					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: PII15-FS					Dokumenttitel: **Politik for håndtering af PII-hændelser og brud på persondatasikkerheden i den finansielle sektor**						
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025			Dokumentejer:						
X	Politik		Standard		Procedure		Formular		Register		Andet

Revisionshistorik				
Revisionsnummer	**Revisionsdato**	**Ændringer**	**Gennemgået af**	**Procesejer**

Godkendelser			
Navn	**Stilling**	**Dato**	**Underskrift**

Tilpasset relevante standarder og regler

Standard / regulering	Klausul / kontrol / artikel	Anvendelighed	Dækningstype	Kommentar
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	PIMS-kommunikation og dokumenteret hændelsesbevismateriale
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Operationel styring, risikovurdering vedrørende databeskyttelse og sammenhæng til risikobehandling
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Overvågning, evaluering, afvigelser, korrigerende handling og forbedring
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Planlægning og forberedelse af hændelsesstyring for behandling af PII
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Respons på informationssikkerhedshændelser, der involverer PII
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Retlige, lovbestemte, regulatoriske og kontraktlige krav samt beskyttelse af registreringer
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Databehandlerens kundeaftale og understøttelse af kundens forpligtelser
GDPR	Article 5(2); Article 24	Controller	Supporting	Ansvarlighed og den dataansvarliges ansvar
GDPR	Article 26	Joint Controller	Supporting	Koordinering af ansvar for hændelser mellem fælles dataansvarlige
GDPR	Article 28	Both	Supporting	Databehandlerbistand og kontraktlige forpligtelser for databehandlere
GDPR	Article 32	Both	Supporting	Behandlingssikkerhed og kapacitet til detektion af brud
GDPR	Article 33	Both	Primary	Anmeldelse af brud på persondatasikkerheden og dokumentation af brud
GDPR	Article 34	Controller	Primary	Kommunikation af brud på persondatasikkerheden til berørte registrerede

GDPR	Article 39	Conditional	Supporting	DPO-rådgivning, overvågning, samarbejde og understøttelse af kontaktpunkt
DORA Regulation (EU) 2022/2554	Article 17	Conditional	Primary	Proces for håndtering af IKT-relaterede hændelser for omfattede finansielle enheder
DORA Regulation (EU) 2022/2554	Article 18	Conditional	Primary	Klassifikationskriterier for IKT-relaterede hændelser og væsentlige cybertrusler
DORA Regulation (EU) 2022/2554	Article 19	Conditional	Primary	Rapportering af større IKT-relaterede hændelser og underretning om væsentlige cybertrusler
DORA Regulation (EU) 2022/2554	Article 20	Conditional	Supporting	Rapportindhold, frister, skabeloner og procedurer
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Rapportering af væsentlige hændelser, hvor relevant
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Principper for informationssikkerhed og efterlevelse af databeskyttelse
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Ansvar for håndtering af PII-hændelser og rapportering af hændelser
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Hændelsesplanlægning, vurdering, respons, læring og indsamling af bevismateriale
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Livscyklus for hændelsesstyringsprocessen
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Hændelsespolitik, plan, bevidstgørelse, test og læring
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9;	Both	Supporting	Drift vedrørende detektion, underretning, triage, analyse, respons og rapportering

	Clause 10; Clause 11; Clause 12			
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Forventninger til underretning fra offentlig cloud-databehandler og registrering af brud

1. Omfang

1.1 Denne politik fastsætter kravene til at identificere, rapportere, triagere, klassificere, vurdere, inddæmme, underrette om, dokumentere, lukke og forbedre på baggrund af PII-hændelser og brud på persondatasikkerheden inden for PIMS-omfang i den finansielle sektor.

1.2 **Implementeringsmeddelelse:** Denne politik er en erstatningsvariant for PII15 for den finansielle sektor. Den må ikke implementeres samtidigt med PII15 for samme PIMS-omfang, forretningsenhed, produkt, kundemiljø, regulerede tjeneste eller bevisgrænse. Organisationer skal vælge enten PII15 eller PII15-FS for samme omfang for at undgå dobbelte hændelsesstyringsforpligtelser, dobbelte registre og dobbelt arbejde med revisionsbevismateriale.

