Versie: 3.0

Datum: 1 februari 2026

Organisatie: ADO Amsterdam B.V., MWM2 B.V., Crowdtech B.V., InnerVoice B.V.

Generaal Vetterstraat, 82
1059 BW Amsterdam
Nederland

Scope: ISO27001:2022 en ISO27701:2019

ISO27001
Informatiebeveiliging gerelateerd aan het ontwikkelen van software en het leveren van advies en diensten voor markt- en medewerkersonderzoek en data-analyse.

ISO27701
Bescherming van persoonlijk identificeerbare informatie (PII) gerelateerd aan het ontwikkelen van software en het leveren van advies en diensten voor markt- en medewerkersonderzoek en data-analyse in de rol van PII-verwerkingsverantwoordelijke en PII-verwerker.

ISO27001:2022

						Trigger				Van toepassing in haar rol als	
Nummer	Van toepassing	Beheersmaatregel	Volledig ingevoerd	Niet ingevoerd	Verantwoordelijke	Beleid	Wet- en regelgeving	Contractuele eis	Risico-analyse	Verwerker	Verwerkings-verantwoordelijke
A.5 Organisatorische beheersmaatregelen											
A.5.1	√	Informatiebeveiligingsbeleid en onderwerpspecifieke beleidsregels moeten worden gedefinieerd, goedgekeurd door het management, gepubliceerd, gecommuniceerd aan en erkend door relevant personeel en relevante belanghebbenden en met geplande tussenpozen en als zich significante wijzigingen voordoen, worden beoordeeld.	√		Security Officer	√			√	√	√
A.5.2	√	Rollen en verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie.	√		Security Officer	√				√	√
A.5.3	√	Conflicterende taken en conflicterende verantwoordelijkheden moeten worden gescheiden.	√		Security Officer	√			√	√	√
A.5.4	√	Het management moet van al het personeel eisen dat ze informatiebeveiliging toepassen overeenkomstig het vastgestelde informatiebeveiligingsbeleid, de onderwerpspecifieke beleidsregels en procedures van de organisatie.	√		HR Manager	√		√	√	√	√
A.5.5	√	De organisatie moet contact met de relevante instanties leggen en onderhouden.	√		Security Officer	√	√			√	√

A.5.6	√	De organisatie moet contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen leggen en onderhouden.	√		Security Officer	√				√	√
A.5.7	√	Informatie met betrekking tot informatiebeveiligingsdreigingen moet worden verzameld en geanalyseerd om informatie over dreigingen te produceren.	√		Security Officer	√	√	√	√	√	√
A.5.8	√	Informatiebeveiliging moet worden geïntegreerd in projectmanagement.	√		Security Officer	√			√	√	√
A.5.9	√	Er moet een inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van de eigenaren, worden opgesteld en onderhouden.	√		IT Beheer & Kantoor-automatisering	√			√	√	√
A.5.10	√	Regels voor het aanvaardbaar gebruik van en procedures voor het omgaan met informatie en andere gerelateerde bedrijfsmiddelen moeten worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	√		IT Beheer & Kantoor-automatisering	√		√	√	√	√
A.5.11	√	Personeel en andere belanghebbenden, al naar gelang de situatie, moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst retourneren.	√		HR Manager	√				√	√
A.5.12	√	Informatie moet worden geclassificeerd volgens de informatiebeveiligingsbehoeften van de organisatie, op basis van de eisen voor vertrouwelijkheid, integriteit, beschikbaarheid en relevante eisenvan belanghebbenden.	√		Security Officer	√			√	√	√
A.5.13	√	Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	√		Security Officer	√			√	√	√
A.5.14	√	Er moeten regels, procedures of overeenkomsten voor informatieoverdracht zijn ingesteld voor alle soorten van communicatiefaciliteiten binnen de organisatie en tussen de organisatie en andere partijen.	√		IT Beheer & Kantoor-automatisering	√				√	√
A.5.15	√	Er moeten regels op basis van bedrijfs- en informatiebeveiligingseisen worden vastgesteld en geïmplementeerd om de fysieke en logische toegang tot informatie en andere gerelateerde bedrijfsmiddelen te beheersen.	√		IT Beheer & Kantoor-automatisering	√			√	√	√
A.5.16	√	De volledige levenscyclus van identiteiten moet worden beheerd.	√		IT Beheer & Kantoor-automatisering	√			√	√	√
A.5.17	√	De toewijzing en het beheer van authenticatie-informatie moet worden beheerst door middel van een beheerproces waarvan het adviseren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.	√		IT Beheer & Kantoor-automatisering	√				√	√
A.5.18	√	Toegangsrechten voor informatie en andere gerelateerde bedrijfsmiddelen moeten worden verstrekt, beoordeeld, aangepast en verwijderd overeenkomstig het onderwerpspecifieke beleid en de regels inzake toegangsbeveiliging van de organisatie.	√		IT Beheer & Kantoor-automatisering	√			√	√	√
A.5.19	√	Er moeten processen en procedures worden vastgesteld en geïmplementeerd om de informatiebeveiligingsrisico's in verband met het gebruik van producten of diensten van de leverancier te beheersen.	√		Security Officer	√			√	√	√

