JAARUPDATE IT & IT-outsourcing

2022

De mens centraal stellen, is één van de doelen van de Europese Unie in de digitale transitie. Dit heeft geleid tot de ondertekening van een Europese Verklaring over digitale rechten en beginselen. De ontwikkelingen op het gebied van digitalisering volgen elkaar razendsnel op. Ook de regelgeving neemt in rap tempo toe, onder meer om het hoofd te bieden aan toenemende cyberdreigingen en tegelijkertijd de kansen te benutten die digitalisering biedt. Wij schetsen deze en andere ontwikkelingen. Ook was er het afgelopen jaar weer een breed palet aan IT-rechtspraak. Inmiddels klassieke IT-onderwerpen zoals de zorgplicht en aansprakelijkheid voor het ontbreken van back-ups, maar ook de uitleg van IT-overeenkomsten waren regelmatig voorwerp van geschil. De uitdrukking “voor elk(e situatie) wat wils” leek goed op te gaan. In deze IT-update passeren deze en andere IT-geschillen kort de revue.

Ontwikkelingen

Europees niveau

Digitaal decennium

Op 19 december 2022 heeft de Europese Unie (“EU”) het beleidsprogramma ter uitvoering van het Digitaal Kompas bekendgemaakt. De nadruk ligt op het versterken van de grondrechten, transparantie en veiligheid en op het bevorderen van digitale vaardigheden. De Europese Commissie (“Commissie”) zal met de lidstaten voor elke doelstelling EU-trajecten ontwikkelen. De lidstaten stellen nationale trajecten op, inclusief geplande regelgeving en investeringen om de doelstellingen te bereiken. De vooruitgang zal worden gemeten op basis van de index van de digitale economie en samenleving (DESI). Ook zullen er meerlandenprojecten worden gestart. Daarbij zullen EU-, nationale en particuliere middelen worden gebundeld. Een eerste lijst van deze projecten omvat onder meer high-performance computing, blockchain, 5G-communicatie, digitale vaardigheden en digitale innovatiehubs.

Onderdeel van de digitale transitie betreft de verklaring over digitale rechten en beginselen voor het digitale decennium. De Raad, het Europees Parlement en de Commissie hebben deze verklaring in december 2022 ondertekend. In de verklaring staat voorop dat mensen en hun rechten centraal moeten worden gesteld bij de digitale transformatie. Ook komen onderwerpen als veiligheid, beveiliging en duurzaamheid aan de orde. De digitale rechten en beginselen die in de verklaring worden uiteengezet, vormen een aanvulling op bestaande rechten, zoals de rechten op grond van het Handvest van de grondrechten van de EU en op de wetgeving inzake gegevensbescherming en privacy. Zie ook deze factsheet op de website van de Europese Commissie.

In dit kader is tevens een voorstel voor een Europese digitale identiteit gedaan. Dit voorstel wijzigt de eIDAS-verordening uit 2014. Het voorstel moet voorzien in een universele toegang voor personen en bedrijven tot veilige en betrouwbare elektronische identificatie en authenticatie. De lidstaten worden verplicht een digitale portemonnee af te geven in het kader van een aangemeld eID-stelsel, op basis van gemeenschappelijke technische normen en na een verplichte certificering. Het raamwerk voor de cyberbeveiligingsverordening zal volledig van toepassing zijn. De Raad heeft op 25 november 2022 een gemeenschappelijk standpunt hierover aangenomen. Dat betekent dat de onderhandelingen met het Europees Parlement kunnen beginnen, zodra ook deze zijn standpunt heeft bepaald.

Ten behoeve van de financiering van de digitale transformatie is het subsidieprogramma Digitaal Europa in het leven geroepen. Hiermee wordt financiering verstrekt op onder meer de gebieden AI, cyberbeveiliging en geavanceerde digitale vaardigheden. Het betreft een aanvulling op de financiering via andere programma’s.

