Toelichtings-document Wetgeving inz. IX

10 juli 2025, versie 1.0

Toelichtingsdocument Wetgeving inz. IX

Dit is een document van CIIIC, opgesteld door Considerati.

Versie 1.0, datum: 10 juli 2025

Inhoudsopgave

Inleiding

Binnen Nederland en de EU bestaat een breed palet aan regels dat van toepassing is op immersieve technologieën. De Algemene verordening gegevensbescherming, de Telecommunicatiewet, AI Act, de Algemene wet gelijke behandeling en het Burgerlijk Wetboek vormen het fundament voor bescherming van persoonsgegevens, non-discriminatie, transparantie en consumentenbescherming. Sectorspecifieke regels, zoals bijvoorbeeld de Medical Device Regulation en de Wet Geneeskundige Behandelingsovereenkomst in de zorg, vullen dit aan.

In deze notitie bespreken wij de belangrijkste wettelijke kaders voor immersieve toepassingen en ervaringen (verder: immersieve ervaringen). In hoofdstuk 2 bespreken wij een aantal wetten en regels die nagenoeg altijd relevant zijn voor immersieve ervaringen, ongeacht de context van het gebruik. In hoofdstuk 3 bespreken wij een aantal specifieke juridische kaders die van toepassing kunnen zijn in de relatie tot de in het CIIIC programma genoemde thema's: Gezondheidszorg, Training & Onderwijs, Entertainment, Infrastructuur, Werkplek/ Kantoor, Kunst en de Publieke ruimte (inclusief mobiliteit).

De wetten en regels kunnen van toepassing zijn op de IX-aanbieder, maar ook op de gebruiker van de immersieve ervaring. Voor de IX-aanbieder is het dan relevant om de toepassing aan te bieden op een dusdanige wijze dat de gebruiker aan diens wettelijke verplichtingen kan voldoen.

Houd er rekening mee dat het antwoord op de vraag welke wetgeving van toepassing is altijd afhankelijk is van de specifieke toepassing. Voor een individuele immersieve ervaring kan het dus zijn dat (delen van) de in deze notitie besproken wettelijke kaders niet van toepassing zijn, of juist aanvullende regels gelden.

2 Algemene regels

In dit hoofdstuk bespreken wij een aantal relevante wetten en regels waarmee rekening moet worden gehouden, ongeacht de soort toepassing.

2.1 Algemene verordening gegevensbescherming

De AVG is van toepassing op immersieve ervaringen wanneer bij het gebruik van deze ervaringen persoonsgegevens worden verwerkt. Persoonsgegevens zijn alle gegevens die betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon. Immersieve ervaringen kunnen grote hoeveelheden (gevoelige) persoonsgegevens verwerken, waaronder bewegings- en gedragsdata, irisscans en neurodata. Het betreffen hier doorgaans de gegevens van de eindgebruiker(s), maar er kunnen ook gegevens van omstanders worden verwerkt.

De AVG stelt eisen aan de rechtmatigheid, transparantie, doelbinding en beveiliging van deze gegevens. De AVG is technologie-neutraal en geldt voor alle verwerkingen van persoonsgegevens, ongeacht het type apparaat of interface. De IX-aanbieder (de verwerkingsverantwoordelijke) moet er zorg voor dragen dat:

1. de toepassing rechtmatig is (het hebben van een duidelijk doel met een wettelijke grondslag);
2. de toepassing transparant is (de betrokkene moet worden geïnformeerd);
3. de gegevens niet voor andere doeleinden worden gebruikt (doelbinding);
4. alleen gegevens worden verwerkt die noodzakelijk zijn (dataminimalisatie);
5. de gegevens niet langer worden bewaard dan noodzakelijk (opslagbeperking);
6. de gegevens goed worden beveiligd.
7. Verder moet de verwerkingsverantwoordelijke de rechten van de betrokkene respecteren, zoals diens recht op inzage, correctie en verwijdering.

Wat in de context van immersieve ervaringen en gegevensbescherming nog van groot belang is, is dat de IX-aanbieder veelal gebruik maakt van de hardware- en software platforms van andere partijen (denk bijvoorbeeld aan Meta). Deze partijen verwerken mogelijk ook persoonsgegevens voor hun eigen doeleinden. De IX-aanbieder moet beoordelen in hoeverre de derde partij toegang heeft tot gegevens van eindgebruikers en omstanders en bepalen wat deze partij allemaal doet met deze gegevens. Waar relevant moet de IX-aanbieder schriftelijke

afspraken maken met deze partijen over het gebruik van de gegevens (verwerkersovereenkomsten).

