Jaaroverzicht IT 2023

In het jaaroverzicht van 2022 hebben we vanuit de Europese Unie op het gebied van data en digitalisering veel wetgevingsinitiatieven gezien. In 2023 zijn veel van deze initiatieven omgezet in definitieve richtlijnen of verordeningen die de komende jaren in werking zullen treden. In dit jaaroverzicht IT 2023 geven wij in vogelvlucht een beeld van de belangrijkste (Europese en nationale) ontwikkelingen op wetgevingsgebied.

Europees en nationaal niveau

Digital Service Act & Digital Markets Act

Op 16 november 2022 is de Digital Service Act (DSA) in werking getreden met als doel te zorgen voor een veilige, voorspelbare en betrouwbare online omgeving, het waarborgen van grondrechten van gebruikers en een gelijk speelveld voor de aanbieders van online tussenhandelsdiensten.

De DSA harmoniseert de regels die van toepassing zijn op aanbieders van online tussenhandelsdiensten en breidt daarbij ook de geldende regels voor online zakendoen zoals die gelden onder de e-commerce richtlijn uit. Denk daarbij aan:

- beleid inzake content moderatie en 'notice en takedown' procedures
- jaarlijkse rapportage over content moderatie
- duidelijke en gebruiksvriendelijke algemene voorwaarden die uitleg bevatten over het beleid rondom content moderatie
- 'know your business customer' verplichtingen voor online marktplaatsen
- het aansprakelijkheidsregime uit de e-commercerichtlijn wordt voortgezet met de toevoeging dat het te goeder trouw actief opsporen van illegale content een beroep op de aansprakelijkheidsvrijstelling niet meer in de weg staat.

Daarnaast bevat de DSA specifieke regels die gelden voor hosting service providers, online platforms, online marktplaatsen alsmede grote online platforms (VLOPs) en online zoekmachines (VLOSEs). Voor de laatste categorie heeft de Europese Commissie inmiddels de grootste platforms en online zoekmachines aangewezen.

Voor de online platforms en zeker de aangewezen grote online platforms gaan uitgebreide zorgvuldigheidsverplichtingen gelden, waaronder:

- invoering van een klachtsysteem voor gebruikers tegen verwijdering of beëindiging van informatie of diensten
- maatregelen tegen partijen die illegale content verspreiden
- safety-by-design-maatregelen (waaronder de bescherming van minderjarigen).

Voor VLOPs en VLOSEs gelden in aanvulling uitgebreidere verplichtingen:

- inspraak van gebruikers, waaronder melding illegale inhoud, informatie over profilering, informatie over partijen die achter advertenties zitten en de begrijpelijkheid van algemene voorwaarden
- sterkere bescherming van de rechten van minderjarigen
- zorgvuldig modereren van de inhoud van aangeboden informatie en het voorkomen van de verspreiding van desinformatie
- meer transparantie en verantwoordelijkheid, waaronder de uitvoering van risicobeoordelingen, toegang van onderzoekers tot openbare gegevens en een register van alle advertenties en bijbehorende partijen.

De DSA treedt met stappen in werking. Voor de VLOPs en VLOSEs geldt dat zij reeds op 25 augustus 2023 aan de genoemde verplichtingen moeten voldoen. Overige online dienstverleners hebben tot 17 februari 2024 om aan de verplichtingen uit de DSA te voldoen. Er is een wetsvoorstel Uitvoeringswet Digitale Dienstenverordening aanhangig gemaakt, maar die is op het moment van schrijven van dit overzicht nog niet aangenomen. In de uitvoeringswet wordt de ACM (en gedeeltelijk de AP) als toezichthouder aangewezen. De ACM heeft inmiddels een concept leidraad voor aanbieders van online diensten gepubliceerd. Hierop kan tot 16 februari worden gereageerd.

Eveneens op 16 november 2022 is de Digital Markets Act (DMA) in werking getreden. De DMA beoogt de macht van als poortwachter aangewezen platformen in te perken en een eerlijker digitaal speelveld te creëren. Een poortwachter is een platform dat aanzienlijke impact heeft op de interne markt, controle heeft over een belangrijke toegangspoort voor zakelijke gebruikers naar eindgebruikers en een bestendige en duurzame positie heeft. De Europese Commissie heeft inmiddels grote online platformen en zoekmachines die vallen onder de reikwijdte van de DMA aangewezen (let op: deze zijn niet identiek aan de onder de DSA vallende online platformen en zoekmachines). Deze aangewezen online platformen en zoekmachines hebben tot maart 2024 de tijd om aan de verplichtingen op grond van de DMA te voldoen.

In april 2023 is er een wetsvoorstel 'Uitvoeringswet digitalemarktenverordening' van de Minister van Economische Zaken verschenen waarin onder andere het toezicht op de DMA is opgenomen. De Raad van State heeft inmiddels advies gegeven over het wetsvoorstel. Als het wetsvoorstel wordt aangenomen, wordt de ACM straks het meldpunt voor mogelijke overtredingen van de DMA en kan de ACM onderzoek doen, alleen of samen met de Europese Commissie. De Europese Commissie neemt uiteindelijk de besluiten, maar doet dat in nauwe samenwerking met de nationale toezichthouders van de EU-lidstaten.

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 9 november 2023 heeft het Europese parlement de Data Act aangenomen. Na publicatie in het publicatieblad van de Europese Unie zal de Data Act 20 dagen later in werking treden. Na de datum van inwerkingtreding volgt er een periode van 20 maanden waarin organisaties zich kunnen voorbereiden op de verplichtingen uit de verordening. Afhankelijk van de publicatie zal de Data Act dus waarschijnlijk eind 2025 daadwerkelijk van toepassing zijn.

De Data Act bevat onder andere 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 opheffen om over te stappen van dataverwerkingsdienst, geeft de Data Act regels die interoperabiliteit moeten bevorderen en regels voor de internationale toegang tot niet-persoonsgegevens.

