Wat is ISO 27701?

De ISO 27701 norm is een uitbreiding op de ISO 27001 norm voor informatiebeveiliging, maar geeft specifieke beheersmaatregelen voor privacy.

Waarom heeft ISO deze norm gepubliceerd?

Het doel van deze norm is om organisaties een praktisch kader te bieden waarmee zij het bestaande ISMS (Information Security Management System) kunnen uitbreiden naar een PIMS (Privacy Information Management System).

Voor wie is de ISO 27701 norm geschikt?

De ISO 27701 is voor organisaties welke al gestart zijn met de implementatie van ISO 27001 en gaat dan ook uit van dit raamwerk, met daarin ook de PDCA-cyclus en risicoanalyse zoals deze vereist wordt in de ISO 27001 norm. Met deze uitbreiding kan een organisatie laten zien dat ze als organisatie in control zijn en de PDCA-cyclus hebben ingericht en risicoanalyse hebben gedaan volgens de beheersmaatregelen welke genoemd worden voor privacy in de ISO 27701.

Is ISO 27701 verplicht en te certificeren?

Nee, ISO 27701 is geen verplichting. U kunt deze norm eigenlijk vergelijken met de andere uitbreidingen op de ISO 27001, zoals de ISO 27799 welke specifieke beheersmaatregelen geeft voor de zorg of de 27017 voor clouddiensten. Deze zijn allen niet verplicht maar geven u een praktisch kader en specifieke beheersmaatregelen voor een niche markt. We weten nog niet of de ISO 27701 te certificeren is. Hierover is nog geen officiële uitspraak gedaan, de mogelijkheden hiervoor worden onderzocht door de NEN.

Hoe starten met de implementatie van ISO 27701?

Om te kunnen starten met de implementatie van de ISO 27701 moet u eerst de ISO 27001 norm begrijpen en hieraan invulling geven. Bij 12secure-u geven we 2daagse ISO 27001 implementatie trainingen, maar ook een 5 daagse training om een Lead Auditor (IRCA) te worden. Wilt u specifiek een training op ISO 27701, omdat u ISO 27001 en 27002 al geïmplementeerd heeft? Neem dan contact met ons op over de mogelijkheden voor een ISO 27701 training.

Is ISO 27701 een AVG | GDPR certificering?

Nee, de ISO 27701 geeft beheersmaatregelen welke als handvaten dienen om uw organisatie in control te laten zijn t.a.v. de AVG | GDPR. Echter vereist de privacy wetgeving (AVG | GDPR) een ander type accreditatie en certificatieschema dan dat de ISO 27001 gebruikt. De wetgeving eist namelijk een ISO 17065 accreditatie waarmee producten, diensten of processen worden gecertificeerd en niet het bedrijf gecertificeerd wordt.

Wanneer voldoe ik aan de AVG | GDPR?

In de wet (Artikel 5, lid 2) staat dat u als organisatie 'aantoonbaar moet voldoen' aan de wet. Er zijn drie verschillende manieren om dit aan te kunnen tonen. 1: Op verzoek van de autoriteit alles beschikbaar stellen als bewijs dat uw organisatie voldoet. 2: Doormiddel van een goedgekeurde gedragscode. 3: Door de AVG certificering. Op het moment van schrijven zijn er nog geen officieel goedgekeurde gedragscodes of AVG certificeringen in Nederland. Bekijk de website van de Autoriteit Persoonsgegevens voor de actuele status.