Discussion paper

‘Hints en tips bij de implementatie van de ISO27701’

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. De eerste paper: ‘Wat is de ISO27701 en waarom is dit belangrijk voor mij of mijn organisatie?’ en de tweede paper: “Hoe verhoudt de ISO27701 zich tot andere raamwerken? “ zijn te vinden op de ISACA-website.
In deze derde paper kijken we op welke wijze en met welke aandachtspunten de ISO27701 geïmplementeerd kan worden.

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

Implementatie ISO27701 in combinatie met de ISO27001

Integratie ISMS en PIMS

ISO-normen hebben grotendeels dezelfde structuur en daardoor is integratie, zeker op managementsysteemniveau, relatief eenvoudig. Onderdelen zoals risicoanalyse, PDCA-cyclus, monitoring en dergelijke komen in alle managementsystemen voor. De meeste (zo niet alle) organisaties hebben al een ISO27001-certificering afgerond als zij starten met een ISO27701-implementatie. Zij gebruiken het ISMS als een fundament voor de implementatie van het (Privacy Information Management System) PIMS van de ISO27701.

Voordat je een implementatietraject voor de ISO27701 opstart is het van belang om eerst gedegen de scope te bepalen. Dit kan veel onduidelijkheid wegnemen en brengt focus aan. De scopebepaling is essentieel voor het goed inrichten van je PIMS. Hierbij ben je mede afhankelijk van de scope van je ISMS; het is essentieel dat deze managementsystemen goed op elkaar aansluiten!

Denk ook goed na over de interne bedrijfsondersteunende processen. Het wel of niet opnemen van processen met betrekking op personeelsbeheer- en administratie bijvoorbeeld, kunnen van grote invloed zijn op het te verrichten werk. De toegevoegde waarde van het opnemen van deze processen in je scope is niet direct zichtbaar voor klanten, maar wel van belang voor de eigen medewerkers.

Beleidsdocumentatie

Naast de integratie van de managementsystemen ISO27001 en ISO27701 is het ook van belang een keuze te maken over de integratie van de vereiste beleidsdocumenten. Zo kan een organisatie kiezen voor een informatiebeveiligingsbeleid én een separaat privacybeleid of kiezen voor een informatiebeveiligings- en privacybeleid (geïntegreerd). ISO laat de organisatie daarin vrij.

In de praktijk wordt vaak ook de integratie van de ISO9001-norm meegenomen, resulterend in één Managementsysteem dat kwaliteit, informatiebeveiliging en privacy beheerst.

TIP!

Integratie van ISO-normen zal steeds meer standaard worden. Met de introductie van de Harmonized Structure (HS), voorheen de High Level Structure (HLS) genaamd, wordt daar al op ingespeeld. De HS wordt dan de basisstructuur van alle ISO-managementsystemen. Dat betekent dat managementsysteemnormen als ISO9001, ISO14001, ISO27001 en uiteraard de ISO27701 voortaan dezelfde hoofdstuk- en paragraafindeling kennen. Deze eenduidige structuur vergemakkelijkt het integreren van managementsystemen sterk.
NB: het zal enige tijd duren voordat alle normen op deze nieuwe structuur zijn geënt. De huidige versie van de ISO27701 (2019) is nog gebaseerd op de HLS, maar deze is al wel bruikbaar voor toekomstige integratie.

ISO27701 en AVG

Uiteraard dient elke organisatie zich aan de wet te houden en voor privacy betekent dat onder andere voldoen aan de AVG. Afhankelijk van de organisatie en de primaire processen kunnen ook nog aanvullende eisen worden gesteld, denk bijvoorbeeld aan de strafrechtketen, zorg- en telecomsector. Hoe gestructureerder en uitgebreider een organisatie de wettelijke richtlijnen heeft verwerkt, hoe eenvoudiger het zal zijn om deze in het ISO27701-certificeringsproces op te nemen.

