ISO 27701 Certificering Privacy Management Systeem

De ISO/IEC 27701 - een uitbreiding op de norm ISO 27001 – bevat specifieke beheersmaatregelen voor de bescherming van privacygevoelige informatie. Organisaties die al werken met een Information Security Management System (ISMS) kunnen dit aan de hand van de ISO 27701 upgraden tot een Privacy Information Management System (PIMS). Als expert op het gebied van datasecurity-certificering kan Kiwa u helpen het ISO 27701-certificaat snel en efficiënt te behalen.

Met een ISO 27701 certificaat laten organisaties hun stakeholders zien dat ze de bescherming van de privacy bij de verwerking van (persoons)gegevens goed hebben geregeld. Bovendien wordt met ISO 27701 certificering aangetoond dat de organisatie zó is ingericht dat op een juiste en zorgvuldige manier met privacygevoelige informatie wordt omgegaan. Net als in de AVG, een wettelijke regeling, draait het hierbij om een optimaal samenspel tussen organisatorische ‘werkbaarheid’ en de technische maatregelen die getroffen moeten worden in het kader van ISO/IEC 27701.

PDCA-cyclus

Een organisatie die al werkt volgens de norm ISO 27001 en dit wil uitbreiden met de add-on ISO 27701, moet een geheel van richtlijnen en procedures opstellen en implementeren. Het is daarbij belangrijk dat het gaat om een doorlopende cyclus (PDCA-cyclus), waarin wijzigingen die impact hebben op het PIMS op de juiste manier worden verwerkt, geïmplementeerd en gecontroleerd. Op deze manier blijft het PIMS up-to-date en dat is niet alleen voor de interne werking van belang, maar ook om te blijven voldoen aan de vereisten voor certificatie.

Géén AVG-norm

De ISO/IEC 27701 is een internationale norm waarmee niet automatisch wordt voldaan aan alle aspecten van de Europese privacywetgeving AVG (GDPR). Wél geeft een ISO 27701-certificeerde organisatie bij in- en externe stakeholders het signaal af dat op een goede manier wordt omgegaan met privacygevoelige gegevens. Daarnaast kan deze norm middels omzettingstabellen worden gebruikt voor diverse internationale normen, zoals de eerder genoemde AVG of de ISO 29100.

Expert Center Cybersecurity
Kiwa Nederland
cybersecurity@kiwa.com
+31 (0)88 998 30 20

Wanneer ISO 27701-certificering?

Certificering volgens de norm ISO/IEC 27701 is van toegevoegde waarde voor elke organisatie die wil of moet laten zien dat er op een verantwoorde manier wordt omgegaan met privacygevoelige informatie, vooral als deze informatie terug te voeren is op een individu, de zogenoemde Persoonlijk Identificeerbare Informatie (PII). Certificering kan ook noodzakelijk zijn als aantoonbaarheid door middel van een certificaat, afgegeven een onafhankelijke certificerende instelling als Kiwa is gewenst, bijvoorbeeld bij een aanbestedings- of offertetraject.

Kiwa ISO 27701-diensten

Als het gaat om de ISO 27701 kan Kiwa op een aantal manieren van dienst zijn:

- Trainingen waarin de norm wordt uitgelegd en uitgediept;
- Uitvoeren van een GAP-analyse/nulmeting of proef audit, zodat u een beeld heeft van de stand van zaken van het niveau van de ISO 27701 vereisten in uw organisatie en daarmee de nog te nemen stappen;
- Uitvoeren van een certificeringsaudit, waarna u bij goed gevolg door middel van een certificaat kunt aantonen dat door uw organisatie aan de vereisten van de internationale ISO norm 27701 wordt voldaan.

Expert Center Cybersecurity
Kiwa Nederland
cybersecurity@kiwa.com
+31 (0)88 998 30 20