# Informatiebeveiliging & Privacy

Informatiebeveiliging en privacy worden belangrijk geacht door de Rijksoverheid. AZ heeft daarnaast binnen de Rijksoverheid een bijzondere positie en verantwoordelijkheid, als ministerie van de Minister President.

DPC is niet slechts verantwoordelijk voor haar eigen systemen, maar als inkopende dienst van raamovereenkomsten, ook voor een praktische, veilige en efficiënte mogelijkheid tot het aangaan van daar uit voortvloeiende nadere overeenkomsten. Om dit te bereiken zal DPC dus eisen opleggen die (voor zover te voorzien) afdoende zijn voor de te sluiten raamovereenkomsten. De gemaakte keuzes, mogelijkheden en beperkingen, worden gedocumenteerd en gedeeld met de potentiële nadere opdrachtgevers en leveranciers.

In deze presentatie proberen we in *10* slides inzicht te geven in onze werkwijze.

# De eisen.

Binnen de Overheid wordt de Baseline Informatiebeveiliging Overheid gebruikt. AZ heeft besloten hier, in het geval van **niet-kritische externe systemen c.q. dienstverlening**, van af te wijken.

Om redelijke proportionaliteit toe te passen, wil AZ zo veel mogelijk aansluiten bij marktconforme normenkaders.

We vragen daarom om aan de normen (controls) van de **ISO 27001** te voldoen en zullen de controls, behorende tot de Rijks-interpretatie van ISO 27002 slechts in uitzonderlijke situaties uitvragen wanneer daar specifieke redenen voor zijn.

Naast de **ISO 27001** kunnen de controls van drie aanvullende ISO-normen van toepassing zijn:

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

# De eisen: ISO normen in het kort 1/3

**De ISO 27001 – Informatiebeveiliging**

Deze norm beschrijft de eisen van een managementsysteem voor informatiebeveiliging (Information Security Management System/ISMS).

De norm specificeert eisen voor de implementatie van beveiligingsmaatregelen die zijn aangepast aan de behoeften van afzonderlijke organisaties of delen daarvan. Het ISMS is ontworpen om de keuze van adequate en proportionele beveiligingsmaatregelen die de informatie beschermen en vertrouwen bieden aan belanghebbenden te waarborgen. De eisen in deze internationale norm zijn algemeen en bedoeld om van toepassing te zijn op alle organisaties, ongeacht type, omvang of aard.

# De eisen: ISO normen in het kort 2/3

**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. Voor veel afnemers geeft een ISO 27018 certificering van de clouddienst aanbieder extra zekerheid dat deze gevoelige data niet in verkeerde handen komt. De norm is ook gebaseerd op de ISO 27002, maar heeft een aanvullende set van beheersmaatregelen specifiek gericht op het beschermen van persoonsgegevens. Denk daarbij aan toestemming, gegevensminimalisatie en privacy klachten. Geheel in lijn met de eisen uit de AVG.

# De eisen: ISO normen in het kort 3/3

**ISO 27701:2019 – Privacy**

De internationale standaard rondom privacy management.
Deze geeft richtlijnen voor het vaststellen en uitvoeren van de voorschriften, het onderhouden en voortdurend verbeteren van een 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.

AZ komt tot de criteria van haar uitvraag door het uitvoeren van een QuickScan. Deze QuickScan gebruiken 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 (BBN1 t/m BBN3) en er wordt bepaald of een systeem 'bedrijfskritisch' is.

# Proces: Voldoen aan de eisen.

AZ 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 AZ 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:**

AZ kan vragen om een initiële/tijdelijke Fit/Gap analyse te leveren, hierin zijn ook te nemen maatregelen en de realisatie-data van de maatregelen opgenomen.

AZ controleert of aangeleverde certificaten (incl. audit scope en verklaring van toepasselijkheid) voldoende relevant zijn.

AZ controleert of de definitieve Fit/Gap analyse aan de vormvereisten voldoet, en als dat zo is:

Controleert AZ of de Fit/Gap analyse aannemelijk is en inhoudelijk lijkt te kloppen.

# Proces: Controle van naleving 2/2.

**Tijdens de contractperiode:**

Leveranciers stellen AZ 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.

AZ kan inspecties op naleving laten uitvoeren.