HelloID bijdrage aan NIS2 compliancy van klantorganisaties

Deze checklist toont hoe de HelloID dienstverlening bijdraagt aan het NIS2 compliant maken van klantorganisaties. De checklist richt zich dus specifiek op NIS2 verplichtingen bij klanten waaraan HelloID een bijdrage kan leveren. De checklist is opgesteld aan de hand van de artikelen in de NIS2 richtlijn (RICHTLIJN (EU) 2022/2555). Alleen die artikelen zijn opgenomen waarin HelloID relevant is.

Let op: De checklist is dus géén volledige compliancylijst van de HelloID dienstverlening zelf. NIS2 is in Nederland geïmplementeerd in de Cyberbeveiligingswet (Cbw). Tools4ever is binnen dat kader een belangrijke entiteit en de tools4ever en HelloID dienstverlening zijn daarom ingericht om te voldoen aan de NIS2 eisen.

Hfst I Algemene bepalingen

Art. 1	Onderwerp	n.v.t.
Art. 2	Toepassingsgebied	n.v.t.
Art. 3	Essentiële en belangrijke entiteiten	n.v.t.
Art. 4	Sectorspecifieke rechtshandelingen van de Unie	n.v.t.
Art. 5	Minimum-harmonisatie	n.v.t.
Art. 6	Definities	n.v.t.

Hfst II Gecoördineerde kaders op het gebied van cyberbeveiliging

Art. 7	Nationale cyberbeveiligingsstrategie	n.v.t.
Art. 8	Bevoegde autoriteiten en centrale contactpunten	n.v.t.

Art. 9	Nationale kaders voor cybercrisis-beheer	n.v.t.
Art. 10	Computer security incident response teams (CSIRT's)	n.v.t.
Art. 11	Eisen, technische capaciteiten en taken van de CSIRT's	n.v.t.
Art. 12	Gecoördineerde bekendmaking van de kwetsbaarheden en een Europese kwetsbaarheids-database	n.v.t.
Art. 13	Samenwerking op nationaal niveau	n.v.t.

Hfst III Samenwerking op unie- en internationaal niveau

Art. 14	Samenwerkings-groep	n.v.t.
Art. 15	CSIRT-netwerk	n.v.t.
Art. 16	Het Europese netwerk van verbin-dingsorganisaties voor cybercrises (EU-CyCLONe)	n.v.t.
Art. 17	Internationale samenwerking	n.v.t.
Art. 18	Verslag over de stand van zaken op het gebied van de cyberbeveiliging in de Unie	n.v.t.
Art. 19	Collegiale toetsingen	n.v.t.

Hfst IV Risicobeheersmaatregelen en rapportageverplichtingen op het gebied van cyberbeveiliging

Art. 20	Governance	n.v.t.
Art. 21	Maatregelen voor het beheer van cyber-beveiligingsrisico's	Binnen het beheer van cyberbeveiligingsrisico's, borgt HelloID het toegangsbeheer tot systemen en gegevens binnen organisaties. Dit kan ook de fysieke toegangsbeveiliging omvatten, via koppelingen met fysieke toegangbeheersystemen. HelloID user provisioning automatiseert de uitgifte en het beheer van accounts en toegangs-rechten voor gebruikers. Dit dekt de hele identity lifecycle af, vanaf iemands onboarding tot en met diens vertrek. Hierbij wordt gebruik gemaakt van Attribute Based Access Control, waarbij de actuele gegevens uit HR-applicaties en andere bronsystemen worden geraadpleegd om te bepalen welke IT-faciliteiten nodig zijn. Aanvul-lend kunnen individuele toegangsrechten worden verstrekt en beheerd met behulp van service automation en self-service. Via configureerbare workflows kunnen individuele verzoeken worden beoordeeld door hiervoor aangewezen functionaris(sen). Voor het real-time access management kan HelloID gebruik maken van sepa-rate identity providers (IdP) zoals Active Directory of Entra ID, maar het platform beschikt ook over een ingebouwde IdP. Deze onder-steunt Single Sign-On (SSO) en meerdere Multi-Factor Authenticatie (MFA) methodes, inclusief FIDO2-compliant hardware keys. HelloID genereert logs en informatie ten behoeve van analyses, rapportages en audits. ***Daarnaast is er een ruime set aan governance tools om individueel verstrekte rechten regelmatig planmatig te opnieuw te beoordelen, de uitgifte van conflicterende rechten te voorkomen, inconsistenties tussen de IAM-registratie en doelsystemen te detecteren, en het account- en rechtenbeheer periodiek te evalue-ren, actualiseren en verbeteren.***
Art. 22	Op Unieniveau gecoördineerde beveiligingsrisico-beoordelingen van kritieke toeleverings-ketens	n.v.t.
Art. 23	Rapportage-verplichtingen	HelloID genereert logs en informatie ten behoeve van analyses, rapportages en audits. Alle binnen en door HelloID uitgevoerde acties worden opgeslagen in Elastic reporting met uitgebreide rapportage mogelijkheden. Dat omvat onder andere: - Provisioning: Naast een overzicht van alle businessrules (en wijzi-gingen), per systeem en gebruiker alle acties omtrent het creëren, enablen, updaten, verplaatsen, disablen, het verwijderen van accounts, en het toekennen en intrekken van permissies. - Service Automation met alle (self) service acties omtrent aanvra-gen, workflows, goedkeuringen, formulierdata en configuratiewijzi-gingen. Zo worden bij alle wijzigingen binnen HelloID vastgelegd wie