A.5.20	√	Relevante Informatiebeveiligingseisen moeten worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie worden overeengekomen.	√		Security Officer	√			√	√	√
A.5.21	√	Er moeten processen en procedures worden bepaald en geïmplementeerd om de informatiebeveiligingsrisico's in verband met de toeleveringsketen van ICT-producten en -diensten te beheersen.	√		Security Officer	√			√	√	√
A.5.22	√	De organisatie moet de informatiebeveiligingspraktijken en de dienstverlening van leveranciers regelmatig monitoren, beoordelen, evalueren en veranderingen daaraan beheren.	√		Security Officer	√			√	√	√
A.5.23	√	Processen voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten moeten overeenkomstig de informatiebeveiligingseisen van de organisatie worden opgesteld.	√		Security Officer	√			√	√	√
A.5.24	√	De organisatie moet plannen opstellen voor, en zich voorbereiden op, het beheren van informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatiebeveiligingsincidenten te definïeren, vast te stellen en te communiceren.	√		Security Officer	√			√	√	√
A.5.25	√	De organisatie moet informatiebeveiligingsgebeurtenissen beoordeelen en beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten.	√		Security Officer	√			√	√	√
A.5.26	√	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	√		Security Officer	√			√	√	√
A.5.27	√	Kennis die is opgedaan met informatiebeveiligingsincidenten moet worden gebruikt om de beheersmaatregelen voor informatiebeveiliging te versterken en te verbeteren.	√		Security Officer	√				√	√
A.5.28	√	De organisatie moet procedures vaststellen en implementeren voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs met betrekking tot informatiebeveiligingsgebeurtenissen.	√		Security Officer	√			√	√	√
A.5.29	√	De organisatie moet plannen maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.	√		Security Officer	√			√	√	√
A.5.30	√	De ICT-gereedheid moet worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoelstellingen en ICT-continuïteitseisen.	√		IT Beheer & Kantoor-automatisering	√		√	√	√	√
A.5.31	√	Wettelijke, statuaire, regelgevende en contractuele eisen die relevant zijn voor informatiebeveiliging en de aanpak van de organisatie om aan deze eisen te voldoen, moeten worden geïdentificeerd, gedocumenteerd en actueel gehouden.	√		Security Officer	√	√		√	√	√
A.5.32	√	De organisatie moet passende procedures implementeren om intellectuele-eigendomsrechten te beschermen.	√		Security Officer	√	√		√	√	√
A.5.33	√	Registraties moeten worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.	√		IT Beheer & Kantoor-automatisering	√	√	√	√	√	√
A.5.34	√	De organisatie moet de eisen met betrekking tot het behoud van privacy en bescherming van persoonsgegevens volgens de toepasselijke wet- en regelgeving en contractuele eisen identificeren en eraan voldoen.	√		Security Officer	√	√	√	√	√	√