1.3 Denne politik gælder for:

1.3.1 organisationen, når den handler som dataansvarlig for PII i en finansiel sektor-kontekst;

1.3.2 organisationen, når den handler som fælles dataansvarlig, hvor koordinering af ansvar for hændelser eller brud er påkrævet;

1.3.3 organisationen, når den handler som databehandler for kunder i den finansielle sektor;

1.3.4 organisationen, når den handler som underdatabehandler for kunder i den finansielle sektor eller upstream-databehandlere;

1.3.5 systemer, applikationer, tjenester, processer, leverandører, databehandlere, underdatabehandlere og tredjeparter, der behandler, lagrer, transmitterer, understøtter, tilgår eller på anden måde påvirker PII inden for PIMS-omfanget for den finansielle sektor.

1.4 Denne politik anvender REG10 - PII Incident and Breach Register som det primære evidensobjekt for håndtering af PII-hændelser og brud på persondatasikkerheden i den finansielle sektor.

1.5 Denne politik anvender understøttende evidensobjekter som følger:

1.5.1 REG01 for PIMS-omfang, relevante interesserede parter samt sektor-, kunde-, kontrakt- og rapporteringskontekst.

1.5.2 REG02 for berørte behandlingsaktiviteter, PII-kategorier, kategorier af registrerede, formål, systemer og tjenester.

1.5.3 REG03 for Anvendelseserklæring og opdateringer af kontrolanvendelighed, herunder erstatning af PII15 med PII15-FS for samme omfang.

1.5.4 REG04 for sammenhæng til risikovurdering vedrørende databeskyttelse, DPIA, restrisiko og risikobehandling.

1.5.5 REG08 for bevismateriale vedrørende grænseflader for hændelser med databehandlere, underdatabehandlere, kunder, leverandører og tredjeparter.

1.5.6 REG09 for sammenhæng til internationale overførsler, når en hændelse påvirker grænseoverskridende behandling.

1.5.7 REG11 for bevismateriale vedrørende træning, bevidstgørelse og kompetence i hændelseshåndtering.

1.5.8 REG12 for bevismateriale vedrørende revision, afvigelser, korrigerende handling, ledelsens gennemgang og forbedring.

1.6 Denne politik bygger på relaterede PIMS-politikker for specialiserede kontroller:

1.6.1 PII03 regulerer fortegnelse over behandlingsaktiviteter og registreringer af behandlingsgrundlag.

1.6.2 PII04 regulerer privatlivsmeddelelse og gennemsigtighedskontroller uden for brudspecifik kommunikation.

1.6.3 PII06 regulerer rettighedsanmodninger fra registrerede, der opstår før, under eller efter en hændelse.

1.6.4 PII07 regulerer metodik for risikovurdering vedrørende databeskyttelse og DPIA.

1.6.5 PII08 regulerer kontroller for databeskyttelse gennem design og standardindstillinger.

1.6.6 PII10 regulerer kontroller for opbevaring, sletning og bortskaffelse.

1.6.7 PII12 regulerer kontroller for databeskyttelsesrelationer med databehandlere, underdatabehandlere, leverandører og tredjeparter.

1.6.8 PII13 regulerer mekanismer for internationale overførsler af PII og registreringer af overførselsrisici.

1.6.9 PII14 regulerer forebyggende og detekterende PII-sikkerheds- og adgangskontroller.

1.6.10 PII16 regulerer træning, bevidstgørelse og kompetence vedrørende databeskyttelse.

1.6.11 PII17 regulerer dokumenteret information og styring af bevismateriale.

1.6.12 PII18 regulerer overvågning, intern revision, ledelsens gennemgang, afvigelser, korrigerende handling og løbende forbedring.

1.6.13 PII23 regulerer kontroller for cloud-PII-databehandlere, hvor cloud-databehandlerforpligtelser er omfattet.

1.7 I denne politik:

1.7.1 "PII-hændelse" betyder en mistænkt eller bekræftet hændelse, der har påvirket, kan have påvirket eller med rimelighed kunne påvirke fortroligheden, integriteten, tilgængeligheden, den lovlige behandling eller den autoriserede håndtering af PII.

1.7.2 "brud på persondatasikkerheden" betyder en bekræftet PII-hændelse, der involverer uautoriseret, ulovlig, utilsigtet eller ikke tilsigtet tilintetgørelse, tab, ændring, videregivelse af, adgang til, utilgængelighed af eller kompromittering af PII.