In het kader van het financieringsprogramma heeft de Commissie bedrijven, overheidsdiensten en andere organisaties uitgenodigd om voorstellen voor innovatieve cyberbeveiligingsoplossingen in te dienen. Dit kan nog tot 15 februari 2023.

Verder heeft de Commissie op 8 september 2022 het Nederlandse Herstel- en Veerkrachtplan positief beoordeeld. Daardoor zal de EU 4,7 miljard euro aan subsidies kunnen uitkeren aan Nederland.

Digital Markets Act

Onderdeel van de digitale strategie van de EU is de Digital Markets Act (DMA). Deze verordening is op 1 november 2022 in werking getreden. De DMA stelt regels voor grote online platforms – "poortwachters" – die een belangrijke verbinding vormen tussen zakelijke gebruikers en consumenten. De DMA heeft tot doel te voorkomen dat poortwachters oneerlijke voorwaarden opleggen aan bedrijven en eindgebruikers. Ook het waarborgen van de transparantie van belangrijke digitale diensten is een doel van de DMA. Hiermee moet een einde worden gemaakt aan de negatieve effecten die zich voordoen op de markt als gevolg van bepaalde gedragingen van online platforms. Om als poortwachter te worden aangemerkt moet aan drie criteria zijn voldaan: (i) een omvang die van invloed is op de interne markt, (ii) de controle over een toegangspoort voor zakelijke gebruikers naar eindgebruikers, en (iii) een bestendige en duurzame positie op de interne markt. Poortwachters hebben tot uiterlijk 3 juli 2023 de tijd om hun kernplatformdiensten aan te melden bij de Commissie. Nadat de Commissie een onderneming heeft aangewezen als poortwachter, heeft deze maximaal zes maanden de tijd om aan de vereisten uit de verordening te voldoen. Hiervan moet binnen diezelfde termijn verslag worden gedaan aan de Commissie. Zie ook deze factsheet op de website van de Europese Unie. Van 9 december 2022 tot en met 9 januari 2023 stond er een consultatie open ten aanzien van het eerste concept van de Uitvoeringsverordening voor de DMA.

Digital Services Act

Twee weken na de Digital Markets Act is op 16 november 2022 de Digital Services Act (DSA) in werking getreden. De DSA moet ervoor zorgen dat Europese burgers online beter worden beschermd, bijvoorbeeld tegen illegale inhoud, online intimidatie en bepaalde vormen van reclame. De DSA bouwt voort op de e-Commerce Directive uit 2000 en legt verplichtingen op aan online tussenhandeldiensten. Daarbij kan worden gedacht aan ISP's, hostingdiensten, online zoekmachines en online platforms. Online tussenhandeldiensten die onder het toepassingsgebied van de DSA vallen, moeten op uiterlijk 17 februari 2024 aan hun verplichtingen voldoen. Al op uiterlijk 17 februari 2023 moeten online tussenhandeldiensten op hun website informatie bekend maken over het gemiddelde aantal actieve afnemers van de dienst in de EU. Dat moeten zij vervolgens elke zes maanden blijven doen. Op basis van deze cijfers bepaalt de Commissie of een platform of zoekmachine moet worden aangewezen als een zeer groot online platform of zeer grote online zoekmachine. Indien die aanwijzing plaatsvindt, moet het betreffende platform of de zoekmachine al vier maanden na die aanwijzing aan de verplichtingen op grond van de DSA voldoen. Zie ook deze factsheet op de website van de Europese Unie.

Data Governance Act

Een belangrijke pijler van de datastrategie ter uitvoering van de digitale transformatie is de Data Governance Act. Deze is op 23 juni 2022 in werking getreden. De verordening heeft als doel meer gegevens beschikbaar te stellen en de uitwisseling van gegevens tussen sectoren en EU-landen te vergemakkelijken. Dit moet worden gerealiseerd door bepaalde categorieën van gegevens die in het bezit zijn van overheidsinstanties beschikbaar te stellen, tools te creëren voor data altruïsme en een Europees Comité voor gegevensinnovatie in het leven te roepen. Ook worden regels vastgesteld voor gegevensbemiddelingsdiensten, in de hoop dat organisaties meer vertrouwen krijgen in het delen van hun gegevens. De Data Governance Act is van toepassing vanaf 24 september 2023.