A.5.35	√	De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan, met inbegrip van mensen, processen en technologieën, moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, worden beoordeeld.	√		Security Officer	√			√	√	√
A.5.36	√	De naleving van het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en de normen van de organisatie moet regelmatig worden beoordeeld.	√		Security Officer	√			√	√	√
A.5.37	√	Bedieningsprocedures voor informatieverwerkende faciliteiten moeten worden gedocumenteerd en beschikbaar gesteld aan het personeel dat ze nodig heeft.	√		IT Beheer & Kantoor-automatisering	√			√	√	√
A.6 Mensgerichte beheersmaatregelen												
A.6.1	√	De achtergrond van alle kandidaten voor een dienstverband moet worden gecontroleerd voordat ze bij de organisatie in dienst treden en daarna op gezette tijden worden herhaald. Hierbij moet rekening worden gehouden met de toepasselijke wet- en regelgeving en ethische overwegingen, en deze controle moet in verhouding staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.	√		HR Manager	√	√	√	√	√	√
A.6.2	√	In arbeidsovereenkomsten moet worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging.	√		HR Manager	√		√	√	√	√
A.6.3	√	Personeel van de organisatie en relevante belanghebbenden moeten een passende bewustwording van, opleiding en training in informatiebeveiliging en regelmatige updates over het informatiebeveiligingsbeleid, onderwerpspecifieke beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie, krijgen.	√		HR Manager	√			√	√	√
A.6.4	√	Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te ondernemen tegen personeel en andere belanghebbenden die zich schuldig hebben gemaakt aan een schending van het informatiebeveiligingsbeleid.	√		HR Manager	√		√	√	√	√
A.6.5	√	Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband moeten worden gedefinieerd, gehandhaafd en gecommuniceerd aan relevant personeel en andere belanghebbenden.	√		HR Manager	√		√	√	√	√
A.6.6	√	Vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie inzake de bescherming van informatie weerspiegelen, moeten worden geïdentificeerd, gedocumenteerd, regelmatig worden beoordeeld en ondertekend door personeel en andere relevante belanghebbenden.	√		HR Manager	√		√		√	√
A.6.7	√	Wanneer personeel op afstand werkt, moeten er beveiligingsmaatregelen worden geïmplementeerd om informatie te beschermen die buiten het gebouw en/of terrein van de organisatie wordt ingezien, verwerkt of opgeslagen.	√		Security Officer	√			√	√	√
A.6.8	√	De organisatie moet voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligingsgebeurtenissen tijdig via passende kanalen kan melden.	√		Security Officer	√			√	√	√
A.7 Fysieke beheersmaatregelen												

A.7.1	√	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, moeten worden beschermd door beveiligingszones te definiëren en te gebruiken.	√		Security Officer	√				√	√
A.7.2	√	Beveiligde zones moeten worden beschermd door passende toegangsbeveiligingsmaatregelen en toegangspunten.	√		IT Beheer & Kantoor-automatisering	√				√	√
A.7.3	√	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en geïmplementeerd.	√		IT Beheer & Kantoor-automatisering	√			√	√	√
A.7.4	√	Het gebouw en terrein moet voortdurend worden gemonitord op onbevoegde fysieke toegang.	√		Security Officer	√				√	√
A.7.5	√	Er moet bescherming tegen fysieke en omgevingsdreigingen, zoals natuurrampen en andere opzettelijke of onopzettelijke fysieke dreigingen voor de infrastructuur, worden ontworpen en geïmplementeerd.	√		Security Officer	√				√	√
A.7.6	√	Voor het werken in beveiligde zones moeten beveiligingsmaatregelen worden ontwikkeld en geïmplementeerd.	√		Security Officer	√				√	√
A.7.7	√	Er moeten 'clear desk'-regels voor papieren documenten en verwijderbare opslagmedia en 'clear screen'-regels voor informatieverwerkende faciliteiten worden gedefinieerd en op passende wijze worden afgedwongen.	√		Security Officer	√			√	√	√
A.7.8	√	Apparatuur moet veilig worden geplaatst en beschermd.	√		IT Beheer & Kantoor-automatisering	√				√	√
A.7.9	√	Bedrijfsmiddelen buiten het gebouw en/of terrein moeten worden beschermd.	√		IT Beheer & Kantoor-automatisering	√			√	√	√
A.7.10	√	Opslagmedia moeten worden beheerd gedurende hun volledige levenscyclus van aanschaf, gebruik, transport en verwijdering overeenkomstig het classificatieschema en de hanteringseisen van de organisatie.	√		IT Beheer & Kantoor-automatisering	√				√	√
A.7.11	√	Informatieverwerkende faciliteiten moeten worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.	√		IT Beheer & Kantoor-automatisering	√			√	√	√
A.7.12	√	Voedingskabels en kabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen onderschepping, interferentie of beschadiging.	√		IT Beheer & Kantoor-automatisering	√				√	√
A.7.13	√	Apparatuur moet op de juiste wijze worden onderhouden om de beschikbaarheid, integriteit en betrouwbaarheid van informatie te waarborgen.	√		IT Beheer & Kantoor-automatisering	√				√	√
A.7.14	√	Onderdelen van de apparatuur die opslagmedia bevatten, moeten worden gecontroleerd om te waarborgen dat gevoelige gegevens en in gelicentieerde software zijn verwijderd of veilig zijn overschreven voordat ze worden verwijderd of hergebruikt.	√		IT Beheer & Kantoor-automatisering	√				√	√
A.8 Technologische beheersmaatregelen											

