TOOLS4EVER

Whitepaper V1.0 / 25 11 2022

NEN 7510

en de rol van Identity Management

Inhoudsopgave

Inleiding 1
Van ISO 27001 en ISO 27002 naar NEN 7510 2
Controls en overheidsmaatregelen 3
Identity Management en NEN 7510 4
Provisioning van gebruiksaccounts en -rechten 4
Automation: standaardisatie met ruimte voor uitzonderingen 5
Access Management 6
Cloud based Identity Management met hoge beschikbaarheid 6
Reporting 7
Meer weten? 7

Inleiding

NEN 7510 is een Nederlandse informatiebeveiligingsnorm die specifiek is bedoeld voor organisaties die persoonlijke gezondheidsinformatie verwerken. Voor cliënten en patiënten is het natuurlijk enorm belangrijk dat medische gegevens zorgvuldig worden beheerd en dat zorgmedewerkers alleen toegang hebben tot zulke gegevens ten behoeve van de behandeling en zorg. De Autoriteit Persoonsgegevens rangschikt patiëntgegevens dan ook onder de categorie 'bijzondere persoonsgegevens' die extra beschermd moeten worden.

Tegelijkertijd zijn voor de beveiliging van medische gegevens natuurlijk ook veel beveiligingsmaatregelen nodig die ook al voor 'gewone gegevens' worden gebruikt. Bovendien verwerken zorgorganisaties natuurlijk niet alleen maar bijzondere persoonsgegevens. Men zocht dus voor medische organisaties naar beveiligingsrichtlijnen die zo goed mogelijk aansluiten op algemeen geaccepteerde informatiebeveiligingsnormen. NEN 7510 is daarom ontwikkeld als een naadloze aanvulling op ISO 27001, de internationale standaard voor informatiebeveiliging.

ISO 27001 helpt organisaties een managementsysteem voor informatiebeveiliging in te richten met daarin alle noodzakelijke beveiligingsmaatregelen. NEN 7510 vult deze basisrichtlijnen aan met aanvullende (of meer gedetailleerde) maatregelen waarmee ook de specifieke medische gegevens voldoende worden beveiligd. De maatregelen richten zich vooral op een zorgvuldige omgang met patiëntgegevens, een veilige toegang tot die gegevens en een goede registratie van alle handelingen met de data. Ook gaat het niet alleen om de verwerking van medische gegevens binnen een zorginstelling, maar ook de uitwisseling van gegevens tussen zorginstellingen onderling en met toeleveranciers en externe dienstverleners. Ook zulke niet-medische organisaties zullen in dat geval vaak moeten voldoen aan NEN 7510.

In deze whitepaper geven we eerst een overzicht van de NEN 7510 standaard. Vervolgens tonen we welke rol Identity Management speelt bij het NEN 7510 compliant maken van organisaties.

Van ISO 27001 en ISO 27002 naar NEN 7510

NEN 7510 is dus gebaseerd op ISO 27001. Deze internationale standaard richt zich op informatiebeveiliging managementsystemen en beschrijft vooral hoe informatiebeveiliging procesmatig ingericht moet worden, zodat de vertrouwelijkheid, beschikbaarheid en integriteit van informatie is gegarandeerd. Het uitgangspunt is daarbij een uitgebreide risico analyse naar mogelijke dreigingen en de impact ervan. Aan de hand hiervan wordt bepaald welke maatregelen nodig zijn en welke resterende risico's nog acceptabel zijn. Informatiebeveiliging gaat dus niet om het simpelweg afvinken van een standaard lijst met maatregelen; de grootste risico's moeten daadwerkelijk de hoogste prioriteit krijgen. Ook moet er een Plan-Do-Check-Act cyclus zijn geïmplementeerd waarin voortdurend wordt gemonitord of de bestaande beveiligingsmaatregelen nog voldoen of moeten worden aangepast.

Vervolgens bevat ISO 27001 een bijlage met concrete aanbevelingen voor beveiligingsmaatregelen. Deze maatregelen (ook wel 'controls' genoemd) zijn nog verder in detail uitgewerkt in de ISO 27002 standaard met daarin 114 beheersmaatregelen. De ISO certificering van organisaties betreft altijd de ISO 27001 standaard, maar de ISO 27002 geeft dus een concretere invulling.