Data Act

Waar de Data Governance Act het gemakkelijker moet maken om data te delen, is het doel van de Data Act om toegang tot en gebruik van data door bedrijven en consumenten gemakkelijker te maken. Het voorstel voor de verordening is op 23 februari 2022 ingediend. De Data Act moet zorgen voor een eerlijke digitale omgeving. Dit wordt gerealiseerd door regels op te stellen voor het gebruik van gegevens die door apparaten van het internet der dingen (Internet of Things; IoT) worden gegenereerd. Denk hierbij aan producten die zijn gekoppeld aan het internet zoals slimme lampen, horloges en televisies. Op verzoek van de gebruiker moeten de data bovendien met derden worden gedeeld. Dit moet innovatie stimuleren en het voor consumenten gemakkelijker maken om hun producten te laten repareren op de secundaire markt. Daarnaast poogt de verordening om de onderhandelingspositie van micro-, kleine en middelgrote ondernemingen te verbeteren door eenzijdig opgelegde oneerlijke bedingen niet-bindend te verklaren. Verder krijgen overheden middelen om toegang te krijgen tot data die in het bezit zijn van de particuliere sector en die noodzakelijk zijn voor specifieke doeleinden van algemeen belang. Denk hierbij bijvoorbeeld aan overstromingen en bosbranden. Tot slot moet overstappen tussen cloud- en edgediensten gemakkelijker worden. Volgens de Commissie zullen door de verordening meer gegevens beschikbaar zijn voor gebruik, wat innovatie binnen de EU moet bevorderen. Voor een statusupdate klik hier.

Artificial Intelligence Act

Een essentieel onderdeel van de digitale transformatie betreft het door de Commissie in april 2021 ingediende voorstel voor een Artifical Intelligence Act. Het voorstel verdeelt AI-systemen in vier risiconiveaus: (i) onaanvaardbaar risico – en daarom verboden, (ii) hoog risico – deze systemen moeten voldoen aan strenge eisen en verplichtingen, (iii) beperkt risico – deze systemen hoeven slechts te voldoen aan transparantieverplichtingen, en (iv)

minimaal risico – voor deze systemen gelden geen aanvullende eisen. De verordening richt zich met name op de aanbieders en gebruikers van AI-systemen met een hoog risico, zoals systemen op het gebied van kritieke infrastructuren, personeelsbeheer, onderwijs en biometrische identificatie. Deze systemen moeten onder meer uitgebreide technische documentatie bijhouden en een conformiteitsbeoordeling ondergaan voordat ze op de markt mogen worden gebracht. Het Europees Parlement heeft duizenden wijzigingen aangedragen ten aanzien van de voorgestelde verordening. Deze zien onder andere op het strikter toepassen van de definitie van AI, meer verantwoordelijkheden naar gebruikers van AI-systemen met een hoog risico en een complete ban op databanken die biometrische gegevens bevatten. Op 25 november 2022 heeft de Raad zijn gemeenschappelijk standpunt aangenomen. De Raad zal gaan onderhandelen met het Europees Parlement zodra dit zijn definitieve standpunt heeft bepaald, om tot een akkoord te komen.

Global gateway

Met de op 1 december 2021 gelanceerde Global Gateway-strategie wil de EU slimme, schone en veilige verbindingen in de digitale, energie- en vervoerssector stimuleren en de gezondheids-, onderwijs- en onderzoekssystemen in de hele wereld versterken. Het is de bedoeling dat hiervoor tussen 2021 en 2027 tot 300 miljard euro aan investeringen wordt uitgetrokken. Voor de digitale sector betekent de nieuwe strategie dat de EU de banden met de rest van de wereld wil aanhalen en partnerlanden wil helpen om de digitale kloof aan te pakken.