A.8.1	√	Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user endpoint devices' moet worden beschermd.	√		IT Beheer & Kantoor-automatisering	√				√	√
A.8.2	√	Het toewijzen en het gebruik van speciale toegangsrechten moet worden beperkt en beheerd.	√		IT Beheer & Kantoor-automatisering	√			√	√	√
A.8.3	√	De toegang tot informatie en andere gerelateerde bedrijfsmiddelen moet worden beperkt overeenkomstig het vastgestelde onderwerpspecifieke beleid inzake toegangsbeveiliging.	√		IT Beheer & Kantoor-automatisering	√				√	√
A.8.4	√	Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken moet worden beperkt.	√		IT Manager	√				√	√
A.8.5	√	Er moeten beveiligde authenticatietechnologieën en -procedures worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerpspecifieke beleid inzake toegangsbeveiliging.	√		IT Beheer & Kantoor-automatisering	√			√	√	√
A.8.6	√	Het gebruik van middelen moet worden gemonitord en aangepast overeenkomstig de huidige en verwachte capaciteitseisen.	√		IT Beheer & Kantoor-automatisering	√				√	√
A.8.7	√	Bescherming tegen malware moet worden geïmplementeerd en ondersteund door een passend gebruikersbewustzijn.	√		IT Beheer & Kantoor-automatisering	√				√	√
A.8.8	√	Er moet informatie worden verkregen over technische kwetsbaarheden van in gebruik zijnde informatiesystemen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en passende maatregelen moeten worden getroffen.	√		IT Manager	√			√	√	√
A.8.9	√	Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken moeten worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.	√		IT Beheer & Kantoor-automatisering	√				√	√
A.8.10	√	In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie moet worden gewist als deze niet langer vereist is.	√		IT Beheer & Kantoor-automatisering	√	√	√	√	√	√
A.8.11	√	Gegevens moeten worden gemaskeerd overeenkomstig het onderwerpspecifieke beleid inzake toegangsbeveiliging en andere gerelateerde onderwerpspecifieke beleidsregels, en bedrijfseisen van de organisatie, rekening houdend met de toepasselijke wetgeving.	√		Security Officer	√	√	√		√	√
A.8.12	√	Maatregelen om gegevenslekken te voorkomen moeten worden toegepast in systemen, netwerken en andere apparaten waarop of waarmee gevoelige informatie wordt verwerkt, opgeslagen of getransporteerd.	√		IT Manager	√	√	√	√	√	√
A.8.13	√	Back-ups van informatie, software en systeemen moeten worden bewaard en regelmatig worden getest overeenkomstig het overeengekomen onderwerpspecifieke beleid inzake back-ups.	√		IT Beheer & Kantoor-automatisering	√	√	√	√	√	√
A.8.14	√	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	√		IT Beheer & Kantoor-automatisering	√		√		√	√