Op soortgelijke wijze bestaat de NEN 7510 norm ook uit twee delen, de 7510-1 en de 7510-2. Het eerste deel is vergelijkbaar met ISO 27001 en omschrijft de feitelijke norm waarvoor je gecertificeerd kan worden. 7510-2 biedt net als ISO 27002 verdiepingsmateriaal . De hoofdtekst van NEN 7510-1 (en specifiek de hoofdstukken 4 t/m 10) lijkt sterk op de ISO 27001 hoofdtekst en richt zich op de bestuurlijke en procesmatige inbedding van de informatiebeveiliging. De NEN 7510 specifieke zaken vind je vervolgens in de maatregelen. Deze zijn als bijlage opgenomen in NEN 7510-1 en worden verder uitgewerkt in NEN 7510-2. Ook hier vormen de bestaande maatregelen van ISO 27001 en 27002 het uitgangspunt. 33 van de bestaande 114 ISO maatregelen zijn uitgebreid om deze 'zorg-proof' te maken. Ook zijn er drie aanvullende maatregelen toegevoegd. Hieronder vind je een voorbeeld van zo'n zorg-specifieke aanvulling:

A.9.4	**Toegangsbeveiliging van systeem en toepassing**	
A.9.4.1	Beperking toegang tot informatie	*Beheersmaatregel* Toegang tot informatie en systeemfuncties van toepassingen moet worden beperkt in overeenstemming met het beleid voor toegangsbeveiling. **Zorgspecifieke beheersmaatregel** Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten de identiteit van gebruikers vaststellen en dit moet worden gedaan door middel van authenticatie waarbij ten minste twee factoren betrokken worden. De toegang tot functies van informatie- en toepassingssystemen in verband met het verwerken van persoonlijke gezondheidsinformatie moet geisoleerd (en gescheiden) worden van de toegang tot informatieverwerkingsinfrastructuur die geen verband houdt met het verwerken van persoonlijke gezondheidsinformatie.

In bovenstaand voorbeeld – beheersmaatregel 9.4.1. voor toegangsbeperking – vind je onder de blauwe koptekst de algemene ISO 27001 richtlijn op dit gebied. De NEN 7510 aanvulling vind je onder het rode kopje. In dit specifieke voorbeeld stelt NEN 7510 dat voor medische gegevens multi-factor authenticatie en gescheiden infrastructuren moeten worden gebruikt.

[1] De NEN standaarden worden wanneer nodig uiteraard bijgewerkt. De actuele NEN 7510 standaarden zijn NEN 7510-1: 2017 + A1: 2020 en NEN 7510-2: 2017

Controls en overheidsmaatregelen

De NEN 7510 controls en maatregelen zijn ingedeeld in 14 verschillende categorieën (hoofdstuk 5 t/m 18):

5.	Informatiebeveiligingsbeleid	Als aanvulling op het algemene organisatiebeleid moet ook een specifiek informatiebeveiligingsbeleid worden opgesteld en regelmatig geëvalueerd.
6.	Organisatie van informatiebeveiliging	Er is niet alleen een informatiebeveiligingsbeleid nódig, het moet ook worden geïmplementeerd en beheerd. Welke rollen zijn nodig met welke verantwoordelijkheden en bevoegdheden? Rolscheiding is daarbij een belangrijk aandachtspunt en ook is er vandaag de dag veel aandacht nodig voor online werken en het gebruik van (eigen) mobiele apparaten.
7.	Veilig personeel	Uiteraard moeten medewerkers voldoende zijn opgeleid en zich bewust zijn van het belang van informatiebeveiliging. Dat betreft het hele 'dienstverband', van de juiste werving van medewerkers tot en met de benodigde beveiligingsmaatregelen als mensen de organisatie weer verlaten.
8.	Beheer van bedrijfsmiddelen	Bedrijfsmiddelen om informatie te verwerken (zoals software en computersystemen) moeten goed geregistreerd en beheerd worden. Wie mag de systemen gebruiken en worden bedrijfsmiddelen en gebruiksrechten na beëindiging van de werkzaamheden weer teruggegeven? Alle informatie moet goed worden geclassificeerd en voldoende veilig opgeslagen.
9.	Toegangsbeveiliging	Er zijn maatregelen nodig om te zorgen dat medewerkers alleen toegang krijgen tot netwerken, systemen en gegevens die ze nodig hebben voor hun eigen werkzaamheden.
10.	Cryptografie	Gegevens moeten voldoende versleuteld worden om zowel de vertrouwelijkheid als de integriteit van gegevens te kunnen garanderen.
11.	Fysieke beveiliging en beveiliging van de omgeving	Organisaties moeten voorkomen dat onbevoegden toegang krijgen tot computers en gegevensdragers op kantoorlocaties. Dat betekent ook dat bij bijvoorbeeld stroomuitval of een calamiteit de informatiebeveiliging intact moet blijven. En bij afvoer van apparatuur moeten de gegevens verwijderd zijn.
12.	Beveiliging bedrijfsvoering	Er moeten duidelijke afspraken en procedures zijn om informatiesystemen veilig te gebruiken en de systemen te beschermen tegen malware. Ook zijn er duidelijke back-up en monitoring maatregelen nodig.
13.	Communicatiebeveiliging	Zowel de interne netwerkfaciliteiten als de externe netwerkcommunicatie moeten beveiligd zijn tegen onbevoegde toegang en misbruik.