In het kader van de Global Gateway-strategie heeft de Raad op 18 juli 2022 de conclusies over de digitale diplomatie van de EU goedgekeurd. Deze hebben onder meer tot doel de wereldwijde rol van de EU in digitale aangelegenheden te versterken. Daarbij bestaat bijzondere aandacht voor landen van strategisch belang of zeer kwetsbare landen. De veerkracht van de EU-partners moet worden versterkt en er moet proactief worden gepleit voor innovatievriendelijke en op mensenrechten gebaseerde technologiegovernance, aldus de conclusies.

Cybersecurity

Op 23 mei 2022 heeft de Raad conclusies aangenomen ter uitvoering van de in 2020 gepresenteerde cybersecuritystrategie. De Raad benadrukt in de conclusies de toename van cybersecurityrisico's en de noodzaak om de cyberhouding van de EU te ontwikkelen. Dit moet worden gedaan door capaciteitsopbouw, ontwikkeling, training en door krachtig te reageren op cyberaanvallen tegen de EU en haar lidstaten. In dit kader wordt onder meer de wens tot spoedige vaststelling van de Richtlijnen NIS-2 en DORA genoemd. In de conclusies wordt opgeroepen om mogelijke gezamenlijke reacties van de EU op cyberaanvallen in kaart te brengen, met inbegrip van sanctiemogelijkheden en deze vóór het einde van het eerste kwartaal van 2023 voor te leggen aan de Raad.

Op 15 september 2022 is er een voorstel gedaan voor een wet inzake cyberveerkracht voor *producten* met digitale elementen, oftewel de Cyber Resilience Act (CRA). De huidige regelgeving van de EU heeft met name geen betrekking op de beveiliging van niet-ingebedde software, terwijl cyberaanvallen wel steeds vaker gericht zijn op kwetsbaarheden in deze producten. Het wetsvoorstel heeft als doel om te zorgen voor een betere beveiliging van goederen met digitale elementen vanaf de ontwerp- en ontwikkelingsfase en gedurende de hele levenscyclus. Onder de reikwijdte van de CRA vallen alle producten met digitale elementen, waarvan het (redelijk voorstelbaar) gebruik een directe of indirecte verbinding tot een eindapparaat of netwerk bevat. In Annex III bij de CRA zijn bovendien twee categorieën kritieke producten met digitale elementen opgenomen die een hoger cybersecurityrisico met zich meebrengen. Voor die categorieën worden zwaardere eisen aan de conformiteits-beoordelingsprocedure gesteld. Klik hier voor een samenvatting van de impact assessment die de Europese Commissie in verband met het voorstel heeft gemaakt. Hier is de Nederlandse positie ten aanzien van het voorstel te vinden.

Op 16 januari 2023 is de NIS-2 Richtlijn in werking getreden. Deze betreft de cyberbeveiliging van de verlening van *diensten* door essentiële en belangrijke entiteiten. De NIS-2 Richtlijn moet door middel van minimumregelgeving de verschillen wegnemen tussen regels voor en aanpak van cyberbeveiliging in de verschillende lidstaten. Met NIS-2 wordt het toepassingsgebied van de bestaande NIS-Richtlijn uitgebreid naar diverse sectoren die belangrijk zijn voor de economie en samenleving. Verder worden beveiligingsverplichtingen scherper en toezichts-maatregelen voor nationale autoriteiten strenger. De lidstaten moeten op uiterlijk 17 oktober 2024 de NIS-2 Richtlijn hebben omgezet in nationale wetgeving.