A.8.15	√	Er moeten logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, worden geproduceerd, opgeslagen, beschermd en geanalyseerd.	√		IT Manager	√		√	√	√	√
A.8.16	√	Netwerken, systemen en toepassingen moeten worden gemonitord op afwijkend gedrag en er moeten passende maatregelen worden getroffen om potentiële informatiebeveiligingsincidenten te evalueren.	√		IT Beheer & Kantoor-automatisering	√		√	√	√	√
A.8.17	√	De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, moeten worden gesynchroniseerd met goedgekeurde tijdbronnen.	√		IT Beheer & Kantoor-automatisering	√				√	√
A.8.18	√	Het gebruik van systeemhulpmiddelen die in staat kunnen zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, moet worden beperkt en nauwkeurig worden gecontroleerd.	√		IT Beheer & Kantoor-automatisering	√			√	√	√
A.8.19	√	Er moeten procedures en maatregelen worden geïmplementeerd om het installeren van software op operationele systemen op veilige wijze te beheren.	√		IT Beheer & Kantoor-automatisering	√			√	√	√
A.8.20	√	Netwerken en netwerkapparaten moeten worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	√		IT Beheer & Kantoor-automatisering	√				√	√
A.8.21	√	Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten moeten worden geïdentificeerd, geïmplementeerd en gemonitord.	√		IT Beheer & Kantoor-automatisering	√				√	√
A.8.22	√	Groepen informatiediensten, gebruikers en informatiesystemen moeten in de netwerken van de organisatie worden gesegmenteerd.	√		IT Beheer & Kantoor-automatisering	√				√	√
A.8.23	√	De toegang tot externe websites moet worden beheerd om blootstelling aan kwaadaardige inhoud te beperken.	√		IT Beheer & Kantoor-automatisering	√				√	√
A.8.24	√	Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, moeten worden gedefinieerd en geïmplementeerd.	√		IT Manager	√				√	√
A.8.25	√	Voor het veilig ontwikkelen van software en systemen moeten regels worden vastgelegd en toegepast.	√		IT Manager	√				√	√
A.8.26	√	Er moeten eisen aan de informatiebeveiliging worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.	√		Security Officer	√				√	√
A.8.27	√	Uitgangspunten voor het ontwerpen van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het ontwikkelen van informatiesystemen.	√		IT Manager	√				√	√
A.8.28	√	Er moeten principes voor veilig coderen worden toegepast op softwareontwikkeling.	√		IT Manager	√				√	√
A.8.29	√	Processen voor het testen van de beveiliging moeten worden gedefinieerd en geïmplementeerd in de ontwikkelcyclus.	√		IT Manager	√			√	√	√
A.8.30	√	De organisatie moet de activiteiten in verband met uitbestede systeemontwikkeling sturen, bewaken en beoordelen.	√		IT Manager	√				√	√

A.8.31	√	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden en beveiligd.	√		IT Manager	√				√	√
A.8.32	√	Wijzigingen in informatieverwerkende faciliteiten en informatiesystemen moeten onderworpen zijn aan procedures voor wijzigingsbeheer.	√		IT Manager	√			√	√	√
A.8.33	√	Testgegevens moeten op passende wijze worden geselecteerd, beschermd en beheerd.	√		IT Manager	√				√	√
A.8.34	√	Audittests en andere auditactiviteiten waarbij operationele systemen worden beoordeeld, moeten worden gepland en overeengekomentussen de tester en het verantwoordelijke management.	√		IT Manager	√				√	√

ISO27701:2019

						Trigger				Van toepassing in haar rol als	
Nummer	Van toepassing	Beheersmaatregel	Volledig ingevoerd	Niet ingevoerd	Verantwoordelijke	Beleid	Wet- en regelgeving	Contractuele eis	Risico-analyse	Verwerker	Verwerkings-verantwoordelijke
Voorwaarden voor het verzamelen en verwerken											
A.7.2.1	√	De organisatie moet de specifieke doeleinden waarvoor de PII wordt verwerkt, identificeren en documenteren	√		Privacy officer	√	√				√
A.7.2.2	√	De organisatie moet de relevante rechtsgrond voor het verwerken van PII voor de geidentificeerde doeleinden vaststellen documenteren en eraan voldoen.	√		Privacy officer	√	√				√
A.7.2.3	√	De organisatie moet een proces vaststellen en documenteren aan de hand waarvan zij kan aantonen of, wanneer en hoe toestemming voor het verwerken van PII is verkregen van PII-betrokkenen.	√		Privacy officer	√	√		√		√
A.7.2.4	√	De organisatie moet toestemming van de PII-betrokkenen verkrijgen en registreren overeenkomstig de gedocumenteerde processen.	√		Privacy officer	√	√				√
A.7.2.5	√	De organisatie moet beoordelen of een privacy-effectbeoordeling nodig is en deze indien van toepassing implementeren, telkens als er nieuwe verwerkingen van PII of veranderingen aan de bestaande verwerking van PII gepland zijn.	√		Privacy officer	√			√		√
A.7.2.6	√	De organisatie moet een schriftelijke overeenkomst hebben met elke PII-verwerker waarvan zij gebruikmaakt en moet bewerkstelligen dat de overeenkomst met PII-verwerkers ingaan op de implementatie van de passende beheersmaatregelen in Bijlage B.	√		Privacy officer	√	√	√			√

