					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P16S					Dokumenttitel: **Policy för datamaskering och pseudonymisering**							
Version: 1.0		Ikraftträdandedatum: 01.01.2025			Dokumentägare:							
X	Policy		Standard		Rutin		Formulär		Register		Övrigt	

Revisionshistorik				
Revisionsnummer	**Revisionsdatum**	**Ändringar**	**Granskad av**	**Processägare**

Godkännanden			
Namn	**Titel**	**Datum**	**Underskrift**

Juridiskt meddelande (upphovsrätt och användningsbegränsningar)

(C) 2025 Clarysec LLC. All rights reserved.

Detta dokument är Clarysec LLC:s immateriella egendom. Ingen del av detta dokument får kopieras, återanvändas, distribueras eller ändras för kommersiella eller implementeringsändamål utan uttryckligt skriftligt förhandstillstånd.
Obehörig användning är strängt förbjuden och kan leda till rättsliga åtgärder.
För licensiering, kontakta: info@clarysec.com

Anpassning till standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 6.1.3, klausul 8	Informationssäkerhetsrisker och nödvändiga kontroller, inklusive maskering och pseudonymisering
ISO/IEC 27002:2022	Kontroller 8.11, 8.12	Vägledning om maskering och förebyggande av dataläckage
NIST SP 800-53 Rev.5	SC-12, SC-28, PT-2, PT-3	Dataobfuskering och integritetsförstärkande tekniker
EU:s NIS2-direktiv	Artikel 21(2)(c)	Proportionerliga tekniska åtgärder, inklusive pseudonymisering som kontroll
EU:s DORA-förordning	Artikel 10(1)	IKT-riskkontroller, inklusive skyddsåtgärder för datatransformering
COBIT 2019	DSS05.01, DSS06	Dataskydd samt obfuskering och pseudonymisering
EU:s GDPR	Artiklarna 4(5), 5(1)(c), 32	Uppgiftsminimering och pseudonymisering som teknisk kontroll

1. Syfte

1.1. Denna policy fastställer bindande krav för användning av datamaskering och pseudonymisering för att skydda känsliga, personrelaterade och konfidentiella data inom små och medelstora företag (SME).

1.2. Dessa tekniker är obligatoriska när verkliga data inte behövs, exempelvis vid utveckling, analys eller i scenarier som involverar tredjepartsleverantörer, för att minska riskerna för exponering, missbruk eller överträdelser.

1.3. Denna policy stödjer direkt efterlevnad av ISO/IEC 27001:2022-certifiering samt europeiska regelverkskrav såsom GDPR, EU:s NIS2-direktiv och EU:s DORA-förordning.

1.4. Genom att transformera data innan de används utanför sitt ursprungliga verksamhetssammanhang begränsar organisationen ansvarsexponeringen och stärker sin förmåga att visa tillbörlig aktsamhet avseende dataskydd och informationssäkerhet.

2. Omfattning

2.1. Denna policy gäller för alla strukturerade och ostrukturerade data som klassificeras som personrelaterade, konfidentiella eller känsliga, oavsett om de lagras eller behandlas:

2.1.1. I produktions-, test- eller utvecklingsmiljöer

2.1.2. På lokala enheter, servrar eller molnplattformar

2.1.3. Av intern personal, entreprenörer eller tredjepartsleverantörer

2.2. Policyn omfattar även alla verktyg för datatransformering (maskering, tokenisering, pseudonymisering), oavsett om de är baserade på öppen källkod, kommersiella eller internt utvecklade.

2.3. Användningsfall enligt denna policy omfattar:

2.3.1. Förberedelse av test- eller utvecklingsdataset

2.3.2. Export av data till analyssystem

2.3.3. Leverantörers eller konsulters åtkomst till operativa system

2.3.4. Uppgiftsminimering för registrerade i syfte att minska behandlingsrisker

3. Mål

3.1. Säkerställa att verkliga personuppgifter eller känsliga data aldrig exponeras i miljöer med lägre säkerhetsnivå där de inte behövs.

3.2. Kräva maskering eller pseudonymisering när verkliga identifierare inte är strikt nödvändiga för uppgiften.

3.3. Förhindra obehörig åtkomst till eller missbruk av data genom att kräva transformationskontroller innan data överförs eller behandlas.

3.4. Säkerställa att alla processer för maskering och pseudonymisering är spårbara, granskningsbara och utförs med godkända verktyg.

3.5. Uppfylla tillämpliga rättsliga och regulatoriska krav som kräver uppgiftsminimering, konfidentialitet och skyddsåtgärder för datatransformering.

4. Roller och ansvar

4.1. Verkställande direktör (VD)

4.1.1. Äger och godkänner denna policy

4.1.2. Säkerställer att samtliga avdelningar och leverantörer efterlever kraven på datatransformering

4.1.3. Granskar undantag, riskbedömningar och transformationsloggar

4.1.4. Samordnar juridiska, operativa eller leverantörsrelaterade åtgärder vid överträdelser

4.2. IT-supportleverantör / intern IT-funktion

4.2.1. Väljer och förvaltar verktyg för maskering eller pseudonymisering

4.2.2. Säkerställer att lämpliga transformationsmetoder tillämpas utifrån datatyp

4.2.3. Upprätthåller loggar över transformerade dataset och rutiner för nyckelhantering

4.2.4. Säkerställer att maskering sker innan data används för test, delas med leverantörer eller används för analys

[... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ...]

