					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: P16					Dokumenttitel: **Politik for datamaskering og pseudonymisering**						
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 lovkrav

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 6.1	Generelle krav til risikostyring og operationelle kontroller for maskering og pseudonymisering
ISO/IEC 27002:2022	Kontroller 8.11, 8	Vejledning om implementering af maskering og pseudonymisering
NIST SP 800-53 Rev.5	PM-17, PT-2, PT-3, SC-12, SC-28, SC-30	Kontroller for databeskyttelse og fortrolighed ved dataminimering, datatransformation og begrænsning af adgang
EU GDPR	Artikel 4(5), 5(1)(c,f), 32	Retsgrundlag og krav til pseudonymisering og databeskyttelsesforanstaltninger
EU NIS2	Artikel 21(2)(c)	Krav om tekniske og organisatoriske foranstaltninger, herunder privatlivsfremmende teknologier (PETs)
EU DORA	Artikel 10(1), 10(2)(e)	Styring af IKT-risici og fortrolighedskontroller for datamaskering og pseudonymisering
COBIT 2019	DSS05.01, DSS06.06, MEA03	Styringskontroller for databeskyttelse ved brug af maskering og vurdering af efterlevelse

1. Formål

1.1 Denne politik fastlægger organisationens tilgang til implementering af datamaskering og pseudonymisering som privatlivsfremmende teknologier (PETs) med henblik på at reducere identificerbarhed og eksponering af personoplysninger eller følsomme data.

1.2 Politikken understøtter sikker anvendelse af oplysninger i test, analyse og drift, samtidig med at juridiske og regulatoriske krav overholdes, konsekvenserne af brud på persondatasikkerheden begrænses, og principperne om dataminimering og fortrolighed håndhæves.

1.3 Politikken er tilpasset ISO/IEC 27001:2022, understøtter GDPR artikel 4(5) om pseudonymisering og integrerer en risikobaseret implementering i overensstemmelse med NIST-, NIS2-, DORA- og COBIT 2019-rammeværkerne.

2. Omfang

2.1 Denne politik gælder for:

2.1.1 Alle medarbejdere, kontrahenter, tredjeparter og leverandører med adgang til systemer, der behandler personoplysninger, fortrolige oplysninger eller følsomme data.

2.1.2 Alle datamiljøer, herunder produktion, udvikling, test og staging.

2.1.3 Alle former for datamaskering (f.eks. statisk, dynamisk, deterministisk, tokenisering) og pseudonymiseringsteknikker, der anvendes til at reducere databeskyttelsesrisici.

2.1.4 Alle datatyper (strukturerede eller ustrukturerede), systemer (on-premises eller cloud-hostede systemer) og applikationer, der omfatter personoplysninger eller regulerede data.

2.2 Omfanget omfatter anvendelse i:

2.2.1 Applikationsudvikling og QA-/testmiljøer

2.2.2 Analyse- eller rapporteringsplatforme

2.2.3 Dataudveksling med tredjeparter eller tredjepartsleverandører

2.2.4 Systemer til sikkerhedskopiering, arkivering eller gendannelse

3. Mål

3.1 Sikre ensartet og effektiv anvendelse af maskering og pseudonymisering for at reducere risikoen for dataeksponering eller misbrug.

3.2 Sikre, at reelle data aldrig anvendes i ikke-produktionsmiljøer, medmindre de er transformeret ved hjælp af godkendte PET-teknikker.

3.3 Opretholde referentiel integritet, anvendelighed og formatbevarende transformationer, når dette er nødvendigt for operationel konsistens.

3.4 Håndhæve streng adgangsstyring til originale data, maskerede data og nøgler til genidentifikation.

3.5 Behandle maskerede eller pseudonymiserede datasæt som følsomme data, underlagt logning af adgang, opbevaringskontroller og procedurer for hændelseshåndtering.

3.6 Validere effektiviteten af disse kontroller gennem løbende test, overvågning og revisionsprocedurer.

4. Roller og ansvar

4.1 Direktionen

4.1.1 Godkender denne politik og sikrer dens håndhævelse som led i den overordnede IT-styring og organisationens databeskyttelsesinitiativer.

4.2 CISO / ISMS-ansvarlig

4.2.1 Fører tilsyn med implementeringen og den løbende efterlevelse.

4.2.2 Sikrer overensstemmelse med ISO/IEC 27001 klausul 6.1.3 (risikobehandling) og klausul 8.1 (operationel planlægning og styring).