1.7.3 "PII-hændelse i den finansielle sektor" betyder en PII-hændelse, der påvirker, kan påvirke eller med rimelighed er forbundet med regulerede finansielle tjenester, kunder i den finansielle sektor, finansielle modparter, finansielle transaktioner, finansielle operationer eller behandling af PII i den finansielle sektor.

1.7.4 "større hændelse i den finansielle sektor" betyder en PII-hændelse i den finansielle sektor eller relateret IKT-hændelse, der opfylder dokumenterede væsentligheds- eller rapporteringskriterier i REG10.

1.7.5 "væsentlig cybertrussel" betyder en cybertrussel registreret i REG10, som væsentligt kan påvirke omfattede finansielle sektortjenester, PII-behandling, kunder, modparter eller operationer.

1.7.6 "vurdering af brud" betyder den dokumenterede evaluering af, om en PII-hændelse er et brud på persondatasikkerheden, hvilke PII og hvilke registrerede der er berørt, hvilke risici der kan opstå, hvilke anmeldelser, underretninger eller kommunikationer der kræves, og hvilke afhjælpende handlinger der er nødvendige.

1.7.7 "kendskab" betyder det tidspunkt, hvor organisationen har en rimelig grad af sikkerhed for, at en sikkerheds- eller databeskyttelseshændelse er indtruffet, og at PII er blevet eller kan være blevet kompromitteret.

1.7.8 "PII-hændelse med stor betydning i den finansielle sektor" betyder en PII-hændelse, der involverer højrisikobehandling, særlige kategorier af personoplysninger eller meget følsomme PII, PII i stor skala, sårbare personer, regulerede kunder, væsentlige driftsafbrydelser, finansielle modparter, finansielle transaktioner, påvirkning i flere jurisdiktioner, kompromittering af privilegeret adgang, offentlig eksponering, ransomware, utilgængelighed af tjenester eller væsentlig operationel, kunde-, finansiel eller omdømmemæssig påvirkning.

1.7.9 "væsentlig ændring i hændelsesoplysninger" betyder nye eller ændrede oplysninger, der påvirker hændelsens omfang, alvorlighed, PII-kategorier, påvirkning af registrerede,

tjenestepåvirkning, klassifikation for den finansielle sektor, underretningsbeslutning, kundepåvirkning, rodårsag, inddæmning, genopretning, korrigerende handling eller eksterne rapporteringsforpligtelser.

2. Formål

2.1 Formålet med denne politik er at sikre, at PII-hændelser og brud på persondatasikkerheden i finansielle sektorkontekster håndteres ensartet, hurtigt, lovligt, sikkert og med revisionsklart bevismateriale.

2.2 Denne politik understøtter ansvarlighed ved at kræve, at PII-hændelser og brud på persondatasikkerheden i den finansielle sektor registreres i REG10 og knyttes til berørte behandlingsregistreringer, privatlivsrisici, databehandler- og underdatabehandlerrelationer, overførselsregistreringer, korrigerende handlinger, træningsregistreringer, rapporteringsbeslutninger for den finansielle sektor og bevismateriale til ledelsens gennemgang, hvor dette udløses.

2.3 Denne politik sikrer, at forpligtelser for dataansvarlig, fælles dataansvarlig, databehandler og underdatabehandler håndteres gennem særskilte anvendelighedsregler, samtidig med at der opretholdes én integreret evidensmodel for hændelser og brud i den finansielle sektor.

3. Mål

3.1 Målene med denne politik er at:

3.1.1 sikre, at mistænkte PII-hændelser i den finansielle sektor rapporteres og registreres hurtigt;

3.1.2 sikre, at PII-hændelser i den finansielle sektor triageres og klassificeres efter ensartede kriterier for databeskyttelse, sikkerhed, drift og sektorforhold;

3.1.3 sikre, at vurderinger af brud tager højde for berørte PII, registrerede, systemer, tjenester, behandlingsaktiviteter, databehandlere, underdatabehandlere, overførsler, risici, kunder, modparter og afhjælpende handlinger;

3.1.4 sikre, at beslutninger om anmeldelse fra dataansvarlig og kommunikation til registrerede dokumenteres;

