					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: P17					Dokumenttitel: **Databeskyttelses- og privatlivspolitik**						
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/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 5.1, 6.1.3, 8.1, 10	Relevante generelle, tekniske og løbende forbedringskontroller for databeskyttelse
ISO/IEC 27002:2022	Kontroller 5.34, 8.10, 8.11, 8.12	Kontroller for håndtering af personhenførbare oplysninger (PII), opbevaring, sletning, anonymisering og registreredes rettigheder
NIST SP 800-53 Rev.5	AR-1, AR-2, AR-4, AR-5; PL-2, PL-8; AC-2, AC-6; AU-2, AU-6, AU-9; IR-4, IR-5, IR-6; PM-1, PM-21, PM-23	Krav til styring, risikostyring, adgangsstyring, logning, håndtering af brud og privatlivsprogram
EU GDPR	Artikel 5, 6, 12–23, 25, 28, 30, 32–34; betragtning 78	Alle centrale krav til privatliv, ansvarlighed, registreredes rettigheder, anmodninger fra registrerede, brud samt principper om databeskyttelse gennem design og som standard
EU NIS2	Artikel 21(2)(e), (f)	Risikobaserede sikkerhedskontroller for væsentlige og vigtige enheder
EU DORA	Artikel 6(2)(d), 11(1)(c), 15(1), 17	Styring, tredjepartsrisiko og frister for sikker databehandling
COBIT 2019	APO12, DSS01, DSS05, MEA	Risikostyring, sikker drift og tilsyn med efterlevelse

1. Formål

1.1 Denne politik fastsætter obligatoriske organisatoriske principper og tekniske krav til beskyttelse af personoplysninger og håndhævelse af databeskyttelse gennem design på tværs af alle miljøer.

1.2 Den formaliserer organisationens ansvar efter internationale standarder og regulatoriske rammeværker og sikrer, at personoplysninger indsamles, behandles, opbevares, deles og bortskaffes lovligt, sikkert og gennemsigtigt.

1.3 Denne politik styrker også efterlevelsen af gældende regler og rammeværker for databeskyttelse og privatliv, herunder EU's generelle forordning om databeskyttelse (GDPR), EU's NIS2-direktiv, EU's forordning om digital operationel modstandsdygtighed (DORA), ISO/IEC 27001:2022 og COBIT 2019.

2. Omfang

2.1 Denne politik gælder for alle organisatoriske enheder, medarbejdere og systemer, der indgår i behandling af personoplysninger, herunder:

2.1.1 Medarbejdere, kontrahenter, konsulenter og tredjepartsleverandører.

2.1.2 Data indsamlet fra interne og eksterne kilder på tværs af alle forretningsfunktioner.

2.1.3 Fysiske og digitale medier, herunder cloudtjenester, SaaS-platforme, mobile enheder og papirbaserede registre.

2.1.4 Alle miljøer, herunder produktions-, udviklings-, test- og backupsystemer, hvor personoplysninger kan forekomme.

2.2 Politikken omfatter alle behandlingsaktiviteter, der er reguleret af gældende databeskyttelseslovgivning og standarder, herunder, men ikke begrænset til:

2.2.1 Indsamling, lagring, anvendelse, overførsel og bortskaffelse af personoplysninger.

2.2.2 Håndhævelse af registreredes rettigheder, dokumentation af behandlingsgrundlag og styring af samtykke.

2.2.3 Grænseoverskridende overførsler, anmeldelse af brud og deling af data med tredjeparter.

2.2.4 Sikker systemudformning og håndhævelse af databeskyttelse som standard i systemer og processer.

3. Mål

3.1 Sikre lovlig, gennemsigtig og ansvarlig behandling af personoplysninger i overensstemmelse med ISO/IEC 27001:2022 og tilhørende retlige krav.

3.2 Integrere principperne om databeskyttelse gennem design og databeskyttelse som standard i alle informationssystemer, tjenester og forretningsprocesser.

3.3 Håndhæve tekniske og organisatoriske foranstaltninger (TOM'er), der beskytter fortrolighed, integritet og tilgængelighed af personoplysninger gennem hele deres livscyklus.

3.4 Definere styringsroller og -strukturer for ansvarlighed i forhold til databeskyttelse, herunder ansvar for databeskyttelsesrådgiveren (DPO), informationssikkerhed, jura og compliance samt dataejere.

