NORM

NEN-ISO/IEC 27701:2019 (nl)

Veiligheidstechnieken – Uitbreiding op ISO/IEC 27001 en ISO/IEC 27002 voor privacy-informatiemanagement – Eisen en richtlijnen

Nederlandse norm

ICS 35.030

September 2019

NEN

DE WERELD OP ÉÉN LIJN.

Nederlandse norm

NEN-ISO/IEC 27701

(nl)

Veiligheidstechnieken – Uitbreiding op ISO/IEC 27001 en ISO/IEC 27002 voor privacy-informatiemanagement – Eisen en richtlijnen

Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines

ICS 35.030

september 2019

Dit document bevat de vertaling in het Nederlands van de internationale norm ISO/IEC 27701:2019. De internationale norm ISO/IEC 27701:2019 heeft de status van Nederlandse norm.

Normcommissie 381027 'Informatiebeveiliging, Cyber security en Privacy'

Inhoud

Voorwoord

ISO (International Organization for Standardization) en IEC (International Electrotechnical Commission) vormen tezamen een stelsel dat gespecialiseerd is in wereldwijde normalisatie. Nationale organisaties die lid zijn van ISO of IEC, participeren in het ontwikkelen van internationale normen via technische commissies die door de desbetreffende organisatie zijn ingesteld ten behoeve van de normalisatie in specifieke technische werkvelden. Technische commissies van ISO en IEC werken samen bij onderwerpen waarin zij een gemeenschappelijk belang hebben. Andere internationale organisaties, zowel overheidsinstanties als ngo's, nemen in samenwerking met ISO en IEC ook deel aan deze werkzaamheden.

De procedures die zijn gebruikt voor het ontwikkelen van dit document en de procedures die zijn bedoeld voor het verdere onderhoud ervan, worden beschreven in deel 1 van de ISO/IEC-richtlijnen. Hierbij wordt met name gewezen op de verschillende goedkeuringscriteria die nodig zijn voor de verschillende soorten documenten. Dit document is opgesteld volgens de redactionele regels die zijn opgenomen in deel 2 van de ISO/IEC-richtlijnen (zie www.iso.org/directives).

Er wordt gewezen op de mogelijkheid dat sommige elementen van dit document onderwerp zijn van patentrechten. ISO en IEC zijn niet verantwoordelijk voor identificatie van dergelijke patentrechten. Nadere informatie over eventuele patentrechten die zijn geïdentificeerd tijdens het ontwikkelen van het document, is te vinden in de inleiding en/of de ISO-lijst met ontvangen patentverklaringen (zie www.iso.org/patents) of de IEC-lijst met ontvangen patentverklaringen (zie http://patents.iec.ch).

Eventuele handelsnamen die in dit document worden gebruikt, zijn verstrekt voor het gemak van de gebruikers en houden geen aanbeveling in.

Uitleg over de vrijwillige aard van normen, de betekenis van ISO-specifieke termen en uitdrukkingen met betrekking tot conformiteitsbeoordeling, evenals informatie over hoe ISO voldoet aan de in de Technical Barriers to Trade (TBT) vervatte beginselen van de Wereldhandelsorganisatie (WTO), wordt gegeven op de volgende URL: www.iso.org/iso/foreword.html.

Dit document is opgesteld door Joint Technical Committee ISO/IEC JTC 1, 'Information technology', SC 27, 'Security techniques'.

Eventuele feedback of vragen over dit document behoren te worden gericht aan het nationale normalisatie-instituut voor de gebruiker. Een volledig overzicht van deze instituten is te vinden op www.iso.org/members.html.

Inleiding

0.1 Algemeen

Vrijwel elke organisatie verwerkt persoonlijk identificeerbare informatie (PII). Bovendien wordt er steeds meer PII verwerkt, nemen de te verwerken soorten PII toe en zijn er steeds meer situaties waarin het nodig is dat een organisatie met betrekking tot het verwerken van PII met andere organisaties samenwerkt. De bescherming van privacy in de context van het verwerken van PII is een maatschappelijke noodzaak en is wereldwijd het onderwerp van specifieke wet- en/of regelgeving.