De Raad heeft de Digital Operational Resilience ACT (DORA) op 28 november 2022 aangenomen. DORA stelt uniforme vereisten vast voor de beveiliging van netwerk- en informatiesystemen van bedrijven en organisaties die actief zijn in de *financiële sector* en van cruciale derde partijen die hen ICT-gerelateerde diensten verlenen. Nu is het aan de EU-lidstaten om DORA in wetgeving om te zetten. De betrokken Europese toezichthoudende autoriteiten zullen technische normen ontwikkelen waaraan alle instellingen voor financiële diensten zich moeten houden.

Verder zijn de Europese cybersecurity- en certificeringsschema's nog steeds in ontwikkeling. Klik hier voor een statusupdate.

Europese Cloud

In onze vorige update berichtten we dat Microsoft gaat investeren in een cloud voor Europese bedrijven en overheden, waarbij alle gegevens worden opgeslagen op servers binnen de Europese grenzen. Inmiddels heeft Microsoft aangekondigd dat zij haar klanten vanaf 1 januari 2023 de mogelijkheid biedt om hun klantgegevens op te slaan en te verwerken binnen de EU Data Boundary voor Microsoft 365, Azure, Power Platform en Dynamics 365 diensten.

Nationaal niveau

ARBIT 2022

Op 10 september 2022 zijn de nieuwe Algemene Rijksinkoopvoorwaarden bij IT-overeenkomsten (ARBIT) in werking getreden. Hiermee wordt de eerdere versie uit 2018 vervangen. De aanpassingen betreffen onder andere het contracteren van clouddiensten en agile ontwikkeltrajecten. Daarnaast is de aansprakelijkheid ten aanzien van bescherming van persoonsgegevens breder getrokken dan in de eerdere versie het geval was. Op het gebied van AI zijn geen bepalingen in de ARBIT opgenomen. Dit heeft te maken met de ontwikkelingen op dit gebied in de regelgeving van de EU.

Verkoop goederen en Levering digitale inhoud

Op 27 april 2022 is de Implementatiewet richtlijnen verkoop goederen en levering digitale inhoud in werking getreden. Het betreft de implementatie van de Europese richtlijnen inzake Verkoop van Goederen en Levering Digitale Inhoud en Digitale Diensten. Deze richtlijnen hebben maximum-harmonisatie van het consumentenkooprecht als uitgangspunt. 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.

Digitaliseringsstrategie

Op 10 januari 2022 is Alexandra van Huffelen als (eerste) staatssecretaris Digitalisering beëdigd. Klik hier voor de hoofdpunten inzake digitalisering in het coalitieakkoord van 15 december 2021. Zoals vorig jaar al was aangekondigd, heeft de Tweede Kamer een vaste Kamercommissie Digitale Zaken ingesteld (Kamercommissie DiZa). Hier is de agenda te vinden met activiteiten op de korte termijn en tevens de commissieverslagen.

In de Kamerbrief hoofdlijnen beleid voor digitalisering van 8 maart 2022 bespreken de betrokken bewindslieden een viertal thema's rond de invulling van digitalisering uit het coalitieakkoord. In het kader van het thema "Digitaal fundament" wordt onder meer melding gemaakt van de wijziging van de Wet beveiliging netwerk- en informatiesystemen (Wbni). Deze zorgt voor een uitbreiding van de bevoegdheid van het NCSC (Nationaal Cyber Security Centrum) om informatie te verstrekken aan niet-vitale aanbieders over dreigingen en incidenten betreffende hun netwerk- en informatiesystemen. Tevens is het wetsvoorstel Bevorderen digitale weerbaarheid bedrijven ingediend. Met dit wetsvoorstel verkrijgt het DTC (Digital Trust Center) een wettelijke basis om informatie te geven aan het niet-vitale bedrijfsleven over specifieke digitale dreigingen en kwetsbaarheden, terwijl het voorheen slechts algemene informatie mocht verstrekken. Daarbij zal het DTC ook een zo praktisch mogelijk handelingsperspectief aanreiken aan het betreffende bedrijf. Bij het thema "Digitale overheid" komen onderwerpen aan de orde als de I-strategie 2021-2025 van het Rijk en het omarmen van een agile werkwijze. Het thema "Digitale samenleving" betreft het bouwen aan een digitale samenleving met sterke publieke instellingen, waarin voorzieningen als zorg, onderwijs en mobiliteit zijn geborgd. Ten aanzien van het thema "Digitale economie" wordt onder meer verslag gedaan over het Nationaal Groeifonds (zie verderop). In het Kabinetsbeleid Digitalisering zijn de vier bovengenoemde thema's terug te vinden evenals de Werkagenda Digitalisering.

