Jaaroverzicht IT 2022

Het jaar 2022 laat op Europees en nationaal niveau een veelheid aan wetgevings- en beleidsinitiatieven met betrekking tot IT en data zien. De Europese Commissie heeft de oproep van haar voorzitter uit 2021 om de digitale transformatie vorm te geven, serieus genomen, met name op het terrein van data, artificial intelligence en cybersecurity. Ook op nationaal niveau hebben we in 2022 op die terreinen veel zien gebeuren.

In de IT-rechtspraak is opnieuw aandacht voor de zorgplicht en er lijkt veel te worden geprocedeerd over de afgifte van data. Ook zuiver verbintenisrechtelijke uitspraken die relevant zijn voor de IT-praktijk zijn in dit jaaroverzicht meegenomen.

Europees niveau

Digitale rechten en beginselen

De uitgangspunten van de digitale transformatie van de Europese Commissie zijn neergelegd in het digitaal kompas 2030 en de digitale rechten en beginselen. In het digitaal kompas zijn vier assen benoemd waaraan de doelstellingen van digitale transformatie in 2030 kunnen worden getoetst: a) een digitaal vaardige bevolking en zeer vaardige digitale professionals, b) veilige, goed presterende en duurzame digitale infrastructuren, c) digitale transformatie van bedrijven en d) digitalisering van publieke dienstverlening.

Op 26 januari 2022 heeft de Europese Commissie een verklaring uitgebracht voor de digitale rechten en beginselen. Deze verklaring is gebaseerd op het bestaande Handvest grondrechten in de EU. In de verklaring staat op welke wijze de grondrechten en de Europese waarden in een digitale wereld moeten worden toegepast. De verwachting is dat de lidstaten, de Europese Raad en het Europese Parlement de verklaring in januari 2023 zullen ondertekenen.

Bij digitale rechten moet gedacht worden aan het recht op een passende bescherming in een digitale leefomgeving, het recht op de vrijheid van online meningsuiting, het recht op online bescherming van persoonsgegevens en het digitale recht op vertrouwelijke communicatie. In het kader van de beginselen worden verschillende vormen van online toegang genoemd zoals onder meer universele toegang tot betaalbare digitale verbindingen, online toegang tot publieke diensten, toegang tot de voordelen van het gebruik van AI en vrije keuze in online diensten.

Digital Services Act & Digital Markets Act

Op 23 april 2022 is er een politiek akkoord bereikt tussen de Europese Commissie en de Europese Lidstaten over de Digital Services Act (DSA) en de Digital Markets Act (DMA).

Op 12 oktober 2022 is de Digital Services Act gepubliceerd in het officiële journaal van de Europese Unie en is vervolgens op 1 november 2022 van kracht geworden. Online dienstverleners die vallen onder de reikwijdte van de Digital Services Act hebben vervolgens tot 1 januari 2024 de tijd om aan de verplichtingen uit de Verordening te voldoen. Ook de Digital Markets Act is op 12 oktober 2022 gepubliceerd in het officiële journaal van de Europese Unie en is op 1 november 2022 van kracht geworden. Grote online platformen en zoekmachines die vallen onder de reikwijdte van de Digital Markets Act worden door de Europese Commissie naar verwachting halverwege 2023 aangewezen en hebben vervolgens vier maanden de tijd om aan de verplichtingen uit deze Verordening te voldoen.

De Digital Services Act biedt een kader van gelaagde verantwoordelijkheden voor onlinediensten welk begrip ruim is opgezet zoals tussenpersonen, social media, hosting-diensten en online platforms. Ten dele is de DSA een uitbreiding van de E-commerce Richtlijn (2000/31/EU) die regels geeft voor online zakendoen en de aansprakelijkheid van online tussenpersonen. De DSA bevat daarnaast ruimere regels voor online diensten, waarbij de invloed en macht van de platformen, de rol van de platformen als belangrijke infrastructuren en de afhankelijkheden van deze platformen worden geadresseerd. Zo bevat de DSA regels die betrekking hebben op de bescherming van de rechten van consumenten, de aanpak van illegale content, democratische controle op 'systeem' platformen (ook door de DMA) en het mitigeren van de risico's van manipulatie en desinformatie.

De Digital Markets Act introduceert verplichtingen voor de wereldwijd opererende tien tot vijftien grootste online platforms met een poortwachtersfunctie. De DMA is gericht op het mogelijk maken van open en eerlijke digitale markten en geeft regels over de beslismacht die poortwachters hebben over het toelaten van andere dienstenaanbieders. Zo moet er toegang mogelijk zijn tot de data die gegenereerd worden met het gebruik van het platform van de poortwachter. Bedrijven moeten verder in staat zijn hun aanbod ook buiten het platform van de poortwachter aan te bieden en poortwachters mogen hun eigen diensten niet bevoordelen boven andere aanbieders. Ook mogen poortwachters consumenten niet hinderen om buiten het platform in contact te treden met een aanbieder.

Artificial Intelligence

Op 12 april 2021 heeft de Europese Commissie een voorstel gedaan voor een Artificial Intelligence Act (AI-Verordening), waarmee regels worden gesteld voor het gebruik van Artificial Intelligence (AI) en de ontwikkeling van AI-systemen. Daarnaast heeft de Commissie op 28 september 2022 een pakket met twee voorstellen met betrekking tot aansprakelijkheidsregels voor AI gepresenteerd. In de eerste plaats gaat het om de richtlijn inzake de aanpassing van de wettelijke regels met betrekking tot niet-contractuele aansprakelijkheid aan AI (de Richtlijn AI-aansprakelijkheid). In de tweede plaats gaat het om een voorstel voor een herziening van de Richtlijn productaansprakelijkheid (Herziening productaansprakelijkheidsrichtlijn), die de huidige

regels van productaansprakelijkheid moderniseert voor toepassing in het digitale tijdperk. Deze richtlijnen zijn nauw verbonden en vullen elkaar aan om een effectief civiel aansprakelijkheidssysteem te vormen.