3.1.5 sikre, at databehandleres og underdatabehandleres underretninger om brud til kunder eller upstream-parter sker uden unødig forsinkelse og i overensstemmelse med gældende aftaler;

3.1.6 sikre, at rapporteringsudløsere for den finansielle sektor evalueres, dokumenteres og spores, hvor det er relevant;

3.1.7 sikre, at bevismateriale bevares og beskyttes under hændelseshåndtering;

3.1.8 sikre, at inddæmning, fjernelse, genopretning og validering spores via REG10;

3.1.9 sikre, at væsentlige cybertrusler og større hændelser i den finansielle sektor dirigeres til relevante beslutnings- og rapporteringsarbejdsgange;

3.1.10 sikre, at læring fra hændelser resulterer i korrigerende handling, træning, kontrolforbedring og ledelsens gennemgang;

3.1.11 sikre, at hændelses- og brudregistreringer er tilgængelige for revision, ledelsens gennemgang, kundedokumentation og regulatorisk gennemgang, hvor det er relevant;

3.1.12 sikre, at PII15-FS erstatter PII15 for samme finansielle sektor-omfang og ikke duplikerer PII15-evidensarbejde.

4. Politikkerklæringer

4.1 Aktivering af variant, beredskab og modtagelse

4.1.1 [Conditional] Privacy Lead / PIMS Manager SKAL dokumentere aktivering af PII15-FS i REG01 og REG03, før denne politik anvendes for et PIMS-omfang i den finansielle sektor.

4.1.2 [Conditional] Privacy Lead / PIMS Manager SKAL dokumentere i REG03 og REG12, at PII15 ikke er implementeret samtidigt for samme PIMS-omfang i den finansielle sektor, før PII15-FS godkendes.

4.1.3 [All] Incident Response Coordinator SKAL registrere enhver rapporteret eller detekteret mistænkt PII-hændelse i den finansielle sektor i REG10 inden for én arbejdsdag efter modtagelse eller tidligere, hvor en gældende underretnings-, kunde- eller rapporteringsfrist kan blive udløst.

4.1.4 [Conditional] Privacy Lead / PIMS Manager SKAL vedligeholde kriterier for håndtering af PII-hændelser og brud på persondatasikkerheden i den finansielle sektor i REG10 mindst årligt og efter enhver væsentlig ændring i PIMS-omfang, retlig kontekst, kundeforpligtelser, kontraktlige forpligtelser, sektorbestemt rapporteringskontekst eller højrisikobehandling.

4.1.5 [Both] Information Security Lead SKAL bekræfte krav til bevarelse af hændelsesbevismateriale i REG10 inden for 24 timer efter, at en mistænkt hændelse påvirker et system, en tjeneste eller en applikation, der behandler PII.

4.1.6 [Conditional] Vendor / Procurement Owner SKAL vedligeholde krav til hændelseskontakt og routing af bevismateriale for tredjeparter i den finansielle sektor i REG08 før onboarding og mindst årligt for omfattede databehandlere, underdatabehandlere, leverandører og udliciterede rapporteringsudbydere.

4.2 Klassifikation og vurdering af brud

4.2.1 [All] Incident Response Coordinator SKAL klassificere hver REG10-post inden for 24 timer efter modtagelse som en ikke-PII-hændelse, mistænkt PII-hændelse, bekræftet PII-hændelse, bekræftet brud på persondatasikkerheden, PII-hændelse i den finansielle sektor, større hændelse i den finansielle sektor, væsentlig cybertrussel eller post med afventende klassifikation.

4.2.2 [Conditional] Information Security Lead SKAL vurdere berørte tjenester, klienter, modparter, transaktioner, nedetid for tjenester, geografisk udbredelse, datatab, tjenestekritikalitet og økonomisk påvirkning i REG10, når en PII-hændelse kan påvirke finansielle sektortjenester eller operationer.

4.2.3 [Both] Privacy Lead / PIMS Manager SKAL identificere den berørte behandlingsaktivitet, PII-kategorier, kategorier af registrerede, systemer, databehandlere, underdatabehandlere, overførselslokationer og privatlivsrisici i REG02, REG04, REG08, REG09 og REG10, før beslutningen om anmeldelse/underretning ved brud færdiggøres.