14.	Acquisitie, ontwikkeling en onderhoud van informatie-systemen	Organisaties moeten bij inkoop, ontwikkeling en beheer van IT systemen rekening houden met de beveiliging van de systemen en data. Daarbij gaat het niet alleen om operationele systemen. Ook bijvoorbeeld ontwikkel-, demo- en testsystemen moeten voldoende beveiligd zijn.
15.	Leveranciersrelaties	Organisaties zijn afhankelijk van leveranciers voor hun IT systemen. Dat geldt zowel voor systemen en software die on-premises worden geleverd, als leveranciers die gevoelige cloud data beheren. Er zijn duidelijke afspraken met leveranciers nodig om de informatiebeveiliging te garanderen.
16.	Beheer van informatiebeveiligingsincidenten	Ondanks alle beveiligingsmaatregelen kan er toch een incident plaatsvinden. Hiervoor moeten goede procedures met duidelijke verantwoordelijkheden aanwezig zijn, inclusief afspraken over de verdere rapportage en oplossing.
17.	Informatiebeveiligings-aspecten van bedrijfs-continuïteitsbeheer	Bij incidenten met de IT voorzieningen moet er specifiek op worden gelet dat de continuïteit van de informatiebeveiliging altijd gegarandeerd blijft.
18.	Naleving	Als organisatie moet je voortdurend kunnen aantonen dat je voldoet aan alle geldende wet- en regelgeving.

