					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: PII16					Dokumenttitel: **Politik for træning, bevidstgørelse og kompetence vedrørende databeskyttelse**						
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**

Juridisk meddelelse (ophavsret og brugsbegrænsninger)

(C) 2025 Clarysec LLC. All rights reserved.

Dette dokument er Clarysec LLC's intellektuelle ejendom. Ingen del af dette dokument må kopieres, genbruges, distribueres eller ændres til kommercielle eller implementeringsmæssige formål uden udtrykkelig skriftlig tilladelse.
Uautoriseret brug er strengt forbudt og kan medføre retslige skridt.
For licensiering kontakt: info@clarysec.com

Tilpasset relevante standarder og regler

Standard / regulering	Klausul / kontrol / artikel	Anvendelighed	Dækningstype	Kommentar
ISO/IEC 27701:2025	Clause 7.2; Clause 7.3	Both	Primary	Kompetence og bevidstgørelse
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Kommunikation og dokumenteret bevismateriale
ISO/IEC 27701:2025	Clause 8.1; Clause 9.1; Clause 10.2	Both	Supporting	Operationel styring, måling og forbedring
ISO/IEC 27701:2025	Annex A.3.17	Both	Primary	Bevidstgørelse, uddannelse og træning vedrørende PII-behandling
GDPR	Article 5(2); Article 24; Article 28; Article 32; Article 39	Both	Supporting	Ansvarlighed, databehandlerstyring, sikkerhed og DPO-opgaver
ISO/IEC 27001:2022	Clause 7.2; Clause 7.3; Annex A control 6.3	Both	Supporting	Kompetence, bevidstgørelse og træning
ISO/IEC 27002:2022	Control 6.3	Both	Supporting	Vejledning om bevidstgørelse, uddannelse og træning
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Informationssikkerhed og efterlevelse af databeskyttelseskrav

1. Omfang

1.1 Denne politik fastlægger organisationens krav til træning, bevidstgørelse og kompetence vedrørende databeskyttelse inden for Privacy Information Management System.

1.2 Denne politik gælder for personale, kontrahenter, midlertidigt personale, relevante tredjeparter, databehandlere, underdatabehandlere og andre interessenter, hvis arbejde kan påvirke PII-behandling, PIMS-performance, registreredes rettigheder, risiko vedrørende databeskyttelse, informationssikkerhed relateret til PII, databehandlerinstrukser, PII-hændelser, dokumenterede oplysninger eller dokumentation for efterlevelse.

1.3 Denne politik gælder i kontekster for dataansvarlig, fælles dataansvarlig, databehandler og underdatabehandler.

1.4 Denne politik omfatter:

1.4.1 identifikation af målgrupper for træning i databeskyttelse;

1.4.2 onboarding-træning;

1.4.3 årlig genopfriskningstræning;

1.4.4 rollebaseret og hændelsesudløst træning;

1.4.5 bevismateriale for gennemført træning;

1.4.6 eskalering ved manglende gennemførelse;

1.4.7 gennemgang af træningseffektivitet;

1.4.8 dokumentation for træningsassurance for databehandlere, underdatabehandlere og tredjeparter.

1.5 Denne politik opretter ikke en særskilt træningsmatrix, et træningsdashboard, et HR-register, et kompetenceregister, et disciplinærregister eller et kundetræningsregister. Træningstildelinger, gennemførelser, påmindelser, kompetencebevismateriale og bevidstgørelsesbevismateriale registreres i REG11, mens undtagelser, eskaleringer, afvigelser, korrigerende handlinger og bevismateriale for gennemgang registreres i REG12. Dokumentation for træningsassurance for databehandlere, underdatabehandlere og tredjeparter registreres i REG08, hvor det er relevant.