De Europese Commissie geeft in de AI-Verordening een technologieneutrale definitie voor AI-systemen binnen het Europese recht. Verder werkt de AI-Verordening met een classificatie voor AI-systemen met verschillende eisen en verplichtingen, afhankelijk van het risico gekoppeld aan de classificatie. AI-systemen die 'onaanvaardbare risico's' meebrengen kunnen worden verboden. 'Hoge risico' AI-systemen kunnen worden toegelaten binnen de Europese Markt, mits ze voldoen aan eisen en verplichtingen die de AI-Verordening stelt. Er geldt voor 'beperkte risico' AI-systemen een lichter regime voor toegang tot de EU-markt, waarin aan bepaalde transparantieregels moet worden voldaan. De laatste categorie zijn de 'minimaal risico' AI-systemen. Voor aanbieders van deze systemen geldt dat ze kunnen volstaan met het opstellen van gedragscodes.

Elke lidstaat krijgt een eigen AI-toezichtsorgaan. Er komt een Europese AI board dat ook Europese instellingen kan beboeten. Toegelaten 'hoog risico'-toepassingen krijgen voor maximaal 5 jaar een CE keurmerk, dat kan worden verlengd. Alle toegelaten 'hoog risico'-toepassingen worden bewaard in een openbare Europese database.

De Richtlijn AI-aansprakelijkheid (in samenhang met de Herziening productaansprakelijkheidsrichtlijn) beoogt 'slachtoffers' van door (alle soorten) AI-systemen veroorzaakte schade te helpen, zonder daarbij afbreuk te doen aan bestaande aansprakelijkheidsregimes binnen de lidstaten. De Richtlijn stelt een bewijsvermoeden voor: als er een fout wordt vastgesteld die relevant is voor de schade en een oorzakelijk verband met het gebruikte AI-systeem redelijkerwijs waarschijnlijk is, dan is de producent aansprakelijk (die het vermoeden uiteraard kan weerleggen). De Richtlijn geeft 'slachtoffers' verder de mogelijkheid om de rechter te verzoeken om informatie te geven over AI-systemen met een hoog risico. Met deze informatie kunnen slachtoffers vervolgens beter beoordelen wie aansprakelijk kan worden gesteld en wat er fout is gegaan. Indien de producent van het AI-systeem deze informatie niet verstrekt of onvolledig verstrekt dan wordt de gebrekkigheid van het AI-systeem vermoed. Tot slot geeft de Herzieningsrichtlijn nieuwe mogelijkheden om de bewijslast te verlichten in het algemeen en in het bijzonder ook bij complexe producten zoals AI-systemen.

Data Act & Data Governance Act

Twee verordeningen die een belangrijke rol spelen in de datastrategie van de Europese Commissie en belemmeringen voor het gebruik van data moeten wegnemen zijn de Data Act (DA of Data Verordening) en de Data Governance Act (DGA of de Data Governance Verordening). Op 23 februari 2022 heeft de Europese Commissie haar voorstel gedaan voor de Data Act die regels geeft voor de eerlijke toegang tot en het gebruik van data binnen de Europese Unie. Er is nauwe samenhang met de Data Governance Act, waarvoor de Europese Commissie al in november 2020 een voorstel heeft gedaan. In mei 2022 is de DGA door de Europese Raad en het Europese Parlement in haar finale vorm aangenomen, en de eindtekst is op 3 juni 2022 gepubliceerd. Deze Verordening heeft tot doel om data-uitwisseling binnen de EU en tussen sectoren te bevorderen.

De Data Act bevat geharmoniseerde regels om: a) data gegenereerd door het gebruik van een product of service toegankelijk te maken voor de gebruiker van een product of service, b) data beschikbaar te stellen door (private) datahouders aan datagebruikers en c) data van private datahouders beschikbaar te stellen aan overheden in geval van een buitengewone noodzaak in het algemeen belang. Verder stelt de Data Act eisen die belemmeringen moeten weghalen om te veranderen van dataverwerkingsdienst, geeft de Data Act regels die interoperabiliteit moeten bevorderen en regels voor de internationale toegang tot niet-persoonsgegevens. Tot slot verduidelijkt de DA hoe de verhouding is met de rechthebbenden op data zoals gereguleerd in de databankenrichtlijn.

De Data Governance Act heeft tot doel de hoeveelheid data die beschikbaar is voor (her)gebruik van data te vergroten. In de eerste plaats gaat het daarbij om de regulering van het hergebruik van overheidsdata (die buiten de reikwijdte van de Open Data Richtlijn vallen). Het gaat dan om overheidsgegevens waarop vertrouwelijkheid rust, persoonsgegevens en gegevens waarop intellectueel eigendom van derden rust. Lidstaten dienen een of meer bevoegde organisaties aan te wijzen die de overheidsdatahouders ondersteunen, bijvoorbeeld bij het verwerken van aanvragen voor gebruik. Er dient een centraal informatiepunt te zijn waar iedereen de voorwaarden en kosten van gebruik kan vinden voor datasets en waar iedereen aanvragen kan indienen.