Het in ISO/IEC 27001 gedefinieerde managementsysteem voor informatiebeveiliging ('Information Security Management System', ISMS) is dusdanig opgezet dat sectorspecifieke eisen kunnen worden toegevoegd zonder dat het nodig is om een nieuw managementsysteem te ontwikkelen. ISO-normen voor managementsystemen, waaronder de sectorspecifieke normen, worden dusdanig opgezet dat ze los of als gecombineerd managementsysteem kunnen worden geïmplementeerd.

Eisen en richtlijnen voor de bescherming van PII variëren afhankelijk van de context van de organisatie, met name indien er sprake is van bestaande nationale wet- en/of regelgeving. Een eis van ISO/IEC 27001 is dat men inzicht heeft in deze context en dat hiermee rekening wordt gehouden. Dit document omvat kruisverwijzingen naar:

— het kader en de beginselen voor privacy zoals gedefinieerd in ISO/IEC 29100;

— ISO/IEC 27018;

— ISO/IEC 29151; en

— de Algemene verordening gegevensbescherming (AVG) van de EU. *)

Het kan echter nodig zijn deze te interpreteren om rekening te houden met lokale wet- en/of regelgeving.

Dit document kan worden gebruikt door PII-verwerkingsverantwoordelijken (ook zij die mede-PII-verwerkingsverantwoordelijken zijn) en PII-verwerkers (ook zij die PII-verwerkers als onderaannemer inzetten en PII-verwerkers die PII als onderaannemer voor andere PII-verwerkers verwerken).

Een organisatie die aan de eisen in dit document voldoet, genereert documentair bewijsmateriaal van hoe zij omgaat met de verwerking van PII. Dit bewijsmateriaal kan worden gebruikt om overeenkomsten met zakenrelaties mogelijk te maken waarbij het verwerken van PII voor beide partijen relevant is. Dit kan ook nuttig zijn bij relaties met andere stakeholders. Het gebruik van dit document in combinatie met ISO/IEC 27001 kan, indien gewenst, onafhankelijke verificatie van dit bewijsmateriaal opleveren.

Dit document was oorspronkelijk ontwikkeld als ISO/IEC 27552.

*) Nederlandse voetnoot: Binnen de AVG van de EU wordt de definitie 'persoonsgegevens' toegepast en niet de definitie 'PII'. De keuze om PII toe te passen is gemaakt om zo dicht mogelijk bij de originele tekst van ISO/IEC 27701 te blijven. Op het eerste gezicht lijken de definities van PII en persoonsgegevens op elkaar, maar ze kunnen niet een-op-een worden uitgewisseld. Het verschil is voornamelijk te vinden in het gebruik ervan. PII wordt gebruikt om individuen te identificeren of van elkaar te onderscheiden. De term persoonsgegevens heeft een bredere betekenis: alle informatie die naar een (natuurlijk en levend) persoon verwijst of aan een persoon verbonden kan worden.

0.2 Compatibiliteit met andere managementsysteemnormen

In dit document wordt het door ISO ontwikkelde kader voor het verbeteren van afstemming tussen haar managementsysteemnormen toegepast.

Dit document stelt een organisatie in staat haar PIMS af te stemmen op of te integreren met de eisen van andere managementsysteemnormen.

Veiligheidstechnieken – Uitbreiding op ISO/IEC 27001 en ISO/IEC 27002 voor privacy-informatiemanagement – Eisen en richtlijnen

1 Onderwerp en toepassingsgebied

Dit document specificeert eisen en geeft richtlijnen voor het inrichten, implementeren, onderhouden en continu verbeteren van een managementsysteem voor privacy-informatie ('Privacy Information Management System', PIMS) in de vorm van een uitbreiding op ISO/IEC 27001 en ISO/IEC 27002 voor privacymanagement binnen de context van de organisatie.