2.2 Artikel 11.7a Telecommunicatiewet (cookiewet)

Artikel 11.7a van de Telecommunicatiewet verplicht IX-aanbieders tot het verkrijgen van voorafgaande toestemming voor het plaatsen of uitlezen van informatie op randapparatuur van gebruikers, zoals headsets, smartphones en wearables. Dit geldt voor cookies, device-fingerprinting, cookieless tracking en vergelijkbare technologieën. Uitzonderingen gelden alleen voor strikt noodzakelijke functionaliteiten.

2.3 Algemene Wet gelijke behandeling

De Awgb verbiedt discriminatie op grond van onder meer ras, geslacht, leeftijd, seksuele gerichtheid en beperking. Immersieve ervaringen moeten non-discriminatoir functioneren. Dit betekent dat aanbieders van immersieve ervaringen maatregelen moeten nemen om directe en indirecte discriminatie door of via hun systemen tegen te gaan.

2.4 AI Verordening

De Europese AI Verordening is nieuwe Europese productwetgeving die eisen stelt aan AI-systemen. Wanneer een immersieve ervaring een AI-component bevat, dan bestaat er een kans dat deze toepassing onder de AI Act valt. De AI Act is van toepassing op ontwikkelaars en gebruikers van AI-systemen, ongeacht of deze binnen of buiten de EU zijn ontwikkeld, mits ze op de Europese interne markt worden aangeboden of gebruikt. De AI Act maakt een onderscheid tussen verboden systemen, hoog-risico systemen en overige systemen (laag risico).

2.4.1 Verboden systemen

Sommige AI-toepassingen zijn geheel verboden, zoals systemen voor schadelijke manipulatie of social scoring. Ook systemen die emotiedetectie op de werkplek of in het onderwijs mogelijk maken zijn verboden.

2.4.2 Hoog-risico AI systemen

Toepassingen die een hoog risico voor de gezondheid, veiligheid of rechten van personen met zich mee kunnen brengen worden onderworpen aan strenge eisen. Het gaat dan onder andere om eisen op het gebied risicobeheer, veiligheid, accuraatheid, menselijk toezicht en transparantie.[1] Een AI-systeem wordt gekwalificeerd als hoog-risico wanneer het een product is dat reeds valt onder bestaande Europese productregulering, of een veiligheidscomponent is van zo'n

product. Een AI-systeem is ook hoog-risico wanneer het wordt gebruikt in een hoog-risico context.[2] Onder andere toepassingen in de gezondheidszorg, HR en kritieke infrastructuren kunnen daaronder vallen. Hoog-risico AI-systemen mogen alleen in de handel worden gebracht of in gebruik gesteld nadat zij CE gekeurd zijn.

2.4.3 Overige AI systemen

Voor systemen die niet verboden zijn en ook geen hoog risico vormen, gelden beperkte eisen. Het gaat dan met name om transparantie. Zo moet onder andere worden aangegeven wanneer iemand met een AI contact heeft (zoals bijvoorbeeld een chatbot) en moet bij het gebruik van generatieve AI duidelijk zijn dat er bijvoorbeeld gebruik wordt gemaakt van deep fakes.

2.5 Digital services act (DSA)

De DSA geldt voor digitale diensten, waaronder platforms en IX-omgevingen, en stelt eisen aan transparantie, gebruikersbescherming, het tegengaan van illegale content en het bieden van toegankelijke klachtenprocedures. De DSA verplicht aanbieders verder tot het uitleggen van moderatiebeslissingen en het bieden van gebruikersvriendelijke bezwaarprocedures. De DSA is primair van toepassing op (grote) online platformen, dit betekent dat de DSA niet altijd van toepassing is op een immersieve ervaring. Het hangt van de kenmerken en de omvang van de toepassing of deze onder de DSA valt.