3.5 Muliggøre fuld efterlevelse af GDPR artikel 5, 6, 25, 30 og 32 samt krav til risikoreduktion og robusthed efter NIS2 og DORA.

3.6 Opretholde registreredes rettigheder, herunder indsigt, berigtigelse, sletning, begrænsning, dataportabilitet, indsigelse og beskyttelse mod automatiserede afgørelser.

3.7 Reducere regulatoriske, omdømmemæssige, juridiske og operationelle risici, der følger af uautoriseret adgang, misbrug eller tab af personoplysninger.

4. Roller og ansvar

4.1 Direktionen

4.1.1 Udøver strategisk tilsyn og allokerer tilstrækkelige ressourcer til at understøtte privatlivsprogrammet.

4.1.2 Godkender denne politik og sikrer håndhævelse på tværs af organisationen.

4.2 Databeskyttelsesrådgiver (DPO)

4.2.1 Handler uafhængigt med henblik på at føre tilsyn med efterlevelse af databeskyttelsesreglerne.

4.2.2 Vedligeholder fortegnelsen over behandlingsaktiviteter (RoPA) i henhold til GDPR artikel 30.

4.2.3 Leder dialogen med myndigheder, gennemfører konsekvensanalyser vedrørende databeskyttelse (DPIA'er) og styrer processer for anmeldelse af brud.

4.2.4 Gennemgår privatlivsundtagelser og vedligeholder registeret over privatlivsundtagelser.

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

9. Krav til gennemgang og opdatering

9.1 Denne politik skal gennemgås mindst årligt eller tidligere under følgende forhold:

9.1.1 Væsentlige juridiske eller regulatoriske opdateringer (f.eks. ændringer i GDPR eller DORA-frister)

9.1.2 Nye systemer eller behandlingsaktiviteter, der omfatter personoplysninger

9.1.3 Revisionskonstateringer fra intern revision, der indikerer mangler i politikken

9.1.4 Væsentlige brud eller tilbagemeldinger fra tilsynsmyndigheder

9.2 Ansvar for gennemgang

9.2.1 DPO'en skal igangsætte gennemgangen af politikken i koordinering med jura, risikostyring, informationssikkerhed og direktionen.

9.2.2 Alle opdateringer skal registreres i ISMS'ets dokumentstyringsregister og distribueres til berørte interessenter.

9.3 Ændringsstyring

9.3.1 Enhver revision af denne politik skal formelt godkendes af direktionen.

9.3.2 Forældede versioner skal arkiveres sikkert, og den opdaterede version skal indeholde en dokumenteret ændringshistorik.

10. Relaterede politikker og sammenhænge

10.1 P1 – Informationssikkerhedspolitik. Fastlægger de overordnede principper for sikkerhedsstyring, der understøtter denne databeskyttelses- og privatlivspolitik. P1 understøtter fortrolighed, integritet og tilgængelighed af personoplysninger på tværs af alle systemer og tjenester.

10.2 P6 – Politik for risikostyring. Definerer organisationens metode for risikobehandling, som er afgørende for vurdering af privatlivsrisici, DPIA-processer og evaluering af restrisiko, som kræves efter GDPR og ISO/IEC 27001 klausul 6.1.3.

10.3 P13 – Politik for dataklassificering og mærkning. Vejleder i kategorisering af personoplysninger og følsomme data og danner grundlag for anvendelse af passende privatlivskontroller, herunder håndhævelse af opbevaring, begrænsning af adgang og sikker bortskaffelse.

10.4 P14 – Dataopbevaringspolitik og politik for bortskaffelse. Understøtter direkte krav til databeskyttelse efter GDPR artikel 5(1)(e) og 17 og sikrer, at personoplysninger kun opbevares så længe som nødvendigt og bortskaffes sikkert i overensstemmelse med retlige forpligtelser.

10.5 P16 – Politik for datamaskering og pseudonymisering. Fastlægger kontroller til reduktion af identificerbarheden af personoplysninger gennem tekniske foranstaltninger såsom tokenisering, dynamisk maskering og pseudonymisering og håndhæver dermed GDPR artikel 32 og kontrol 5.34 i ISO/IEC 27002.