A.7.2.7	√	De organisatie moet respectievelijke rollen en verantwoordelijkheden vaststellen voor het verwerken van PII (met inbegrip van eisen voor bescherming en beveiliging van PII) met een mede PII-verwerkersverantwoordelijke.	√		Privacy officer	√	√				√
A.7.2.8	√	De organisatie moet de noodzakelijke registraties ter ondersteuning van haar verplichtingen voor het verwerken van PII vaststellen en op beveiligde wijze bijhouden.	√		Privacy officer	√	√				√
Verplichtingen naar PII-betrokkenen												
A.7.3.1	√	De organisatie moet haar verplichtingen vanwege wet- en regelgeving en haar zakelijke verplichtingen naar PII-betrokkenen in verband met het verwerken van hun PII vaststellen en documenteren en voorzien in de middelen om aan deze verplichtingen te voldoen.	√		Privacy officer	√	√				√
A.7.3.2	√	De organisatie moet de aan PII-betrokkenen te verstrekken informatie met betrekking tot de verwerking van hun PII en het moment waarop die informatie verstrekt wordt, vaststellen en documenteren.	√		Privacy officer	√	√				√
A.7.3.3	√	De organisatie moet PII-betrokkenen voorzien van duidelijke en gemakkelijk toegankelijke informatie waarin de PII-verwerkersverantwoordelijke wordt geidentificeerd en de verwerking van hun PII wordt beschreven.	√		Privacy officer	√			√		√
A.7.3.4	√	De organisatie moet voorzien in een mechanisme waarmee PII-betrokkenen hun toestemming kunnen aanpassen of intrekken.	√		Privacy officer	√	√		√		√
A.7.3.5	√	De organisatie moet voorzien in een mechanisme waarmee PII-betrokkenen bezwaar kunnen maken tegen de verwerking van hun PII.	√		Privacy officer	√	√		√		√
A.7.3.6	√	De organisatie moet beleidsregels, procedures en/of mechanismen implementeren om te voldoen aan haar verplichtingen naar PII-betrokkenen met betrekking tot toegang tot en het corrigeren en/of wissen van hun PII.	√		Privacy officer	√	√		√		√
A.7.3.7	√	De organisatie moet derden met wie PII is gedeeld, in kennis stellen van alle aanpassingen, intrekkingen of bezwaren met betrekking tot gedeelde PII, en hiervoor passende beleidsregels procedures en/of mechanismen implementeren.	√		Privacy officer	√	√				√
A.7.3.8	√	De organisatie moet in staat zijn een kopie van de verwerkte PII te verstrekken wanneer de PII-betrokkene daarom verzoekt.	√		Privacy officer	√	√		√		√
A.7.3.9	√	De organisatie moet beleidsregels en procedures definieren en documenteren voor het omgaan met en reageren op legitieme verzoeken van PII-betrokkenen.	√		Privacy officer	√					√
A.7.3.10	√	De organisatie moet verplichtingen, met inbegrip van juridische verplichtingen, naar de PII-betrokkenen identificeren en oppakken die voortkomen uit door de organisatie genomen besluiten die verband houden met de PII-betrokkene, uitsluitend gebaseerd op geautomatiseerde verwerking van PII.	√		Privacy officer	√	√	√	√		√
Privacy by design' en 'privacy by default'												
A.7.4.1	√	De organisatie moet het verzamelen van PII beperken tot het minimum dat relevant, proportioneel en nodig is voor de geidentificeerde doeleinden.	√		Privacy officer	√	√		√		√
A.7.4.2	√	De organisatie moet het verwerken van PII beperken tot wat toereikend, relevant en nodig is voor de geidentificeerde doeleinden.	√		Privacy officer	√	√		√		√