In het jaaroverzicht 2022 gaven we al aan dat de DGA in mei 2022 door het Europese Parlement en de Europese Raad was aangenomen en de eindtekst op 3 juni 2022 gepubliceerd is in het publicatieblad van de EU. Op 24 september 2023 is de DGA formeel van kracht geworden.

De Data Governance Act heeft tot doel de hoeveelheid data die beschikbaar is voor (her)gebruik 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.

In oktober 2023 heeft de Minister van economische Zaken een wetsvoorstel 'Uitvoeringswet datagovernanceverordening' ingediend. De Raad van State heeft advies gegeven over het wetsvoorstel. Deze uitvoeringswet wijst de Autoriteit Consument en Markt (ACM) aan als toezichthouder en bevoegde autoriteit voor databemiddelingsdiensten en data-altruïsme. In oktober 2023 heeft de ACM dan ook een oproep aan partijen gedaan om zich te registeren. De Autoriteit Persoonsgegevens (AP) adviseert over de voorwaarden uit de verordening die verband houden met de bescherming van persoonsgegevens.

Data Spaces

Binnen zogenaamde 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 Data Act en met name de Data Governance Act praktisch worden uitgewerkt. In het jaaroverzicht 2022 gaven we aan dat de Europese Commissie een overzicht had gepubliceerd met de actuele stand van zaken over de Data Spaces die op de verschillende gebieden worden ontwikkeld.

In het jaaroverzicht 2022 hebben we vermeld dat de meest ver gevorderde data space, de Data Space voor gezondheid is: de European Health Data Space. Op 3 mei 2022 is er een voorstel gepubliceerd voor een Verordening betreffende de Europese Ruimte voor gezondheidsgegevens. Dit voorstel van de Europese Commissie ligt nog steeds ter bespreking bij de Europese Raad en het Europese Parlement.

Inmiddels zijn er in 2023 wel ontwikkelingen op de terreinen van andere Data Spaces. Zo is inmiddels een

Data Space op het terrein van data op het gebied Europees cultureel erfgoed en een Data Space voor data gegenereerd bij aanbestedingen. Ook op het terrein van data die samenhangen met onderzoek en innovatie is er een Data Space in de vorm van de 'European Open Science Cloud'.

Artificial Intelligence

Op het terrein van Artificial Intelligence ('AI') is er aan het einde van 2023 een voorlopig politiek akkoord bereikt over de AI Verordening waarvoor de Europese Commissie al in april 2021 een voorstel had gedaan. Onder andere de discussie over de regulering van 'general purpose' AI-systemen (die voor brede toepassingen kunnen worden ingezet) heeft veel tijd gevergd.

Evenals in het voorstel gebruikt de AI-Verordening een technologie-neutrale 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 die 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.

Nieuw ten opzichte van het voorstel is de expliciete regulering van 'general purpose' AI. Voor zeer krachtige 'general purpose' AI-modellen die systeem risico's met zich kunnen meebrengen, gelden verplichtingen die toezien op het beheersen van deze risico's, het monitoren van incidenten, het uitvoeren van evaluaties op de AI-modellen en het testen van de AI-modellen.

Verder zal er een nieuwe Europese AI autoriteit komen waarvan het doel is de coördinatie en afstemming tussen nationale AI autoriteiten op landelijk niveau. Daarnaast houdt deze Europese AI autoriteit toezicht op de implementatie en de handhaving van de nieuwe regels die gelden voor de 'general purpose' AI modellen.

Het wachten is nog op de formele goedkeuring van het bereikte politieke akkoord door het Europese Parlement en de Europese Raad en de publicatie van de AI-verordening in het Publicatieblad van de Europese Unie. Twintig (20) dagen na deze publicatie treedt de AI-verordening dan in werking. Twee (2) jaar na de inwerkintreding wordt de AI-verordening van toepassing, met uitzondering van verbodsregels (zoals het verbod van AI-systemen met onaanvaardbare risico's die al na 6 maanden van toepassing worden en de regels die gelden voor 'general purpose' AI die na 12 maanden van toepassing worden.

Op 30 oktober 2023 bereikten de leiders van de G7 een overeenstemming over een reeks internationale principes voor kunstmatige intelligentie en een vrijwillige gedragscode voor AI-ontwikkelaars. De betreffende principes en gedragscode zullen een aanvulling vormen op de juridisch bindende regels die momenteel worden afgerond binnen AI-verordening en benadrukken risicobeheer, transparantie, verantwoordingsplicht en beveiliging gedurende de levenscyclus van AI-systemen. De Gedragscode biedt praktische richtlijnen voor het ontwikkelen van AI.

Op nationaal niveau heeft de Autoriteit Persoonsgegevens in juli 2023 haar Rapportage Algoritmerisico's gepubliceerd. Dit biedt een overzicht van ontwikkelingen, risico's en uitdagingen rond het gebruik van algoritmes. Het streven is om elk halfjaar een rapportage uit te brengen, om de actuele ontwikkelingen en risico's te belichten. De kernboodschap van de rapportage is dat er een ecosysteem van risicobeheersing en verantwoording moet worden opgezet bij de toepassing van algoritmes.

Cybersecurity

In het jaaroverzicht 2022 hebben wij melding gemaakt van de inwerkingtreding van de NIS-2 richtlijn. Nederland heeft tot en met 3 oktober 2024 de tijd om deze richtlijn de implementeren in nationale wetgeving. Het belangrijkste verschil met de NIS-1 richtlijn is 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, nadruk komt meer te liggen op de beheersing van beveiligingsrisico's van leveranciers en strengere sancties (vergelijkbaar met de AVG) worden van kracht.

Implementatie van de NIS-2 richtlijn zal gebeuren via aanpassing van de Wet beveiliging Netwerk en Informatiesystemen (Wbni) waarin nu de implementatie van de NIS-1 richtlijn is opgenomen. Alhoewel de consultatie van de (aangepaste) Wbni was voorzien voor 2023, is er nog geen wetsvoorstel gepubliceerd. Het wetsvoorstel en een bijbehorende consultatie zijn nu gepland in het eerste kwartaal van 2024.

