DATA & INSIGHTS NETWORK

ISO NORMEN – ISO 27001:2017 Informatiebeveiliging

Het onderwerp ‘databeveiliging’ staat sterk in de belangstelling. Dit heeft enerzijds te maken met de complexiteit rond de beveiliging van digitale informatie: elke dag vinden op dit gebied wel weer nieuwe ontwikkelingen plaats. Anderzijds heeft de belangstelling ook te maken met de grote nadruk die momenteel op ‘privacy’ wordt gelegd. Vanaf mei 2018 is de ‘AVG’ (Algemene Verordening Gegevensbescherming) van kracht. Deze verordening stelt hoge eisen aan databescherming.

De algemene marktonderzoeksnorm ISO 20252:2019 schrijft weliswaar voor dat data op een goede wijze bewaard en beschermd dienen te worden maar heel concreet hierover is deze norm niet.

Veel specifieker is de databeveiligingsnorm ISO 27001:2017, een norm die met grote regelmaat geactualiseerd wordt. Het is een norm die op dit moment door veel opdrachtgevers geëist wordt van hun marktonderzoekbureau. Een groeiend aantal onderzoekbureaus is inmiddels voor deze norm gecertificeerd.

In de norm ISO 27001:2017 gaat het feitelijk om 3 hoofdthema’s:

- Het zodanig beveiligen van data dat alleen formeel toegelaten personen er toegang toe hebben
- Het bewaken van de integriteit van data, dus vermijden dat onbevoegden veranderingen kunnen aanbrengen in databestanden
- De omgang met incidenten: het waarborgen dat databestanden behouden blijven in het geval van bijvoorbeeld brand of stroomuitval

De ISO 27001:2017 norm is qua structuur vergelijkbaar met ISO 9001:2015 en ISO 14001:2015:

- Context van organisatie (welke rol spelen data voor de organisatie?)
- Leiderschap (wie bepaalt het beleid en wie is verantwoordelijk?)
- Planning (een belangrijk onderdeel hierbij is de risicobeoordeling)
- Ondersteuning (de middelen om tot informatiebeveiliging te komen, inclusief communicatie en informatie hierover)- Uitvoering (inclusief de behandeling van informatiebeveiligingsrisico’s)
- Evaluatie (beoordeling informatiebeveiligingsbeleid)
- Verbetering (acties genomen op basis van de evaluatie).

Belangrijke documenten bij de voorbereiding op ISO 27001:2017 vormen enerzijds de risicobeoordeling waarbij geanalyseerd wordt welke risico’s een organisatie loopt op het gebied van databeveiliging en wat de mogelijke gevolgen daarvan kunnen zijn voor de

organisatie. Deze beoordeling bepaalt de mate en volgorde waarin onderwerpen op het gebied van databeveiliging moeten worden aangepakt. Anderzijds dient een bureau te beschikken over een ISMS ('Information Security Management System') waarin wordt beschreven hoe de databeveiliging binnen een marktonderzoekbureau georganiseerd is en wie daarvoor verantwoordelijk zijn Dit ISMS dient uiteraard aan te sluiten op de risicobeoordeling.

Een derde belangrijk document bij ISO 27001:2017 is de zogenaamde 'Statement of Applicability', de Applicatielijst. In deze lijst komt een groot aantal beheers-doelstellingen en beheersmaatregelen aan de orde. Deze beheers-aspecten staan in detail beschreven in bijlage A van de normtekst ISO 27001:2017. Ze lopen uiteen van bijvoorbeeld de vraag welke mobiele devices medewerkers mogen gebruiken tot de eis van een 'clean desk' beleid. In feite komen alle onderwerpen die met databeveiliging te maken hebben aan de orde in deze applicatielijst. Per onderwerp moet worden aangegeven hoe het bureau ermee omgaat en welke documenten, software, etc. er betrekking op hebben (en waar die documentatie zich bevindt). De Nederlandstalige tekst van ISO 27001:2017 is verkrijgbaar via www.nen.nl.

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!