!

Informatiebeveiliging & Privacy

Marc van de Graaf
CISO & Privacy Officer

Amber van Krimpen
IB- & Privacy Adviseur

Informatiebeveiliging & Privacy

Informatiebeveiliging en privacy belangrijk

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

Ketenverantwoordelijkheid

- Partners/leveranciers (relevante normen)
- Persoonlijke systemen ingehuurden
- Eisen opdrachtgever (NOK) t.a.v. Ingehuurden
  - Verklaring Omtrent Gedrag (VOG) *en/of* Verklaring van Geen Bezwaar (VGB)
  - Geheimhoudings- en Integriteitsverklaring

De eisen.

Redelijke proportionaliteit -> marktconforme normenkaders.
DPC hanteert geen ‘explains’. Eisen dienen onverkort te worden nageleefd.

Overheid:	Baseline Informatiebeveiliging Overheid
DPC:	Niet-kritische externe systemen c.q. dienstverlening: Géén Rijksnormen.
(U)AVG	Geest van de wet: Beschermen belangen betrokkenen
Cloudbeleid DPC	Meerdere categorieën persoonsgegevens: Cloudleverancier ISO 27001, ISO 27017 en ISO 27018 Encryptie in rest & in transit, sleutelbeheer opdrachtnemer.

BIO-controls van de **ISO 27001/27002**, plus:

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

De eisen: ISO normen in het kort 1/2

De ISO 27001 – Informatiebeveiliging

Deze norm beschrijft de eisen van een managementsysteem voor informatiebeveiliging (Information Security Management System/ISMS). De eisen in deze internationale norm zijn algemeen en bedoeld om van toepassing te zijn op alle organisaties, ongeacht type, omvang of aard.

ISO 27017 – Cloud beveiliging

De ISO 27017 stelt eisen aan de cloudleveranciers maar ook aan de afnemers van deze clouddiensten, waarbij het niet uitmaakt wat voor soort gegevens er wordt verwerkt.

ISO 27018 – Cloud Privacy bescherming

De ISO 27018 is alleen bedoeld voor cloudaanbieders die persoonsgegevens verwerken en richt zich op de beveiliging en behandeling van deze gegevens. De norm is ook gebaseerd op de ISO 27002, maar heeft een aanvullende set van beheersmaatregelen specifiek gericht op het beschermen van persoonsgegevens.

De eisen: ISO normen in het kort 2/2

ISO 27701:2019 – Privacy

De internationale standaard rondom privacy management. Privacy Informatie Management Systeem (PIMS). Van deze norm zijn voor ons (in deze context) slechts de volgende annexen van toepassing:

ISO/IEC 27701:2019 Annex A:

Indien er persoonsgegevens worden verwerkt als Verwerkingsverantwoordelijke.

ISO/IEC 27701:2019 Annex B:

Indien er persoonsgegevens worden verwerkt als Verwerker.

Proces: Vaststelling van de Eisen.

- DPC komt tot de criteria voor haar uitvraag door het uitvoeren van een QuickScan, waarmee wij om de IB- en Privacy risico's in kaart te brengen.
- Dit gebeurt o.b.v. criteria als het belang van het systeem, beschikbaarheid, integriteit, vertrouwelijkheid en het dreigingsprofiel.
- Uit deze scan komt een Basis Beveiligingsniveau (BBN2) en er wordt bepaald of een systeem 'bedrijfskritisch' is.

Proces: Voldoen aan de eisen.

- DPC vraagt geen ISO-certificering aan haar leveranciers, maar wel het voldoen aan de controls van een ISO-norm.
- Is een leverancier wél in het bezit van relevante geldige certificering(en), én dekkende audit scope en verklaring van toepasselijkheid, dan accepteren wij deze vanzelfsprekend als bewijsvoering van naleving.
- Het beheren/aanpassen/inrichten van een managementsysteem voor informatiebeveiliging is aan de leverancier. Hier is DPC geen partij in.
- Wanneer de leverancier acht aan de eisen te voldoen, levert deze een Fit/Gap analyse aan als bewijsvoering van de naleving.

Proces: Controle van naleving 1/2.

Vóór acceptatie:

- DPC vraagt om een initiële/tijdelijke Fit/Gap analyse te leveren, hierin zijn ook te nemen maatregelen en de realisatie-data van de maatregelen opgenomen.
- O.b.v. aannemelijkheid kan DPC adviseren kennis in te huren.
- DPC controleert of aangeleverde certificaten (incl. audit scope en verklaring van toepasselijkheid) voldoende relevant zijn.
- DPC controleert of de definitieve Fit/Gap analyse aan de vormvereisten voldoet, en als dat zo is:
- Controleert DPC of de Fit/Gap analyse aannemelijk is en inhoudelijk klopt.

Proces: Controle van naleving 2/2.

Tijdens de contractperiode:

- De Fit/Gap analyses hebben een geldigheid, conform contractduur.
- Leveranciers stellen DPC op de hoogte van eventuele wijzigingen in de Fit/Gap verklaring, inclusief de te nemen maatregelen en bijbehorende planning. Nadat deze maatregelen zijn genomen dient er een actuele Fit/Gap te worden geleverd.
- Leveranciers verklaren jaarlijks (laatste week van november) dat de Fit/Gap analyse nog actueel en valide is.
- Eventuele IB-beleidswijzigingen worden tijdens de standaard contractduur slechts naar leveranciers doorgezet indien van aantoonbare meerwaarde en/of noodzaak.
- Audits/controles bij leveranciers kunnen op basis van een auditplan, gebaseerd op BBN-niveau, plaatsvinden.

?