Een tweede grote wetgevingsoperatie op het gebied van cybersecurity en digitale weerbaarheid is 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. In een blogserie hebben zijn wij ingegaan op het raamwerk van DORA en de gevolgen van DORA voor IT-leveranciers.

DORA is in november 2022 formeel aangenomen en zal in januari 2025 van kracht worden. Op de lidstaten rust nu de verplichting om de noodzakelijke aspecten hiervan in nationale wetgeving om te zetten. Nederland heeft dat inmiddels gedaan door middel van het Wetsvoorstel 'Implementatiewet digitale operationele weerbaarheid' dat ter goedkeuring bij de Tweede Kamer ligt. Daarnaast zullen de relevante Europese toezichthouders als onderdeel van DORA in de loop van 2024 technische normen ontwikkelen waaraan alle financiële dienstverleners zich moeten houden.

In september 2022 werd het voorstel voor een Cyber Resilience Act (CRA) door de Europese Commissie gepresenteerd. In dit oorspronkelijke voorstel werd geconstateerd dat producten met digitale elementen kwetsbaar zijn voor cyberaanvallen. Dit voorstel voor een 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.

Vanuit het Europese Parlement zijn er in juli 2023 aanvullingen voorgesteld op de CRA die met name zien op duidelijkere definities en een eerlijkere verdeling van verantwoordelijkheden tussen consumenten, toezichthouders en producenten.

Op 1 december is er, mede door opname van de genoemde aanvullingen, een politiek akkoord over de CRA bereikt tussen het Europese Parlement en de Europese Raad. Na publicatie in het publicatieblad van de EU treedt deze verordening 20 dagen daarna in werking. Vervolgens hebben producenten, importeurs en distributeurs van hardware en software 36 maanden de tijd om producten en diensten aan de eisen van de CRA aan te passen, dus ergens in de loop van 2026.

Een belangrijke ontwikkeling op het gebied van de digitale identiteit en authenticatie is de eID-wallet. In het kader van het toenemende belang van het gebruik van digitale omgevingen in het dagelijkse leven heeft de Europese Commissie in 2021 een voorstel gedaan voor een eID Verordening. Het is een combinatie van digitale authenticatiemiddelen waarmee zowel toegang kan worden gekregen tot particuliere diensten als overheidsdiensten. De eID-wallet is daarmee vergelijkbaar met de DigID die in Nederland wordt gebruikt. Het voorstel voor de verordening dient ter vervanging van de eIDAS verordening, uit 2014 die ook betrekking had op digitale identiteit en authenticatie.

In juni 2023 hebben de Europese Raad en het Europese Parlement een politiek akkoord bereikt over de eID verordening. Het voorlopige akkoord omvat veel aspecten die samenhangen met de Europese digitale identiteit, waaronder de verduidelijking dat de afgifte en het gebruik voor authenticatie en de intrekking van de eID Wallet kosteloos moeten zijn voor particulieren. Via de eID Wallet kunnen particulieren ook gratis elektronische handtekeningen gebruiken. Daarnaast breidt de verordening de lijst van vertrouwensdiensten uit met nieuwe gekwalificeerde diensten. De herziene verordening moet verder gebruikmaken van, steunen op en verplichten tot het gebruik van bestaande certificeringsregelingen uit de eerder genoemde CRA om te certificeren, zodanig dat de eID Wallet voldoet aan de cyberbeveiligingsvoorschriften.

Aangezien de eID verordening nog moet worden aangevuld met technische normen en standaarden

alvorens formele goedkeuring en publicatie in het publicatieblad kan plaatsvinden, is nog onduidelijk wanneer de eID verordening in werking zal treden.

Jurisprudentie

In de jurisprudentie zijn in 2023 een aantal interessante arresten gewezen door de Hoge Raad op (o.a.) het gebied van het contractenrecht. In lagere rechtspraak wordt als altijd veel geprocedeerd over de uitleg van overeenkomsten. Er zijn redelijk wat uitspraken rondom 'fatale termijnen'. Een rode draad hebben wij daar nog niet in ontdekt. Een beroep op de zorgplicht van de IT-leverancier werd niet vaak gehonoreerd in 2023. In dit jaaroverzicht treft u een bloemlezing van de wat ons betreft belangrijkste uitspraken.

Europees niveau

Europese Hof van Justitie

Volgens de Europese Commissie schond Valve, exploitant van het gameplatform Steam, het mededingingsrecht door bepaalde videogamers op basis van hun locatie te blokkeren (geoblocking). Hierdoor werd de verkoop van videogames in specifieke regio's voor een bepaalde periode beperkt. Valve vorderde nietigverklaring van het besluit, maar het Gerecht oordeelde dat de Europese Commissie voldoende had aangetoond dat de onderling afgestemde feitelijke gedragingen van Valve en andere game-ontwikkelaars de parallel-invoer door middel van geoblocking beperkte. Het Gerecht oordeelde dat geoblocking niet werd gebruikt ter bescherming van auteursrechten, maar om hogere prijzen te verkrijgen. Auteursrechten zijn bedoeld om beschermd materiaal beschikbaar te stellen tegen vergoeding, niet om ontwikkelaars de hoogst mogelijke vergoeding te garanderen.

A-G Szpunar concludeerde in de zaak LA Quadrature du Net e.a. waarin de vraag centraal staat of IP-adressen en daarmee overeenkomende identificatiegegevens van internetgebruikers mogen worden verzameld om te voorkomen dat inbreuk wordt gemaakt op intellectuele eigendomsrechten online, zonder voorafgaande controle van een rechterlijke instantie. Volgens Szpunar is de Franse nationale regeling tot het verzamelen van deze identificerende gegevens door een onafhankelijke autoriteit niet in strijd met het Unierecht omdat met deze werkwijze alleen gegevens verzameld kunnen worden ten aanzien van de inbreuk en niet om andere conclusies te trekken over het privéleven van deze persoon. Toegang tot deze gegevens hoeft ook niet vooraf door een rechter te worden getoetst omdat dit het enige middel is om de inbreukmaker te identificeren, aldus de A-G.

