DATA & INSIGHTS NETWORK

ISO NORMEN – ISO 27701:2019

Sinds september 2019 is er een voor de onderzoekwereld interessante uitbreiding van ISO 27001 gekomen: de norm ISO 27701:2019 Privacy-informatiemanagement. Deze norm vult het gat tussen de behoefte van de opdrachtgever aan zekerheden met betrekking tot privacybescherming enerzijds en het informatiebeveiligingssysteem van het bureau anderzijds. Certificering voor ISO 27701:2019 is alleen mogelijk indien het betrokken bureau al over een ISO 27001 certificaat beschikt.

In de tekst van ISO 27701:2019 komen enkele begrippen veelvuldig voor die onderzoekers bekend in de oren zullen klinken:

- PII: Personally Identifiable Information: dit betreft alle tot individuele personen (dus ook respondenten) herleidbare informatie
- PIMS: Privacy Information Management System: dit beschrijft de wijze waarop binnen het bureau met privacy wordt omgegaan
- PII Verwerkingsverantwoordelijke: dit is degene, resp. de organisatie, die uiteindelijk verantwoordelijk is voor het verwerken van privacygevoelige informatie (veelal de opdrachtgever)
- PII Verwerker: dit is degene, resp. de organisatie, die in opdracht van de PII Verwerkingsverantwoordelijke privacygevoelige informatie verwerkt, veelal in een rol als onderzoekbureau of onderaannemer van een bureau.

ISO 27701 geeft aanvullingen op ISO 27001
ISO 27701:2019 stelt aanvullende eisen aan hoofdstuk 4 (Context van de organisatie) en hoofdstuk 6 (Planning) van ISO 27001. Daarnaast worden aanvullende beheersmaatregelen genoemd (in aanvulling op Bijlage A van ISO 27001). Tenslotte heeft ISO 27701:2019 een nieuwe Bijlage B getiteld ‘PIMS-specifieke referentie-beheers-doelstellingen en -maatregelen’, bedoeld voor PII verwerkers.

Een nuttig onderdeel van ISO 27701:2019 is Bijlage D, getiteld ‘Kruisverwijzing naar de Algemene verordening gegevensbescherming’. Hierin wordt de relatie gelegd tussen de AVG (resp. GDPR) en ISO 27701:2019.

De Bijlagen B en D in ISO 27701:2019 beschrijven een aantal beheers-doelstellingen en -maatregelen die specifiek gelden voor PII-Verwerkers (dus voor bureaus) en geven het verband met de AVG weer:

- Een eerste set maatregelen heeft betrekking op de voorwaarden voor het verzamelen en verwerken van PII. Eer moet toestemming van de respondent zijn, het eventuele andere gebruik moet beschreven en overeen gekomen zijn, de

verplichtingen van alle betrokkenen moeten beschreven zijn en het moet duidelijk zijn hoe de verwerking van PII geregistreerd wordt.
- Voor PII-Verwerkers (dus: bureaus) gelden ook regels met betrekking tot tijdelijke bestanden, het overdragen van bestanden, het registreren van deze overdracht, het vermelden van onderaannemers die PII verwerken, etc.
- De zeer uitvoerige Bijlage D geeft gedetailleerd aan welke onderdelen van de AVG aan de orde komen in de verschillende paragrafen van ISO 27701:2019.

Het lijkt complex, maar de norm ISO 27701:2019 is zonder meer haalbaar voor ISI 27001-gecertificeerde organisaties.

Meer informatie of een afspraak maken met Toetsingsbureau KCC? Neem dan contact op met Ed van Eunen via ed.van.eunen@toetsingsbureau-kcc.nl onder vermelding van het ISO-nummer.

MET HET DATA & INSIGHTS NETWORK, WEET JE MEER EN WEET JE HET EERDER!