DUIJNBORGH
CERTIFICATION

Certificering ISO 27701:2019

ISO/IEC 27017:2019 ‘Beveiligingstechnieken - Uitbreiding tot ISO / IEC 27001 en ISO / IEC 27002 voor privacyinformatiebeheer - Vereisten en richtlijnen’

Deze internationale standaard biedt aanvullende richtlijnen voor organisaties die persoonlijk identificeerbare informatie (PII) verwerken. De hoeveelheid en soorten verwerkte PII neemt toe, evenals het aantal situaties waarin een organisatie moet samenwerken met andere organisaties met betrekking tot de verwerking van PII. Bescherming van de persoonlijke levenssfeer in het kader van de verwerking van PII is een maatschappelijke behoefte, evenals het onderwerp van specifieke wet- en/ of regelgeving over de hele wereld.

Het Information Security Management System (ISMS) gedefinieerd in ISO/IEC 27001 is ontworpen om de toevoeging van sectorspecifieke vereisten mogelijk te maken, zonder de noodzaak om een nieuw managementsysteem te ontwikkelen. ISO-managementsysteem-normen, inclusief de sectorspecifieke, zijn ontworpen om afzonderlijk of als een gecombineerd managementsysteem te kunnen worden geïmplementeerd.

Zekerheid op het gebied van de verwerking van PII

ISO 27701is de eerste internationale standaard die organisaties helpt privacy-informatie te beheren en aan wettelijke eisen te voldoen. De beheersmaatregelen in de ISO 27701 zijn een aanvulling op de ISO 27001:2013 en de ISO 27002:2013. Het gaat om additionele maatregelen voor hoofdstukken 4 (Context van de organisatie) en 6 (Planning) van de managementsysteem eisen in de ISO 27001:2013 en alle hoofdstukken van de ISO 27002:2013, met uitzondering van hoofdstuk 17 (business continuïteit). Bij een aantal beheersmaatregelen wordt onderscheid gemaakt in maatregelen voor de Verwerkingsverantwoordelijke (controller) en de Verwerker (processor).

Waarom Duijnborgh Certification?

Wij zijn een certificerende instantie, gespecialiseerd in certificeringen op het gebied van ICT. Wij zijn op grond van de Wet aanwijzing nationale accreditatie-instanties door de Raad voor Accreditatie (RvA) geaccrediteerd voor certificering tegen de ISO-IEC 27001 norm (ook bekend onder de naam Code voor informatiebeveiliging). Ook voor andere ICT gerelateerde normen zoals de NEN 7510, de ISO 27017, ISO 27018, ISO 20000 en de ISO 22399 kunt u bij ons terecht. Wij zijn geen ‘certificeringsfabriek’, noch krijgt u bij ons het certificaat ‘kado’. Als u -samen met ons- de overtuiging heeft dat certificatie geen doel op zichzelf is, maar een middel om te komen tot betere bedrijfsprestaties, dan bent u bij ons aan het goede adres.

De ISO 27001 en ISO 27701 in samenhang

De ISO 27701 is primair van belang voor organisaties die persoonsgegevens verwerken. Zoals hiervoor opgemerkt, is deze norm zowel voor de Verwerkingsverantwoordelijke als voor de (sub)verwerker van toepassing en wordt een certificatietraject doorgaans in samenhang met de ISO 27001 uitgevoerd. De ISO 27701 steunt op het managementsysteem van de ISO 27001.

Indien uw organisatie niet gecertificeerd is tegen de norm ISO 27001, en dit ook niet gewenst is, kunnen we samen met u bekijken welke elementen uit de ISO 27001 in uw organisatie moeten worden geïmplementeerd om een afzonderlijke certificatie tegen ISO 27701 mogelijk te maken.

Certificering tegen ISO 27701 in 5 stappen.

Het volgende stappenplan kan gehanteerd worden bij het voldoen aan ISO 27701 en het laten uitvoeren van een certificatie audit:

Stap 1: Risicoprofiel en beheersingsdoelstellingen vaststellen

Met behulp van de bestaande risico behandelmethodiek brengt u de risico's in beeld die gerelateerd zijn aan cloud computing. Tevens wordt in kaart gebracht welke wettelijke, contractuele, regulerende of andere specifieke informatiebeveiligingseisen van toepassing zijn. De focus is hierbij gericht op de manier waarop IT-middelen technisch zijn ontworpen, worden beheerst en beheerd. In beginsel gebruikt u hiervoor het bestaande managementsysteem (ISMS) van ISO 27001. De geïdentificeerde risico's worden vertaald in beheersingsdoelstellingen en op basis van deze doelstellingen worden de beheersmaatregelen geselecteerd.

Stap 2: Pre-audit en terugkoppeling

De beheersmaatregelen worden in opzet en bestaan in een korte tijd gecontroleerd om een eerste indruk te verkrijgen. De bevindingen worden aan u teruggekoppeld. Op basis van de uitkomsten van de pre-audit wordt tevens vastgesteld wanneer het certificatie-onderzoek kan starten.

Stap 3: Iteratief verbeterproces

Op basis van de uitkomsten van de pre-audit brengt uw organisatie gewenste verbeteringen aan. Duijnborgh Certification is gedurende deze periode –en waar dat binnen haar auditrol past- beschikbaar voor het tussentijds beoordelen van de verbeteracties. Hierdoor worden verrassingen achteraf voorkomen en wordt de kans van slagen bij de eindbeoordeling aanzienlijk vergroot.

Stap 4: Audit opzet en bestaan beheersmaatregelen

Op het moment dat uw organisatie aangeeft klaar te zijn voor het certificatie-onderzoek zullen wij een audit uitvoeren ter beoordeling van de opzet en het bestaan van de op cloud computing gericht beheersmaatregelen.

Stap 5: Certificatie

Op basis van de resultaten uit de voorgaande stappen zal worden besloten of er overgegaan wordt tot certificering en het verstrekken van het certificaat. Indien er (nog) onvoldoende aan de eisen vanuit de norm wordt voldaan dient de organisatie maatregelen te treffen. Na het corrigeren van de tekortkomingen, kan het resultaat worden geëvalueerd en alsnog worden overgegaan tot certificering. Een certificaat is drie jaar geldig, waarbij jaarlijks een controle-audit wordt uitgevoerd gericht op de effectieve werking van de beheersmaatregelen.

Duijnborgh Certification BV
WTC Papendorp
Papendorpseweg 100
3528 BJ Utrecht
T 31(0)88 160 1750
F 31(0)88 160 1799
E info@dbcert.nl

DUIJNBORGH CERTIFICATION®