Volgens de Oostenrijkse toezichthouder zou met ingang van de DSA ook nationale Oostenrijkse wetgeving van toepassing zijn op platforms. Tiktok, Meta Platforms Inc en Google hebben het Hof van Justitie van de Europese Unie in reactie hierop prejudiciële vragen gesteld. Zij stellen dat het standpunt van de Oostenrijkse toezichthouder in strijd is met het 'country of origin'-prinicpe uit de Richtlijn elektronische handel, volgens welke een platform in beginsel enkel aan het recht van het vestigingsland wordt onderworpen. A-G Szpunar concludeert dat een lidstaat slechts mag afwijken van de vrijheid van vestiging als dit op een 'case-by-case' basis gebeurt na overleg met de 'country of origin' en goedkeuring van de Europese Commissie.

Nationaal niveau

Contractenrecht

De Hoge Raad oordeelde dat partijen een van de Haviltex-afwijkende contractuele uitlegmaatstaf overeen kunnen komen. Voor de uitleg van het uitlegbeding zelf lijkt wel nog steeds de Haviltex-maatstaf te gelden.

De Hoge Raad heeft geoordeeld dat een maker van een bewerking van een auteursrechtelijk beschermd werk (waaronder ook software), geen rechten kan ontlenen aan auteursrechtelijke elementen in het eerste en oorspronkelijke werk. Het auteursrecht van de maker van de bewerking is dus beperkt tot de (nieuwe) auteursrechtelijke elementen in de bewerking. In dat geval is de bewerking een zelfstandig werk waarop de bewerker auteursrechten heeft, als een verveelvoudiging van het oorspronkelijke werk.

De Hoge Raad oordeelde dat partijen die in een huurovereenkomst hadden opgenomen dat de huurder het recht had om de overeenkomst per direct te ontbinden, van het wettelijke regime, 6:265 BW waren afgeweken. Of de ontbinding regelmatig is, dient aan de hand van het contractuele regime te worden beoordeeld. Dit heeft mede tot gevolg dat niet nog de toets kan worden aangelegd of de tekortkoming de ontbinding rechtvaardigt.

Een groothandel kwalificeert als een dienst in de zin van de Dienstenrichtlijn, zo oordeelt de Hoge Raad. De toepasselijkheid van de Dienstenrichtlijn is daarbij niet afhankelijk van de specifieke activiteiten die worden verricht. Of de dienst de algemene voorwaarden gemakkelijk elektronisch toegankelijk heeft gemaakt als bedoeld in artikel 6:230c onder 3 BW hangt af van de omstandigheden van het geval. "*Indien de algemene voorwaarden zonder noemenswaardige inspanning gevonden kunnen worden op of via de website waarnaar*

op de facturen is verwezen, moet worden aangenomen dat de algemene voorwaarden gemakkelijk elektronisch toegankelijk zijn."

De Hoge Raad oordeelt dat de overeenkomst tot levering van lijngoten – ondanks een overeengekomen afnameverplichting – mocht worden vernietigd op grond van dwaling omdat de wederpartij, anders dan zij had medegedeeld niet in staat bleek om *tijdig* te leveren. Dwaling ziet niet alleen op een voorstelling van zaken die een partij heeft ten aanzien van de te leveren zak zelf, maar kan ook worden gebaseerd op de voorstelling van zaken ten aanzien van andere rechten en verplichtingen die uit de overeenkomst voortvloeien, zoals tijdige levering. Daarnaast mocht het hof niet – zonder dat daartegen gegriefd werd – oordelen dat het Weens Koopverdrag wél van toepassing was, in tegenstelling tot het oordeel van de rechtbank.

Uitleg overeenkomst

Partijen zijn in geschil over de verschuldigdheid van licentievergoedingen. Appelante stelt dat de licentievergoedingen van het softwarepakket 'voor eeuwig' zijn afgekocht. Het hof stelt vast dat de oorspronkelijke overeenkomst stilzwijgend is verlengd. In de overeenkomst wordt nergens gesproken van een licentievergoeding. Daarnaast acht het hof van betekenis dat geïntimeerde geen enkel document heeft overgelegd waaruit blijkt dat zij op haar beurt licentievergoedingen heeft afgedragen aan Microsoft. Niets wijst erop dat partijen bij het verlengen van de overeenkomst de wil of bedoeling hadden om alsnog een licentievergoeding overeen te komen. Wel zijn partijen kennelijk stilzwijgend andere tarieven overeengekomen.

Webstores heeft in opdracht van Heigo een online platform ontwikkeld. Volgens Heigo heeft Webstores daarbij gebruik gemaakt van verouderde software en geen updates uitgevoerd waardoor een totale herbouw nodig is van het platform. Webstores stelt dat zij 'slechts' ontwikkelcapaciteit ter beschikking zou stellen en geen afspraken zijn gemaakt over de toe te passen software bij de ontwikkeling van het platform. De rechtbank oordeelt dat door Heigo onvoldoende is onderbouwd dat Webstores zich heeft verbonden tot het leveren van een product met een bepaalde levensduur tegen een bepaald bedrag, maar dat de overeenkomst inderdaad slechts ziet op het beschikbaar stellen van capaciteit. Er waren namelijk alleen afspraken gemaakt over het aantal af te nemen sprints en de tarieven. Ten aanzien van de door Webstores gebruikte software stelt de rechtbank vast dat die bij aanvang van de werkzaamheden gangbaar waren en dat Webstores Heigo op tijd heeft gewezen op de 'End Of Life' van deze software.