2.6 Informatiebeveiliging

Er zijn diverse wetten die regels stellen op het gebied van informatiebeveiliging. Zo vereist artikel 32 AVG dat de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen neemt om persoonsgegevens te beschermen.[3] Binnen de financiële sector gelden specifieke beveiligingseisen op grond van onder andere de DORA wetgeving.[4]

2.6.1 Cyberbeveiligingswet (NIS2)

De Cyberbeveiligingswet vervangt binnenkort de Wet Beveiliging Netwerk- en Informatiesystemen (WBNI), de Nederlandse implementatie van de NIS1 richtlijn. De Cyberbeveiligingswet (de Nederlandse implementatie van de NIS2 richtlijn) zal in de meeste gevallen niet direct van toepassing zijn op IX-aanbieders. Toch is deze wet wel relevant, omdat ze wel van toepassing kan zijn op de afnemers van immersieve ervaringen. De Cyberbeveiligingswet stelt eisen aan organisaties die aangemerkt zijn als essentiële of belangrijke entiteiten (denk aan gas-, water- en elektriciteitsbedrijven, banken, luchthavens et cetera). Wanneer binnen deze organisaties immersieve ervaringen worden gebruikt, dan moet het gebruik passen binnen het beveiligingsbeleid van de organisatie. De beveiligingseisen die worden

gesteld aan essentiële en belangrijke entiteiten worden voorgeschreven door de Cyberbeveiligingswet. Verder hebben essentiële en belangrijke entiteiten de verantwoordelijkheid om afspraken te maken over digitale veiligheid met hun toeleveranciers.

2.6.2 Cyber resilience act (CRA)

De Cyber Resilience Act (CRA) is een Europese productreguleringsverordening die geldt voor ‘producten met digitale elementen’. IX-technologieën (hardware, software en combinaties daarvan) kunnen onder de reikwijdte van de CRA vallen.[5] Dit betekent dat XR-toepassingen afhankelijk van het soort toepassing aan specifieke beveiligingsvereisten moeten voldoen.[6] De CRA is al van kracht, maar heeft ten tijde van het schrijven van deze memo nog geen rechtstreekse werking in de lidstaten. In 2026 krijgt de CRA rechtstreekse werking in de EU en moeten aanbieders voldoen aan de regels van de CRA. Voor IX-aanbieders is het met name relevant om te beoordelen of de hardware en software die zij gebruiken gecertificeerd is.

2.6.3 Beveiligingsstandaarden

Naast wettelijke verplichtingen zijn er tal van standaarden op het gebied van informatiebeveiliging. De meest bekende zijn de ISO 27001 en de ISO27002. ISO 27001 beschrijft de inrichtingen van informatiebeveiliging binnen een organisatie (een Information Security Management System of ISMS). ISO 27002 beschrijft diverse beveiligingsmaatregelen (controls) en de wijze om deze effectief te implementeren (een code of practice). Voor de overheid geldt de Baseline Informatiebeveiliging Overheid (BIO). Toepassingen die binnen de overheid worden gebruikt moeten in lijn zijn met de vereisten uit de BIO. De BIO is gebaseerd op de ISO 27001 en 27002 standaarden.

2.7 European Accessibility Act

Sinds juni 2025 geldt de European Accessibilty Act. Dit betekent dat websites en apps van overheden en bedrijven moeten voldoen aan (digitale) toegankelijkheidscriteria. Afhankelijk van de context kunnen immersieve ervaringen óók onder deze richtlijn vallen.[7] Dit betekent dat de ervaring ook goed toegankelijk/bruikbaar moet zijn voor mensen met een beperking. Dit raakt ontwerp, functionaliteit en gebruiksvriendelijkheid van immersieve ervaringen. In Nederland is de EEA geïmplementeerd in de Wet gelijke behandeling op grond van handicap of chronische ziekte.

Voor de praktische invulling van de vereisten moet aangesloten moet worden bij standaarden op het gebied van digitale toegankelijkheid zoals de Web Content Accessibility Guidelines (WCAG).[8]

2.8 Algemene wet bestuursrecht

Wanneer overheidsinstanties immersieve ervaringen inzetten, bijvoorbeeld voor dienstverlening of handhaving, dan zijn de algemene beginselen van behoorlijk bestuur uit de Awb van toepassing. Deze beginselen stellen eisen aan de transparantie, motivering en zorgvuldigheid van besluitvorming.

3 Domein- of sectorspecifieke regels

Naast de regels die naar verwachting op alle immersieve ervaringen van toepassing zijn, zijn er per toepassingsgebied mogelijk nog aanvullende of specifiekere regels die gelden. In dit hoofdstuk zetten wij voor de CIIIC domeinen de meest relevante wet- en regelgeving op een rij.

3.1 Gezondheidszorg

3.1.1 Medical device regulation

Wanneer immersieve ervaringen worden ingezet als medisch hulpmiddel (bijvoorbeeld voor diagnose, behandeling of revalidatie), geldt de Europese Medical Device Regulation (MDR). Dit brengt strenge eisen met zich mee op het gebied van veiligheid, prestaties, klinische evaluatie en CE-markering. In Nederland is dit nader uitgewerkt in de Wet medische hulpmiddelen. Afhankelijk van het type toepassing is een conformiteitsbeoordeling door een derde partij nodig.

