Discussion paper

‘De ISO27701: certificering en toekomstverwachtingen’

Inleiding en introductie discussion papers ISO27701

In augustus 2019 is de privacy gerelateerde standaard: “ISO/IEC[2] 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines” (hierna ISO27701) uitgebracht.

Vanuit de focusgroep ISO27701 brengen wij een serie van discussion papers (hierna papers) over de ISO27701 uit. Dit is de vierde en laatste paper in deze reeks.

In deze paper kijken we specifiek naar de aspecten die belangrijk zijn bij het certificeringsproces voor de ISO27701 en de verwachtingen voor de toekomst van ISO27701.

Door: drs. ing. Jessica Maes CISA Lead Auditor ISO27001, drs. Harry van den Brink RE CISM CRISC CDPSE Lead Auditor ISO27001 Lead Auditor ISO27701 en Stephan van der Ende MScBA CISM CISA CRISC Lead Implementer ISO27001.

Privacy certificeringen

Alhoewel het uitgangspunt van deze paper de ISO27701 standaard is, wordt in deze paper ook breder stilgestaan bij het certificeren op het gebied van privacy, waaronder ook de AVG-aandachtspunten.

In de Algemene verordening gegevensbescherming (AVG) wordt het onderwerp certificering genoemd (Afdeling V, met name artikel 42 en 43). In artikel 40 komt ook het onderwerp gedragscodes aan bod. In deze paper behandelen we de volgende categorieën van certificering:

- **ISO-certificering niet onder accreditatie van de Raad van Accreditatie (RvA)**
- **ISO-certificering onder accreditatie van de RvA**
- **Certificering als genoemd in de AVG**
- **Overige privacy specifieke certificeringen**

Uitgangspunten van de ISO27701-certificeringen

Een ISO27701-certificering geeft aan dat de vereisten voor het opzetten, implementeren, onderhouden en voortdurend verbeteren van een Privacy Information Management System (PIMS) zijn getoetst en voldoende zijn bevonden. Dit hebben wij ook in onze eerdere discussion papers uiteengezet en toegelicht. De certificering van de conformiteit met ISO27701 kan alleen in samenhang met de ISO27001 worden bereikt. De ISO27701 breidt de eisen van ISO27001 uit om rekening te houden met de bescherming van de persoonsgegevens. Ook aan alle eisen van ISO27001 moet worden voldaan om een ISO27701-certificering te kunnen behalen.

Er zijn twee opties voor deze ISO-certificering: onder accreditatie en niet onder accreditatie.

ISO Certificering onder accreditatie RvA

Bij het certificeren onder accreditatie gaat het om organisaties, die door de RvA zijn geaccrediteerd.

De RvA controleert daartoe of certificerende instellingen competent zijn. In conformiteitsbeoordelingsschema's (hierna te noemen: schema's) zijn de eisen vastgelegd voor instellingen die audits ten behoeve van het certificeren van een PIMS uitvoeren. Denk hierbij aan de opleidingseisen voor auditors, het beschikbaar zijn van een auditprogramma en dossiervorming. De RvA voert ook controles uit op de naleving van de door haar gestelde eisen.

Het schema NCS 27701, genaamd 'Conformiteitsbeoordeling – Eisen aan instellingen die audits ten behoeve van certificatie van privacy-informatiemanagementsystemen uitvoeren volgens ISO/IEC 27701', is inhoudelijk opgesteld door het College van Deskundigen (CvD), met begeleiding van NEN en onder het toezicht van de Commissie Schemabeheer. Accreditatie is dus eigenlijk het certificeren van de certificatie instelling op basis van een onafhankelijk onderzoek.

ISO Certificering niet onder accreditatie RvA

In principe kan ieder bedrijf een certificaat afgeven. De hierboven uitgelegde accreditatie is niet verplicht, wel hebben certificatie instellingen zich te houden aan de eisen uit de internationale norm voor Certificerende Instellingen (CI's): [1]. De waarde van het certificaat is dan gebonden aan het vertrouwen dat de gebruikers van het certificaat hebben in het bedrijf wat het certificaat heeft afgegeven.