In een brief van 17 augustus 2022 informeert staatssecretaris Van Huffelen de Kamer over de voortgang inzake de Europese Digitale Identiteit. Het voorstel van de Europese Commissie heeft het nodige stof doen opwaaien.

Noemenswaardig is verder dat Nederland na drie jaar is teruggekeerd in de top 3 van de EU-ranglijst digitale economie. Nederland staat op nummer 3 achter de nieuwe koplopers Finland en Denemarken. Deze ranglijst wordt samengesteld door de Digital Economy and Society Index (DESI) van de EU. Wanneer het gaat om het aantal afgestudeerden in een ICT-richting, scoort Nederland iets beneden gemiddeld in de EU.

Nationaal Groeifonds

Het hierboven kort aangestipte Nationaal Groeifonds is in 2020 gestart. Dit fonds houdt in dat het kabinet voor de periode 2021-2026 twintig miljard euro beschikbaar stelt voor projecten op het gebied van kennisontwikkeling, onderzoek en innovatie en infrastructuur. Afgelopen jaar heeft de *tweede ronde* plaatsgevonden. Dat heeft geresulteerd in een advies om geld toe te kennen of te reserveren voor achtentwintig voorstellen, op onder meer de gebieden biotechnologie, fotonica, digitale infrastructuur en digitaal onderwijs. Op 22 maart 2022 is het voorstel voor een Tijdelijke wet Nationaal

Groeifonds aangenomen door de Tweede Kamer. Daarmee is het Nationaal Groeifonds als een apart begrotingsfonds ingesteld.

Cybersecurity

De Uitvoeringswet cyberbeveiligingsverordening is op 9 april 2022 in werking getreden. De wet voorziet in bepalingen met betrekking tot procedures, handhaving, rechtsbescherming en de aanwijzing van uitvoeringsorganen.

In een brief van 29 juni 2022 heeft minister Adriaansens het Evaluatierapport Roadmap Digitaal Veilige Hard- en Software aan de Kamer aangeboden. Genoemde Roadmap maakt onderdeel uit van de Rijksbrede aanpak voor digitale veiligheid in de Nederlandse Cyber Security Agenda (NCSA). Deze bestaat uit een combinatie van Europese en nationale maatregelen. De Roadmap is door KWINKgroep geëvalueerd. De minister gaf aan de aanbevelingen mee te nemen in de nieuwe cybersecuritystrategie. In oktober 2022 is de nieuwe Nederlandse Cybersecuritystrategie 2022-2028 gepubliceerd. Het doel van de strategie is om de scheefgroei tussen digitale dreiging en digitale weerbaarheid zo klein mogelijk te maken en te houden. Zie ook het bijbehorende Actieplan.

Het Nederlandse bedrijfsleven is op 14 februari 2022 gestart met het Security Meldpunt. Het Security Meldpunt automatiseert het delen van dreigingsinformatie en wil op die manier bijdragen aan een hogere cyberveiligheid in Nederland.

Zerodays

Het eerder door ons genoemde wetsvoorstel Zerodays is op 17 mei 2022 vervallen vanwege het ontbreken van initiatiefnemers.