4.2.3 Gennemgår logfiler og validerer kontroludførelsen.

[... 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 én gang årligt eller tidligere i tilfælde af:

9.1.1 Regulatoriske ændringer, der påvirker maskering eller pseudonymisering

9.1.2 Indførelse af nye IT-systemer, der behandler følsomme data

9.1.3 Væsentlige ændringer i organisationens ordning for dataklassificering

9.1.4 Revisionskonstateringer, der indikerer kontrolsvigt

9.1.5 Fremkomst af nye trusler eller maskeringsteknologier

9.2 ISMS-ansvarlig skal lede gennemgangen i samråd med DPO'en, dataejere, IT-sikkerhed og Jura. Opdateringer skal være underlagt versionsstyring, godkendes af topledelsen og kommunikeres til alle berørte interessenter.

10. Relaterede politikker og sammenhænge

10.1 P13 - Politik for dataklassificering og mærkning. Beslutninger om maskering og pseudonymisering afhænger direkte af klassificeringen af datafelter og de følsomhedsniveauer, der er defineret i P13.

10.2 P14 - Politik for dataopbevaring og bortskaffelse. Transformerede datasæt skal opbevares og bortskaffes i overensstemmelse med livscyklusreglerne i P14, så det sikres, at maskerede og pseudonymiserede data behandles som følsomme data.

10.3 P17 - Databeskyttelses- og privatlivspolitik. Angiver privatlivsprincipper og regulatorisk grundlag for anvendelse af pseudonymisering som en compliant behandlingsaktivitet efter GDPR og tilsvarende lovgivning.

10.4 P22 - Lognings- og overvågningspolitik. Muliggør centraliseret revision og alarmering af hændelser vedrørende maskering og pseudonymisering i overensstemmelse med strukturerede procedurer for sikkerhedsovervågning.

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001

11.1.1 Klausul 6.1.3 - risikobehandlingsplan: Etablerer maskering og pseudonymisering som mekanismer til risikobehandling for at reducere identificerbarheden af følsomme data i ikke-essentielle behandlingsmiljøer.

11.1.2 Klausul 8.1 - operationel planlægning og styring: Fastsætter tekniske og proceduremæssige sikkerhedsforanstaltninger for sikker datatransformation under behandling, lagring eller overførsel.

11.2 ISO/IEC 27002:2022

11.2.1 Kontroller 8.11, 8: Vejledning om datamaskering og pseudonymisering for at minimere risici for genidentifikation og datalækage.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-17 - Beskyttelse af personhenførbare oplysninger (PII): Implementering af privatlivsfremmende teknologier såsom maskering og pseudonymisering.

11.3.2 PT-2, PT-3: Minimering og sikker behandling af personhenførbare oplysninger (PII) - transformation for at reducere identificerbarhed og håndhæve adgangsstyring.

11.3.3 SC-12, SC-28, SC-30: Datafortrolighed og dataintegritet - kontroller for fortrolighed og sløring ved lagring, transmission og anvendelse.

11.4 EU GDPR (2016/679)

11.4.1 Artikel 4(5): Formel definition af pseudonymisering.

11.4.2 Artikel 32: Behandlingssikkerhed - organisatoriske og tekniske foranstaltninger til pseudonymisering.

11.4.3 Artikel 5(1)(c,f): Dataminimering og fortrolighed ved brug af pseudonymisering og maskering.

11.5 EU NIS2-direktivet (2022/2555)

11.5.1 Artikel 21(2)(c): Kræver PETs såsom maskering og pseudonymisering som sikkerhedsforanstaltninger.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 10(1): Styringsramme for IKT-risiko omfatter kontroller for maskering og pseudonymisering.

11.6.2 Artikel 10(2)(e): Kræver anvendelse af transformationsteknologier for at beskytte personoplysninger og finansielle data.

11.7 COBIT 2019

11.7.1 DSS05.01: Beskyt informationsaktiver - krav til maskering og pseudonymisering.

11.7.2 DSS06.06: Sikker test og analyse - maskering i miljøer uden for produktion.

11.7.3 MEA03: Overvågning af efterlevelse for effektiviteten af maskering og pseudonymisering.