A.7.4.3	√	De organisatie moet bewerkstellingen en documenteren dat PII gedurende de volledige levenscyclus van de PII zo juist, volledig en actueel is als nodig voor de doeleinden waarvoor de PII wordt verwerkt.	√		Privacy officer	√	√		√		√
A.7.4.4	√	De organisatie moet doelstellingen voor minimale gegevensverwerking en de mechanismen (zoals het niet-identificeerbaar maken) die worden gebruikt om die doelstellingen te bereiken, definieren en documenteren.	√		Privacy officer	√	√	√	√		√
A.7.4.5	√	De organisatie moet PII wissen of omzetten in een vorm waardoor PII-betrokkenen niet langer geidentificeerd of geheridentificeerd kunnen worden, zodra de orginele PII niet meer nodig is voor het (de) geidentificeerde doeleinde(n).	√		Privacy officer	√					√
A.7.4.6	√	De organisatie moet bewerkstelligen dat tijdelijke bestanden die als gevolg van het verwerken van PII worden aangemaakt, binnen een gespecificeerde, gedocumenteerde periode volgens gedocumenteerde procedures worden verwijderd (bijv. gewist of vernietigd).	√		Privacy officer	√	√	√	√		√
A.7.4.7	√	De organisatie mag PII niet langer bewaren dan nodig is voor de doeleinden waarvoor de PII wordt verwerkt.	√		Privacy officer	√	√				√
A.7.4.8	√	De organisatie moet beschikken over gedocumenteerde beleidsregels, procedures en/of mechanismen voor de verwijdering van PII.	√		Privacy officer	√	√	√	√		√
A.7.4.9	√	De organisatie moet via een netwerk voor gegevensoverdracht verzonden PII (bijv. aan een andere organisatie) onderwerpen aan passende beheersmaatregelen die ervoor zijn ontworpen om te bewerkstelligen dat de gegevens hun beoogde bestemming bereiken.	√		Security Officer	√	√		√		√
PII delen, doorgeven en verstrekken.											
A.7.5.1	√	De organisatie moet de relevante grondslag voor de doorgifte van PII tussen rechtsgebieden identificeren en documenteren.	√		Privacy officer	√	√	√	√		√
A.7.5.2	√	De organisatie moet de landen en internationale organisaties specificeren en documenteren waaraan PII mogelijk kan worden doorgegeven.	√		Privacy officer	√	√	√	√		√
A.7.5.3	√	De organisatie moet doorgiften van PII aan of vanuit derden registeren en samenwerking bewerkstelligen met die derden ter ondersteuning van toekomstige verzoeken in verband met verplichtingen naar de PII-betrokkenen.	√		Privacy officer	√	√				√
A.7.5.4	√	De organisatie moet de verstrekking van PII aan derden registreren, met inbegrip van welke PII is versterkt, aan wie en wanneer.	√		Privacy officer	√	√	√	√		√
Voorwaarden voor verzamelen en verwerken.											
B.8.2.1	√	De organisatie moet waar relevant bewerkstellingen dat de overeenkomst voor het verwerken van PII ingaat op de rol van de organisatie bij het ondersteunen van de verplichtingen van de klant (rekening houdend met de aard van de verwerking en de informatie beschikbaar is voor de organisatie)	√		Privacy officer	√	√	√	√	√	
B.8.2.2	√	De organisatie moet bewerkstelligen dat names de klant verwerkte PII uitsluitend wordt verwerkt voor de doeleinden die worden aangegeven in de schriftelijke opdracht van de klant.	√		Privacy officer	√		√		√	

