**ISACA Kennisgroep Privacy & GDPR**
**Discussion Paper 01 - ISO27701**

# Wat is de ISO27701 en waarom is dit belangrijk voor mij of mijn organisatie?

## Inleiding

Sinds de invoering van de Wbp (2001) en het van toepassing worden van de AVG (2018) is er in Nederland veel ervaring opgedaan met het implementeren van privacy gerelateerde wet- en regelgeving. Deze implementaties brengen uitdagingen met zich mee voor organisaties, met name op het gebied van – het kunnen aantonen van – compliance.

Om meer richting te geven aan deze implementatievraagstukken hebben de International Organization for Standardization (ISO) en de International Electrotechnical Commission (IEC) een standaard ontwikkeld die als benchmark en best practice kan functioneren. In augustus 2019 is deze privacy gerelateerde standaard uitgebracht onder de naam: "ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines" (hierna aangeduid als ISO27701).

In deze discussion paper wordt nader ingegaan op de rol en betekenis van de ISO27701.

## Introductie discussion papers ISO27701

De focusgroep ISO27701, onderdeel van de kennisgroep Privacy & GPDR van ISACA NL Chapter, brengt een serie van discussion papers over de ISO27701 uit. In deze serie brengen wij context en duiding met betrekking tot de betekenis van ISO27701. Deze discussion paper is de eerste van deze serie. De ontwikkelingen rondom de implementatie van en certificering op grond van ISO27701 zijn nog volop in beweging. Daarom is de status van verschillende facetten ofwel nog onbekend, dan wel niet definitief.

## Wat is de ISO27701?

ISO27701 is een Privacy Information Management System (PIMS) dat zorgdraagt voor een beheersingssysteem voor de bescherming van persoonsgegevens. Dit is een wereldwijde standaard.
De norm ISO27701 is van toepassing op alle typen organisaties, ongeacht hun omvang, zowel publieke als private ondernemingen, overheidsinstanties en non-profitorganisaties die werken met persoonlijk identificeerbare informatie (PII). Dit kan zijn als PII-verwerkingsverantwoordelijke of mede PII-verwerkingsverantwoordelijke, PII-verwerker, of beide.
Voor Europa (Nederland) geldt wetgeving voor de bescherming/verwerking van persoonsgegevens (Personally Identifiable Information: PII) op basis van de GDPR (AVG)[1], naast bestaande normatieve kaders (bijvoorbeeld: Telecommunicatiewet, Richtlijn bescherming gegevensbescherming Politie en Justitie).
De scope van ISO27701 is wel anders dan die van de AVG. ISO27701 is een internationale norm als onderdeel van de ISO27000-serie inzake information security en privacy, waaronder een set van controls die gebruikt kunnen worden bij de implementatie van het privacy framework.

[1] GDPR (General Data Protection Regulation), AVG (Algemene Verordening Gegevensbescherming)

Hierbij wordt veelal gedacht dat de toezichthouder, de Autoriteit Persoonsgegevens (AP), de aangewezen instantie is om goedkeuring aan de norm te geven. Dit is onjuist: de AP is als toezichthouder op naleving van de AVG niet in het leven geroepen om bij organisaties op de implementatie van maatregelen een ‘stempel’ te geven. Wel is het zo dat in ANNEX D (Informative) van de ISO27701 een mapping naar de GDPR is opgenomen.
Veel organisaties hebben de behoefte belanghebbenden aan te tonen dat er wordt voldaan aan de AVG in zijn geheel. Daar dit momenteel niet direct mogelijk is, richt men zich op de managementsystemen ter bescherming van persoonsgegevens. Om dit aan de buitenwereld te tonen kunnen derde partijen worden gevraagd een oordeel te geven. Voor onze ISACA leden is de ISO27001 (information security) waarschijnlijk het meest bekende voorbeeld van een onafhankelijke normenset met bijbehorende certificering. Geaccrediteerde instellingen met gecertificeerde auditors kunnen op basis van een audit overgaan tot afgifte van een certificaat waarbij een organisatie kan aantonen 'in control' te zijn over het normenkader van het desbetreffende onderwerp. ISO (en in Nederland NEN) regelt deze normenkaders wereldwijd. ISO27701 zal die rol moeten gaan vervullen, gelijk aan ISO27001, op het gebied van het verwerken van PII. Door het implementeren van een PIMS kan je als organisatie belanghebbenden laten zien dat je voldoet aan de normen uit de ISO27701.