Volstrekt nieuwe concepten zijn 'datadeeldiensten' en 'data-altruïsme'. Een datadeeldienst moet ervoor zorgen dat de uitwisseling van gegevens tussen organisaties via intermediairs tot stand komt. Een intermediair of 'datadeeldienst' mag data en bijbehorende metadata alleen gebruiken voor de datadeeldienst, niet voor andere doeleinden, en moet daarom in een aparte rechtspersoon zijn ondergebracht. Datadeeldiensten moeten gelijkelijk toegang tot de data bieden aan iedereen. Een aan te wijzen bevoegde organisatie houdt bij of datadeeldiensten aan hun vereisten voldoen en kan maatregelen nemen als dat niet het geval is. Data-altruïsme is het geven van toestemming voor het gebruik van persoonsgegevens door individuen of van niet-persoonsgebonden gegevens door andere organisaties, voor het gebruik in het algemeen belang, zoals wetenschappelijk onderzoek of het verbeteren van publieke diensten. Een aan te wijzen bevoegde organisatie houdt een openbaar nationaal register bij van erkende gebruikers van via data-altruïsme verkregen gegevens.

Data Spaces
De Europese eenheidsmarkt voor data moet vorm krijgen in zogenaamde 'Data Spaces'. Binnen dergelijke Data Spaces moeten zowel data-gebruikers als data-verstrekkers data kunnen delen, uitwisselen en gebruiken. Het is de bedoeling dat in de Data Spaces de (abstracte) aspecten uit de hierboven genoemde Verordeningen praktisch worden uitgewerkt. De Europese datastrategie uit 2020 noemde 10 sectoren waarbinnen Data Spaces zouden moeten worden gecreëerd waaronder gezondheid, landbouw, energie, mobiliteit en verduurzaming. Op 23 februari 2022 heeft de Europese Commissie een overzicht gepubliceerd met de actuele stand van zaken over de Data Spaces die op de verschillende gebieden worden ontwikkeld.

Het meest ver gevorderd is de Data Space voor gezondheid: de European Health Data Space. Op 3 mei 2022 is er een voorstel gepubliceerd voor een Verordening betreffende de Europese Ruimte voor gezondheidsgegevens. Het doel van deze Verordening is om individuen door middel van digitale middelen meer mogelijkheden te geven tot toegang tot en controle op hun elektronische medische gegevens, zowel op een nationaal als EU-niveau. Hiermee moet het vrije verkeer van medische persoonsgegevens worden bevorderd, net zoals het tot stand komen van een Europese eenheidsmarkt van elektronische medische dossiers, relevante medische hulpmiddelen en hoog risico AI-systemen. De Verordening bevat daartoe specifieke regels die rekening houden met de hoge gevoeligheid van medische persoonsgegevens.

Cybersecurity
Op het terrein van de cyberbeveiliging zijn er in 2022 flinke stappen gezet om de NIS-richtlijn uit 2018 (NIS-1) te vervangen door een nieuwe NIS-richtlijn (NIS-2). Eveneens is in 2022 een regelgevend kader voor de vergroting van de digitale weerbaarheid van de financiële sector een stap dichterbij gekomen met de Digital Operational Resilience Act (DORA). Ook is er in 2022 een voorstel door de Europese Commissie gedaan voor een betere beveiliging van hardware en softwareproducten door middel van de Cyber Resilience Act (CRA).

Op 13 mei 2022 hebben de Europese Commissie en het Europese Parlement overeenstemming bereikt over de tekst van de NIS-2 richtlijn. Op 28 november heeft de Europese Raad de NIS-2 richtlijn aangenomen, en op 14 december 2022 is de richtlijn gepubliceerd in het officiële journaal van de Europese Unie. Dat betekent dat vanaf de twintigste dag na deze publicatie de NIS-2 Richtlijn binnen 21 maanden dient te zijn geïmplementeerd in nationale wetgeving. Nederland heeft tot en met 3 oktober 2024 de tijd om deze richtlijn de implementeren. De belangrijkste verschillen met de NIS-1 richtlijn zijn de uitbreiding van sectoren en partijen ('Essential Entities' en 'Important Entities') waarop de (beveiligings)verplichtingen van toepassing zullen zijn. De beveiligingsmaatregelen worden aangescherpt met een lijst met 7 basisbeveiligingselementen, de regels voor de meldplichten worden verduidelijkt en strenge sancties (vergelijkbaar met de AVG) worden van kracht.

In het jaarverslag van afgelopen jaar schreven wij al over de Digital Operational Resilience Act (DORA). Deze verordening heeft als doel om de digitale veerkrachtigheid van de financiële sector te vergroten en op die manier cyberbedreigingen te beperken. DORA stelt eisen aan de beveiliging van netwerk- en informatiesystemen van financiële ondernemingen. Op 10 november 2022 heeft het Europees Parlement ingestemd met DORA en de Wijzigingsrichtlijn eisen Digital Operational Resilience. Daarna heeft de Raad op 28 november 2022 DORA en de Richtlijn aangenomen. De aanname van de Richtlijn door de Raad is de laatste stap in het wetgevingsproces. Nu DORA formeel is aangenomen, zullen de lidstaten de noodzakelijke aspecten hiervan in nationale wetgeving moeten omzetten. Daarnaast zullen de relevante Europese toezichthouders tegelijkertijd technische normen ontwikkelen waaraan alle financiële dienstverleners zich moeten houden.