Organisatie, functies en rollen

Door het op een gestructureerde manier willen beheersen van privacy in combinatie met informatiebeveiliging, komen ook meer afdelingen en functies/rollen in beeld waarbij uiteraard ook het uitbreiden van bestaande rollen een optie is. Dit heeft gevolgen voor de governance, en het inrichten en beheersen van het informatiebeveiligings- en privacybeleid (ISO27001, ISO27701).

De belangrijkste functies en rollen om rekening mee te houden worden hieronder besproken.

Functionaris Gegevensbescherming (FG) / Data Protection Officer (DPO)

De FG moet toezien op de toepassing en naleving van de AVG binnen de organisatie. In de AVG is een aparte sectie opgenomen over de FG. Hierin staat:

- Wanneer een organisatie verplicht is een FG aan te stellen (artikel 37);
- Welke eisen er zijn t.a.v. de positionering van de FG, denk hierbij bijvoorbeeld aan onafhankelijkheid (artikel 38);
- Wat het minimale takenpakket is van de FG, denk hierbij bijvoorbeeld aan het monitoren van de naleving van de AVG en meer specifiek het geven van advies over Data Protection Impact Assessments (DPIA's) (artikel 39).

TIP!

De FG heeft conform artikel 38 van de AVG een onafhankelijke en toezichthoudende rol die niet met een CISO-functie te combineren valt.

Privacy Officer (PO)

De PO heeft een meer uitvoerende taak dan de FG. Anders dan de FG heeft de PO geen toezichthoudende rol. De PO kan bijvoorbeeld beleid en processen ontwikkelen en de organisatie helpen met implementatie hiervan. Afhankelijk van de behoefte van de organisatie kan de invulling van de rol verschillen. Soms is er naast de PO ook een rol ingericht voor een Privacy Jurist en richt de PO zich meer op implementatie en coördinatie. Zeker bij kleinere organisaties is deze tweedeling er vaak niet en houdt de PO zich ook met juridische aspecten bezig.

Databeheer functies

Het belang van een goede beheersing van data en de daarvoor bijbehorende functies (bijvoorbeeld data managers, data custodians en data stewards) is zeer groot bij organisaties die veel persoonsgegevens verwerkt.

Privacy Champion

Analoog aan de rol ‘Security Champion’ zien wij steeds meer de rol van ‘Privacy Champion’ opkomen. Ook bij het werken in een agile omgeving komen dergelijke champions regelmatig voor. In de praktijk is dit een rol (waar beperkte tijd beschikbaar voor gesteld wordt), met relatief weinig bevoegdheden. Het zijn meestal – centrale of lokale – aanspreekpunten op het gebied van privacy als ‘Subject Matter Expert (SME)’ en wij zien ze zowel in de lijnorganisatie als bij ontwikkelteams. Het is aan te bevelen om deze Privacy Champions op regelmatige basis, kennis met elkaar uit te laten wisselen.

Legal / juridische zaken – Privacy Jurist

De afdeling juridische zaken heeft in ieder geval een expertfunctie bij bijvoorbeeld het afsluiten van (verwerkers)overeenkomsten, Service Level Agreements (SLA’s) en voorwaarden. Soms zijn er één of meerdere privacyjuristen die zich specifiek bezighouden met het interpreteren en ‘vertalen’ van de wettelijke privacyvereisten in richtlijnen of procedures voor de organisatie op het gebied van privacy.

Interne bedrijfsondersteunende functies op het gebied van Marketing, Finance en HR

Direct of indirect heeft bijna iedere afdeling met het beschermen van persoonsgegevens te maken en moeten de processen voldoen aan de eisen uit de ISO27701. Voor marketing kan bijvoorbeeld gedacht worden aan het gebruik maken van SaaS-tools om nieuwsbrieven te sturen, finance houdt mogelijk gegevens bij die betrekking hebben op de financiën van medewerkers en houdt daarnaast vaak ook contactgegevens van medewerkers van bedrijven bij (of kan ze benaderen) en uiteraard heeft Human Resources veel gegevens over zowel eigen als inhuurpersoneel.