OfficeGrip Holding was op grond van de contractuele afspraken niet gehouden om een back-up te maken van i-schrijfdata bij de oude IT-leverancier van Pit, maar was enkel gehouden tot het maken en beheren van een nieuwe IT-omgeving. In de contractuele documentatie wordt de term migratie niet enkel gebruikt voor datamigratie, maar ook voor migratie van de structuur van de IT-omgeving van Pit. Hieruit hoefde OfficeGrip volgens de rechtbank dus niet af te leiden dat migratie van de data toch gewenst was. Bovendien heeft Pit niet aan OfficeGrip gemeld dat de aanname dat Pit de i-schijf ook had opgeslagen in de Sharepoint back-up onjuist was. Daarom was er geen aanleiding voor OfficeGrip om de i-schijfdata alsnog veilig te stellen.

Volgens Ziekenhuis het Groene Hart maakt Medned – leverancier van medische software – misbruik van haar machtspositie. Medned zou na het wisselen van IT-leverancier door het Groene Hart hoge naheffingspercentages van 20% in rekening te brengen voor het raadplegen van oude patiëntgegevens. Medned vordert betaling van de facturen en het Groene Hart vordert in reconventie matiging van de facturen omdat deze in de branche ongebruikelijk zouden zijn en MedNed de implementatie van dit zogenaamde 'raadpleegpakket' zou vertragen. De rechtbank oordeelt dat partijen afspraken hebben gemaakt over de heffingen. Hoewel deze afspraken in het nadeel zijn van Groene Hart is er geen reden om een andere uitleg van de overeenkomst aan te nemen. Bovendien is de vertraging van de implementatie aan het Groene Hart zelf te wijten, doordat zij niet aan de contractuele voorwaarden voor de overstap naar het raadpleegpakket voldeed.

Bij de gemeente Hof van Twente heeft een cyberaanval plaatsgevonden waarbij de systemen van het netwerk van de gemeente en de back-up zijn versleuteld en ontoegankelijk zijn gemaakt en vele virtuele servers zijn verwijderd. De gemeente stelt haar IT-leverancier aansprakelijk. Volgens de gemeente was de IT-leverancier contractueel verplicht tot onder meer het monitoren van het functioneren van de servers, opslag en netwerk-voorzieningen. De rechtbank legt de contractuele afspraken uit aan de hand van de meer objectieve uitlegmaatstaf, de CAO-norm, omdat de contractuele documentatie is opgesteld in het kader van een Europese Aanbestedingsprocedure. De rechtbank stelt vast dat slechts 'functionele' monitoring is overeengekomen, en geen security monitoring. Hieruit volgt dat de IT-leverancier signalen die invloed hadden op de beschikbaarheid moest oppikken maar niet specifiek op beveiligingsrisico's hoefde te monitoren. De bijzondere zorgplicht die op de IT-leveranciers rust, strekt ook niet zo ver dat hierdoor, daar waar functionele

monitoring wordt overeengekomen, ook security monitoring onder valt, nog daargelaten of er plaats is voor de zorgplicht in het licht van het transparantiebeginsel uit het Europese Aanbestedingsrecht. Het hof van Twente heeft beroep ingesteld tegen de uitspraak van de rechtbank.

Blauw eist informatie over een cyberaanval op de servers van Nebu, waarbij data is ontvreemd. Mogelijk betreft dit data van Blauw. De rechtbank oordeelt dat uit de verwerkersovereenkomst tussen partijen volgt dat Nebu verplicht is om Blauw direct op de hoogte te stellen van incidenten met betrekking tot de verwerking van persoonsgegevens. De vraag is hoever het contractuele instructierecht van Blauw in dit kader reikt. De voorzieningenrechter oordeelt dat dit instructierecht ruim dient te worden uitgelegd omdat dit – blijkens de tekst – bedoeld is om Blauw in staat te stellen een incident met persoonsgegevens behoorlijk te onderzoeken, haar reactie te bepalen en maatregelen te kunnen nemen. Daarmee verhoudt zich niet dat het instructierecht beperkt wordt uitgelegd. Nebu dient hieraan op een loyale en royale wijze mee te werken.

Tussen TNO en Uscoutfor is een licentieovereenkomst tot stand gekomen voor de exploitatie van software voor doelpuntherkenning. Omdat de software nog in ontwikkeling was op het moment van het sluiten van de overeenkomst waren partijen een beëindigingsclausule overeengekomen voor het geval de software niet naar behoren werkt. Uiteindelijk leidt de software niet tot een werkend systeem, maar partijen werken wel verder samen om de software werkend te maken voor een ander doel. TNO vordert op enig moment daarom betaling van niet volledig betaalde licentievergoedingen. Uscoutfor vordert op haar beurt ontbinding omdat TNO zou zijn tekortgeschoten in oplevering van software.
De rechtbank stelt vast dat partijen door een beëindigingsregeling af te spreken (impliciet) zijn afgeweken van de wettelijke regeling voor ontbinding. Uscoutfor was daarom alleen bevoegd tot ontbinding conform het contractuele regime. Hieraan is niet voldaan dus Uscoutfor kan de licentieovereenkomst niet ontbinden. Vervolgens oordeelt de rechtbank dat niet aan alle voorwaarden voor het betalen van de licentievergoedingen is voldaan. Zo is onvoldoende werkende technologie voor doelpuntherkenning, of voor Uscoutfor vergelijkbare technologie tot stand gebracht, zodat Uscoutfor de licentievergoedingen niet aan TNO hoeft te voldoen.

Fatale termijnen?

Synergy schakelt IPS in om software te ontwikkelen en beheren. De termijnen voor de oplevering worden telkens niet gehaald, maar er wordt (telkens) een nieuwe termijn bepaald. De rechtbank oordeelt dat de afgesproken termijnen (een oplevertermijn van 24 weken) voldoende concreet is en dus fataal was. Ook de daarna afgesproken data betroffen fatale termijnen en IPS verkeert daarom in verzuim. Wel oordeelt de rechtbank dat de tekortkoming de ontbinding niet rechtvaardigt aangezien er nog maar één blok van de tien dient te worden opgeleverd. Dit leidt de rechtbank af uit enerzijds het karakter van het project en de aard van de overeenkomst (een IT-project waarbij werd gewerkt met de scrum methode). Het slagen van het project hing af van een gezamenlijke inspanning en samenwerking. Ten slotte hebben partijen doorgewerkt aan het project tot het bijna afgerond was. Al met al kan de niet tijdige oplevering van de software de ontbinding van de gehele overeenkomst niet rechtvaardigen.

