Informatiebeveiliging & Privacy

Marc van de Graaf
Chief Information Security Officer
Privacy Officer

Informatiebeveiliging & Privacy

Informatiebeveiliging en privacy belangrijk

- Ministerie van de Minister President
- IUC / Raamovereenkomsten
- Level playing field

Ketenverantwoordelijkheid

- Partners/leveranciers (relevante normen)
- Persoonlijke systemen ingehuurden
- Ingehuurden o.b.v. eisen opdrachtgever (NOK)
    - VOG en/of VGB
    - Geheimhoudingsverklaring
    - Integriteitsverklaring

De eisen.

Redelijke proportionaliteit -> marktconforme normenkaders.

Overheid:	Baseline Informatiebeveiliging Overheid
DPC:	Niet-kritische externe systemen c.q. dienstverlening: Géén Rijksnormen.
AVG	Geest van de wet: Beschermen belangen betrokkenen
Cloudbeleid DPC	Niet-openbaar & Eén categorie persoonsgegevens: Cloudleverancier ISO 27001, ISO 27017 en ISO 27018

Normen/controls van de **ISO 27001** (niet Rijks-interpretatie ISO 27002) Plus:

1. **ISO 27018**
2. **ISO 27019**
3. **ISO/IEC 27701:2019**

De eisen: ISO normen in het kort 1/2

ISO 27001 – Informatiebeveiliging

Managementsysteem voor IB. (Information Security Management System/ISMS).

Adequate en proportionele beveiligingsmaatregelen die de informatie beschermen en vertrouwen bieden aan belanghebbenden te waarborgen, ongeacht type, omvang of aard van de organisatie.

ISO 27002 – Informatiebeveiliging → Hoe ingericht?

ISO 27017 – Cloud beveiliging

De ISO 27017 stelt eisen aan de cloud-leveranciers maar ook aan de afnemers van deze clouddiensten. De norm bevat cloud-specifieke beheersmaatregelen, waarbij het niet uitmaakt wat voor soort gegevens er wordt verwerkt.

ISO 27018 – Cloud Privacy bescherming

De ISO 27018 is alleen bedoeld voor cloud aanbieders die persoonsgegevens verwerken en richt zich op de beveiliging en behandeling van deze gegevens.

De eisen: ISO normen in het kort 2/2

ISO 27701 – Privacy

De internationale standaard rondom privacy management.
Slechts de volgende annexen van toepassing:

ISO/IEC 27701 Annex A:

Indien er persoonsgegevens worden verwerkt als Verwerkingsverantwoordelijke.

(Leverancier levert persoonsgegevens van gegadigden.)

ISO/IEC 27701 Annex B:

Indien er persoonsgegevens worden verwerkt als Verwerker.

(Leverancier verwerkt persoonsgegevens van opdrachtgevers.)

Proces: Vaststelling van de Eisen

QuickScan: IB- en Privacy risico's -> Basis Beveiligingsniveau (BBN)

o.b.v. criteria als beschikbaarheid, integriteit, vertrouwelijkheid en dreigingsprofiel.

Proces: Voldoen aan de eisen.

- ISO-certificering , óf voldoen aan de controls van een ISO-norm.
    - Certificering: relevantie: audit scope en verklaring van toepasselijkheid.
- Het IB-managementsysteem is aan de leverancier. Hier is AZ geen partij in.
- Fit/Gap analyse = verklaring naleving.

Proces: Controle van naleving

Vóór acceptatie:

- Initiële/tijdelijke Fit/Gap analyse (maatregelen en realisatie-data)
- Certificaat controle (incl. audit scope en verklaring van toepasselijkheid) voldoende relevant zijn.
- Definitieve Fit/Gap analyse (vormvereisten, aannemelijkheid en correctheid)

Tijdens de contractperiode:

- Relevante wijzigingen -> actuele Fit/Gap
- Jaarlijkse verklaring (laatste week van november) actualiteit en validiteit
- Audits

?