass Aufzeichnungen zu Vorfällen und Verletzungen für Audit, Managementbewertung, Kundensicherung und regulatorische Überprüfung verfügbar sind, soweit anwendbar;

3.1.12 sicherzustellen, dass PII15-FS PII15 für denselben Finanzsektor-Geltungsbereich ersetzt und keine PII15-Nachweisarbeiten dupliziert.

4. Richtlinienaussagen

4.1 Variantenaktivierung, Bereitschaft und Eingang

4.1.1 [Conditional] Privacy Lead / PIMS Manager MUSS die Aktivierung von PII15-FS in REG01 und REG03 dokumentieren, bevor diese Richtlinie für einen PIMS-Geltungsbereich des Finanzsektors verwendet wird.

4.1.2 [Conditional] Privacy Lead / PIMS Manager MUSS in REG03 und REG12 dokumentieren, dass PII15 nicht gleichzeitig für denselben PIMS-Geltungsbereich des Finanzsektors umgesetzt ist, bevor PII15-FS genehmigt wird.

4.1.3 [All] Incident Response Coordinator MUSS jeden gemeldeten oder erkannten vermuteten Datenschutzvorfall im Finanzsektor innerhalb eines Geschäftstags nach Eingang in REG10 erfassen, oder früher, wenn eine anwendbare Melde-, Kunden- oder Berichtsfrist ausgelöst werden kann.

4.1.4 [Conditional] Privacy Lead / PIMS Manager MUSS Kriterien für die Behandlung von PII-Vorfällen und Verletzungen des Schutzes personenbezogener Daten im Finanzsektor mindestens jährlich und nach jeder wesentlichen Änderung des PIMS-Geltungsbereichs, des rechtlichen Kontexts, der Kundenpflichten, vertraglicher Pflichten, des sektoralen Meldekontexts oder der Hochrisikoverarbeitung in REG10 pflegen.

4.1.5 [Both] Information Security Lead MUSS Anforderungen an die Sicherung von Vorfallsnachweisen in REG10 innerhalb von 24 Stunden bestätigen, nachdem ein vermuteter Vorfall ein System, einen Dienst oder eine Anwendung betrifft, die personenbezogene Daten verarbeitet.

4.1.6 [Conditional] Vendor / Procurement Owner MUSS Anforderungen an Kontaktstellen und Nachweisweiterleitung bei Drittparteienvorfällen im Finanzsektor vor dem Onboarding und mindestens jährlich für in den Geltungsbereich fallende Auftragsverarbeiter, Unterauftragsverarbeiter, Lieferanten und ausgelagerte Meldeanbieter in REG08 pflegen.

4.2 Klassifizierung und Bewertung der Datenschutzverletzung

4.2.1 [All] Incident Response Coordinator MUSS jeden REG10-Eintrag innerhalb von 24 Stunden nach Eingang als Nicht-PII-Ereignis, vermuteten Datenschutzvorfall, bestätigten Datenschutzvorfall, bestätigte Verletzung des Schutzes personenbezogener Daten, Datenschutzvorfall im Finanzsektor, schwerwiegenden Vorfall im Finanzsektor, erhebliche Cyberbedrohung oder Eintrag mit ausstehender Klassifizierung klassifizieren.

4.2.2 [Conditional] Information Security Lead MUSS betroffene Dienste, Kunden, Gegenparteien, Transaktionen, Serviceausfall, geografische Ausbreitung, Datenverlust, Kritikalität des Dienstes und wirtschaftliche Auswirkungen in REG10 bewerten, wenn ein Datenschutzvorfall Finanzsektordienste oder -betriebsabläufe betreffen kann.

4.2.3 [Both] Privacy Lead / PIMS Manager MUSS die betroffene Verarbeitungstätigkeit, Kategorien personenbezogener Daten, Kategorien betroffener Personen, Systeme, Auftragsverarbeiter, Unterauftragsverarbeiter, Übermittlungsorte und Datenschutzrisiken in REG02, REG04, REG08, REG09 und REG10 identifizieren, bevor die Entscheidung über die Meldung der Datenschutzverletzung finalisiert wird.

4.2.4 [Controller] Data Protection Officer / Privacy Advisor MUSS das Risiko für betroffene Personen für jede bestätigte oder vernünftigerweise vermutete Verletzung des Schutzes personenbezogener Daten bewerten und die Meldeempfehlung, Risikobegründung und Beratung in REG10 erfassen, bevor die externe Meldeentscheidung getroffen wird.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager MUSS die Zuweisung der Verantwortung gemeinsam Verantwortlicher für Vorfälle in REG08 und REG10 innerhalb von 24 Stunden nach Identifizierung gemeinsamer Verantwortung für eine vermutete oder bestätigte Verletzung des Schutzes personenbezogener Daten erfassen.