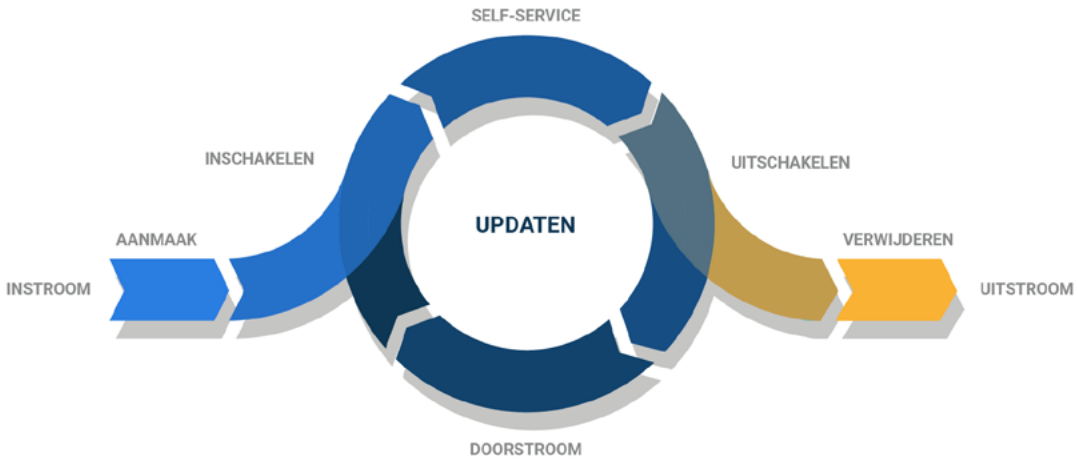
Identity Management en NEN 7510

NEN 7510 vult dus de standaard ISO controls aan met maatregelen die een zorg organisatie moet implementeren om alle informatie – inclusief medische informatie en patiëntgegevens - goed te beveiligen. Het beheer van eindgebruikers en hun rechten worden daarbij steeds belangrijker. Zorgmedewerkers, partners en patiënten mogen alleen toegang krijgen tot applicaties en data op een 'need to know' basis. Ook is het noodzakelijk dat alle IT activiteiten zijn te traceren tot het niveau van individuele gebruikers. Het maakt Identity Management een belangrijk gereedschap bij de realisatie van een 'zorg-proof' informatiebeveiliging. In dit hoofdstuk beschrijven we hoe we met een state-of-the-art Identity Management oplossing verschillende NEN 7510 maatregelen kunnen faciliteren. Dit illustreren we aan de hand van onze eigen HelloID cloudbased Identity & Access Management (IAM) platform.

Provisioning van gebruiksaccounts en -rechten

Groepsaccounts zijn in het algemeen binnen de zorg niet toegestaan, evenals het 'copy user' principe voor nieuw binnenkomende medewerkers. Toegangsrechten moeten vandaag de dag eenduidig zijn gekoppeld aan individuele gebruikersaccounts. Er moet op ieder moment duidelijk zijn wie er toegang heeft tot specifieke (patiënt)data en applicaties en wie bepaalde handelingen uitvoert. En natuurlijk moeten de accountgegevens en toegangsrechten altijd up-to-date zijn. Dus steeds in lijn met iemands huidige rol en positie binnen de organisatie. Professioneel en geautomatiseerd gebruikersaccountmanagement is daarvoor cruciaal.

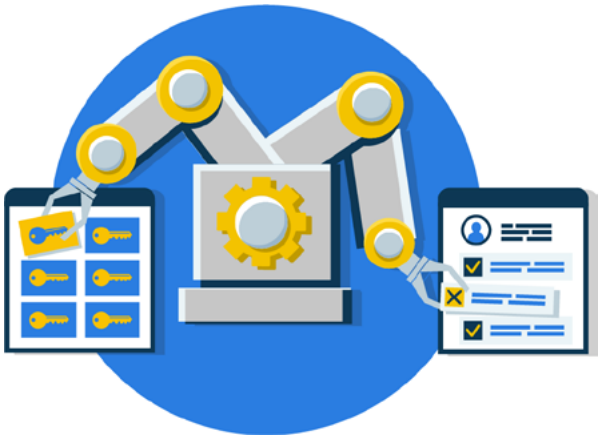
Binnen HelloID borgen we dit door middel van geautomatiseerde provisioning. Hiermee zijn iemands digitale identiteit en toegangsrechten altijd in lijn met de informatie zoals geregistreerd in het HR systeem. Dankzij een rechtstreekse koppeling tussen dat HR systeem en HelloID ontvangt de nieuwe medewerker bij onboarding direct een gebruikersaccount met daaraan gekoppeld de faciliteiten en rechten die passen bij diens rol. Ook tijdens het verdere dienstverband houden we dit automatisch actueel. Verandert iemands rol, dan past HelloID ook direct de toegangsrechten aan. En verlaat iemand de organisatie, dan zorgt



HelloID dat automatisch het account wordt geblokkeerd en de vertrekkende medewerker geen toegang meer heeft. Stapeling van rechten en accounts die per ongeluk toegankelijk blijven, zijn niet langer mogelijk. Ook kunnen we specifieke accountbeheer processen inrichten voor tijdelijke krachten en flex-werkers.

Automation: standaardisatie met ruimte voor uitzonderingen

Goede informatiebeveiliging leunt op duidelijke beleidsregels, heldere processen en weinig ruimte voor individueel en ongecontroleerd maatwerk. Om dat te borgen willen we identity management processen zoveel als mogelijk standaardiseren en automatiseren. Daarbij moet het mogelijk zijn concepten als Role Based access te ondersteunen en processen te implementeren met een duidelijke scheiding van rollen. Tegelijkertijd zijn er altijd uitzonderingen en moet iedere organisatie een eigen balans zoeken tussen gebruiksvriendelijkheid en bedrijfsveiligheid. Automatisch te veel rechten verstrekken, leidt tot ongewenste beveiligingsrisico's. Maar medewerkers steeds onnodig laten wachten op hun toegangsrechten belemmert hun werk.