		deze heeft aangevraagd, welke persoon het verzoek heeft goedgekeurd en tot welke exacte wijzigingen in achterliggende systemen dit heeft geleid. - Access Management met alle succesvolle en mislukte aanmeldingen, de geografische locatie van de gebruiker, gebruikte apparaten, geïnitieerde wachtwoordresets, toegangspogingen voor applicaties en mislukte toegangspogingen als gevolg van het toegangsbeleid. Deze gegevens kunnen worden geanalyseerd om kwetsbaarheden te herkennen en problemen te voorkomen. Ook kunnen gegevens worden gedeeld met bijvoorbeeld SIEM (Security Information and Event Management) systemen. ***Daarnaast kunnen bijvoorbeeld onbeheerde accounts worden ontdekt met behulp van reconciliation functionaliteit.***
Art. 24	Gebruik van Europese cyberbeveiligings-certificerings-regelingen	n.v.t.
Art. 25	Normalisatie	n.v.t.

Hfst V Jurisdictie en registratie

Art. 26	Jurisdictie en territorialiteit	n.v.t.
Art. 27	Register van entiteiten	n.v.t.
Art. 28	Database met domeinnaam-registratiegegevens	n.v.t.

Hfst VI Informatie-uitwisseling

Art. 29	Informatie-uitwisselingsregelingen op het gebied van cyberbeveiliging	HelloID genereert logs en informatie ten behoeve van analyses, rapportages en audits (zie art. 23). Deze informatie kan waar relevant worden gebruikt om gezamenlijk cyberdreiging aan te pakken.
Art. 30	Vrijwillige melding van relevante informatie	n.v.t.

Hfst VII Toezicht en handhaving

Art. 31	Algemene aspecten van het toezicht en de handhaving	n.v.t.
Art. 32	Toezichts- en handhavingsmaatregelen met betrekking tot essentiële entiteiten	HelloID genereert logs en informatie ten behoeve van analyses, rapportages en audits (zie art. 23). Deze vormen belangrijke input voor onder andere audits en beveiligingsscans, ook ten behoeve van het toezicht en de handhaving.
Art. 33	Toezichts- en handhavingsmaatregelen met betrekking tot belangrijke entiteiten	HelloID genereert logs en informatie ten behoeve van analyses, rapportages en audits (zie art. 23). Deze vormen belangrijke input voor onder andere audits en beveiligingsscans, ook ten behoeve van het toezicht en de handhaving.
Art. 34	Algemene voorwaarden voor het opleggen van administratieve geldboeten aan essentiële en belangrijke entiteiten	n.v.t.
Art. 35	Inbreuken die een inbreuk in verband met persoonsgegevens inhouden	HelloID genereert logs en informatie ten behoeve van analyses, rapportages en audits (zie art. 23). Deze vormen belangrijke input voor onder andere audits en beveiligingsscans, ook ten behoeve van het toezicht en de handhaving.
Art. 36	Sancties	n.v.t.
Art. 37	Wederzijdse bijstand	n.v.t.

Hfst VIII Gedelegeerde handelingen en uitvoeringshandelingen

Art. 38	Uitoefening van de bevoegdheidsdelegatie	n.v.t.
Art. 39	Comitéprocedure	n.v.t.

Hfst IX Slotbepalingen

Art. 40	Evaluatie	n.v.t.
Art. 41	Omzetting	n.v.t.

Art. 42	Wijziging van Verordening (EU) nr. 910/2014	n.v.t.
Art. 43	Wijziging van Richtlijn (EU) 2018/1972	n.v.t.
Art. 44	Intrekking	n.v.t.
Art. 45	Inwerkingtreding	n.v.t.
Art. 46	Adressaten	n.v.t.