De Europese Commissie heeft op 15 september 2022 het voorstel Cyber Resilience Act (CRA) gepresenteerd. De Commissie merkt op dat producten met digitale elementen kwetsbaar zijn voor cyberaanvallen. Deze verordening introduceert een zorgplicht voor fabrikanten met betrekking tot de cyberveiligheid van producten met digitale elementen voor de hele levensduur van de producten. De verplichtingen voor de fabrikanten zijn op te delen in ex ante verplichtingen en ex post verplichtingen. Zo moeten fabrikanten rekening houden met de cyberbeveiliging vanaf de plannings- en ontwikkelingsfase tot het eind van de levenscyclus van het product en moeten zij alle cyberbeveiligingsrisico's documenteren. Voorts moeten fabrikanten melding maken van kwetsbaarheden en incidenten die zich gerealiseerd hebben. Ook moeten fabrikanten verzekeren dat kwetsbaarheden effectief afgehandeld worden tijdens de verwachte levenscyclus van het product of anders minimaal in de eerste vijf jaar van het in het verkeer gebrachte product. Tot slot moeten de fabrikanten zorgen voor duidelijke en begrijpelijke instructies voor het gebruik van de producten en moeten zij voor een minimumperiode van vijf jaar beveiligingsupdates beschikbaar stellen aan de gebruikers.

Nationaal niveau

Verkoop goederen en Levering digitale diensten en digitale inhoud
Vorig jaar hebben wij reeds geschreven over de Implementatiewet Richtlijnen Verkoop goederen en Levering digitale diensten & digitale inhoud. De verwachte inwerkingtreding van de implementatiewet was 1 januari 2022, maar deze wet is pas op 27 april 2022 in werking getreden. Het doel van de richtlijnen is om meer rechtszekerheid te geven aan de consument en om ondernemingen een duidelijk contractueel kader te bieden op het gebied van de verkoop van goederen en de levering van digitale diensten en

digitale inhoud. Een belangrijke vernieuwing ten opzichte van het huidige consumentenkooprecht is dat consumenten zowel voor digitale inhoud (bijvoorbeeld games, applicaties), digitale diensten (bijvoorbeeld streaming), als voor goederen met een digitaal element (bijvoorbeeld een smart TV) recht krijgen op (beveiligings-)updates zolang zij die redelijkerwijs mogen verwachten.

Artificial Intelligence

Ook op nationaal niveau is er aandacht voor AI. In een brief die dateert uit 2021 heeft het kabinet geconstateerd dat het huidige nationale (algemene) wettelijk kader (onder meer mensenrechtenverdragen, de Grondwet, de Algemene wet bestuursrecht (Awb), het Burgerlijk Wetboek (BW), gelijke behandelingswetgeving, en de Algemene verordening gegevensbescherming (AVG)) voldoende waarborgen kan bieden. Wel is een aantal knelpunten en vraagstukken met betrekking tot deze kaders gesignaleerd. Ook is vastgesteld dat deze kaders veelal uit open normen bestaan, waardoor onzekerheid bestaat over de praktische uitleg van deze normen wanneer een organisatie AI inzet.

De brief is aanleiding voor een aantal (voortgezette) acties in 2022. Zo zijn er richtlijnen opgesteld voor het toepassen van algoritmen door de overheid en het uitvoeren van data-analyses door de overheid. Een andere actie is de opzet van zogenaamde algoritmeregisters waarmee de transparantie over de inzet van algoritmen door overheden kan worden vergroot. In dat kader heeft de Rijksdienst voor Identiteitsgegevens de door haar gebruikte algoritmen in een algoritmeregister geplaatst. Eerder hebben de gemeenten Amsterdam, Rotterdam en Utrecht maar ook het UWV al dergelijke algoritmeregisters gepubliceerd.

Staatssecretaris van Huffelen (Koninkrijksrelaties en Digitalisering) heeft in een brief aan de Tweede Kamer aangekondigd dat de algoritmetoezichthouder vanaf januari 2023 bij de Autoriteit Persoonsgegevens van start gaat om algoritmes te controleren op transparantie, discriminatie en willekeur.

Arbit-voorwaarden

Op 10 september 2022 zijn de nieuwe Arbit (Algemene Rijksvoorwaarden bij IT inkoop)-voorwaarden van kracht geworden. Deze Arbit 2022 vervangen de eerdere versie uit 2018. De voorwaarden worden door de Rijksoverheid, zoals ministeries, zelfstandige bestuursorganen en toezichthouders, maar ook andere overheden gebruikt voor de inkoop van IT-diensten en IT-producten. Onderwerpen waarop de Arbit 2022 met name zouden moeten zijn aangepast zijn Agile, Clouddiensten en Artificial Intelligence. Bij nadere bestudering is de uitwerking in de Arbit 2022 van die onderwerpen beperkt. Wel zijn wijzigingen doorgevoerd op de onderwerpen kwaliteitsborging en audits, verwerking van persoonsgegevens, informatiebeveiliging, exit en de nakoming van service levels.

Cybersecurity

Op nationaal niveau is op het gebied van cyberbeveiliging een aantal zaken gepubliceerd. Op 29 juni 2022 heeft minister Adriaansens in een brief de Tweede Kamer geïnformeerd over het evaluatierapport Roadmap Digitaal Veilige Hard- en Software, dat opgesteld is door KWINK Groep. Het doel van deze Roadmap is om maatregelen aan te bieden om te zorgen voor veilige hard- en software. Een aantal aanbevelingen is gedaan in het evaluatierapport betreffende de focus van de Roadmap. Volgens het evaluatierapport moet meer aandacht besteed worden aan ketens en ketenveiligheid, verbinding tussen maatregelen, acties en betrokken partijen, prioritering van maatregelen, participatie van het ministerie van Economische Zaken in Europa en tot slot moet de focus gericht zijn op fabrikanten en leveranciers. Naast de aanpassing van de huidige focus van de Roadmap zijn ook aanbevelingen gedaan over onderwerpen die ontbraken in de focus van de Roadmap: gegevensbescherming, privacywetgeving, valorisatie en transparantie.