Cloudservices

In het kader van het agendathema “Digitale economie” heeft de ACM onderzocht hoe de markt voor clouddiensten functioneert. Daarbij kwam onder meer naar voren dat er weinig overstap plaatsvindt tussen clouddiensten van verschillende cloudaanbieders. Vooral gebruikers van PaaS- en SaaS-diensten kunnen moeilijkheden ervaren bij het overstappen. De ACM beveelt de Europese Raad en het Europese Parlement aan om de cloudgerelateerde voorstellen in de Data Act te omarmen en daarbij aanvullend verplichtingen op te nemen die interoperabiliteit verbeteren. De ACM beveelt gebruikers aan om bewust een afweging te maken tussen de meerwaarde van een specifieke clouddienst en de mate van lock-in en daarbij alleen lock-in te accepteren als het gebruik van de dienst heel grote voordelen heeft ten opzichte van alternatieven.

Jurisprudentie

Kwalificatie overeenkomst

Het hof Den Bosch oordeelde dat de kooptitel van het BW van toepassing was op een overeenkomst tot digitalisering van door monteurs gebruikte werkbonnen. Daaraan deed niet af dat de IT-leverancier ook aanvullende dienstverlening aanbood en enig maatwerk had ontwikkeld. Er was namelijk niet gesteld of gebleken dat sprake was van meer dan relatieve aanpassingen ten behoeve van de afnemer. Volgens het hof zou in zoverre ook sprake kunnen zijn van aanneming van werk, maar dat sluit toepassing van de conformiteitsregeling uit de kooptitel niet uit.

In een geschil tussen een softwareontwikkelaar en een groothandelaar ging het beroep op een overeenkomst van aanneming van werk niet op. Het voorwerp van de overeenkomst betrof namelijk de ontwikkeling van software. Er was dus geen sprake van het tot stand brengen van een werk van stoffelijke aard. De overeenkomst was een overeenkomst van opdracht, ook al bevatte de overeenkomst elementen die kenmerkend zijn voor aanneming van werk. In de titel van aanneming van werk ontbreken (schakel)bepalingen waaruit een verruiming van de titel kan worden afgeleid voor wat betreft het voorwerp van de overeenkomst, aldus het hof Arnhem-Leeuwarden.

Uitleg overeenkomst

De rechtbank Oost-Brabant overwoog dat de uitleg van alle stukken die tijdens de aanbestedingsprocedure zijn gewisseld, moet plaatsvinden naar objectieve maatstaven. Het ging om stukken die door één partij waren opgesteld zonder dat over de inhoud was onderhandeld, aldus de rechtbank. De stukken waren bedoeld voor alle potentiële inschrijvers. Daarom waren, gelet op de gelijke behandeling van de deelnemers aan de aanbestedingsprocedure, de bewoordingen van de stukken van doorslaggevende betekenis voor de uitleg. De rechtbank nam ook een objectieve uitleg als uitgangspunt ten aanzien van de SLA, die na de aanbestedingsprocedure was overeengekomen. De reden was precies het tegenovergestelde van de argumentatie bij de aanbestedingsstukken, namelijk het feit dat er uitgebreid over de tekst van de SLA was onderhandeld.

In dezelfde uitspraak overwoog de rechtbank Oost-Brabant dat de mededeling van de IT-leverancier dat de applicatie de mogelijkheid bood om werkprocessen in te regelen zoals de afnemer dat wenste, *niet* inhield dat de afnemer mocht verwachten dat de software (exact) conform de gewenste werkprocessen kon worden ingericht. Hierbij woog mee dat de afnemer in de aanbesteding had gekozen voor een opsomming van functionaliteiten die in de standaardapplicatie

moesten zitten en niet exact had voorgeschreven op welke manier die functionaliteiten moesten werken.

In een geschil tussen een IT-leverancier en een factureerbedrijf heeft de rechtbank Limburg geoordeeld dat voorbereidende werkzaamheden in beginsel moeten worden betaald. De stelling van de afnemer dat er werkzaamheden waren verricht zonder dat er een overeenkomst was, ging niet op. De rechtbank overwoog dat partijen de mondelinge afspraken daarover met terugwerkende kracht hadden vastgelegd in een schriftelijke overeenkomst.