[1] **zie isoregister.nl**

Certificering van ISO27701 in relatie tot de AVG

Sinds de invoering van de AVG zien we dat veel organisaties zich afvragen hoe zij precies aan de AVG kunnen voldoen en hoe ze dit kunnen aantonen.
Niet alleen Europese organisaties maar juist ook organisaties buiten Europa zijn geïnteresseerd in een AVG-certificering. De mate waarin is afhankelijk van de relatie van het desbetreffende land met de EU en de mate waarin hun klanten eisen stellen aan privacy compliance. De toegevoegde waarde varieert van een instrument voor marketing, tot een betere concurrentiepositie bij tenders, tot het afdekken van privacy risico's. In hoeverre ISO27701 daar een (tijdelijke) oplossing voor kan zijn, is afhankelijk van de inschatting van het individuele bedrijf.

Er wordt nog weleens gedacht dat een ISO27701-certificering betekent dat daarmee AVG-compliance aangetoond kan worden. Dit is echter niet juist, In de volgende alinea's wordt dit toegelicht.

Artikel 42 AVG

Artikel 42 gaat over de certificering zelf. Als verantwoordelijke of verwerker kunt u vrijwillig een AVG-certificaat aanvragen bij een certificerende instelling voor een product, proces of dienst[2] · Een AVG-certificaat geeft hiermee aan, dat op een bepaald onderdeel of proces voldaan wordt aan de AVG. De organisatie blijft verantwoordelijk voor naleving van de AVG op alle onderdelen[3]. Deze certificering is hiermee slechts een element in het leveren van betrouwbaar bewijs voor naleving van de bescherming van persoonsgegevens [4].

Een dergelijk certificaat is bedoeld als verklaring van conformiteit. Hiermee kan worden aangetoond dat op het moment van certificeren voor het betreffende product, proces of dienst wordt voldaan aan de verplichtingen betreffende de passende technische en organisatorische maatregelen (artikel 24, 25 en 32 AVG). Op dit moment worden geen certificaten verstrekt zoals bedoeld in artikel 42 van de AVG, omdat er nog geen certificerende instellingen zijn geaccrediteerd door de RvA voor uitgifte van een dergelijke certificering. Er zijn wel een aantal certificerende instellingen hard bezig dit te realiseren.

---

[2] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/avg-certificaat
[3] https://autoriteitpersoonsgegevens.nl/nl/nieuws/samenwerking-ap-en-rva-goedkeuring-avg-certificaten#subtopic-6518
[4] Zie richtsnoer EDPB:
https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_nl.pdf

Artikel 43 AVG

In artikel 43 wordt met name de accreditatie behandeld van de certificerende instelling. Naast de gecertificeerde instelling moet namelijk ook de certificerende instelling aan een aantal eisen voldoen. Hierin staat onder andere dat er geaccrediteerd wordt tegen de ISO17065, eisen voor certificerende instellingen die certificaten toekennen aan producten, processen en diensten.

Relatie AVG-certificering en ISO27701-certificering

De ISO27701 gaat over een managementsysteem (namelijk het PIMS) en geldt voor de verwerking van persoonsgegevens voor de gehele organisatie. Het ISO27701-certificaat toont aan dat een organisatie op een gestructureerde manier met persoonsgegevens omgaat met behulp van het PIMS. Het wijkt hiermee in reikwijdte af van de certificering van artikel 42 die specifieke eisen aan producten, processen of diensten stelt en niet gericht is op het managementsysteem van de organisatie. Daarom wordt de ISO27701 niet tegen de ISO17065 geaccrediteerd, maar tegen de ISO17021. In de ISO17021 staan eisen voor certificerende instellingen die managementsystemen beoordelen.

Omdat er op het moment van schrijven nog geen ervaringen zijn met certificeren op basis van artikel 42 en 43 AVG is er geen praktijkinformatie beschikbaar om dit onderscheid verder te duiden.

Gedragscodes en overige AVG-certificeringen

Alhoewel een gedragscode niet expliciet is opgenomen in de ISO27701 noemen wij toch de mogelijkheid tot certificering door het opstellen van een gedragscode. Deze wordt namelijk wel genoemd in de AVG[5]: de artikelen 40 en 41 hebben hier betrekking op. In een gedragscode is meer concreet dan in de AVG uitgewerkt hoe een groep verantwoordelijken of verwerkers omgaat met persoonsgegevens. Op dit moment is er één voorlopig goedgekeurde gedragscode door de Autoriteit Persoonsgegevens van Data Pro Code Nederland. Dit is een gedragscode specifiek voor verwerkers. Een organisatie kan zich laten certificeren tegen de gedragscode en zich laten opnemen in het register. Er moet nog wel een toezichthoudend orgaan worden aangesteld die zorgt voor accreditatie. Als dit gebeurt is de Data Pro Code de eerste goedgekeurde gedragscode in Nederland.