Toomba ontwikkelt een nieuwe applicatie voor appellant. Op enig moment ontbindt appellant de overeenkomst. Het hof oordeelt echter – in tegenstelling tot de rechtbank in de uitspraak hierboven inzake Synergy – dat Toomba niet in verzuim verkeert omdat de opleverdatum van 1 september 2019 géén overeengekomen fatale termijn betrof. Er zijn immers telkens nieuwe oplevertermijnen afgesproken. Bovendien was de tijdsindicatie van 10 tot 12 weken van Toomba in de offertes onvoldoende eenduidig om daaruit een fatale termijn af te leiden. De brief die appellant stuurde kan niet als ingebrekestelling kwalificeren nu daarin de tekortkoming niet is beschreven en ook niet wat appellant precies van Toomba verwachtte. Bovendien zijn de punten waarvan appellant later per e-mail aangaf dat die moesten worden hersteld ook daadwerkelijk hersteld. Daarna heeft appellant niet meer naar voren gebracht welke tekortkomingen Toomba nog zou moeten herstellen. Los van het verzuim heeft appellant ook de tekortkoming onvoldoende onderbouwd. Mede in het licht van de eerdere offertes die Toomba heeft uitgebracht op basis van de door appellant opgestelde blueprint, kon appellant afleiden dat in deze overeenkomst slechts een *minimum viable product* ('MVP') zou worden gerealiseerd en dat de blue print niet het uitgangspunt was. Uit het deskundigenrapport blijkt niet dat Toomba is tekortgeschoten in de oplevering van een MVP. Dit rapport is immers opgesteld in de veronderstelling dat partijen waren overeengekomen dat de app zou worden opgeleverd conform de blueprint.

EoF Europe, recensent van restaurants, vordert betaling en afgifte van de broncode van een app van

een softwareontwikkelaar. EoF Europe had gedaagde opdracht gegeven om een app te ontwikkelen via welke recensies voor restaurants kunnen worden ingezien. Partijen verwijten elkaar over en weer dat de overeenkomst niet is nagekomen. Anders dan EoF stelt, waren de overeengekomen termijnen volgens de rechtbank niet fataal nu wordt gesproken van een 'target date voor de release', en ook blijkens overige correspondentie tussen partijen waarin telkens een andere releasedatum wordt genoemd. De vorderingen tot een verklaring voor recht, afgifte van de broncode en ongedaanmaking van de betaalde facturen worden afgewezen. Gedaagde heeft de overeenkomst geldig partieel ontbonden. De vordering tot betaling van nog verschuldigd loon wordt in dit kader toegewezen.

In navolging op het tussenvonnis uit april 2022, oordeelt de rechtbank in dit eindvonnis dat Info Support aansprakelijk is voor de schade die Peelgemeenten leiden als gevolg van de onregelmatige opzegging van de overeenkomsten door Info Support. Voor berekening van de toerekenbare schade dient de feitelijke situatie die is ontstaan te worden vergeleken met de hypothetische situatie zoals die zonder opzegging zou zijn ontstaan volgens de redelijke verwachting van de rechtbank. De schade van Peelgemeenten bestaat uit het één jaar eerder beëindigen van deze overeenkomsten.

Aanbestedingsrecht

TenneT maakt gedurende de aanbestedingsprocedure bekend dat zij zal splitsen in twee entiteiten en dat daarom twee identieke maar losse clouds dienen te worden ingericht. Arvato, een van de inschrijvers, vordert staking van de aanbestedingsprocedure en stelt dat sprake is van een 'wezenlijke wijziging' van de opdracht die niet zou zijn toegestaan. Inschrijver Arvato legt aan deze vordering ten grondslag dat de mogelijke splitsing van TenneT NL en TenneT D vergaande gevolgen heeft voor de aanbestede opdracht, welke gevolgen op dit moment nog niet in volle omvang zijn te overzien. TenneT voert aan dat alle inschrijvers is gevraagd onvoorwaardelijk akkoord te gaan met elke materiële wijziging van de opdracht vanwege de mogelijke splitsing. Arvato heeft dat akkoord ook gegeven. De voorzieningenrechter oordeelt dat het standpunt van Arvato, dat vanwege deze uitbreiding van de opdracht de parameters op basis waarvan moet worden geoffreerd niet duidelijk zijn, niet worden gevolgd. De opmerking van Arvato dat twee 'identieke' clouds in dit geval niet werkelijk identiek kunnen zijn, is onvoldoende onderbouwd en daarmee niet aannemelijk geworden. Gedurende de gehele procedure konden vragen worden gesteld aan TenneT. Niet blijkt dat TenneT de door haar voorgeschreven procedure niet heeft gevolgd. Er is aldus geen sprake van een wezenlijke wijziging en/of strijd met het transparantiebeginsel. De vordering tot staking van de aanbestedingsprocedure wordt afgewezen.

Consumentenrecht

Een beding uit algemene voorwaarden kan onder meer worden vernietigd als dat beding onredelijk bezwarend is. In overeenkomsten met consumenten geldt dat in ieder geval de bedingen uit de zwarte en vermoedelijk de bedingen op de grijze lijst onredelijk bezwarend zijn. De Hoge Raad heeft de reikwijdte van deze lijsten verruimd door te bevestigen dat een beroep daarop ook mogelijk is voor een niet-consument maar de overeenkomst geen betrekking heeft op de beroeps- of bedrijfsactiviteiten. In die gevallen kan de omstandigheid dat het beding voorkomt op de zwarte of grijze lijst, relevant zijn voor de beoordeling of het een onredelijk bezwarend beding betreft.