Het is van groot belang dat alle afdelingen voor hun bedrijfsproces. weten hoe ze moeten voldoen aan de gestelde eisen van ISO27701. Dit vereist dat voor activiteiten als bijvoorbeeld het bijhouden van een mailinglist de betrokkenen wel op de hoogte moeten zijn van privacyaspecten zoals een onderbouwde grondslag en, zeker indien van partijen buiten de EU gebruikgemaakt wordt, dat de systemen/leveranciers aan alle (privacy) eisen moeten voldoen. Ook het gebruiken van een marketingwebsite waarbij (potentiële) klanten zich kunnen registreren voor extra informatie, moet aan eisen voldoen. Denk bijvoorbeeld aan het voldoen aan regels voor toestemming en de wetgeving inzake cookies en direct mailings (telecommunicatiewet).

PIMS documentatie

Voor het PIMS zijn een aantal documenten nodig die geborgd zijn in het privacybeleid. Het beleid kan een uitbreiding zijn op het bestaande informatiebeveiligingsbeleid of een apart privacybeleid.

Voorbeelden van additionele privacydocumenten (deels wettelijk verplicht) zijn:

- Register van verwerkingen
- Vastleggen van toestemming van gebruiker
- Data Privacy Impact Assessments (DPIA's)
- Verwerkersovereenkomsten/ overeenkomsten bij gedeelde verwerkingsverantwoordelijkheid
- Documentatie rondom data transfers naar landen buiten EER waaronder Data Transfer Impact Assessments (DTIA's)
- Documentatie over hoe de organisatie invulling geeft aan de rechten van de betrokkenen
- Privacyverklaring (intern/extern)
- Documentatie over het invullen van privacy-by-design en privacy-by-default

Bovenstaand lijst is slechts een indicatie van de meest belangrijke additionele documentatie die bij de implementatie een PIMS komt kijken. Het is geen uitputtende lijst. Overigens is het opstellen en gebruik van bovenstaande documentatie vaak onderdeel van een proces in de organisatie. Het is binnen de ISO-systematiek belangrijk om deze processen te documenteren. Een voorbeeld hiervan is het proces voor het uitvoeren, opvolgen en onderhouden van DPIA’s en de gesignaleerde privacy risico’s.

Verwerkingsverantwoordelijkheid

Er is bij privacy extra aandacht nodig voor de onderlinge verantwoordelijkheden ten aanzien van de verwerkingen die partijen in de keten expliciet moeten vastleggen. De verantwoordelijkheden worden vastgelegd in overeenkomsten die organisaties met elkaar sluiten. Breng de leveranciers in kaart en vraag af wie het doel en de middelen stelt. De FG kan meedenken over twijfelgevallen.

Zeker binnen de overheid worden vaak gegevens gedeeld om te informeren. Hier wordt in veel gevallen een gegevensleveringsovereenkomst voor afgesloten, waarin ook doel en eventueel risico mitigerende maatregelen instaan.

TIP!

Let goed op, derden worden nog te vaak gezien als verwerker waardoor er soms onnodig verwerkersovereenkomsten worden afgesloten. Derden kunnen zelfstandig verwerkingsverantwoordelijke zijn en een verwerkersovereenkomst is dan niet vereist. Het afsluiten van overeenkomsten is daarmee tevens een juridisch aandachtspunt waar een deskundig oordeel voor vereist is. Voor meer informatie zie onder andere de sites van European Data Protection Board en de Autoriteit Persoonsgegevens.