Naast de certificeringsmogelijkheden die genoemd worden in de AVG zijn er ook organisaties die een eigen AVG certificaat afgeven. Deze organisaties zijn veelal gespecialiseerd in (IT) audits en het afgeven van certificaten. Dit staat los van zowel de mogelijkheden genoemd in de AVG als van de ISO27701-certificering. De waarde van deze certificaten is afhankelijk van de gestelde eisen door de organisatie die het certificaat afgeeft, de kwaliteit van de audit en de opvolging.

---

[5] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/avg-gedragscode

Gerelateerde (niet primair privacy) beoordelingen

Bedrijven die opgaan voor een ISO27701-certificering kunnen ook te maken hebben met certificeringen, beoordelingen en audits vanuit andere eisen en/of partijen. Denk hierbij bijvoorbeeld aan SOC1 en SOC2 rapporten die met name voor processen bekend zijn met een financieel effect en gebaseerd zijn op de criteria van de AICPA[6].
SOC2 richt zich specifiek op operational IT-controls die zijn uitbesteed, waarbij een type 2 audit staat voor de toets op opzet, het bestaan en werking van de controls. Dit raamwerk omvat naast de controls op het gebied van Security, Availability, Processing Integrity en Confidentiality ook Privacy controls. In Nederland heeft NOREA handreikingen opgesteld voor SOC2 rapporten. Zie voor meer informatie de handleiding van NOREA.[7]

Vooruitblik

Wijzigingen binnen ISO27xxx

Er zijn wijzigingen op komst met betrekking tot de inhoud van de ISO27002 en daarmee ook op de ISO27701. De huidige ISO27002 norm dateert uit 2013. In 2018 is besloten deze te actualiseren. De verwachting is dat dit begin 2022 leidt tot het van kracht worden van de nieuwe norm. Het aantal beheersmaatregelen gaat terug in aantal. Dit leidt niet tot inhoudelijke verwijdering van normen, het betreft vooral samenvoegingen. Er zijn ook een aantal nieuwe controls opgenomen, waaronder Threat Intelligence, Data Leakage prevention en Secure coding.

Aangezien ISO27002 de basis is voor bijlage A van ISO27001, zal een update naar ISO27002 onvermijdelijk van invloed zijn op de controleset in ISO27001. Deze wijzigingen zullen naar verwachting worden verwerkt in bijlage A van ISO27001 na de officiële release van de bijgewerkte ISO27002 om ervoor te zorgen dat de informatie uit beide standaarden consistent is. Dit zal ongetwijfeld gevolgen hebben voor de ISO27701. Echter voorlopig is het nog niet duidelijk welk effect dit heeft op de ISO27701.

Aansluiting ISO bij wet- en regelgeving in Europa

Inmiddels wordt er door CEN/CENELEC gewerkt aan een 'Privacy information Management System per ISOIEC27701 – Refinements in European context'. Hierin wordt (in de huidige draft) bijvoorbeeld de rol van de DPO conform de GDPR/AVG nader uitgewerkt.

---

[6] 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy. Including March 2020 update.
[7] https://www.norea.nl/download/?id=6460
NOREA Handreikig voor SOC2 en SOC3 op basis van ISAE3000 / richtlijn 3000A dd December 2019

Marktverwachtingen

We hebben in de afgelopen 2,5 jaar gezien dat de markt kennis neemt van de norm en de eerste organisaties hebben zich ook laten certificeren. Hoewel dit niet de snelle omarming is door de markt die we in discussion paper 1 verwachtte, zien we wel nog steeds de behoefte bij organisaties om op een juiste en gestructureerde manier met privacy en de verwerking van persoonsgegevens om te gaan.

Huidige discussiepunten

Is een ISO27701-certificering interessant voor de bestuurder?

Wij zien regelmatig dat onderwerpen uit de security en privacy wereld met golven aandacht krijgen. Bepalend hiervoor zijn vaak actualiteiten en introductie van nieuwe wet- en regelgeving. De AVG zorgde in 2018 voor een toenemend bewustzijn van privacy bij de bestuurder, waarna organisaties grote trajecten opstartten om te voldoen aan de nieuwe verordening.