4.2.4 [Controller] Data Protection Officer / Privacy Advisor SKAL vurdere risikoen for berørte registrerede for hvert bekræftet eller med rimelighed mistænkt brud på persondatasikkerheden og registrere underretningsanbefalingen, risikobegrundelsen og rådgivningen i REG10, før den eksterne underretningsbeslutning træffes.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager SKAL registrere ansvarsfordelingen for hændelser mellem fælles dataansvarlige i REG08 og REG10 inden for 24 timer efter identificering af delt ansvar for et mistænkt eller bekræftet brud på persondatasikkerheden.

4.2.6 [Processor] Privacy Lead / PIMS Manager SKAL vurdere kundens instrukser, kontraktlige underretningsforpligtelser og samarbejdsforpligtelser i REG08 og REG10 inden for 24 timer efter, at et mistænkt eller bekræftet brud på persondatasikkerheden påvirker behandling udført som databehandler.

4.2.7 [Subprocessor] Vendor / Procurement Owner SKAL identificere upstream-underretningskæden og påkrævet routing af bevismateriale i REG08 og REG10 inden for 24 timer efter, at en mistænkt eller bekræftet PII-hændelse påvirker behandling udført som underdatabehandler.

[... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ...]

9. Undtagelser

9.1.1 [All] Privacy Lead / PIMS Manager SKAL registrere enhver undtagelse fra denne politik i REG12 før implementering eller inden for 24 timer efter nødhandling, hvor forudgående godkendelse ikke var mulig.

9.1.2 [Conditional] Top Management SKAL godkende enhver undtagelse, der væsentligt påvirker timing for anmeldelse/underretning ved brud, timing for rapportering i den finansielle sektor, offentlig kommunikation, kundeforpligtelse, bevarelse af bevismateriale eller risiko for registrerede, før hændelsen lukkes, med godkendelsesbevismateriale opbevaret i REG10 og REG12.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor SKAL dokumentere rådgivning for enhver forsinket underretning, beslutning om ingen underretning, rapporteringsundtagelse eller ekstraordinær kommunikationstilgang før hændelseslukning, med rådgivning opbevaret i REG10.

9.1.4 [Both] Vendor / Procurement Owner SKAL registrere undtagelser hos leverandør, databehandler, underdatabehandler, kunde eller udliciteret udbyder, der påvirker hændelsesrespons i den finansielle sektor, i REG08 og REG12 inden for fem arbejdsdage efter identificering af undtagelsen.

9.1.5 [All] Privacy Lead / PIMS Manager SKAL gennemgå åbne undtagelser fra denne politik mindst månedligt indtil lukning, med gennemgangsstatus opbevaret i REG12.

10. Håndhævelse

10.1.1 [All] Process Owner / Business Owner SKAL eskalere manglende rapportering af en mistænkt PII-hændelse i den finansielle sektor, manglende bevarelse af bevismateriale, manglende efterlevelse af tildelte handlinger eller manglende samarbejde om vurdering af brud til Privacy Lead / PIMS Manager inden for to arbejdsdage efter opdagelse, med bevismateriale opbevaret i REG12.

10.1.2 [Both] Incident Response Coordinator SKAL eskalere sen rapportering, manglende klassifikation, manglende bevismateriale, manglende eskalering eller forsinket inddæmningshandling til Privacy Lead / PIMS Manager inden for én arbejdsdag efter identificering af problemet, med bevismateriale opbevaret i REG10 og REG12.

10.1.3 [Both] Privacy Lead / PIMS Manager SKAL registrere en REG12-afvigelse, når et brud på denne politik påvirker hændelsesmodtagelse, triage, inddæmning, underretning, rapportering, bevismaterialets integritet, kommunikation eller korrigerende handling.

10.1.4 [Both] Vendor / Procurement Owner SKAL iværksætte afhjælpning hos leverandør, databehandler, underdatabehandler eller udliciteret udbyder via REG08 og REG12 inden for fem arbejdsdage, når en tredjepart ikke opfylder aftalte hændelses-, brud-, evidens- eller rapporteringsforpligtelser.

10.1.5 [Conditional] Top Management SKAL gennemgå væsentlige eller tilbagevendende PII15-FS-afvigelser ved næste planlagte ledelsesgennemgang, med beslutninger og påkrævede handlinger opbevaret i REG12.