4.2.6 [Processor] Privacy Lead / PIMS Manager MUSS Kundenweisungen, vertragliche Meldepflichten und Mitwirkungspflichten in REG08 und REG10 innerhalb von 24 Stunden bewerten, nachdem eine vermutete oder bestätigte Verletzung des Schutzes personenbezogener Daten eine als Auftragsverarbeiter durchgeführte Verarbeitung betrifft.

4.2.7 [Subprocessor] Vendor / Procurement Owner MUSS die vorgelagerte Meldekette und die erforderliche Nachweisweiterleitung in REG08 und REG10 innerhalb von 24 Stunden identifizieren, nachdem ein vermuteter oder bestätigter Datenschutzvorfall eine als Unterauftragsverarbeiter durchgeführte Verarbeitung betrifft.

[... Abschnitte 4.3–8 sind in dieser Vorschau nicht enthalten. Erwerben Sie das vollständige Dokument, um auf den gesamten Inhalt zuzugreifen. ...]

9. Ausnahmen

9.1.1 [All] Privacy Lead / PIMS Manager MUSS jede Ausnahme von dieser Richtlinie vor Umsetzung in REG12 erfassen, oder innerhalb von 24 Stunden nach einer Notfallmaßnahme, wenn eine vorherige Genehmigung nicht machbar war.

9.1.2 [Conditional] Top Management MUSS jede Ausnahme genehmigen, die den Zeitpunkt der Meldung von Verletzungen, den Zeitpunkt der Finanzsektor-Berichterstattung, öffentliche Kommunikation, Kundenverpflichtungen, Nachweissicherung oder das Risiko für betroffene Personen wesentlich beeinflusst, bevor der Vorfall abgeschlossen wird; Genehmigungsnachweise sind in REG10 und REG12 aufzubewahren.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor MUSS Beratung zu jeder verzögerten Meldung, Entscheidung zur Nichtmeldung, Berichtsausnahme oder außergewöhnlichen Kommunikationsweise vor Abschluss des Vorfalls dokumentieren; Beratung ist in REG10 aufzubewahren.

9.1.4 [Both] Vendor / Procurement Owner MUSS Ausnahmen von Lieferanten, Auftragsverarbeitern, Unterauftragsverarbeitern, Kunden oder ausgelagerten Anbietern, die die Reaktion auf Vorfälle im Finanzsektor betreffen, innerhalb von fünf Geschäftstagen nach Identifizierung der Ausnahme in REG08 und REG12 erfassen.

9.1.5 [All] Privacy Lead / PIMS Manager MUSS offene Ausnahmen von dieser Richtlinie mindestens monatlich bis zum Abschluss überprüfen; der Überprüfungsstatus ist in REG12 aufzubewahren.

10. Durchsetzung

10.1.1 [All] Process Owner / Business Owner MUSS das Versäumnis, einen vermuteten Datenschutzvorfall im Finanzsektor zu melden, Nachweise zu sichern, zugewiesene Maßnahmen zu befolgen oder bei der Bewertung einer Datenschutzverletzung mitzuwirken,

innerhalb von zwei Geschäftstagen nach Entdeckung an Privacy Lead / PIMS Manager eskalieren; Nachweise sind in REG12 aufzubewahren.

10.1.2 [Both] Incident Response Coordinator MUSS verspätete Meldung, versäumte Klassifizierung, fehlende Nachweise, versäumte Eskalation oder überfällige Eindämmungsmaßnahmen innerhalb eines Geschäftstags nach Identifizierung des Problems an Privacy Lead / PIMS Manager eskalieren; Nachweise sind in REG10 und REG12 aufzubewahren.

10.1.3 [Both] Privacy Lead / PIMS Manager MUSS eine REG12-Nichtkonformität erfassen, wenn ein Verstoß gegen diese Richtlinie den Vorfallseingang, die Triage, Eindämmung, Benachrichtigung, Berichterstattung, Nachweisintegrität, Kommunikation oder Korrekturmaßnahmen betrifft.

10.1.4 [Both] Vendor / Procurement Owner MUSS Mängelbehebung durch Lieferanten, Auftragsverarbeiter, Unterauftragsverarbeiter oder ausgelagerte Anbieter über REG08 und REG12 innerhalb von fünf Geschäftstagen einleiten, wenn eine Drittpartei vereinbarte Pflichten zu Vorfällen, Verletzungen, Nachweisen oder Berichterstattung nicht erfüllt.

10.1.5 [Conditional] Top Management MUSS wesentliche oder wiederkehrende PII15-FS-Nichtkonformitäten bei der nächsten planmäßigen Managementbewertung überprüfen; Entscheidungen und erforderliche Maßnahmen sind in REG12 aufzubewahren.

10.1.6 [All] Privacy Lead / PIMS Manager MUSS innerhalb von 30 Kalendertagen Abhilfeschulungen in REG11 auslösen, wenn eine Richtlinien-Nichtkonformität Rollenbewusstsein, verspätete Meldung, Eskalationsversagen, Fehler bei der Nachweisbehandlung oder Kommunikationsversagen betrifft.

