					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P16S					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 reguleringer

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 6.1.3, klausul 8	Informationssikkerhedsrisici og nødvendige kontroller, herunder maskering/pseudonymisering
ISO/IEC 27002:2022	Kontrol 8.11, 8.12	Vejledning om maskering og forebyggelse af datalækage
NIST SP 800-53 Rev.5	SC-12, SC-28, PT-2, PT-3	Datasløring og privatlivsforbedrende teknologier
EU NIS2	Artikel 21(2)(c)	Proportionale tekniske foranstaltninger, herunder pseudonymisering som kontrol
EU DORA	Artikel 10(1)	IKT-risikokontroller, herunder sikkerhedsforanstaltninger ved datatransformation
COBIT 2019	DSS05.01, DSS06	Databeskyttelse, sløringsteknikker og pseudonymisering
EU GDPR	Artikel 4(5), 5(1)(c), 32	Dataminimering, pseudonymisering som teknisk kontrol

1. Formål

1.1. Denne politik fastsætter bindende krav til brugen af datamaskering og pseudonymisering for at beskytte følsomme, personhenførbare og fortrolige data i små og mellemstore virksomheder (SMV'er).

1.2. Disse teknikker er obligatoriske, når reelle data ikke er nødvendige, f.eks. i udvikling, analyse eller ved anvendelse af tredjepartsleverandører, og bidrager til at reducere risikoen for eksponering, misbrug eller brud på persondatasikkerheden.

1.3. Denne politik understøtter direkte efterlevelse af certificering efter ISO/IEC 27001:2022 samt europæiske regulatoriske krav som GDPR, NIS2-direktivet og DORA-forordningen.

1.4. Ved at transformere data, før de anvendes uden for deres oprindelige forretningsmæssige kontekst, begrænser organisationen ansvar og styrker sin evne til at dokumentere rettidig omhu inden for databeskyttelse og sikkerhed.

2. Omfang

2.1. Denne politik gælder for alle strukturerede eller ustrukturerede data, der er klassificeret som personhenførbare, fortrolige eller følsomme, uanset om de lagres eller behandles:

2.1.1. I produktions-, test- eller udviklingsmiljøer

2.1.2. På lokale enheder, servere eller cloudplatforme

2.1.3. Af interne medarbejdere, kontrahenter eller tredjepartsleverandører

2.2. Den omfatter også alle værktøjer til datatransformation (maskering, tokenisering, pseudonymisering), uanset om de er open source, kommercielle eller udviklet internt.

2.3. Anvendelsestilfælde omfattet af denne politik inkluderer:

2.3.1. Klargøring af test- eller udviklingsdatasæt

2.3.2. Eksport af data til analysesystemer

2.3.3. Leverandørers eller konsulenters adgang til driftssystemer

2.3.4. Dataminimering for registrerede med henblik på at reducere behandlingsrisiko

3. Mål

3.1. Sikre, at reelle personhenførbare eller følsomme data aldrig eksponeres i miljøer med lavere sikkerhedsniveau, hvor de ikke er nødvendige.

3.2. Kræve maskering eller pseudonymisering, når reelle identifikatorer ikke er strengt nødvendige for opgaven.

3.3. Forebygge uautoriseret adgang til eller misbrug af data ved at håndhæve transformationskontroller før dataoverførsel eller behandling.

3.4. Sikre, at alle processer for maskering og pseudonymisering er sporbare, revisionsegnede og håndhæves gennem godkendte værktøjer.

3.5. Efterleve gældende lovgivningsmæssige og regulatoriske krav om dataminimering, fortrolighed og sikkerhedsforanstaltninger ved datatransformation.

4. Roller og ansvar

4.1. Direktør

4.1.1. Ejer og godkender denne politik.

4.1.2. Sikrer, at alle afdelinger og tjenesteudbydere efterlever kravene til datatransformation.

4.1.3. Gennemgår undtagelser, risikovurderinger og transformationslogfiler.

4.1.4. Koordinerer juridiske, driftsmæssige eller leverandørrelaterede tiltag ved overtrædelser.

4.2. IT-supportleverandør / intern IT

4.2.1. Vælger og administrerer værktøjer til maskering eller pseudonymisering.

4.2.2. Sikrer, at passende transformationsmetoder anvendes på baggrund af datatype.

4.2.3. Vedligeholder logfiler over transformerede datasæt og procedurer for nøglestyring.

4.2.4. Sikrer, at maskering gennemføres før anvendelse til test, leverandøradgang eller analyse.

[... 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. Årlig gennemgang

9.1.1. Denne politik skal gennemgås mindst én gang årligt af direktøren for at sikre, at den afspejler:

9.1.1.1. Opdateringer i gældende regulering (f.eks. GDPR, DORA)

9.1.1.2. Nye forretningssystemer eller dataudvekslinger med tredjeparter

9.1.1.3. Input fra revisioner eller hændelser, der involverer brug af umaskerede data

9.2. Løbende gennemgange

9.2.1. Gennemgange skal også finde sted, når:

9.2.1.1. Nye applikationer eller platforme, der håndterer følsomme data, introduceres

9.2.1.2. En væsentlig hændelse afdækker mangler i de nuværende transformationskontroller

9.2.1.3. Ændringer i klassifikationsniveauer påvirker procedurer for datahåndtering