3.1.2 Wgbo

De Wet geneeskundige behandelingsovereenkomst regelt de relatie tussen patiënt en zorgverlener. Voor immersieve ervaringen in een medische context betekent dit onder meer dat patiënten goed geïnformeerd moeten worden over het gebruik van deze technologieën en expliciet toestemming moeten geven voor gegevensverwerking en behandeling.

3.1.3 AI Verordening

Wanneer AI wordt gebruikt in de immersieve toepassing en deze valt onder de wetgeving voor medische hulpmiddelen, dan kwalificeert het AI-systeem in de meeste gevallen als hoog-risico.[9] Er moet dan aan de vereisten voor hoog-risico AI-systemen worden voldaan (meer specifiek artikel 16 AIV).

3.2 Training & Onderwijs

3.2.1 Privacy en gegevensbescherming

Wanneer AI in het primair onderwijs wordt gebruikt dient rekening te worden gehouden met het feit dat de toepassing door minderjarigen wordt gebruikt. Dit betekent dat er strengere eisen worden gesteld aan de verwerking van persoonsgegevens.

3.2.2 AI Verordening

Wanneer AI wordt gebruikt in de immersieve ervaring, dan kan er sprake zijn van de een hoog-risico AI-systeem.[10] Er moet dan aan de vereisten voor hoog risico AI-systemen worden voldaan (meer specifiek artikel 16 AIV).

3.3 Entertainment

3.3.1 Reclamecode

Immersieve ervaringen die worden ingezet voor reclame moeten voldoen aan de Nederlandse Reclame Code (NRC) en de Europese regels voor eerlijke reclame. Dit betekent onder meer dat reclame duidelijk als zodanig herkenbaar moet zijn, geen misleiding mag bevatten en geen gebruik mag maken van verboden targeting, bijvoorbeeld richting kinderen.

3.3.2 Contentaanbod en classificatie

Bij immersieve ervaringen is het van belang om rekening te houden met de aangeboden content, meer specifiek wanneer deze content gericht is op jongeren. Het aanbieden van aanstootgevende content aan minderjarigen is op grond van artikel 151e Wetboek van Strafrecht strafbaar. Nadere regels voor leeftijdsclassificatie zijn uitgewerkt in de Mediawet. Hoewel aanbieders van immersieve ervaringen niet per definitie onder het bereik van de Mediawet vallen, is het raadzaam om (vrijwillige) systemen voor leeftijdsclassificatie, zoals Kijkwijzer en PEGI, te volgen.

3.3.3 Oneerlijke handelspraktijken

De Wet oneerlijke handelspraktijken (Boek 6, titel 3A BW) verbiedt misleidende en agressieve handelspraktijken, ook online en in XR-omgevingen. Bij oneerlijke handelspraktijken kan onder andere worden gedacht aan verborgen kosten, misleidende informatie of ongepaste beïnvloeding via immersieve ervaringen. Als het gaat om misleiding kan de DSA ook nog relevant zijn. Deze verbiedt het gebruik van deceptive of dark patterns.

3.4 Infrastructuur

Wanneer een immersieve ervaring wordt gebruikt in of voor het uitvoeren of beheren van (primaire) processen in kritieke infrastructuren, dan kunnen specifieke wetten gelden.[11] Deze wetgeving stelt met name strenge eisen aan de informatiebeveiliging. Hoewel het doorgaans niet de IX-aanbieders zijn die onder de verplichtingen van deze wetten zullen vallen, heeft het wel consequenties voor hen, omdat de eigenaren van kritieke, essentiële of

belangrijke infrastructuren eisen zullen stellen aan het gebruik en de beveiliging van deze toepassingen.

3.4.1 Cyberbeveiligingswet (NIS2)

De Cyberbeveiligingswet is specifiek van toepassing in de context van (kritieke) infrastructuren. Wanneer de infrastructuur aangemerkt is als essentieel of belangrijk, dan moet aan de regels van de Cyberbeveiligingswet worden voldaan.

3.4.2 AI Verordening

Wanneer AI wordt gebruikt in de immersieve toepassing, dan kan het zijn dat deze toepassing onder de AI Verordening kwalificeert als hoog-risico AI-systeem. Er moet dan aan de vereisten voor hoog-risico AI-systemen worden voldaan (meer specifiek artikel 16 AIV).