1.6 Denne politik duplikerer ikke:

1.6.1 tildeling af rolleansvarlighed i PII02;

1.6.2 krav til fortegnelse over behandlingsaktiviteter og behandlingsgrundlag i PII03;

1.6.3 metodik for risikovurdering vedrørende databeskyttelse og DPIA i PII07;

1.6.4 kontrolporte for databeskyttelse gennem design i PII08;

1.6.5 livscyklusstyring af databehandlere i PII12;

1.6.6 drift af PII-sikkerhed og adgangsstyring i PII14;

1.6.7 arbejdsgang for PII-hændelser og brud på persondatasikkerheden i PII15;

1.6.8 styring af dokumenterede oplysninger i PII17;

1.6.9 overvågning, intern revision og forbedringsstyring i PII18.

2. Formål

2.1 Formålet med denne politik er at sikre, at personer, hvis arbejde påvirker PII-behandling, forstår deres ansvar for databeskyttelse, gennemfører passende træning efter en fastlagt kadence, opretholder rollerelevant kompetence og genererer revisionsbart bevismateriale for træning, bevidstgørelse og eskalering.

2.2 Denne politik understøtter ensartet PIMS-implementering ved at anvende REG11 som det primære evidensobjekt for træning og bevidstgørelse samt REG08, REG10 og REG12 som understøttende evidensobjekter.

3. Mål

3.1 Målene med denne politik er at:

3.1.1 definere målgrupper for træning i databeskyttelse;

3.1.2 definere krav til onboarding-træning;

3.1.3 definere krav til årlig genopfriskningstræning;

3.1.4 definere krav til rollebaseret træning i databeskyttelse;

3.1.5 registrere bevismateriale for gennemførelse i REG11;

3.1.6 eskalere manglende gennemførelse via REG12;

3.1.7 vedligeholde dokumentation for træningsassurance for databehandlere, underdatabehandlere og tredjeparter i REG08, hvor det er relevant;

3.1.8 gennemgå træningseffektivitet uden at oprette overdrevne metrikker eller duplikerende registre;

3.1.9 sikre, at træningsindhold forbliver tilpasset gældende PIMS-politikker og væsentlige databeskyttelsesforpligtelser.

4. Politikkerklæringer

4.1 Målgruppe og tildeling af træning

4.1.1 [All] Privacy Lead / PIMS Manager MUST definere målgruppekategorier for PIMS-træning i REG11, før hver årlig træningscyklus begynder.

4.1.2 [All] Process Owner / Business Owner MUST identificere personale, hvis opgaver omfatter PII-behandling, i REG11 før onboarding, rolletildeling eller væsentlig ændring af arbejdsopgaver.

4.1.3 [Conditional] System Owner / Application Owner MUST identificere brugere, der kræver træning i PII-systemer, privilegeret adgang eller administrativ træning i databeskyttelse, i REG11, før adgang aktiveres eller ændres væsentligt.

4.1.4 [Joint Controller] Privacy Lead / PIMS Manager MUST registrere fordeling af træningsansvar mellem fælles dataansvarlige i REG11 eller REG08, før fælles behandlingsaktivitet begynder eller ændres væsentligt.

4.1.5 [Conditional] Data Protection Officer / Privacy Advisor MUST identificere behov for udvidet træning i databeskyttelse i REG11, før træning tildeles roller, der håndterer højrisikobehandling, særlige kategorier af personoplysninger, registreredes rettigheder, DPIA'er, internationale overførsler eller vurdering af brud.

4.1.6 [All] Privacy Lead / PIMS Manager MUST registrere den tildelte træningsmålgruppe, træningstype, krævet gennemførelsesdato og evidensansvarlig i REG11, før hver årlig træningscyklus begynder.

4.2 Onboarding og årlig træningskadence

4.2.1 [All] Privacy Lead / PIMS Manager MUST tildele grundlæggende bevidstgørelsestræning i databeskyttelse i REG11 inden for 10 arbejdsdage efter onboarding for personale med adgang til PII eller PIMS-ansvar.

4.2.2 [All] Process Owner / Business Owner MUST sikre, at tildelt personale gennemfører onboarding-træning i databeskyttelse i REG11, før uovervåget adgang til PII godkendes, eller inden for 30 dage efter onboarding, alt efter hvad der indtræffer først.