Deze aanbevelingen zijn meegenomen door het kabinet in de Nederlandse Cybersecuritystrategie 2022-2028 (NLCS) en het daarbij behorende Actieplan Nederlandse Cybersecuritystrategie 2022-2028 die op 10 oktober 2022 zijn gepubliceerd. Deze strategie bouwt voort op eerder gepubliceerde cybersecuritystrategieën. In deze strategie wordt de visie beschreven van het kabinet op de digitale samenleving en de rol van de overheid, bedrijven en burgers. Er zijn vier pijlers opgesteld die de visie van het kabinet moeten gaan realiseren. De eerste pijler is het verhogen van de digitale weerbaarheid van de overheid, bedrijven en organisaties. Zo wordt van de overheid verwacht dat zij door middel van actuele kennis informatie verschaft over cyberdreigingen, -incidenten, -trends en kwetsbaarheden. De tweede pijler in de strategie is veilige en innovatieve producten en diensten. Zo zullen eisen gesteld worden aan het ontwerp, de ontwikkeling en de vervaardiging van producten met digitale elementen. Ook moeten leveranciers informatie verschaffen over de beveiliging van hun producten en diensten. De derde pijler is het tegengaan van dreigingen van staten en criminelen en tot slot is de vierde pijler het inzetten op de opleiding van cybersecurityspecialisten en het onderwijs om de digitale veiligheid en weerbaarheid van burgers te bevorderen.

De Uitvoeringswet cyberbeveiligingsverordening is op 9 april 2022 in werking getreden samen met een uitvoeringsregeling en een uitvoeringsbesluit. Deze wetgeving voorziet in de operationalisering van de cyberbeveiligingsverordening 2019/881.

Daarnaast is op 2 maart 2022 de Wet tot wijziging van de Telecommunicatiewet in verband met de implementatie van Richtlijn (EU) 2018/1972 (Telecomcode) in werking getreden. Het doel van de Telecomcode is het verbeteren van de randvoorwaarden voor het realiseren van snelle digitale communicatieverbindingen (connectiviteit) in de EU. De belangrijkste wijziging die de wet met zich

meebrengt is een breder toepassingsbereik van de telecomregulering. Onder elektronische communicatiediensten vallen namelijk nu ook nummeronafhankelijke interpersoonlijke communicatiediensten, zoals WhatsApp, Gmail en Teams.

Tot slot heeft het Nationaal Cyber Security Center (NCSC) een Incidentresponsplan Ransomware opgesteld voor ransomware-aanvallen. Het document dient als inspiratiebron voor een eigen responseplan voor organisaties die getroffen zijn of denken te worden getroffen door ransomware-aanvallen. Zo geeft het NCSC tips over hoe gereageerd moet worden op ransomware-incidenten, hoe bedrijven zich kunnen voorbereiden op dergelijke incidenten, hoe zij deze incidenten kunnen herkennen en hoe ze van deze incidenten kunnen herstellen.

Zorg en ICT

Eveneens op 22 november 2022 heeft de ACM de Leidraad 'Goedwerkende markten voor de zorg' gepubliceerd. In deze leidraad constateert de ACM dat er bij Zorg ICT, waarmee zorginstellingen zorgprocessen en relaties met patiënten en andere betrokken partijen in de zorg regelen, een risico bestaat op een Vendor Lock-in. Bij een dergelijke Vendor Lock-in is een afnemer zo afhankelijk van een leverancier dat een overstap naar een andere leverancier niet mogelijk is zonder grote risico's of overstapkosten. Dit kan komen door de structuur van de markt of gedragingen van IT-leveranciers, maar ook door de contractbepalingen die door de IT-leveranciers worden gehanteerd.

Een van de mogelijke wijzen waarop deze risico's voor de afnemer volgens de ACM kunnen worden beperkt is daarom dan ook het maken van goede contractuele afspraken en contractmanagement. Daarbij wordt door de ACM gewezen op afspraken rondom de implementatie, het onderhoud en de geschillenbeslechting. Maar eveneens op afspraken rondom de beëindiging van een overeenkomst, dataportabiliteit, datatoegang en exit-afspraken. De ACM wijst voor de mogelijkheden van de overstap naar andere leveranciers of koppelingen met andere leveranciers ook op het belang van de aansluiting op (internationale) zorgstandaarden voor dataopslag en data-uitwisseling. Ook afspraken over samenwerking ten behoeve van interoperabiliteit en mogelijkheden tot (inkoop)samenwerking tussen afnemers van Zorg ICT worden genoemd als opties om de afhankelijkheid te verminderen.

Voorstel modernisering consumentenbescherming

Op 28 mei 2022 is de Implementatiewet richtlijn modernisering consumentenbescherming in werking getreden. De wet zal zorgen voor een betere handhaving van Europese consumentenregels en zal enkele regels aanpassen en toevoegen om effectief gebruikt te kunnen worden in het licht van nieuwe (digitale) ontwikkelingen. Deze Implementatiewet zal met name de regels verduidelijken en uitbreiden die van toepassing zijn op online handelaren en aanbieders van online marktplaatsen. De wet wordt geïmplementeerd in de volgende nationale wetgeving: Boek 6 van het BW (wijzigingen oneerlijke handelspraktijken en consumentenrechten), de Prijzenwet en de Wet handhaving consumentenbescherming (Whc).