Nu, begin 2022, zijn de meeste AVG projecten die destijds zijn opgestart wel afgerond. Hoewel er vaak nog veel werk ligt om (blijvend) aan de AVG te voldoen, merken we dat de aandacht van bestuurders voor de AVG weer afneemt. Dergelijk bewustzijn bij de bestuurder heeft natuurlijk ook invloed op de behoefte van een organisatie om zich wel of niet te laten certificeren. Dit kan hiermee gevolgen hebben voor het commitment om een ISO27701-certificeringstraject op te starten.

Hoe dit in de toekomst zich zal ontwikkelen is moeilijk te voorspellen. Het onderwerp kan nieuwe impulsen krijgen door bijvoorbeeld strenge handhaving door de AP. Ook security incidenten zoals Log4j kunnen bijdragen aan meer bewustzijn omdat security en privacy vaak, al dan niet terecht, tezamen worden beschouwd.

Onbekend maakt onbemind?

Momenteel (februari 2022) zijn er slechts negen organisaties opgenomen in het register dat de NEN bijhoudt van gecertificeerde Nederlandse organisaties. Anderhalf jaar nadat de norm is gepubliceerd is dit geen groot aantal in vergelijking met het aantal organisaties dat een ISO27001-certificering heeft. Weliswaar is het NEN-register beperkt daar niet alle Nederlandse certificerende instellingen en geen buitenlandse certificerende instellingen deelnemen, maar het geeft wel een indicatie.

We merken dat de bekendheid van deze, op dit moment nog relatief nieuwe norm, nog niet erg hoog is.

Hiernaast zijn organisaties veelal opzoek naar concrete AVG compliance. Hoewel het voldoen aan de norm hieraan kan bijdragen, betekent een certificering niet dat een organisatie daardoor ook per definitie altijd in lijn met de AVG persoonsgegevens verwerkt. Tot slot is ook van een "license to operate" op dit moment nog geen sprake. We zien de norm nog niet veelvuldig uitgevraagd worden bij inkooptrajecten.

Waarde?

Het is nog steeds moeilijk te voorspellen of de ISO27701 dezelfde positie op het gebied van privacy in kan nemen als de ISO27001 op het gebied van informatiebeveiliging. Veel zal afhangen van de perceptie van de markt. Zal de markt de norm omarmen als de best practice op het gebied van privacy? Een andere belangrijke factor is of de certificering ook door de dataprotectie autoriteiten wordt erkent als certificering waarmee een organisatie kan aantonen deels te voldoen aan de AVG in plaats van de huidige visie als 'best practice'.

Conclusie

Alhoewel een ISO27701 géén 'vrijwaring' richting AP is, geeft het een organisatie wel de mogelijkheid om aan te tonen dat de privacy-processen op orde zijn.

Zoals blijkt uit de uiteenzetting, zijn er nog weinig alternatieven om door middel van een certificering aan te tonen dat men voldoet aan de AVG. Het laten certificeren op basis van een gedragscode of het afnemen van een AVG-certificering opgezet door organisatie die zelf verantwoordelijk zijn voor het kwaliteitsniveau, zijn op dit moment de enige opties.

Wij zijn daarom nog steeds van mening dat een ISO27701-certificering een toegevoegde waarde heeft voor iedere onderneming die ISO27001 gecertificeerd is. De extra inspanning is beperkt (zie ook discussion paper drie over de implementatie), de kwaliteit van het certificaat is geborgd, en een geïntegreerd ISMS/PIMS geeft een organisatie de zekerheid dat de voornaamste processen op security en privacy beheerst worden.

Contact

Voor vragen en opmerkingen kunt u contact opnemen met de focusgroep. Deze kunt u bereiken via ISO27701@gdpr.isaca.nl.

Over 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 werkzaam zijn in privacy, information security, governance en risk. Om de kennis te delen met de overige ISACA-leden organiseren we Round en Square Tables 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, bestaat uit Jessica Maes, Harry van den Brink en Stephan van der Ende. Wij willen de Privacy & GDPR werkgroep, Fokke-Jan van der Tol, Christian Oudenbroek (Brand Compliance) en Marco Bijl (Digitrust) bedanken voor hun inhoudelijke commentaar en aanvullingen, eveneens de ISACA NL Review board.