Dit document specificeert PIMS-gerelateerde eisen en geeft richtlijnen voor PII-verwerkingsverantwoordelijken en PII-verwerkers met verantwoordelijkheid en toerekenbaarheid voor de verwerking van PII.

Dit document is van toepassing op alle organisaties, ongeacht type of omvang, met inbegrip van publieke en private ondernemingen, overheidsentiteiten en organisaties zonder winstoogmerk, die PII-verwerkingsverantwoordelijken en/of PII-verwerkers zijn en PII binnen een ISMS verwerken.

2 Normatieve verwijzingen

Naar de volgende documenten wordt in de tekst zo verwezen dat de bepalingen ervan geheel of gedeeltelijk ook voor dit document gelden. Bij gedateerde verwijzingen is alleen de aangehaalde editie van toepassing. Bij ongedateerde verwijzingen is de laatste editie van het document (met inbegrip van eventuele wijzigingsbladen en correctiebladen) waarnaar is verwezen, van toepassing.

ISO/IEC 27000, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*

ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*

ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls*

ISO/IEC 29100, *Information technology – Security techniques – Privacy framework*

3 Termen, definities en afkortingen

Voor de toepassing van dit document gelden de termen en definities zoals vermeld in ISO/IEC 27000 en ISO/IEC 29100, evenals de onderstaande termen en definities.

ISO en IEC onderhouden op de volgende adressen terminologiedatabases voor gebruik in het kader van normalisatie:

— ISO Online browsing platform: te bereiken op http://www.iso.org/obp

— IEC Electropedia: te bereiken op http://www.electropedia.org/

3.1
mede-PII-verwerkingsverantwoordelijke
PII-verwerkingsverantwoordelijke die de doeleinden van en middelen voor het verwerken van PII gezamenlijk met een of meerdere PII-verwerkingsverantwoordelijken vaststelt

3.2
privacy-informatiemanagementsysteem
PIMS
managementsysteem voor informatiebeveiliging dat invulling geeft aan de bescherming van privacy waar deze mogelijk in het gedrang komt door de verwerking van PII

4 Algemeen

4.1 Structuur van dit document

Dit is een sectorspecifiek document dat verband houdt met ISO/IEC 27001:2013 en ISO/IEC 27002:2013.

Dit document richt zich op PIMS-specifieke eisen. Het voldoen aan dit document is gebaseerd op het naleven van deze eisen en van de eisen in ISO/IEC 27001:2013. Dit document geeft een uitbreiding op eisen van ISO/IEC 27001:2013 om rekening te houden met de bescherming van de privacy van PII-betrokkenen waar deze mogelijk gevolgen kan ondervinden van het verwerken van PII, in aanvulling op informatiebeveiliging. Voor beter inzicht zijn implementatierichtlijnen en overige informatie met betrekking tot de eisen opgenomen.

Hoofdstuk 5 geeft PIMS-specifieke eisen en overige informatie met betrekking tot de informatiebeveiligingseisen in ISO/IEC 27001 die passend zijn voor een organisatie die als PII-verwerkingsverantwoordelijke of als PII-verwerker optreedt.

OPMERKING 1 Voor de volledigheid bevat hoofdstuk 5 een paragraaf voor elk hoofdstuk met eisen in ISO/IEC 27001:2013, zelfs in gevallen waar er geen sprake is van PIMS-specifieke eisen of overige informatie.

Hoofdstuk 6 geeft PIMS-specifieke richtlijnen en overige informatie met betrekking tot de informatiebeveiligingsbeheersmaatregelen in ISO/IEC 27002 en PIMS-specifieke richtlijnen voor een organisatie die als PII-verwerkingsverantwoordelijke of als PII-verwerker handelt.