10.6 P30 – Politik for hændelseshåndtering. Beskriver de obligatoriske protokoller for håndtering af brud, der integrerer frister for håndtering af privatlivsbrud og underretning som krævet efter GDPR artikel 33 og 34.

10.7 P33 – Politik for revisions- og efterlevelsesovervågning. Håndhæver planlagte vurderinger af effektiviteten af privatlivsprogrammet, håndhævelse af politikken og sporing af korrigerende handlinger på tværs af organisatoriske enheder og tredjepartsdatabehandlere.

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001

11.1.1 Klausul 5.1 – Lederskab og forpligtelse: Fastlægger ansvar på direktionsniveau for beskyttelse af personoplysninger og håndhævelse af principper for databeskyttelse og privatliv.

11.1.2 Klausul 6.1.3 – Informationssikkerhedsrisikostyring: Understøtter identifikation, vurdering og behandling af privatlivsrisici via DPIA'er og undtagelser.

11.1.3 Klausul 8.1 – Operationel planlægning og styring: Kræver tekniske og proceduremæssige sikkerhedsforanstaltninger for at sikre, at personoplysninger behandles sikkert.

11.1.4 Klausul 10.1 – Løbende forbedring: Påbyder periodisk evaluering og tilpasning af privatlivsprogrammet.

11.2 ISO/IEC 27002:2022 kontroller 5.34, 8.10, 8.11, 8.12: Giver vejledning om håndtering af personhenførbare oplysninger (PII), håndhævelse af opbevaring, sletning, anonymisering og gennemsigtighed i forhold til registreredes rettigheder.

11.3 NIST SP 800-53 Rev.5

11.3.1 AR-1, AR-2, AR-4, AR-5: Definerer styring, roller, ansvarlighed og ansvar for træning i databeskyttelse og privatliv.

11.3.2 PL-2, PL-8: Kræver integration af privatlivskontroller i systemlivscyklus og virksomhedsarkitektur.

11.3.3 AC-2, AC-6: Håndhæver princippet om mindst privilegium og kontostyring til beskyttelse af personoplysninger.

11.3.4 AU-2, AU-6, AU-9: Påbyder logning, sporbarhed og revisionsintegritet for adgang til personoplysninger.

11.3.5 IR-4, IR-5, IR-6: Definerer strukturerede processer for detektion, analyse og rapportering af privatlivsbrud.

11.3.6 PM-1, PM-21, PM-23: Etablerer et omfattende privatlivsprogram tilpasset strategiske mål for risiko og datastyring.

11.4 EU GDPR (2016/679)

11.4.1 Artikel 5, 6, 12–23, 25, 28, 30, 32–34: Regulerer lovlig behandling, formålsbegrænsning, registreredes rettigheder, ansvarlighed, databeskyttelse gennem design og som standard, tredjepartsforpligtelser og håndtering af brud.

11.4.2 Betragtning 78: Understreger principperne om databeskyttelse gennem design.

11.5 EU NIS2-direktiv (2022/2555)

11.5.1 Artikel 21(2)(e) og (f): Kræver implementering af risikobaserede sikkerhedskontroller og beskyttelse af personoplysninger inden for anvendelsesområdet for væsentlige og vigtige enheder.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 6(2)(d): Håndhæver intern styring af IKT-risiko vedrørende datahåndtering.

11.6.2 Artikel 11(1)(c): Påbyder tilsyn med tredjepartsrisiko for datarelaterede tjenester.

11.6.3 Artikel 15(1) og 17: Kræver sikker databehandling hos tjenesteudbydere og rettidige indberetninger til tilsynsmyndigheder efter IKT-relaterede hændelser.

11.7 COBIT 2019

11.7.1 APO12 – Risikostyring: Integrerer privatlivsrisici i det bredere virksomhedsmæssige risikotilsyn.

11.7.2 DSS01 – Styrede driftsaktiviteter og DSS05 – Sikkerhedstjenester: Sikrer sikker drift, herunder adgangsstyring, opbevaring og systemintegritet.

11.7.3 MEA03 – Overvågning af efterlevelse: Kræver løbende gennemgang af status for efterlevelse i forhold til regulatoriske og politikbaserede forpligtelser vedrørende databeskyttelse og privatliv.