

Checklist

5.34 – Privacy en bescherming van persoonsgegevens

Thema: Organisatorisch | ISO 27002: 5.34 | Gerelateerd: 5.31, 5.33

Doelstelling

Aantonen dat de organisatie persoonsgegevens beschermt conform de AVG en andere privacywetgeving, en de rechten van betrokkenen waarborgt.

Privacy governance

- ☐ Is er een functionaris gegevensbescherming (FG/DPO) aangesteld waar vereist?
- ☐ Is er een privacybeleid vastgesteld en gecommuniceerd aan medewerkers?
- ☐ Zijn verwerkingsactiviteiten vastgelegd in een verwerkingsregister (AVG art. 30)?
- ☐ Worden Privacy Impact Assessments (DPIA's) uitgevoerd voor risicovolle verwerkingen?
- ☐ Is er afstemming tussen de FG/DPO en de CISO over privacy en beveiliging?

Rechtmatigheid van verwerking

- ☐ Is voor elke verwerking een rechtmatige grondslag vastgesteld (toestemming, contract, wettelijke verplichting etc.)?
- ☐ Worden betrokkenen geïnformeerd over de verwerking van hun persoonsgegevens (privacyverklaring)?
- ☐ Worden persoonsgegevens niet langer bewaard dan noodzakelijk?
- ☐ Is dataminimalisatie toegepast (alleen noodzakelijke gegevens worden verwerkt)?
- ☐ Worden verwerkersovereenkomsten afgesloten met alle verwerkers van persoonsgegevens?

Rechten van betrokkenen

- ☐ Is er een procedure voor het behandelen van inzageverzoeken (AVG art. 15)?
- ☐ Is er een procedure voor het behandelen van verzoeken tot rectificatie en verwijdering?
- ☐ Worden verzoeken van betrokkenen binnen de wettelijke termijn (1 maand) beantwoord?
- ☐ Is er een procedure voor het behandelen van bezwaar tegen verwerking?

Datalekken en incidenten

- ☐ Is er een procedure voor het detecteren, beoordelen en melden van datalekken?
- ☐ Worden datalekken met hoog risico gemeld aan de AP binnen 72 uur?

☐ Worden betrokkenen geïnformeerd bij hoog-risico datalekken?

☐ Worden datalekken geregistreerd in een datalekkenregister?

Verantwoordelijke:	_____	Datum controle:	_____
Afdeling:	_____	Score:	___ / 22
Reviewcyclus:	☐ Jaarlijks ☐ Na wijziging ☐ Na incident		Status: ☐ Voldoet ☐ Actiepunt ☐ N.v.t.