OPMERKING 2 Voor de volledigheid bevat hoofdstuk 6 een paragraaf voor elk hoofdstuk met doelstellingen of beheersmaatregelen in ISO/IEC 27002:2013, zelfs in gevallen waar er geen sprake is van PIMS-specifieke richtlijnen of overige informatie.

Hoofdstuk 7 geeft aanvullende richtlijnen van ISO/IEC 27002 voor PII-verwerkingsverantwoordelijken en hoofdstuk 8 geeft aanvullende richtlijnen van ISO/IEC 27002 voor PII-verwerkers.

In bijlage A worden de PIMS-specifieke beheersdoelstellingen en beheersmaatregelen opgesomd voor een organisatie die als PII-verwerkingsverantwoordelijke optreedt (ongeacht of zij al dan niet gebruikmaakt van een PII-verwerker en of zij al dan niet gezamenlijk met een andere PII-verwerkingsverantwoordelijke handelt).

In bijlage B worden de PIMS-specifieke beheersdoelstellingen en beheersmaatregelen opgesomd voor een organisatie die als PII-verwerker optreedt (ongeacht of zij het verwerken van PII al dan niet aan een aparte PII-verwerker uitbesteedt en met inbegrip van organisaties die PII verwerken als onderaannemers van PII-verwerkers).

Bijlage C bevat een kruisverwijzing naar ISO/IEC 29100.

Bijlage D bevat een kruisverwijzing tussen de beheersmaatregelen in dit document en de Algemene verordening gegevensbescherming (AVG) van de EU.

Bijlage E bevat een kruisverwijzing naar ISO/IEC 27018 en ISO/IEC 29151.

Bijlage F legt uit hoe ISO IEC 27001 en ISO/IEC 27002 worden uitgebreid om ook privacybescherming af te dekken bij het verwerken van PII.

4.2 Toepassing van eisen van ISO/IEC 27001:2013

Tabel 1 geeft aan waar PIMS-specifieke eisen zich in dit document bevinden afgezet tegen ISO/IEC 27001.

Tabel 1 — Locatie van PIMS-specifieke eisen en overige informatie voor het implementeren van beheersmaatregelen in ISO/IEC 27001:2013

Hoofdstuk in ISO/IEC 27001:2013	Titel	Paragraaf in dit document	Opmerkingen
4	Context van de organisatie	5.2	Aanvullende eisen
5	Leiderschap	5.3	Geen PIMS-specifieke eisen
6	Planning	5.4	Aanvullende eisen
7	Ondersteuning	5.5	Geen PIMS-specifieke eisen
8	Uitvoering	5.6	Geen PIMS-specifieke eisen
9	Evaluatie van de prestaties	5.7	Geen PIMS-specifieke eisen
10	Verbetering	5.8	Geen PIMS-specifieke eisen

OPMERKING De uitgebreide interpretatie van 'informatiebeveiliging' volgens 5.1 is altijd van toepassing, zelfs als er geen PIMS-specifieke eisen zijn.

4.3 Toepassing van richtlijnen van ISO/IEC 27002:2013

Tabel 2 geeft aan waar PIMS-specifieke richtlijnen zich in dit document bevinden afgezet tegen ISO/IEC 27002.

NEN
CONNECT

ALTIJD DE ACTUELE NORM IN UW BEZIT HEBBEN?

Nooit meer zoeken in de systemen en uzelf de vraag stellen: ‘Is NEN-ISO/IEC 27701:2019 nl de laatste versie?’

Via het digitale platform NEN Connect heeft u altijd toegang tot de meest actuele versie van deze norm. Vervallen versies blijven ook beschikbaar. **U en uw collega’s** kunnen de norm via NEN Connect makkelijk raadplagen, online en offline.

Kies voor slimmer werken en bekijk onze mogelijkheden op **www.nenconnect.nl**.

Heeft u vragen?

Onze Klantenservice is bereikbaar maandag tot en met vrijdag, van 8.30 tot 17.00 uur.

Telefoon: 015 2 690 391
E-mail: klantenservice@nen.nl