11. Überprüfung und Pflege

11.1.1 [Conditional] Privacy Lead / PIMS Manager MUSS diese Richtlinie mindestens jährlich überprüfen und das Überprüfungsergebnis, erforderliche Änderungen und den Genehmigungsstatus in REG12 erfassen.

11.1.2 [Conditional] Incident Response Coordinator MUSS innerhalb von 30 Kalendertagen nach Abschluss jedes Datenschutzvorfalls mit hoher Tragweite im Finanzsektor, jeder bestätigten Verletzung des Schutzes personenbezogener Daten, jedes schwerwiegenden Vorfalls im Finanzsektor oder jeder erheblichen Cyberbedrohung eine Nachprüfung dieser Richtlinie nach dem Vorfall auslösen; Überprüfungsnachweise sind in REG10 und REG12 aufzubewahren.

11.1.3 [Conditional] Privacy Lead / PIMS Manager MUSS diese Richtlinie innerhalb von 30 Kalendertagen nach Kenntnis einer wesentlichen Änderung rechtlicher, sektoraler, kundenbezogener, vertraglicher, auf Auftragsverarbeiter, Unterauftragsverarbeiter, Berichtsvorlagen, Berichtsfristen oder Übermittlungen bezogener Anforderungen an die Vorfallberichterstattung überprüfen; Überprüfungsnachweise sind in REG01, REG08, REG09 und REG12 aufzubewahren.

11.1.4 [Both] Internal Audit / Compliance Reviewer MUSS die Umsetzung dieser Richtlinie mindestens jährlich im Rahmen des PIMS-internen Auditprogramms überprüfen; Auditfeststellungen und Korrekturmaßnahmen sind in REG12 aufzubewahren.

11.1.5 [Conditional] Top Management MUSS Vorfalltrends, erhebliche Verletzungen, Berichtsleistung, überfällige Korrekturmaßnahmen und Wirksamkeit der Richtlinie während der planmäßigen Managementbewertung überprüfen; Ergebnisse sind in REG12 aufzubewahren.

11.1.6 [Conditional] Privacy Lead / PIMS Manager MUSS die Ersetzungsbeziehung zwischen PII15-FS und PII15 mindestens jährlich und nach jeder Änderung des PIMS-Geltungsbereichs überprüfen, um zu verifizieren, dass beide Richtlinien nicht für denselben Finanzsektor-

Geltungsbereich umgesetzt sind; Überprüfungsnachweise sind in REG03 und REG12 aufzubewahren.

12. Verwandte Richtlinien

12.1 Diese Richtlinie sollte zusammen gelesen werden mit:

12.2 PII01 - Richtlinie zum Datenschutz-Informationsmanagementsystem

12.3 PII02 - Richtlinie zu Datenschutzrollen, Verantwortlichkeiten und Rechenschaftspflicht

12.4 PII03 - Richtlinie zum Verzeichnis der PII-Verarbeitung und zu Rechtsgrundlagen

12.5 PII04 - Richtlinie zu Datenschutzhinweis und Transparenz

12.6 PII06 - Richtlinie zum Management der Rechte betroffener Personen

12.7 PII07 - Richtlinie zur Datenschutz-Risikobeurteilung und DPIA

12.8 PII08 - Richtlinie zu Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

12.9 PII10 - Richtlinie zur Aufbewahrung, Löschung und Entsorgung von PII

12.10 PII12 - Richtlinie zum Datenschutzmanagement für Auftragsverarbeiter, Unterauftragsverarbeiter und Dritte

12.11 PII13 - Richtlinie zu internationalen PII-Übermittlungen

12.12 PII14 - Richtlinie zu PII-Sicherheit und Zugriffskontrolle

12.13 PII16 - Richtlinie zu Datenschutzschulung, Sensibilisierung und Kompetenz

12.14 PII17 - Richtlinie zum Management dokumentierter PIMS-Informationen und Nachweise

12.15 PII18 - Richtlinie zu PIMS-Überwachung, Audit und Verbesserung

12.16 PII23 - Richtlinie für Cloud-PII-Auftragsverarbeiter, soweit Pflichten von Cloud-Auftragsverarbeitern im Finanzsektor im Geltungsbereich liegen

12.17 PII15 - Richtlinie zum Management von PII-Vorfällen und Verletzungen des Schutzes personenbezogener Daten ist die Basisrichtlinie für Vorfälle und Verletzungen. PII15-FS ist eine Ersatzvariante für PII15 im Finanzsektor. PII15 und PII15-FS dürfen nicht gleichzeitig für denselben PIMS-Geltungsbereich, dieselbe Geschäftseinheit, dasselbe Produkt, dieselbe Kundenumgebung, denselben regulierten Dienst oder dieselbe Nachweisgrenze umgesetzt werden.

13. Referenzstandards und Rahmenwerke

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].