ISO27701: de norm

De norm ISO27701 is opgebouwd volgens de “High Level Structure” die gebruikt wordt door ISO voor eisen aan managementsystemen. Verder zijn er in de norm vier belangrijke hoofdstukken te onderkennen:

- PIMS-specifieke eisen (requirements) voor ISO27001 (managementsysteem)
- PIMS-specifieke richtlijnen (guidelines)voor ISO27002 (maatregelen)
- PIMS-specifieke beheersmaatregelen (controls) voor verwerkingsverantwoordelijken
- PIMS-specifieke beheersmaatregelen (controls) voor verwerkers

Hieronder wordt toelichting gegeven op de opbouw van de norm en wordt apart ingegaan op ieder van de bovengenoemde vier hoofdstukken. Het managementsysteem bestaat uit 10 clausules die in elke ISO-standaard voor een managementsysteem terugkomen:

1. Scope
2. Normative references
3. Terms and definitions
4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

PIMS-specifieke eisen voor ISO27001 (managementsysteem)

De ISO27701 bouwt op de requirements (vereisten) die in de ISO27001 worden genoemd. In de ISO27701 worden hier voor het PIMS wel enkele requirements aan toegevoegd en worden bestaande requirements uitgebreid. Dit is het geval bij de onderwerpen “context van de organisatie” en bij “planning”. Bij het onderdeel planning zijn requirements aangepast die betrekking hebben op risicomanagement De overige onderwerpen blijven in de ISO27701 grotendeels ongewijzigd ten opzichte van de ISO27001. Een algemene wijziging die voor de gehele norm geldt is dat daar waar in de ISO27001 gesproken wordt over informatiebeveiliging dit bij de ISO27701 logischerwijs wordt uitgebreid met privacy.

TIP!

Let bij context van de organisatie er goed op dat, waar het om belanghebbenden gaat, vanuit privacy perspectief de rol van de betrokkene erg belangrijk is. In het PIMS zal de focus daar voor een groot deel op liggen.

Onderwerp in ISO27001	**Aanvullende of gewijzigde requirements in ISO27701**
Context van de organisatie	Ja
Leiderschap	Nee
Planning	Ja
Ondersteuning	Nee
Uitvoering	Nee
Evaluatie van de prestatie	Nee
Verbetering	Nee

Tabel 1: Aanvullende of gewijzigde requirements per onderwerp

PIMS-specifieke richtlijnen voor ISO27002 (maatregelen)

In de ISO27701 zijn voor elk van de onderwerpen in de ISO27002, behalve voor bedrijfscontinuïteitmanagement, extra richtlijnen beschreven. Vaak wordt in de richtlijnen aangegeven dat de organisatie in control moet zijn ten aanzien van het verwerken van persoonsgegevens. Bijvoorbeeld als het gaat om het classificeren van data is het ook van belang dat er een of meerdere categorieën qua privacygevoeligheid zijn voor persoonsgegevens.

Er zijn ook richtlijnen die wat meer verandering met zich meebrengen, denk bijvoorbeeld aan het inbedden van de rol van de functionaris gegevensbescherming in de organisatie of het implementeren van een proces voor privacyincidenten en datalekken.

PIMS-specifieke controls voor verwerkingsverantwoordelijken

De norm ISO27701 kent 31 extra controls voor verwerkingsverantwoordelijken (zie ISO27701 ANNEX A). Deze zijn in lijn met wat in de AVG staat. Denk hierbij bijvoorbeeld aan het invulling geven aan de principes van doelbinding en dataminimalisatie. Maar ook zaken als het hebben van een verwerkingsregister en een privacyverklaring komen hierin terug. De rechten van betrokkene(n) moeten in de processen worden opgenomen.

PIMS-specifieke controls voor verwerkers

De norm kent 18 controls voor verwerkers (zie ISO27701 ANNEX B). Deze controls hebben betrekking op de situatie waarin de eigen organisatie verwerker is. Denk aan het bijvoorbeeld van doelbinding, hetgeen ook een control voor de verwerkingsverantwoordelijke is.

Een specifieke control voor de verwerker is bijvoorbeeld dat bij wijziging van een sub-verwerker eerst de verwerkingsverantwoordelijke hiermee akkoord moet zijn.