De wet brengt onder meer een verbod op nepreviews met zich mee en een verplichting voor handelaren om de consument te informeren of, en zo ja hoe, zij zelf controleren of reviews ook daadwerkelijk afkomstig zijn van consumenten die het product of dienst hebben gekocht. Ook moeten handelaren consumenten informeren, indien sprake is van een gepersonaliseerd prijsaanbod dat tot stand is gekomen door middel van geautomatiseerde besluitvorming. Voorts moeten handelaren informatie verschaffen over wie de verantwoordelijke is voor de levering en verdere afhandeling van retourzendingen. Ook zijn nieuwe informatieverplichtingen van kracht voor aanbieders van gratis digitale diensten waarbij de consument zijn persoonsgegevens moet verstrekken of zich ertoe verbindt deze te verstrekken voor toegang tot de digitale dienst. Zo moeten deze aanbieders informatie verschaffen over de duur van de overeenkomst en de verschillende wijzen van het beëindigen van de overeenkomst. In het geval van deze gratis digitale diensten hebben consumenten het recht om de overeenkomst te ontbinden gedurende de eerste veertien dagen waarbij de handelaar per direct ook moet stoppen met het verwerken van de persoonsgegevens van de consument.

Jurisprudentie

Europees niveau

Europese Hof van Justitie

Het verzoek van Polen om het 'uploadfilter' uit artikel 17 van de DSM-richtlijn nietig te verklaren werd door het Europese Hof van Justitie (HvJ EU) verworpen, nu de regeling duidelijke en nauwkeurige regels over de reikwijdte en de toepassing van het uploadfilter bevat en is omkleed met passende waarborgen ter bescherming van de vrijheid van meningsuiting.

Bij de beoordeling of op een bestelknop in lijn met artikel 8 lid 2 van richtlijn 2011/83 EU, ondubbelzinnig staat vermeld dat de consument een betalingsverplichting aangaat moet uitsluitend worden gekeken naar de bewoordingen op die knop, en hoeft geen rekening te worden gehouden met de context van het bestelproces.

Nationale wetgeving kan bepalen dat de auteursrechtelijke thuiskopie-exceptie ook geldt voor het door natuurlijke personen maken van reservekopieën van auteursrechtelijk beschermde werken in de cloud voor privédoeleinden. Als voorwaarde geldt wel dat de rechthebbenden een billijke compensatie ontvangen.

Nationaal niveau

Contractenrecht

Een beding uit algemene voorwaarden kan – ondanks dat de algemene voorwaarden niet ter hand zijn gesteld – niet worden vernietigd als de wederpartij op een andere manier bekend was of moest zijn met dat beding, bijvoorbeeld als de algemene voorwaarden bij een eerdere overeenkomst tussen partijen wel al eens correct ter hand zijn gesteld. Daarbij is het – zo oordeelde de Hoge Raad – ook niet nodig dat de bekendheid met het beding is ontstaan door toedoen van de gebruiker van de algemene voorwaarden.

De Hoge Raad bevestigde dat de klachtplicht niet ambtshalve mag worden toegepast. Het hof had ten onrechte toepassing gegeven aan de klachtplicht door de koper op grond van artikel 7:23 BW het recht te ontzeggen om een beroep te doen op de tekortkomingen, terwijl verkoper had nagelaten het verweer te voeren dat niet tijdig was geklaagd.

Volgens het hof Arnhem-Leeuwarden kwalificeerde software niet als zaak in de zin van artikel 3:2 BW omdat geen werk van stoffelijke aard tot stand werd gebracht. De overeenkomst tussen partijen kwalificeerde daarom als een overeenkomst van opdracht en niet als een overeenkomst tot aanneming van werk.

Het hof Arnhem-Leeuwarden oordeelde dat een ongebruikte klachttermijn ten aanzien van verstuurde facturen niet kon worden tegengeworpen aan de afnemer die ontevreden was over het verloop van het implementatietraject als geheel.

Tekortkoming / Uitleg overeenkomst

De Hoge Raad heeft opnieuw bevestigd dat de mededelingsplicht van een verkoper boven de onderzoeksplicht van de koper gaat, óók als in de overeenkomst een mogelijkheid tot inspectie van de goederen is opgenomen waarvan geen gebruik is gemaakt door de koper. Ook oordeelde de Hoge Raad dat een geringe omvang van gebreken en het gegeven dat die zijn hersteld op zichzelf niet in de weg staan aan een geslaagd beroep op non-conformiteit op grond van artikel 7:17 BW.

Nu eiser niet kon hardmaken dat de overeengekomen termijnen fatale termijnen betroffen, mocht gedaagde ervan uitgaan dat deze termijnen golden als streefdata. De door eiser overgelegde planning waarop een go live datum stond vermeld, betekende niet dat daardoor sprake was van een fatale termijn. Er was daardoor ook geen sprake van verzuim.

Afnemer hoefde op grond van de overeenkomst niet te begrijpen dat als zij niet tot aanpassing van de door haar in de overeenkomst genoemde wensen bereid zou zijn, dit zou leiden tot ernstige budget- en tijdsoverschrijdingen. Afnemer mocht verwachten dat de IT-leverancier – in ieder geval grotendeels – de uitdrukkelijk geformuleerde eisen en wensen zou realiseren zoals ingeschat, mede in het licht van het uitgebreide precontractuele onderzoek dat was verricht. Op de gerechtvaardigde verwachtingen van afnemer bij aanvang van de overeenkomst zijn de latere waarschuwingen voor budgetoverschrijdingen niet meer van invloed geweest, omdat die zijn gedaan toen de overeenkomst eenmaal was aangegaan.

De rechtbank Rotterdam oordeelde dat Microsoft onvoldoende had onderbouwd dat het OneDrive-account van eiseres een afbeelding bevatte die ongepast, uitbuitend en schadelijk voor kinderen was. Hierdoor was niet komen vast te staan dat eiseres de Microsoft-serviceovereenkomst had geschonden, zodat Microsoft het OneDrive account ten onrechte had geblokkeerd en de overeenkomst ten onrechte had ontbonden.