Friends to Follow exploiteert een platform waar door 'creators' tegen betaling exclusieve content met een erotisch karakter kan worden gedeeld. In de algemene voorwaarden staat een boetebeding van EUR 10.000 bij het plaatsen van content waarop derden staan afgebeeld zonder hun toestemming. Gedaagde stelt dat hij als consument dient te worden gekwalificeerd en dat het boetebeding onredelijk bezwarend is. Volgens de rechtbank maakt het enkele feit dat gedaagde met het uploaden van de inhoud geld heeft verdiend, niet dat sprake is van professioneel handelen. Het betreffende beding is opgenomen in de lijst bijlage bij de Richtlijn oneerlijke bedingen (een beding dat een onevenredig hoge schadevergoeding oplegt aan een consument). Bij de beoordeling van het oneerlijke karakter dienen alle omstandigheden rond het sluiten van de overeenkomst, en alle overige bedingen in aanmerking te worden genomen. Hierbij is enkel relevant hoe het boetebeding in theorie zou kunnen uitpakken en niet hoe het boetebeding in dit geval uitpakt. De ernst van de tekortkoming van gedaagde moet dus buiten beschouwing worden gelaten. Het boetebeding wordt als onredelijk bezwarend aangemerkt omdat het van toepassing is op *iedere* overtreding van de algemene voorwaarden, zonder dat wordt gedifferentieerd in de aard en de ernst van de overtredingen. Bovendien zou de boete cumulatief kunnen worden geïnterpreteerd en treedt deze niet in de plaats van een eventuele schadevergoeding.

Een bestelknop met de tekst 'bestelling plaatsen' of 'bevestig je aanvraag' voldoet volgens de rechtbank niet aan het vereiste dat deze conform artikel 6:230v lid 3 BW een duidelijke en ondubbelzinnige mededeling dient te bevatten dat met het aanklikken ervan een betalingsverplichting wordt aangegaan. Ook

de verzendknop van Innova energie, met de tekst: 'verzenden' voldeed niet.

Auteursrecht

Na 14 jaar procederen van Stichting Brein, tegen de usenetprovider NSE, is het geschil eindelijk definitief beslist. De Hoge Raad concludeerde dat NSE geen auteursrechtinbreuk maakt want er is geen sprake van een mededeling aan het publiek. Van een handeling bestaande uit een mededeling van het publiek is pas sprake als de exploitant van het platform weloverwogen, met volledige kennis van de gevolgen van zijn handelswijze, intervenieert om zijn klanten toegang te verlenen tot een beschermd werk. Het hof heeft niet vastgesteld dat NSE een dergelijke weloverwogen interventie deed.
Daarnaast is NSE niet aansprakelijk voor vermeend inbreukmakende handelingen van gebruikers omdat NSE zich kan beroepen op de aansprakelijkheidsvrijstelling uit artikel 6:196c lid 1 en lid 4 BW. Zoals het Hof van Justitie van de EU overweegt in het Youtube en Cyando arrest (ECLI:EU:C:2021:503) wordt een exploitant uitgesloten van de aansprakelijkheidsvrijstelling, indien deze kennis heeft van de concrete onwettige handelingen van zijn gebruikers met betrekking tot op zijn platform geüploade beschermde inhoud. Niet voldoende is het enkele feit dat de exploitant in het algemeen ervan bewust is dat zijn platform ook wordt gebruikt om inhoud te delen die inbreuk kan maken op intellectuele eigendomsrechten en in die zin abstracte kennis heeft van illegale beschikbaarstelling van beschermde inhoud op zijn platform. Een efficiënte NTD-procedure ontbreekt ook niet bij NSE en 'slechts' 25 meldingen per uur werden verwerkt.

Een softwareontwikkelaar eist de broncode van door hem ontwikkelde software op nadat de samenwerking met SIKN is beëindigd. SIKN heeft namelijk de computer geformatteerd en verkocht waarop de broncode stond. Het hof oordeelt dat het verkopen van de computer niet het auteursrecht van de softwareontwikkelaar raakt. Uit de contractuele afspraken van partijen volgt niet dat duidelijk was of moest zijn dat SIKN ervoor verantwoordelijk was dat de broncode van appellant op een drager behouden bleef. Daarvoor had appellant SIKN in duidelijk bewoordingen moeten waarschuwen en SIKN dit risico moeten accepteren. De eis om de broncode terug te geven is niet toewijsbaar.

EKZ levert software voor zelfbedieningsbalies in bibliotheken. In dit kader heeft EKZ enige tijd samengewerkt met Dialoc. Op enig moment heeft Dialoc eigen software ('MyLib') ontwikkeld en gedistribueerd. Volgens EKZ maakt deze software inbreuk op haar auteursrechten en zij vordert een inbreukverbod. Dialoc stelt dat zij de software zelf geschreven heeft en voor zover nodig gebruik maakt van artikel 45m Auteurswet, op grond waarvan geen sprake is van een auteursrechtinbreuk als die noodzakelijk is voor – kortgezegd – de interoperabiliteit van computerprogramma's. De voorzieningenrechter oordeelt dat ook als van de juistheid van de stellingen van EKZ moet worden uitgegaan, binnen het beperkte bestek van de kortgedingprocedure niet kan worden vastgesteld of Dialoc inbreuk maakt op de auteursrechten van EKZ. Dialoc stelt immers dat partijen hadden afgesproken dat beide partijen de software mochten gebruiken en doorontwikkelen. Hiervoor is nader onderzoek naar de feiten noodzakelijk.