9. Krav för granskning och uppdatering

9.1. Årlig granskning

9.1.1. Denna policy ska granskas minst en gång per år av verkställande direktören för att säkerställa att den återspeglar:

9.1.1.1. Uppdateringar i tillämpliga regelverk (t.ex. GDPR, DORA)

9.1.1.2. Nya verksamhetssystem eller datautbyten med tredje part

9.1.1.3. Återkoppling från revisioner eller incidenter som rör användning av omaskerade data

9.2. Löpande granskningar

9.2.1. Granskningar ska också genomföras när:

9.2.1.1. Nya applikationer eller plattformar som hanterar känsliga data införs

9.2.1.2. En större incident påvisar brister i befintliga transformationskontroller

9.2.1.3. Ändringar i klassificeringsnivåer påverkar rutiner för datahantering

9.3. Versionshantering och ändringshantering

9.3.1. Alla policyändringar ska:

9.3.1.1. Godkännas av VD och dokumenteras i en ändringslogg

9.3.1.2. Kommuniceras tydligt till berörda anställda och tjänsteleverantörer

9.3.1.3. Arkiveras säkert med begränsad åtkomst till inaktuella versioner

10. Relaterade policyer och kopplingar

10.1. Denna policy ska tillämpas tillsammans med följande SME-policyer för att säkerställa ett konsekvent och bindande skydd av känsliga data:

10.1.1. P13S – Policy för dataklassificering och märkning: Definierar klassificeringsnivåerna (t.ex. Konfidentiell – Personrelaterad) som avgör när maskering eller pseudonymisering ska tillämpas. Denna policy styr transformationsregler utifrån datans känslighetsnivå.

10.1.2. P14S – Policy för databevarande och bortskaffande: Säkerställer att transformerade dataset, inklusive säkerhetskopior som innehåller maskerade eller pseudonymiserade data, bevaras och bortskaffas enligt tillämpliga regler, inklusive radering av mappningsnycklar när de inte längre behövs.

10.1.3. P17S – Policy för dataskydd och integritet: Anpassar transformationspraxis till bredare integritetskrav, inklusive krav enligt GDPR på uppgiftsminimering och användning av pseudonymisering som skyddsåtgärd vid behandling av personuppgifter.

10.1.4. P30S – Policy för incidenthantering: Omfattar rapporterings- och eskaleringsrutiner vid obehörigt röjande av data, inklusive felaktig användning eller återställning av maskerade eller pseudonymiserade data.

10.1.5. P2S – Policy för styrningsroller och ansvar: Tilldelar övergripande ansvar för genomförande av policyn, riskacceptans och godkännande av undantag, i första hand till verkställande direktören.

10.2. Dessa policyer utgör ett integrerat ramverk för dataskydd och säkerställer att åtgärder för maskering och pseudonymisering stödjer ISO 27001-certifiering och efterlevnad av flera regelverk.

11. Referensstandarder och ramverk

11.1. ISO/IEC 27001

11.1.1. Klausul 6.1.3: Kräver behandling av informationssäkerhetsrisker, vilket omfattar att minska exponering genom tekniker för datatransformering.

11.1.2. Klausul 8.1: Kräver införande av de kontroller som behövs för att uppfylla säkerhetsmål, inklusive pseudonymisering och maskering.

11.2. ISO/IEC 27002

11.2.1. Kontroll 8.11: Ger vägledning om maskering av känsliga data i test- och utvecklingssystem.

11.2.2. Kontroll 8.12: Ger strategier för att förebygga dataläckage genom kontrollerad transformering och styrd åtkomst.

11.3. NIST SP 800-53 Rev.5

11.3.1. SC-12: Säkerställer konfidentialiteten för information genom dataobfuskering.

11.3.2. SC-28: Skyddar information vid lagring och användning.

11.3.3. PT-2/PT-3: Främjar användning av integritetsförstärkande tekniker, inklusive pseudonymisering, vid behandling av personligt identifierbar information.

11.4. EU:s GDPR

11.4.1. Artikel 4(5): Definierar pseudonymisering rättsligt och kräver kontroller för mappningsnycklar och identifierare.

11.4.2. Artikel 5(1)(c): Stödjer principen om uppgiftsminimering genom maskering.

11.4.3. Artikel 32: Erkänner pseudonymisering som en teknisk kontroll som minskar integritetsrisker.

11.5. EU:s NIS2-direktiv

11.5.1. Artikel 21(2)(c): Kräver proportionerliga tekniska åtgärder för att minimera risker för datasäkerhet, inklusive pseudonymisering som en del av riskhanteringen.

11.6. EU:s DORA-förordning

11.6.1. Artikel 10(1): Kräver IKT-relaterade riskkontroller som omfattar skyddsåtgärder för datatransformering för kontinuitet och konfidentialitet vid outsourcing och systemutveckling.

11.7. COBIT 2019

11.7.1. DSS05.01: Kräver skydd av informationstillgångar, inklusive transformering där så är möjligt.

11.7.2. DSS06.06: Kräver lämpliga tekniker för obfuskering och pseudonymisering för att begränsa dataexponering i miljöer med lägre tillitsnivå.