Zorgplicht

Een IT-leverancier was niet tekortgeschoten in zijn bijzondere zorgplicht, omdat de problemen die waren ontstaan inherent zijn aan IT-projecten met een nieuw product die in een heel korte tijd moeten worden uitgevoerd, iets waar de afnemer zelf om had verzocht. Duidelijk was dat de IT-leverancier alles in het werk had gesteld om de gewenste snelle go live te realiseren. In dat licht kon de IT-leverancier niets verweten worden over de aanpak van het project.

Hoewel géén contractuele afspraken waren gemaakt over de levering van beveiliging voor de aan te leggen IT-infrastructuur, oordeelde de rechtbank Overijssel dat de IT-leverancier was tekortgeschoten in zijn bijzondere zorgplicht, nu de IT-leverancier een 'totaalpakket' zou leveren. Afnemer mocht ervan uitgaan dat daaronder ook beveiliging was begrepen en als dat niet zo was dan had de IT-leverancier daarvoor moeten waarschuwen.

Een andere IT-leverancier schond zijn bijzondere zorgplicht doordat hij onvoldoende tijdig (bij oplevering) gewaarschuwd had dat als de wensen van de afnemer werden gehonoreerd een complete herontwikkeling van het platform nodig was. Volgens de rechtbank kon de IT-leverancier als deskundige partij redelijkerwijs zien aankomen dat de door afnemer gewenste wijzigingen de architectuur van het platform dermate zou aantasten dat die niet meer zou functioneren.

De rechtbank Rotterdam oordeelde in reconventie dat er geen sprake was van een bijzondere zorgplicht voor IT-leverancier, nu de IT-leverancier de rol had van ontwikkelaar en niet die van adviseur. Van haar mocht enkel verwacht worden dat zij handelde als redelijk handelend en redelijk bekwaam webshopleverancier.

Opzegging overeenkomst

Nu partijen een exit agreement hadden gesloten was géén sprake van een niet opzegbare overeenkomst. Partijen hadden door de exit agreement immers rekening gehouden met de mogelijkheid van beëindiging van de samenwerking.

De IT-leverancier hoefde volgens het hof Amsterdam geen opzegtermijn in acht te nemen omdat dit, door de verstoorde verhouding en de voortdurende weigering van de afnemer om de overeenkomst na te leven, in redelijkheid niet van hem verlangd kon worden.

Onrechtmatige daad
Schade ontstaan in het Catherina ziekenhuis als gevolg van een fout van een onderaannemer door een verkeerde software-instelling was onrechtmatig tegenover het Catherina Ziekenhuis. De rechtbank oordeelde dat de onderaannemer bij de instelling van de software van aannames is uitgegaan die onvoldoende waren gevalideerd. De aanname dat een software-update installeren en vervolgens weer verwijderen resulteert in het onveranderd aanwezig zijn van de software-instelling in de oude versie, was volgens de rechtbank niet vanzelfsprekend. De onderaannemer beriep zich op een aansprakelijkheidsbeperking uit de algemene voorwaarden die de hoofdaannemer was overeengekomen met het Catherina Ziekenhuis. Dit is volgens de rechtbank mogelijk, omdat als de onderaannemer direct met het Catherina Ziekenhuis had gecontracteerd, ook dezelfde voorwaarden van toepassing zouden zijn verklaard.

IE recht
De voorzieningenrechter van het hof Amsterdam oordeelde dat het niet doorleggen van de toepasselijke open source licentievoorwaarden waarop een cryptomunt gebaseerd was bij sublicenties, een schending vormde van de – gemeenschappelijke maar afzonderlijk handhaafbare – auteursrechten op het open source softwareproduct. Op grond van artikel 26 Auteurswet was Jelurida ook gerechtigd om op te treden tegen een auteursrechtinbreuk door mede-auteursrechthebbende Apollo, nu Apollo derden toestond om haar bewerking van de Nxt Software te gebruiken onder andere licentievoorwaarden dan eerder door de gezamenlijke auteursrechthebbenden werd toegestaan.

Nu de bepalingen in de algemene voorwaarden over de bescherming van IE-rechten van Creditsafe tussen partijen waren uitgesloten oordeelde de rechtbank Den Haag dat de redelijkheid en billijkheid in de weg stond aan een beroep op het auteursrecht en het databankenrecht door Creditsafe.

E-commerce
Eind 2021 oordeelde de Hoge Raad dat de informatieplichten van webwinkels ambtshalve moeten worden getoetst. Als niet aan de informatieplicht wordt voldaan, kan de rechter de overeenkomst geheel of gedeeltelijk vernietigen. Als gevolg van deze, en de eerder besproken HvJ EU-uitspraak over informatieplichten bij koop op afstand, was er in 2022 aardig wat rechtspraak waarin werd beoordeeld of inderdaad aan die informatieplicht was voldaan.

Een consument dient er voldoende duidelijk op te worden gewezen wanneer deze een betalingsverplichting aangaat. De rechtbank Noord-Nederland oordeelde dat een bestelknop met de woorden: 'bestelling plaatsen' in combinatie met de overige informatie op die pagina de betalingsverplichting voldoende duidelijk maakt.

De rechtbank Noord-Holland vond een bestelknop met 'Aanvraag versturen' onvoldoende duidelijk en daarom was de overeenkomst vernietigbaar. Ook de teksten 'bevestig je aanvraag' en 'bevestig bestelling' waren onvoldoende duidelijk.

Capayable had onvoldoende geïnformeerd over bijkomende kosten van een aankoop, die daarom ook niet hoefden te worden voldaan. Bovendien moet de consument tijdens het bestelproces op het ontbindingsrecht uit artikel 6:230m lid 1 BW worden gewezen, zonder dat hij daar zelf naar op zoek moet.