Workrate heeft drie softwareapplicaties ontwikkeld voor de HR-branche. Op enig moment is Usemate (dochtervennootschap van Workrate) de applicaties gaan exploiteren. Partijen zijn in geschil over de vraag of de auteursrechten zijn overgedragen en of een licentie is verstrekt aan Workrate. De rechtbank oordeelt dat de tussen partijen gesloten koopovereenkomst, in het licht van de gevoerde correspondentie, kwalificeert als een akte van overdracht auteursrechten. Uit de correspondentie rondom de transactie, het handelen nadien en de tekst van de overeenkomst volgt dat partijen het erover eens waren dat het auteursrecht bij PayingIT zou komen te liggen. Ook de omvang van de overdracht beoordeelt de rechtbank aan de hand van contractsonderhandelingen en overige bepalingen van de overeenkomst en volgens de Haviltex maatstaf. Tot slot stelt de rechtbank vast dat de overeenkomst een leemte bevat ten aanzien van de vraag of ook de onderliggende functionaliteit van de software door Workrate mag worden gebruikt. De rechtbank vult die leemte in aan de hand van de redelijkheid en billijkheid, en leidt uit de overige contractuele afspraken af dat de licentie van Workrate ook ziet op de onderliggende functionaliteit.

Artikel 45j Auteurswet bepaalt dat geen inbreuk wordt gemaakt op een auteursrechtelijk beschermd werk voor zover de verveelvoudiging wordt vervaardigd door een rechtmatige verkrijger en die noodzakelijk is voor het met dat werk beoogde gebruik. Het hof Arnhem Leeuwarden legt 'beoogd gebruik' nauw uit en oordeelt dat enkel dient te worden gekeken naar de aard van de software en de wijze waarop die aan de markt werd aangeboden. Subjectieve partijbedoelingen kunnen bij de inkleuring van dit criterium geen rol spelen aangezien de uitzondering daardoor teveel zou worden opgerekt. Als gevolg hiervan maken de onderhoudswerkzaamheden van Transportinfo inbreuk op het auteursrecht van Rainbow Solutions.

Zorgplicht

Volgens Allsafe is appellante tekortgeschoten in de ontwikkeling van een op maat gemaakt softwaresysteem. Allsafe heeft de overeenkomst ontbonden. Het hof oordeelt dat partijen de ontwikkeling van een CRM-systeem met basale functionaliteit zijn overeengekomen. De eerder gemaakte uitgebreidere projectafspraken maken géén onderdeel uit van de afspraken vanwege de overeengekomen *entire agreement clause*. In de prijsopgave zijn ook niet de onderdelen meegenomen waarvan Allsafe stelt dat die in scope zijn. De overgelegde rapporten kunnen niet worden betrokken bij de beoordeling van de tekortkomingen omdat in die rapporten een later systeem is beoordeeld, waarin al veel aanvullende wensen van Allsafe waren verwerkt, en dus niet het systeem betrof zoals appellante op grond van de hier centraal staande overeenkomst moest opleveren. Bovendien is getoetst aan ISO-25010 en niet aan de overeenkomst. Óók als de ISO-norm zonder dat die is overeengekomen invulling geeft aan wat van een redelijke IT-leverancier mag worden verwacht, betekent dit niet dat die los van de afspraken tussen partijen kan worden bezien. Nu een tekortkoming niet vast is komen te staan had Allsafe de overeenkomst niet mogen ontbinden en dient de facturen van appellante te voldoen.

Verano stelt dat GAC de op haar rustende bijzondere zorgplicht van een IT-leverancier heeft geschonden door zich onvoldoende in (de bedrijfsprocessen van) Verano te verdiepen. De rechtbank overweegt dat de reikwijdte en zwaarte van de bijzondere zorgplicht onder meer afhangt van de aard van de werkzaamheden die zijn overeengekomen en de mate van zijn deskundigheid. Bovendien had Verano als klant ook verantwoordelijkheden en had zij bovendien ook IT-deskundigheid in huis. De rechtbank oordeelt dat Verano haar vordering onvoldoende heeft onderbouwd, de vordering wordt dus afgewezen.

Eiser was klant van het beleggingsplatform Coin Meester, toen op enig moment via het hacken van zijn e-mail, toegang werd verschaft tot het Coin Meester account en de crypto valuta werd ontvreemd. Eiser stelt onder meer dat Coin Meester haar diensten onvoldoende heeft beveiligd door ook een optie aan te bieden zonder twee factor authenticatie. De rechtbank oordeelt dat op Cryptoplatform Coin Meester een vergelijkbare zorgplicht rust als de zorgplicht die geldt voor financiële instellingen die volgt uit de regels voor betalingstransacties uit titel 7b van boek 7 BW, omdat de dienstverlening van Coin Meester daarmee zeer vergelijkbaar is. Uit titel 7b van BW 7 volgt dat de betaaldienstverlener in moest staan voor de veiligheid van betalingstransacties. Daarbij is Coin Meester de deskundige partij en het is haar verantwoordelijkheid dat om klanten te beschermen tegen fraude. Het beroep op de aansprakelijkheidsbeperking uit de algemene voorwaarden slaagt niet omdat deze wordt aangemerkt als een oneerlijk beding. De aansprakelijkheidsbeperking verstoort namelijk het evenwicht tussen de uit de overeenkomst voortvloeiende rechten en plichten. Het recht vergoeding van schade wordt de consument zonder goede grond ontnomen.

Overig

Opleidingsinstituut Gilde nam een nieuwe applicatie af van Stucomm. Via de applicatie konden leerlingen informaties over lesroosters en behaalde resultaten inzien. Gilde stelt dat Stucomm tekortschoot omdat niet alle volgens haar overeengekomen informatie via de applicatie kon worden ingezien. De rechtbank overweegt dat een gedeelte daarvan inderdaad was overeengekomen, maar oordeelt dat Gilde niet de benodigde, redelijke en contractueel overeengekomen medewerking heeft geleverd aan Stucomm zodat Gilde in schuldeisersverzuim was. Als gevolg daarvan mocht Gilde de overeenkomst niet ontbinden en dient Gilde de schade van Stucomm als gevolg van de ontbinding te vergoeden.

Esmee Fonville
esmeefonville@turing.law

Huub de Jong
huubdejong@turing.law

Tom de Wit
tomdewit@t

turing
advocaten