9.3. Versionsstyring og ændringsstyring

9.3.1. Alle ændringer af politikken skal:

9.3.1.1. Godkendes af direktøren og dokumenteres i en ændringslog

9.3.1.2. Kommunikeres tydeligt til berørte medarbejdere og tjenesteudbydere

9.3.1.3. Arkiveres sikkert med begrænset adgang til forældede versioner

10. Relaterede politikker og sammenhænge

10.1. Denne politik skal anvendes sammen med følgende SMV-politikker for at sikre ensartet og håndhævelig beskyttelse af følsomme data:

10.1.1. P13S – Politik for dataklassificering og mærkning: Definerer klassifikationsniveauerne (f.eks. "Fortrolig – Personhenførbar"), som afgør, hvornår maskering eller pseudonymisering skal anvendes. Denne politik håndhæver transformationsregler baseret på dataniveauets følsomhed.

10.1.2. P14S – Politik for dataopbevaring og bortskaffelse: Sikrer, at transformerede datasæt, herunder sikkerhedskopier med maskerede eller pseudonymiserede data, opbevares og bortskaffes i overensstemmelse med gældende regler, herunder sletning af mappingsnøgler, når de ikke længere er nødvendige.

10.1.3. P17S – Databeskyttelses- og privatlivspolitik: Tilpasser transformationspraksis til bredere databeskyttelsesforpligtelser, herunder GDPR-krav om dataminimering og brug af pseudonymisering som sikkerhedsforanstaltning ved behandling af personoplysninger.

10.1.4. P30S – Politik for hændelseshåndtering: Omfatter procedurer for rapportering og eskalering i tilfælde af uautoriseret videregivelse af data, herunder uretmæssig brug eller reversering af maskerede eller pseudonymiserede data.

10.1.5. P2S – Politik for styringsroller og ansvarsområder: Tildeler det overordnede ansvar for implementering af politikken, risikoaccept og godkendelse af undtagelser, primært til direktøren.

10.2. Disse politikker udgør samlet en integreret ramme for databeskyttelse, som sikrer, at maskering og pseudonymisering understøtter ISO 27001-certificering og efterlevelse på tværs af reguleringer.

11. Referencestandarder og rammeværk

11.1. ISO/IEC 27001

11.1.1. Klausul 6.1.3: Kræver behandling af informationssikkerhedsrisici, hvilket omfatter reduktion af eksponering gennem datatransformationsteknikker.

11.1.2. Klausul 8.1: Kræver implementering af de kontroller, der er nødvendige for at opfylde sikkerhedsmål, herunder pseudonymisering og maskering.

11.2. ISO/IEC 27002

11.2.1. Kontrol 8.11: Giver vejledning om maskering af følsomme data i test- og udviklingssystemer.

11.2.2. Kontrol 8.12: Angiver strategier til at forebygge datalækage gennem kontrolleret transformation og adgangspraksis.

11.3. NIST SP 800-53 Rev.5

11.3.1. SC-12: Sikrer oplysningers fortrolighed gennem datasløring.

11.3.2. SC-28: Beskytter oplysninger i hvile og under brug.

11.3.3. PT-2/PT-3: Fremmer brugen af privatlivsforbedrende teknologier, herunder pseudonymisering, ved behandling af personhenførbare oplysninger (PII).

11.4. EU GDPR

11.4.1. Artikel 4(5): Definerer juridisk pseudonymisering og kræver kontroller over mappingsnøgler og identifikatorer.

11.4.2. Artikel 5(1)(c): Understøtter principper om dataminimering gennem maskering.

11.4.3. Artikel 32: Anerkender pseudonymisering som en teknisk kontrol, der reducerer databeskyttelsesrisici.

11.5. EU NIS2-direktivet

11.5.1. Artikel 21(2)(c): Kræver proportionale tekniske foranstaltninger til at minimere risikoen for datasikkerhed, herunder pseudonymisering som en del af risikokontrollen.

11.6. EU DORA-forordningen

11.6.1. Artikel 10(1): Kræver IKT-relaterede risikokontroller, som omfatter sikkerhedsforanstaltninger ved datatransformation for forretningskontinuitet og fortrolighed under outsourcing og systemudvikling.

11.7. COBIT 2019

11.7.1. DSS05.01: Kræver beskyttelse af informationsaktiver, herunder transformation, hvor det er muligt.

11.7.2. DSS06.06: Kræver passende slørings- og pseudonymiseringsteknikker for at begrænse dataeksponering i miljøer med lavere tillidsniveau.