**Kan de ISO27701 zonder de ISO27001?**
ISO27701 is een uitbreiding (extensie) van de ISO27001. Je kan de ISO27701daarom niet implementeren zonder te voldoen aan de ISO27001. Privacy en bescherming van persoonsgegevens waren al in ISO27001 opgenomen door een wettelijke vereiste (ISO27001 A.18.1.4), maar door de implementatie van ISO27701 maakt het onderdeel uit van het managementsysteem. Net als bij de ISO27001 is het belangrijk dat de organisatie op basis van een risicomethodiek een managementsysteem heeft geïmplementeerd dat bijdraagt aan dataprotectie.
Het doel van de ISO27701 is dan ook om organisaties een praktisch kader te bieden waarmee zij het bestaande ISMS (Information Security Management System) kunnen uitbreiden met een PIMS (Privacy Information Management System). In de ISO27701 is de PDCA-cyclus en risicoanalyse opgenomen conform de ISO27001.
Met deze uitbreiding kan een organisatie aantonen dat de PDCA-cyclus is geïmplementeerd en risicoanalyses zijn uitgevoerd volgens de beheersmaatregelen genoemd voor privacy in de ISO27701. Daarmee is de organisatie ‘in control’ over haar privacybeleid en implementatie.

**Heeft een organisatie met een ISO27701 certificering een goedkeuring van de Autoriteit Persoonsgegevens?**
De Autoriteit Persoonsgegevens (AP) heeft als toezichthouder geen bemoeienis met deze norm. Een organisatie met een ISO27701-certificaat voldoet niet per definitie aan de AVG.
Het zegt wel iets over de aandacht die een organisatie heeft voor privacy in de processen en verbetercyclus. In deze zin kan je stellen dat het een voorbeeld is van een 'best practice'.
De focus van de ISO27701 is niet gelijk aan die van de AVG. ISO27701 richt zich op het PIMS. Het PIMS richt zich voornamelijk op opzet en bestaan van beleid, maatregelen en procedures. De AVG is als wet anders dan een beheerssysteem: werking (of niet werken) van getroffen maatregelen kan reden zijn om een afwijking te constateren en een sanctie op te leggen. Denk hierbij bijvoorbeeld aan een datalek. Daarbij is een belangrijk onderscheid: de AVG is een EU-verordening, de ISO27701 is een wereldwijd toepasbare normenset.

**Wat is de waarde van een ISO27701-certificaat? Oftewel, moet ik/ mijn klant hier iets mee?**

Certificering heeft, door haar onafhankelijke toetsing, toegevoegde waarde op verschillende gebieden:

- Het is naar potentiële belanghebbenden een bewijs van bestaan van een geïmplementeerd beheersysteem. Dit kan een positief effect hebben op het imago en eventueel de omzet van een organisatie;
- Het versterkt het vertrouwen in de organisatie die persoonsgegevens gebruikt/verwerkt. Hieronder vallen ook niet-commerciële bedrijven en (semi)overheid;
- Certificatie is een goed hulpmiddel bij de selectie van leveranciers en geeft een indicatie van de professionaliteit van de betreffende leveranciers;
- Certificering speelt een rol bij het aantoonbaar naleven van governance codes;
- Het geeft aan dat privacy van afnemers en gebruikers, naast compliance, de aandacht van de organisatie heeft;
- Wij verwachten dat certificering, in lijn met ISO27001, op den duur steeds meer onderdeel van de license-to-operate zal worden;
- Het bespaart kosten (tijd, mensen en geld) in het beantwoorden van vragen en het per klant aantonen dat aan de contractvereisten wordt/kan worden voldaan. Denk hierbij aan een eventueel right-to-audit van de klant;
- Door de (vaak jaarlijkse) certificeringsaudit is er een externe druk om procedures en werking up-to-date te houden wat de kwaliteit van de processen ten goede komt;
- Het geeft organisaties zelf een handvat bij het inregelen van haar informatiebeveiliging en privacy.

Er zijn echter ook argumenten om niet te certificeren:

- De kosten/batenanalyse kan negatief zijn. Het is niet verplicht om te voldoen aan ISO27701. Zeker voor organisaties die weinig persoonsgegevens verwerken en daarbij zeker geen gevoelige/bijzondere persoonsgegevens is de toegevoegde waarde van een PIMS wellicht onvoldoende;
- Nadelen van early adopter: per 1 december 2020 zijn er in Nederland nog geen organisaties gecertificeerd. Hierdoor is kans groot dat organisaties op dit moment als eerste tegen bepaalde problemen aanlopen. Het kost dan meer moeite om te voldoen aan de standaard dan op het moment dat er een uitgebreide 'body of knowledge' is en er al vele implementatietrajecten bij allerlei organisaties zijn afgerond;
- De waarde die de AP aan het certificaat toekent, is nog onduidelijk. Op dit moment heeft deze nog geen uitspraak gedaan over de waarde van ISO27701. De vraag is of de AP dat überhaupt zal gaan doen.

