KEN JE VAK!

ISO 27001 is een goede basis voor de gevolmachtigd agent om actief bezig te zijn met privacy en informatiebeveiliging.

ISO 27001 en AVG

TEKST **JOYCE KOOPS EN RICHARD MEINDERS, SVC GROEP**

ISO 27001 is een standaard voor informatiebeveiliging. Het is een beschrijving voor het beveiligen van informatie binnen een organisatie en daarbuiten, bijvoorbeeld als u gebruik maakt van een externe server of uitbesteding. Het is een internationale norm die gebaseerd is op de kernwaarden: *vertrouwelijkheid (confidentiality), integriteit (integrity)* en *beschikbaarheid (availability)*. Dit wordt ook wel de CIA-triade genoemd. ISO 27001 is toepasbaar voor organisaties die aan willen tonen dat men 'in control' is met betrekking tot de bedrijfsvoering en beveiliging van informatie. De principes die gebruikt worden in ISO 27001 zijn: *context van de organisatie, leiderschap, planning, ondersteuning, uitvoering, evaluaties van prestaties en verbetering.*

De principes van ISO 27001 bieden een basis om de werkprocessen privacy-vriendelijk in te richten. Voldoe je automatisch aan alle vereisten van de AVG als je alle principes van ISO 27001 hebt geïmplementeerd? Het antwoord daarop is nee. ISO 27001 geeft invulling aan de organisatorische maatregelen die de verordening stelt aan gegevensbescherming. De technische maatregelen zijn door middel van ISO 27001, niet voldoende afgedekt of afgehecht. Hierbij kunt u denken aan uw basisbeveiliging (privacy-by-default) en de wijze hoe u met privacy omgaat bij het ontwikkelen van nieuwe producten of diensten (privacy-by design).

Het is, met de komst van de ISO 27701-norm, ook mogelijk om te voldoen aan de technische maatregelen van de verordening. Deze norm is een aanvulling op de bestaande ISO 27001 norm en is daarbij in het leven geroepen om meer bewustwording over privacy te realiseren. De vraag of privacy essentieel is of een fenomeen, wordt met de dag duidelijker. De impact op de privacy van mensen wordt met de komst van nieuwe technologieën en nieuwe werkprocessen elke dag groter. Het waarborgen van privacy is daardoor van essentiële waarde voor organisaties en wordt hierdoor in plaats van een unique selling point een hygiënefactor.

'Door het periodiek toetsen verbetert kwaliteit databeveiliging'

GESCHIKT VOOR UW ORGANISATIE?

ISO 27001 is mogelijk voor elke organisatie, dus ook voor gevolmachtigde agenten. De kosten, tijd en de omgang van de organisatie zijn hierbij bepalend of een organisatie het ISO 27001 traject wil doorlopen. Om ISO 27001 uit te kunnen voeren, dient u ook ISO 27002 te hanteren. Dit is een guideline, waarin alle beheersingsmaatregelen zijn opgenomen, zodat een organisatie deze makkelijker kan implementeren in de bedrijfsvoering.

Het implementeren van ISO 27001 is een proces dat impact heeft op uw organisatie. Het geeft handvatten voor een beheerste en integere bedrijfsvoering die al jaren wordt gebruikt binnen organisaties en een eenmalige investering is. U kunt er daarna jaren de vruchten van plukken. Als de bedrijfsvoering en werkprocessen op een dusdanige wijze zijn ingericht, is het een kwestie van blijven bijhouden en ontwikkelen. U hoeft dan niet meer opnieuw het wiel uit te vinden.

ISO 27001 IN DE PRAKTIJK

Het Werkprogramma Risicobeheersing Volmachten kent diverse taken en controles die te maken hebben met privacy en databeveiliging. Laten we eens een taak oppakken en kijken hoe deze zich verhoudt tot de ISO 27001-norm. Neem de norm AUT-5. Hierin is vastgelegd dat de GA ervoor moet zorgdragen dat de gegevens en de systemen alleen toegankelijk zijn voor geautoriseerde medewerkers en logisch en fysiek zijn beveiligd tegen onbevoegde en ongewenste toegang.

Een van de onderdelen van de ISO 27001-norm is dat je moet zorgen voor veilig personeel. Nu lijkt dat standaard bij een financieel dienstverlener, omdat de Wft hier ook al eisen aan stelt, maar hoe

Joyce Koops LLB en Richard Meinders RGA.

ga je bijvoorbeeld om met ingehuurd personeel of externe gebruikers? Voor de ISO-norm leg je vast wat de beheersingsmaatregel is en voor wie deze geldt. Ook zorg je ervoor dat je nagaat tot welke informatie medewerkers toegang moeten hebben om hun werkzaamheden uit te kunnen voeren. Daarnaast onderzoek je op welke wijze toegang tot informatie, waartoe de betreffende gebruikers niet bevoegd zijn, kan worden voorkomen. Denk bijvoorbeeld aan het inrichten van rechten en bevoegdheden in de assurantieapplicatie, maar ook aan het afsluiten van jouw werkplek op het moment dat je deze verlaat. Door te voldoen aan de ISO 27001-norm, voldoe je ook al automatisch aan deze norm vanuit het Werkprogramma Risicobeheersing Volmachten.

Een ander belangrijk element vanuit ISO 27001 is dat je duidelijk een verantwoordelijke moet aanstellen voor informatiebeveiliging. Door iemand hiervoor aan te wijzen in de organisatie zorg je ook automatisch dat het bij deze persoon 'top of mind' wordt. Als niemand verantwoordelijk is, zal ook niemand zich geroepen voelen om de kwaliteit van dataveiligheid te bewaken. Een ander voordeel zijn de periodieke audits. Deze audits zorgen ervoor dat je als financieel dienstverlener periodiek in de spiegel moet kijken. Door het periodiek toetsen van de kwaliteit van de dataveiligheid zorg je ervoor dat deze kwaliteit continue verbetert.

KOPIE CERTIFICAAT

Als een partij, waarmee u samenwerkt, ISO 27001 gecertificeerd is, dan kunt u hier niet blind op varen. Het is belangrijk om te kijken welke organisatie deze certificering heeft afgegeven (is dit een erkende organisatie?) en voor welke bedrijfsactiviteiten. Het is namelijk niet vastgelegd of je voor alle principes een certificering nodig hebt of dat het ook mogelijk is om een beperkt aantal principes te laten certificeren. Vraag daarom altijd een kopie op van het certificaat en het programma van toepasselijkheid (ISO 27002). Op deze wijze kunt u zelf de waarde van het certificaat vaststellen. ■

Joyce Koops heeft bij SVC Groep haar afstudeeronderzoek gedaan naar de eisen en impact van ISO 27001 en de AVG op gevolmachtigde agenten. Richard Meinders RGA was als partner van SVC Groep haar bedrijfsbegeleider bij het onderzoek.