Afgifte data
Opdrachtgever vorderde op grond van artikel 7:403 lid 2 BW in reconventie afgifte van alle e-mailadressen en digitale zaken en gegevens die opdrachtnemer – die administratieve werkzaamheden verrichtte voor opdrachtgever – onder zich had uit hoofde van de tussen partijen beëindigde overeenkomst. De vordering werd toegewezen. Ook digitale gegevens die opdrachtnemer zelf heeft samengesteld om de opdracht te kunnen uitvoeren vielen hieronder.

Op grond van artikel 7:401 BW (zorgvuldigheidsplicht opdrachtnemer) diende de developer die een game ontwikkelde online toegang tot die game te verstrekken op het moment dat opdrachtgever de ontwikkeling daarvan weer wilde oppakken.

In het kader van een beëindigde samenwerking vorderde de geïntimeerde afgifte van de gegevens van de door hem eerder ingebrachte klanten. Duidelijk was dat nog over de beëindigde samenwerking moest worden afgerekend. Niet viel uit te sluiten dat de betreffende klanten tot de conclusie waren gekomen dat zij klant waren geworden van appellant en niet meer van geïntimeerde en dat zij daarmee (stilzwijgend) hadden ingestemd. Hierdoor was de verwerkingsverantwoordelijkheid onder de Algemene Verordening Gegevensbescherming (AVG) mogelijk overgegaan op appellant. Als gevolg daarvan konden de klantgegevens niet zonder meer weer (exclusief) aan de geïntimeerde ter beschikking worden gesteld.

Microsoft moest aan de curatoren van de failliete Amsterdam Trade Bank ongehinderde toegang verschaffen tot de administratie van die bank die is opgeslagen 'in the cloud' van Microsoft. De curatoren hadden een wettelijke taak op grond van de Faillissementswet en dienden op grond daarvan te kunnen beschikken over de volledige administratie van de gefailleerde. Het werd Microsoft verboden om de online omgeving van de gefailleerde te vernietigen of ontoegankelijk te maken.

Platformaansprakelijkheid
Het hof Arnhem-Leeuwarden heeft geoordeeld dat een website waarop recensies kunnen worden achtergelaten, niet aansprakelijk is voor het plaatsen van een recensie. De website was slechts aansprakelijk voor het enige tijd geplaatst houden van de recensie, nadat de website op de hoogte was gesteld van de (vermeende) onrechtmatigheid ervan.

Via zowel Twitter als Google werden nepadvertenties verspreid waarin bekende Nederlanders de investering in cryptovaluta aanprezen. Google was niet aansprakelijk, omdat de adverteerder dat primair is voor de inhoud van een advertentie. Voor aansprakelijkheid van Google waren volgens de rechtbank Amsterdam bijkomende omstandigheden vereist, bestaande uit eigen verwijtbaar handelen of nalaten van Google. Aan de uitsluiting van aansprakelijkheid van artikel 6:196c BW werd daarom volgens de rechtbank niet toegekomen. Op grond van de Lycos/Pessers-toets diende Google wel identificerende gegevens te verstrekken van de betreffende adverteerder. Ook Twitter was niet aansprakelijk, maar hoefde geen identificerende gegevens te verstrekken omdat deze vordering onvoldoende werd onderbouwd.

De voorzieningenrechter van de rechtbank Noord-Holland oordeelde dat LinkedIn verplicht was om een gebruikersprofiel te reactiveren, nu de opzegging van de gebruikersovereenkomst onzorgvuldig had plaatsgevonden. De indirecte werking van art. 10 EVRM behelsde een zorgvuldigheidsverplichting. Er was geen helder beleid, er was niet of nauwelijks gecommuniceerd en voor zover van communicatie al sprake was bevatte die geen motivering die meer inhield dan een enkele verwijzing naar de gebruikersovereenkomst.

De vordering om alle berichten die verband houden met een vermeend pedo-satanisch netwerk in Bodegraven actief op te sporen en te verwijderen werd door de voorzieningenrechter Den Haag afgewezen. De voorzieningenrechter overwoog daarbij – onder verwijzing naar de uitspraak HvJ EU Glawischnis/Facebook – dat een bevel tot verwijdering van soortelijke informatie alleen kan worden toegewezen als die soortgelijke informatie specifieke gegevens bevat die naar behoren zijn aangewezen door degene die het rechterlijk bevel heeft uitgevaardigd zoals namen en omstandigheden en die door middel van geautomatiseerde technieken kunnen worden gevonden. Een autonome beoordeling van het zoekresultaat kon niet van Twitter worden gevergd.

De rechtbank Amsterdam heeft een massaclaim toegewezen tegen de exploitant van een erotische website voor het online plaatsen zonder toestemming van bepaald beeldmateriaal. De exploitant van de website kon zich niet beroepen op de uitzondering voor aansprakelijkheid van hostingdiensten omdat hij niet slechts een neutrale en passieve rol speelde ten aanzien van de inhoud van de website. De exploitant screende het beeldmateriaal dat werd geüpload namelijk preventief en keurt een substantieel gedeelte van het beeldmateriaal af. Daarmee heeft de website exploitant kennis van het materiaal dat op de website wordt geplaatst.

Overig

Het schadebrengende feit had zich voorgedaan in Nederland, Amsterdam omdat de onrechtmatige openbaarmaking van foto's zich voordeed via een website die in Nederland raadpleegbaar is (en dus ook in Amsterdam) en de homepage verwijst naar de Amsterdamse vestiging waar producten kunnen worden opgehaald. De rechtbank Amsterdam achtte zich daarom relatief bevoegd op grond van artikel 102 Rv.

Meer weten?

Neem dan contact op met een van onze specialisten:


Tom de Wit


Moo Miero


Esmée Fonville


Huub de Jong


Corine d'Hulst


Marijn Rooke