HelloID biedt die gewenste combinatie van standaardisatie en uitzonderingen:

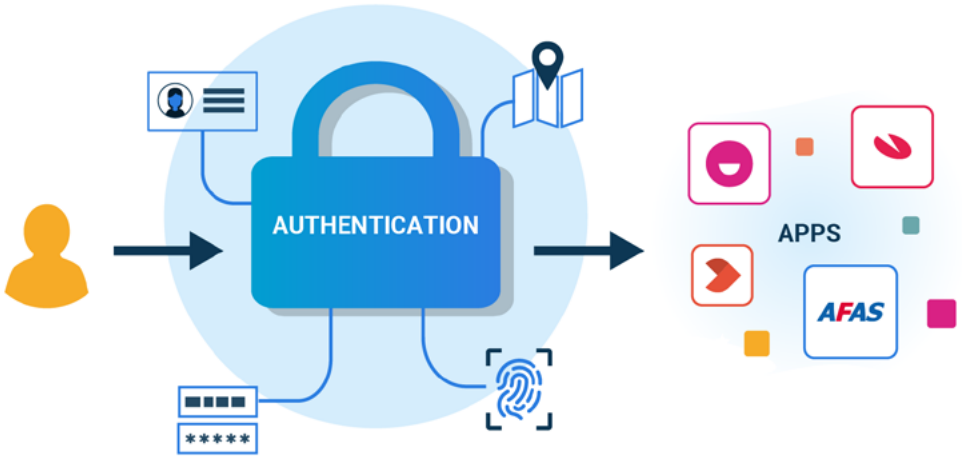
- Standaard kun je binnen HelloID rechten toekennen met behulp van de zogenaamde Attribute Based Access Control (ABAC) functionaliteit. De organisatiestructuur met rollen en bijbehorende werkzaamheden vertalen we in HelloID naar configureerbare business rules die automatisch bepalen welke toegangsrechten een medewerker krijgt. Vanaf de automatisch onboarding bij indiensttreding tot en met de vertrekprocedure bij vertrek.
- Het merendeel van de rechten wordt dus volledig geautomatiseerd uitgegeven, maar zo'n standaard rollenmatrix is nooit volledig dekkend en daarom voorziet HelloID ook in uitzonderingen. Voor specifiekere en moeilijker automatisch uitdeelbare rechten kun je self-service processen ontwerpen. Gebruikers kunnen hiermee zelf online toegang vragen tot applicaties of datashares waarbij automatisch de juiste goedkeuringsstappen worden gevolgd. Na goedkeuring zorgt het geautomatiseerde proces voor de verdere activering zonder risicovolle uitzonderingen of vergissingen.

Geautomatiseerde configuratieregels zorgen dat de dienstencatalogus automatisch up-to-date blijft. Een nieuwe share wordt bijvoorbeeld direct zichtbaar in de catalogus. Op ieder moment kan het systeem een overzicht geven van welke medewerkers actief zijn en welke licenties, applicaties, shares, et cetera zij in

gebruik hebben. Service Automation kan ook worden gebruikt om de gebruikersaccounts en rechten voor flexibele en tijdelijke medewerkers veilig te beheren.

Access management

Een state-of-the-art toegangsmanagement zorgt dat medewerkers - en zo nodig ook partners en cliënten - eenvoudig en uniform toegang krijgen tot applicaties en data. Zoals hiervoor toegelicht is het uitgangspunt dat iedere gebruiker één persoonlijk gebruikersaccount krijgt. Met een concept als Single Sign-On zorg je vervolgens dat mensen maar één keer hoeven in te loggen. Juist zo'n combinatie van gebruiksvriendelijke én veilige toegangsoplossingen voorkom je dat medewerkers onveilige work-arounds verzinnen.



HelloID ondersteunt alle gangbare Single Sign-On protocollen om gebruikers per applicatie te authentiseren. Voor toegang tot applicaties zonder ingebouwde SSO faciliteiten biedt HelloID andere methodes om de toegang te verzorgen. Voor de primaire authenticatie kunnen we HelloID integreren met Active Directory en andere zogenaamde Identity Providers zoals Azure, Google, Salesforce, SAML en OpenID. Ook ondersteunt het platform extra beveiligingsopties die NEN 7510 voorschrijft, zoals Two Factor Authentication (2FA). HelloID herkent contextuele factoren zoals de inloglocatie en het tijdstip en kan afhankelijk daarvan de gebruiker vragen om een extra authenticatie. Naast soft of hard tokens en sms biedt HelloID ook verschillende one time passwords (OTP's) als tweede factor.