10.1.6 [All] Privacy Lead / PIMS Manager SKAL udløse afhjælpende træning i REG11 inden for 30 kalenderdage, når en politikafvigelse involverer rollebevidsthed, sen rapportering, eskaleringssvigt, fejlhåndtering af bevismateriale eller kommunikationssvigt.

11. Gennemgang og vedligeholdelse

11.1.1 [Conditional] Privacy Lead / PIMS Manager SKAL gennemgå denne politik mindst årligt og registrere gennemgangsresultatet, påkrævede ændringer og godkendelsesstatus i REG12.

11.1.2 [Conditional] Incident Response Coordinator SKAL udløse en efterhændelsesgennemgang af denne politik inden for 30 kalenderdage efter lukning af enhver PII-hændelse med stor betydning i den finansielle sektor, bekræftet brud på persondatasikkerheden, større hændelse i den finansielle sektor eller væsentlig cybertrussel, med gennemgangsbevismateriale opbevaret i REG10 og REG12.

11.1.3 [Conditional] Privacy Lead / PIMS Manager SKAL gennemgå denne politik inden for 30 kalenderdage efter at være blevet bekendt med en væsentlig ændring i retlige, sektorbestemte, kunde-, kontraktlige, databehandler-, underdatabehandler-, rapporteringsskabelon-, rapporteringsfrist- eller overførselsrelaterede krav til hændelsesrapportering, med gennemgangsbevismateriale opbevaret i REG01, REG08, REG09 og REG12.

11.1.4 [Both] Internal Audit / Compliance Reviewer SKAL gennemgå implementeringen af denne politik mindst årligt gennem PIMS-programmet for intern revision, med revisionskonstateringer og korrigerende handlinger opbevaret i REG12.

11.1.5 [Conditional] Top Management SKAL gennemgå hændelsestendenser, væsentlige brud, rapporteringspræstation, forsinkede korrigerende handlinger og politikkens effektivitet under planlagt ledelsesgennemgang, med output opbevaret i REG12.

11.1.6 [Conditional] Privacy Lead / PIMS Manager SKAL gennemgå erstatningsforholdet mellem PII15-FS og PII15 mindst årligt og efter enhver ændring i PIMS-afgrænsning for at verificere, at begge politikker ikke er implementeret for samme finansielle sektor-omfang, med gennemgangsbevismateriale opbevaret i REG03 og REG12.

12. Relaterede politikker

12.1 Denne politik bør læses sammen med:

12.1.1 PII01 - Politik for ledelsessystem for privatlivsinformation

12.1.2 PII02 - Politik for roller, ansvar og ansvarlighed vedrørende databeskyttelse

12.1.3 PII03 - Politik for fortegnelse over PII-behandlingsaktiviteter og behandlingsgrundlag

12.1.4 PII04 - Politik for privatlivsmeddelelse og gennemsigtighed

12.1.5 PII06 - Politik for styring af registreredes rettigheder

12.1.6 PII07 - Politik for risikovurdering vedrørende databeskyttelse og DPIA

12.1.7 PII08 - Politik for databeskyttelse gennem design og standardindstillinger

12.1.8 PII10 - Politik for opbevaring, sletning og bortskaffelse af PII

12.1.9 PII12 - Politik for styring af databehandlere, underdatabehandlere og tredjeparter vedrørende databeskyttelse

12.1.10 PII13 - Politik for internationale overførsler af PII

12.1.11 PII14 - Politik for PII-sikkerhed og adgangskontrol

12.1.12 PII16 - Politik for træning, bevidstgørelse og kompetence vedrørende databeskyttelse

12.1.13 PII17 - Politik for PIMS-dokumenteret information og styring af bevismateriale

12.1.14 PII18 - Politik for PIMS-overvågning, revision og forbedring

12.1.15 PII23 - Politik for cloud-PII-databehandlere, hvor cloud-databehandlerforpligtelser i den finansielle sektor er omfattet

12.2 PII15 - Politik for håndtering af PII-hændelser og brud på persondatasikkerheden er baselinepolitikken for hændelser og brud. PII15-FS er en erstatningsvariant for PII15 for den finansielle sektor. PII15 og PII15-FS må ikke implementeres samtidigt for samme PIMS-omfang, forretningsenhed, produkt, kundemiljø, regulerede tjeneste eller bevisgrænse.

13. Referencestandarder og rammeværker

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].