B.8.2.3	√	De organisatie mag krachtens een overeenkomst verwerkte PII niet voor marketing- en reclamedoeleinden gebruiken zonder vast te stellen dat daarvoor vooraf toestemming is verkregen van de desbetreffende PII-betrokkene. De organisatie mag het geven van die toestemming niet als voorwaarde stellen voor het ontvangen van de dienst.	√		Privacy officer	√	√			√	
B.8.2.4	√	De organisatie moet de klant in kennis stellen indien, naar haar mening, een verwerkingsopdracht inbreuk oplevert op toepasselijke wet- en/of regelgeving.	√		Privacy officer	√	√	√		√	
B.8.2.5	√	De organisatie moet de klant voorzien van de passende informatie zodat de klant kan aantonen dat hij aan zijn verplichtingen voldoet.	√		Privacy officer	√	√	√	√	√	
B.8.2.6	√	De organisatie moet de benodigde registraties vaststellen en onderhouden ter ondersteuning van het aantonen van het voldoen aan haar verplichtingen (zoals gespecificeerd in de desbetreffende overeenkomst) voor het verwerken van PII namens een klant.	√		Privacy officer	√	√	√		√	
Verplichtingen naar PII-betrokkenen											
B.8.3.1	√	De organisatie moet de klant van de middelen voorzien om te voldoen aan zijn verplichtingen met betrekking tot PII-betrokkenen.	√		Privacy officer	√	√			√	
Privacy by design' en 'privacy by default'											
B.8.4.1	√	De organisatie moet bewerkstelligen dat tijdelijke bestanden die als gevolg van het verwerken van PII worden aangemaakt, binnen een gespecificeerde, gedocumenteerde periode volgens gedocumenteerde procedures worden verwijderd (bijv. gewist of vernietigd).	√		Privacy officer	√				√	
B.8.4.2	√	De organisatie moet de mogelijkheid bieden om PII op beveiligde wijze te retourneren, over te dragen en/of te verwijderen. Zij moet haar beleid ook aan de klant ter beschikking stellen.	√		Privacy officer	√	√	√	√	√	
B.8.4.3	√	De organisatie moet via een netwerk voor gegevensoverdracht verzonden PII onderwerpen aan passende beheersmaatregelen die ervoor zijn ontworpen om te bewerkstelligen dat de gegevens hun beoogde bestemming bereiken.	√		Security Officer	√		√		√	
PII delen, doorgeven en verstrekken.											
B.8.5.1	√	De organisatie moet de klant tijdig informeren over de grondslag voor de doorgiften van PII tussen rechtsgebieden en over eventuele voorgenomen veranderingen in dit opzicht, zodat de klant bezwaar kan maken tegen dergelijke veranderingen of de overeenkomst kan beëindigen.	√		Privacy officer	√	√	√		√	
B.8.5.2	√	De organisatie moet de landen en internationale organisaties specificeren en documenteren waaraan PII mogelijk kan worden doorgegeven.	√		Privacy officer	√	√	√		√	
B.8.5.3	√	De organisatie moet de verstrekking van PII aan derden registreren, met inbegrip van welke PII is versterkt, aan wie en wanneer.	√		Privacy officer	√				√	
B.8.5.4	√	De organisatie moet de klant kennis geven van eventuele juridisch bindende verzoeken om verstrekking van PII.	√		Privacy officer	√	√	√	√	√	
B.8.5.5	√	De organisatie moet alle verzoeken om de verstrekking van PII afwijzen die niet juridisch bindend zijn, de desbetreffende klant raadplegen alvorens PII te verstrekken en contractueel overeengekomen verzoeken om het verstrekken van PII waarvoor de desbetreffende klant autorisatie heeft gegeven, accepteren.	√		Privacy officer	√	√	√		√	

B.8.5.6	√	De organisatie moet de klant op de hoogte stellen over de eventuele inzit van onderaannemers voor het verwerken van PII aan voordat zij worden ingezet.	√		Privacy officer	√		√		√	
B.8.5.7	√	De organisatie mag alleen een onderaannemer voor het verwerken van Pii inschakelen overeenkomstig de overeenkomst met de klant.	√		Privacy officer	√		√		√	
B.8.5.8	√	De organisatie moet, indien zij algemene schriftelijke autorisatie heeft, de klant in kennis stellen van voorgenomen veranderingen met betrekking tot het toevoegen of vervangen van onderaannemers voor het verwerken van PII, en de klant daarmee de gelegenheid bieden bewaar te maken tegen die veranderingen.	√		Privacy officer	√		√		√	