**Wat zijn de verwachtingen voor de toekomst?**

Op 16 december 2020 heeft de NEN het keurmerk voor privacy informatie management officieel gelanceerd. Dit keurmerk wordt afgegeven aan organisaties die voldoen aan de eisen uit de norm ISO/IEC 27701. De eisen voor onafhankelijke beoordeling door certificerende instellingen zijn vastgelegd in het certificatieschema NCS 27701. Dit certificatieschema is opgesteld onder begeleiding van NEN. Het certificatieschema is nu gereed voor publiek gebruik en de eerste certificaten zijn al uitgereikt (zie website NEN).

Het zal vooral voor organisaties die veel persoonsgegevens verwerken, al een PIMS in opzet geïmplementeerd hebben en al een ISO27001-certificering hebben afgerond interessant zijn om met een relatief kleine inspanning te certificeren. De waarde moet zich echter in de praktijk nog uitwijzen. De waarde van een ISO27001-certificering is inmiddels aangetoond, voor de ISO27701 zal de praktijk dit moeten uitwijzen.

Omdat ISO27701 adopterende organisaties nu naast het ISMS ook een PIMS moeten implementeren, voorzien wij een behoefte om managementsystemen te integreren. Afhankelijk van de organisatie zal men zaken als kwaliteit, informatiebeveiliging en privacy in één geïntegreerd certificeerbaar managementsysteem willen onder te brengen.

**Overige opmerkingen**

In Nederland kennen wij van de ISO27001 verschillende gebruiksvormen. Zo zijn de Baseline Informatiebeveiliging Overheid (BIO) en de NEN7510 (Informatiebeveiliging in de Zorg) ingericht op de structuur en inhoud van de ISO27001 en ISO27002, waarbij er specifieke toelichting en eisen worden gegeven voor overheid en zorg. ISO27701 had ook voor een dergelijke uitwerking kunnen kiezen, gecombineerd met een ANNEX B die de ISO27701 specifieke onderwerpen afdekt.

Door het combineren van ISO27001 gebaseerd op best practices en standaarden onder verantwoordelijkheid van een informatiebeveiliger enerzijds met het aandachtsgebied van de Functionaris Gegevensbescherming, de Privacy Officer en de Data Protection Officer die zich in hun werkzaamheden baseren op wetgeving, anderzijds kan onbegrip en frictie ontstaan bij implementatie en verantwoordelijkheden.

ISO-normen zijn in principe landonafhankelijke standaarden. In de bijlage van de ISO27701 norm (ANNEX D) is een referentie naar EU-wetgeving (GDPR) opgenomen. Inmiddels werkt de community aan het uitbreiden van de referentietabellen. Er komen dan meer referentietabellen (mappings) naar verschillende privacy wet- en regelgeving beschikbaar. Referentietabellen, zoals naar de GDPR, zullen apart gevalideerd worden.

**De volgende discussion papers**

In onze tweede discussion paper gaan wij in op de relatie van ISO27701 met bestaande normen en raamwerken op het gebied van privacy en informatiebeveiliging. Uiteraard zullen wij dan ook op de relatie met ons ISACA-framework COBIT ingaan.
Wij hebben ook plannen voor discussion papers over de implementatie van ISO27701, de integratie van het PIMS in een gemeenschappelijk managementsysteem en de certificering op basis van ISO27701.

**Contact**

Voor vragen en opmerkingen over deze discussion paper kan contact opgenomen worden met de focusgroep via ISO27701@gdpr.isaca.nl.

## Introductie ISACA kennisgroep Privacy & GDPR/focusgroep ISO27701

De kennisgroep Privacy & GDPR is onderdeel van ISACA Netherlands Chapter. De kennisgroep volgt de implementatie van de GDPR/AVG en van andere normatieve kaders op het gebied van bescherming van persoonsgegevens in de EU/EER, waarbij zij context en duiding verschaft rondom relevante, actuele ontwikkelingen en andere aspecten met betrekking tot deze kaders.

De kennisgroep bestaat uit ongeveer tien leden die allemaal werken in dit werkveld. Om de kennis te delen met de overige ISACA-leden organiseren we Round en Square Ttables en schrijven we artikelen, discussion en whitepapers. Binnen de kennisgroep is er een focusgroep die ontwikkelingen over de ISO27701 bijhoudt.

De focusgroep ISO27701, verantwoordelijk voor deze discussion paper, bestond uit Jessica Maes, Harry van den Brink en Stephan van der Ende. Wij willen Jos Maas en de Privacy & GDPR werkgroep bedanken voor hun inhoudelijke commentaar en aanvullingen.