3.5 Werkplek/Kantoor

3.5.1 Goed werkgeverschap & Arbowet

De werkgever heeft een zorgplicht ten opzichte van de medewerkers en moet zorgen voor een goede en veilige werkomgeving. Dit is onder andere vastgelegd in artikel 7:611 BW (goed werkgeverschap) en de Arbowet. Dit betekent onder andere dat onveilige situaties met immersieve ervaringen moeten worden voorkomen.

3.5.2 Wet op de ondernemingsraden

Wanneer immersieve ervaringen invloed hebben op de arbeidsbetrekkingen, dan is het in de meeste gevallen verplicht om de ondernemingsraad te informeren. Afhankelijk van de situatie kan dit ook betekenen dat er instemming van de OR nodig is. Dit geldt ook wanneer persoonsgegevens van medewerkers worden gebruikt.

Wanneer de immersieve ervaring in staat is om het gedrag van medewerkers te monitoren, dan is er sprake van een ‘personeelsvolgsysteem’. Dergelijke systemen moeten niet alleen aan de eisen van de AVG voldoen, er is ook instemming van de ondernemingsraad nodig.[12]

3.5.3 AI Verordening

Wanneer AI wordt gebruikt in de immersieve toepassing, dan kan het zijn dat deze toepassing onder de AI Verordening kwalificeert als hoog-risico AI-systeem. Er moet dan aan de vereisten voor hoog-risico AI-systemen worden voldaan (meer specifiek artikel 16 AIV).

3.6 Kunst en de publieke ruimte (inclusief mobiliteit)

Met betrekking tot de toepassing van immersieve technologieën in de publieke ruimte en in het kader van mobiliteit is het met name relevant dat immersieve technologieën gebruikers kunnen afleiden of anderszins tot gevaarlijke situaties of overlast kunnen leiden.

3.6.1 Weg- en verkeerswet

In relatie tot mobiliteit is artikel 5 Wegenverkeerswet met name relevant. Dit artikel stelt gevaarzettend gedrag op de openbare weg in zijn algemeenheid strafbaar (los van de eventuele consequenties van dit gedrag).

Wanneer iemand die is afgeleid door een immersieve ervaring schade veroorzaakt aan een ander, dan kan er sprake zijn van een onrechtmatige daad (artikel 6:162 BW). Het slachtoffer kan dan de schade verhalen op de degene die de schade heeft veroorzaakt. Wanneer de immersieve ervaring afleidend is en het op voorhand redelijkerwijs voorzienbaar was dat deze toepassing een probleem zou vormen voor de (verkeers)veiligheid, dan is de IX-aanbieder mogelijk ook aansprakelijk.

3.6.2 Algemene plaatselijke verordeningen

Wanneer een immersieve toepassing een gevaar vormt voor de openbare orde en veiligheid of overlast veroorzaakt, dan kan door de gemeente op grond van de Algemene plaatselijke verordening worden opgetreden.

3.6.3 Kunst- en uitingsvrijheid

Bij het gebruik van immersieve toepassingen voor kunst en andere uitingen is het belangrijk om rekening te houden met de grenzen van de uitingsvrijheid en de beperkingen voor reclame. Zo is bijvoorbeeld reclame voor tabak en gokspelen verboden.

Voetnoten

1. Zie artikel 6 AIV jo bijlagen 1 en 3
2. Zie artikel 6 lid 2 jo bijlage 3
3. Wat passend is, is afhankelijk van het risico dat onrechtmatige verwerking van de gegevens kan hebben voor de betrokkene.
4. Digital Operational Resilience Act
5. Zie artikel 2 en 3 CRA jo. bijlage II
6. Zie artikel 6, 7 en 8 CRA jo. bijlage I
7. Zie ook: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0032_EN.html
8. Zie: https://www.w3.org/TR/WCAG21/#background-on-wcag-2
9. Zie artikel 6 lid 1 jo. Bijlage I AIV
10. Zie artikel 6 lid 2 jo. Bijlage III AIV
11. Naast de Cyberbeveiligingswet is ook de Wet weerbaarheid kritieke entiteiten (de Nederlandse implementatie van de CER-richtlijn) van toepassing op kritieke infrastructuren. Omdat deze wetgeving echter primair over fysieke dreigingen gaat, laten we deze hier buiten beschouwing.
12. Zie: https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/ondernemingsraad/de-or-en-personeelsvolgsystemen