Cloud based Identity Management met hoge beschikbaarheid

Steeds meer zorginstellingen migreren hun bestaande IT dienstverlening naar de cloud en ook voor Identity en Access Management zoekt men dus een cloud-based oplossing. De beschikbaarheid, betrouwbaarheid en veiligheid is daarbij cruciaal. Als centrale schakel binnen de dienstverlening moet de 'identity management' keten altijd functioneren en mag de toegangsbeveiliging nooit worden 'kortgesloten'.

HelloID verzorgt Identity & Access Management vanuit de cloud met als voordeel lagere investeringen, een snelle installatie en configuratie terwijl Tools4ever het technische beheer verzorgt, inclusief automatische updates. De oplossing wordt gerealiseerd met behulp van maximaal beveiligde Microsoft Azure- en Google Cloudomgevingen, die bovendien iedere zes maanden grondig wordt gecontroleerd door Deloitte Risk Services. Compliance aan de strenge security-eisen is dan ook gewaarborgd. De dienstverlening heeft bovendien een zeer hoge beschikbaarheid dankzij de ingebouwde redundantie.

Reporting

Binnen zorginstellingen is registratie en rapportage essentieel. Als organisatie moet je kunnen aantonen dat de verschillende processen conform de relevante wet- en regelgeving worden uitgevoerd. Ook moet je bij een beveiligingsincident zoals een datalek kunnen traceren welke gebruikers binnen het netwerk welke handelingen hebben uitgevoerd.

Als cloud based oplossing moet HelloID voldoen aan steeds strengere wet- en regelgeving op het gebied van audits en beveiliging. Alle toegangspogingen, geautomatiseerde en handmatige processen, en het gebruik van ons platform worden daarom geregistreerd en inzichtelijk gemaakt. Zo wordt het authenticatieproces automatisch gemonitord en is via rapportages altijd inzichtelijk wie welke applicaties heeft geraadpleegd, op welk moment en vanaf welke locatie. Dit geeft niet alleen een gedetailleerd beeld van het doorlopen authenticatietraject, maar toont bijvoorbeeld ook inlogpogingen vanaf verdachte IP-adressen. Mogelijke dreigingen kunnen tijdig worden herkend om tegenmaatregelen te nemen.

Extra onderscheidend is dat binnen HelloID de volledige identity lifecycle per systeem én per gebruiker auditable is. Alle uitgevoerde acties worden gelogd, zoals het creëren, inschakelen, updaten, verplaatsen, disablen en verwijderen van accounts. Hetzelfde geldt voor het toekennen en intrekken van permissies. Zijn rechten ad hoc toegekend (buiten de reguliere rollenmatrix) dan is via HelloID precies te zien wie dit heeft aangevraagd, welke persoon het verzoek heeft goedgekeurd en tot welke exacte wijzigingen in achterliggende systemen dit heeft geleid. Daarmee is het HelloID proces volledig transparant, toetsbaar en aanpasbaar.

Meer weten?

Identity Management vormt vandaag de dag een centrale rol binnen je IT beveiliging. Medewerkers, partners en cliënten mogen alleen nog met een eigen account toegang krijgen tot applicaties en data. Rechten moeten altijd worden verstrekt op een ‘need to know’ basis. We moeten bovendien alle IT activiteiten tot het niveau van individuele gebruikers kunnen traceren. Het maakt je Identity Management platform een belangrijk element bij het inrichten van je NEN 7510 compliant informatiebeveiligingssysteem.

Meer weten over de rol die Identity Management kan spelen bij de NEN 7510 compliancy binnen je organisatie? En hoe kun je je IT omgeving veilig houden zonder in te leveren op gebruiksvriendelijkheid? We vertellen je hier graag meer over. Bijvoorbeeld aan de hand van onze reference list NEN 7510 – HelloID. In deze lijst behandelen we alle NEN 7510 controls en maatregelen met per maatregel een toelichting of – en zo ja, hoe – HelloID Identity Management hieraan een bijdrage kan leveren.

TOOLS4EVER

Adres	Amalialaan 126c 3743 KJ Baarn Nederland
Telefoon	+31 (0) 35 54 832 55
Website	Tools4ever.nl
Mail	info@tools4ever.com
Sales	sales@tools4ever.com
Support	tools4ever.nl/support