

Checklist

8.11 – Gegevensmaskering

Thema: Technisch | ISO 27002: 8.11 | Gerelateerd: 5.34, 8.10

Doelstelling

Aantonen dat gevoelige gegevens worden gemaskeerd of gepseudonimiseerd in niet-productieomgevingen en bij verwerking, zodat onnodig gebruik van persoonlijke of vertrouwelijke gegevens wordt voorkomen.

Beleid en toepassingsgebied

- Is er beleid voor het maskeren of pseudonimiseren van gevoelige gegevens?
- Is vastgelegd in welke situaties gegevensmaskering verplicht is (test, ontwikkeling, rapportage)?
- Is het beleid afgestemd op de AVG en andere relevante wet- en regelgeving?
- Zijn de verantwoordelijkheden voor gegevensmaskering belegd bij een eigenaar?
- Worden medewerkers en ontwikkelaars getraind in het toepassen van gegevensmaskering?

Maskering in test- en ontwikkelomgevingen

- Worden productiegegevens nooit ongemaskeerd gebruikt in test- of ontwikkelomgevingen?
- Is er een geautomatiseerd proces voor het aanmaken van gemaskeerde testdata?
- Worden gemaskeerde gegevens gecontroleerd op kwaliteit (realistisch maar niet herleidbaar)?
- Is toegang tot niet-gemaskeerde testomgevingen beperkt tot strikt noodzakelijke personen?

Pseudonimisering en anonimisering

- Wordt pseudonimisering toegepast waar verwerking van persoonsgegevens verminderd kan worden?
- Is de koppelingstabel (pseudoniem ↔ werkelijke identiteit) apart en strikt beveiligd opgeslagen?
- Wordt bij anonimisering getoetst of heridentificatie werkelijk onmogelijk is?
- Worden geanonimiseerde datasets periodiek herbeoordeeld op heridentificatierisico?

Technische implementatie en controle

- Zijn maskeringstechnieken gedocumenteerd (tokenisatie, versleuteling, substitutie, etc.)?
- Wordt gegevensmaskering geautomatiseerd toegepast in de datapipeline?
- Worden logbestanden en foutmeldingen gecontroleerd op onbedoelde opname van gevoelige data?



Is er een auditproces om te verifiëren dat maskering correct is toegepast?

Verantwoordelijke:	_____	Datum controle:	_____
Afdeling:	_____	Score:	___ / 21
Reviewcyclus:	☐ Jaarlijks ☐ Na wijziging ☐ Na incident		Status: ☐ Voldoet ☐ Actiepunt ☐ N.v.t.