Bijlagen ISO27701

Een van de belangrijkste bijlagen van de ISO27701 is in onze ogen ANNEX D, de ‘mapping to the GDPR’. Alhoewel er veel disclaimers in de tekst staan (indicative mapping e.d.) kan dit zeer behulpzaam zijn bij het aantonen van compliance met de GDPR.

TIP!

Inmiddels wordt er door CEN/CENELEC gewerkt aan een ‘Privacy information Management System per ISOIEC 27701 – Refinements in European context’[1]. Hierin wordt (in de huidige draft) bijvoorbeeld de rol van de DPO conform de GDPR/AVG nader uitgewerkt.

[1] https://www.cencenelec.eu/news/brief_news/Pages/TN-2021-018.aspx

ISO27701 implementatie praktijktips

Voor onderstaande tips en aandachtspunten hebben wij gebruikgemaakt van de ervaringen die zijn gedeeld tijdens de NEN-webinar “Privacy in de Praktijk” waar wij als ISACA ook een bijdrage aan hebben geleverd. In het bijzonder zijn wij Michelle Spit dankbaar. Zij is werkzaam bij Zaurus (zaurus.nl), waar zij de implementatie van ISO27701 en certificering heeft geleid. Zaurus levert digitale spreekkamers voor de zorg: gezien het type persoonsgegevens heeft Zaurus als één van de eerste organisaties de ISO27701 omarmd.

De tips van Michelle Spit

- *Zorg dat management verantwoordelijkheid neemt voor de implementatie en jou, als projectleider, met woord en daad ondersteunt;*
- *Klanten (en prospects) hechten waarde aan privacy en de aantoonbaarheid daarvan. De business case is dan snel gemaakt;*
- *Betrek alle medewerkers, zeker de ontwikkelaars (denk aan privacy-by-design), vanaf het begin en laat ze zelf zo veel mogelijk het ‘hoe’ van de norm invullen;*
- *ISO-normen zijn gestructureerd. Richt je project zo veel mogelijk conform de norm in, zodat snel inzicht is of aan de norm wordt voldaan;*
- *Gebruik tooling om repeterende taken in de organisatie uit te zetten en zorg voor dashboard om niet éénmaal per jaar bij de audit, maar continu de compliance te meten en rapporteren.*

Conclusie

Samenvattend, naast alle tips en onderbouwing in de voorgaande paragrafen, hebben wij op hoofdlijnen drie conclusies.

Implementatie ISO27701

Het toevoegen van de ISO27701 is qua inspanning, kosten en doorlooptijd afhankelijk van de mate van volwassenheid van de organisatie. Hieronder vallen onder andere de compliance aan de AVG en het ingerichte ISMS voor informatiebeveiliging. Organisaties die een goed werkend ISMS hebben opgezet kunnen met relatief weinig extra werk de ISO27701 integreren.

Onderhoud managementsysteem informatiebeveiliging en privacy

Als de organisatie bij de implementatie van ISO277001 overgaat naar een geïntegreerd managementsysteem voor zowel informatiebeveiliging als privacy is het onderhoud van beide raamwerken minder intensief en het aantonen van compliance aan deze ISO-normen minder tijdrovend.

Volgordelijkheid implementatie ISO27701

Naast de optie om aanvullend op de ISO27701 de IS27701 te implementeren is het zeker mogelijk om de ISO27001 en ISO27701 tegelijk te implementeren. Voordeel is dat op een natuurlijke wijze een geharmoniseerd managementsysteem zal ontstaan, nadeel is dat er binnen de organisatie nog geen ervaring is met een op ISO gebaseerd managementsysteem voor informatiebeveiliging.

De volgende paper

In onze vierde paper gaan wij in op de certificering op basis van ISO27701.

Contact

Voor vragen en opmerkingen kunt u contact opnemen met de focusgroep. Deze kunt u bereiken 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 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 bedanken voor hun inhoudelijke commentaar en aanvullingen, eveneens de ISACA NL Review board. Ook Michelle Spit, CISO Zaurus, willen wij hartelijk danken voor haar medewerking.