4.2.3 [All] Privacy Lead / PIMS Manager MUST tildele årlig genopfriskningstræning i databeskyttelse i REG11 mindst én gang hver 12. måned.

4.2.4 [All] Process Owner / Business Owner MUST bekræfte status for gennemførelse af årlig genopfriskning for tildelt personale i REG11 senest på den offentliggjorte årlige forfaldsdato.

4.2.5 [Conditional] Privacy Lead / PIMS Manager MUST tildele målrettet genopfriskningstræning i REG11 inden for 30 dage efter en væsentlig ændring af en databeskyttelsespolitik, væsentlig ændring af en PIMS-proces, revisionskonstatering, gentagen træningsfejl eller relevant læring fra en PII-hændelse.

[... 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] Process Owner / Business Owner MUST registrere en anmodning om undtagelse fra træning i databeskyttelse i REG12, før en krævet gennemførelsesfrist forlænges.

9.1.2 [All] Privacy Lead / PIMS Manager MUST godkende eller afvise anmodninger om undtagelser fra træning i databeskyttelse i REG12, før undtagelsen træder i kraft.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor MUST rådgive om træningsundtagelser i REG12 før godkendelse, hvor undtagelsen påvirker højrisikobehandling, særlige kategorier af PII, håndtering af rettigheder, hændelseshåndtering, internationale overførsler eller certificeringsbevismateriale.

9.1.4 [Conditional] Top Management MUST godkende undtagelser fra træning i databeskyttelse i REG12 før aktivering, når undtagelsen påvirker gentagen manglende gennemførelse, privilegeret PII-adgang, PII-behandling med højt konsekvensniveau eller bevismateriale rettet mod tilsynsmyndigheder.

9.1.5 [All] Privacy Lead / PIMS Manager MUST definere undtagelsesejer, udløbsdato, kompenserende handling og gennemgangsdato i REG12, før en undtagelse fra træning i databeskyttelse godkendes.

9.1.6 [All] Process Owner / Business Owner MUST lukke eller forny godkendte undtagelser fra træning i databeskyttelse i REG12 før undtagelsens udløbsdato.

10. Håndhævelse

10.1.1 [All] Privacy Lead / PIMS Manager MUST registrere en træningsafvigelse i REG12 inden for fem arbejdsdage, når bevismateriale for obligatorisk træning i databeskyttelse mangler, er ufuldstændigt, er forfaldent eller ikke kan spores til REG11.

10.1.2 [All] Process Owner / Business Owner MUST sikre, at forfalden obligatorisk træning i databeskyttelse gennemføres eller eskaleres i REG11 eller REG12 inden for 10 arbejdsdage efter, at forfalden status er registreret.

10.1.3 [Conditional] System Owner / Application Owner MUST begrænse ny PII-adgang med højt konsekvensniveau i REG12, når krævet onboarding-træning eller rollebaseret træning i databeskyttelse fortsat ikke er gennemført efter eskalering.

10.1.4 [Processor] Vendor / Procurement Owner MUST eskalere manglende dokumentation for træningsassurance for databehandlere, underdatabehandlere eller ekstern arbejdsstyrke i REG08 og REG12 inden for fem arbejdsdage efter identifikation.

10.1.5 [Conditional] Incident Response Coordinator MUST knytte træningsrelaterede håndhævelsestiltag til REG10 inden for én arbejdsdag, når træningsfejlen har bidraget til en formodet eller bekræftet PII-hændelse.

10.1.6 [All] Internal Audit / Compliance Reviewer MUST verificere lukningsbevismateriale for korrigerende træningshandlinger i REG12 ved næste planlagte revision eller inden for 60 dage efter lukning, alt efter hvad der indtræffer først.

11. Gennemgang og vedligeholdelse

11.1.1 [All] Privacy Lead / PIMS Manager MUST gennemgå denne politik og træningsindhold mindst årligt og registrere resultatet af gennemgangen i REG11 eller REG12.

11.1.2 [All] Privacy Lead / PIMS Manager MUST gennemgå denne politik inden for 30 dage efter en væsentlig ændring af PIMS-omfang, databeskyttelseslovgivning, behandlingsaktiviteter, rollemodel, hændelseslæring, revisionskonstateringer eller resultater vedrørende træningseffektivitet.

11.1.3 [Conditional] Data Protection Officer / Privacy Advisor MUST gennemgå databeskyttelsesvæsentlige politikændringer i REG12 før godkendelse.

11.1.4 [All] Top Management MUST godkende væsentlige ændringer af denne politik i REG12 før offentliggørelse.

11.1.5 [All] Privacy Lead / PIMS Manager MUST opdatere træningsindhold og bevismateriale for tildeling i REG11 inden for 30 dage efter en godkendt væsentlig politikændring.

12. Relaterede politikker

12.1 Denne politik bør læses sammen med:

12.2 PII01 - Politik for Privacy Information Management System;

12.3 PII02 - Politik for privatlivsroller, ansvar og ansvarlighed;

12.4 PII03 - Politik for fortegnelse over PII-behandling og behandlingsgrundlag;

12.5 PII04 - Politik for privatlivsmeddelelse og gennemsigtighed;

12.6 PII05 - Politik for samtykke- og præferencestyring;

12.7 PII06 - Politik for håndtering af registreredes rettigheder;

12.8 PII07 - Politik for risikovurdering vedrørende databeskyttelse og DPIA;

12.9 PII08 - Politik for databeskyttelse gennem design og standardindstillinger;

12.10 PII09 - Politik for indsamling, brug, videregivelse og deling af PII;

12.11 PII10 - Politik for opbevaring, sletning og bortskaffelse af PII;

12.12 PII12 - Politik for styring af databeskyttelse hos databehandlere, underdatabehandlere og tredjeparter;

12.13 PII13 - Politik for international overførsel af PII;

12.14 PII14 - Politik for PII-sikkerhed og adgangsstyring;

12.15 PII15 - Politik for håndtering af PII-hændelser og brud på persondatasikkerheden;

12.16 PII17 - Politik for PIMS-dokumenterede oplysninger og evidensstyring;

12.17 PII18 - Politik for PIMS-overvågning, revision og forbedring.

13. Referencestandarder og rammeværker

13.1 ISO/IEC 27701:2025 - Clause 7.2; Clause 7.3; Clause 7.4. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 7.1.1; 7.1.2; 7.1.3; 11.1.1; 11.1.5].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.4; 4.6.5; 6.1.1; 6.1.2; 6.1.3; 6.1.5; 7.1.7; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 9.1.1; 9.1.2; 9.1.5; 10.1.1; 10.1.2; 10.1.6; 11.1.1; 11.1.2; 11.1.4].

13.3 ISO/IEC 27701:2025 - Annex A.3.17. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 11.1.5].

13.4 GDPR - Article 5(2); Article 24; Article 28; Article 32; Article 39. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.4.4; 4.5.3; 4.5.4; 4.5.5; 5.1.1; 5.1.3; 5.1.7; 6.1.2; 6.1.3; 6.1.4; 7.1.4; 7.1.5; 9.1.3; 9.1.4; 10.1.3; 10.1.4; 10.1.5; 11.1.3].

13.5 ISO/IEC 27001:2022 - Clause 7.2; Clause 7.3; Annex A control 6.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.3; 4.3.1; 4.3.5; 4.4.1; 4.4.3; 4.5.1; 4.5.2; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 6.1.1; 7.1.1; 7.1.2; 8.1.1; 8.1.2; 8.1.3; 11.1.1].

13.6 ISO/IEC 27002:2022 - Control 6.3. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 10.1.2].

13.7 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.5.5; 4.6.4; 4.6.5; 5.1.3; 6.1.2; 6.1.3; 6.1.5; 8.1.5; 9.1.3; 10.1.1; 10.1.6; 11.1.2].