De rechtbank Den Haag overwoog dat partijen met hun beëindigingsregeling in de licentieovereenkomst waren afgeweken van de wettelijke regeling voor ontbinding. Er was niet aan de voorwaarden in de contractuele regeling voldaan en dus kon de overeenkomst niet op de ingeroepen grond worden ontbonden. Dat wilde overigens niet zeggen dat de afnemer de gevorderde licentievergoedingen verschuldigd was (naast de al betaalde licentie-vergoedingen). De technologie die zou worden ontwikkeld, was namelijk niet tot stand gekomen. De wel ontwikkelde technologie werd niet gebruikt. Deze kon qua exploitatiemogelijkheden ook niet worden gelijkgesteld aan de overeengekomen technologie. De rechtbank legde de licentieovereenkomst aldus uit dat de voorwaarde waaronder deze was gesloten, niet was vervuld. De gevorderde licentievergoeding was daarom niet verschuldigd.

De tussen een gemeente en een IT-leverancier gesloten vaststellingsovereenkomst stond niet in de weg aan ontbinding van de hoofdovereenkomst. De vaststellingsovereenkomst was slechts als tijdelijke oplossing bedoeld. Uit de bepalingen in de vaststellingsovereenkomst bleek dat de gemeente zich het recht wilde voorbehouden de gehele kwestie aan de (voorzieningen)rechter voor te leggen om aan de orde te stellen welke verplichtingen uit de hoofdovereenkomst voortvloeien. Dit was gelet op de tussen partijen gewisselde correspondentie ook duidelijk voor de IT-leverancier, althans dit had duidelijk moeten zijn, volgens de rechtbank Gelderland.

Het hof Den Bosch woog bij de uitleg van een overeenkomst mee dat de afnemer moest worden beschouwd als een partij die begrip heeft van de diensten van de IT-leverancier. Partijen steggelden over de vraag of een meerprijs verschuldigd was voor het door de afnemer gebruikte werkgeheugen. Het hof achtte het niet aannemelijk dat het voor de afnemer niet duidelijk was wat partijen waren overeengekomen en welke voorwaarden daarbij van toepassing waren. Het hof baseerde dit oordeel op onder andere de discussie over de capaciteitsoverschrijdingen in de e-mailcorrespondentie tussen partijen en wat de afnemer (zelf ook IT-leverancier) daarin uiteen had gezet. Hier komt het belang van de deskundigheid van de afnemer bij de beoordeling van de verplichtingen van partijen, naar voren.

Ook de rechtbank Gelderland nam in haar beoordeling mee dat de afnemer, een e-commercebedrijf dat een van de grootste online ruitershops van Europa exploiteert, geacht moet worden te weten wat het verschil is tussen een hostingdienstverlener en een webbouwer en hoe de verantwoordelijkheden tussen beide dienstverleners zijn verdeeld.

In een geschil over de betaling van een projectfactuur, constateerde het hof Den Haag dat partijen geen factuurdatum of betalingsdatum in de overeenkomst hadden vastgelegd. Volgens de IT-leverancier waren partijen overeengekomen dat de factuur, die 60% van de totale Consultancy & Development kosten bedroeg, bij aanvang van het project zou worden voldaan. Het hof kon een dergelijke afspraak niet vaststellen. Het hof viel daarom terug op een bepaling in de algemene voorwaarden van de IT-leverancier: “bij gebreke van een overeengekomen betalingsschema zijn alle bedragen die betrekking hebben op het ontwerpen en ontwikkelen van programmatuur en/of websites telkens per kalendermaand achteraf verschuldigd.” Het hof oordeelde dat partijen dus betaling achteraf waren overeengekomen. Om die reden hoefde de afnemer de projectfactuur pas te betalen wanneer de IT-leverancier de overeengekomen Development & Consultancy werkzaamheden helemaal had uitgevoerd (wat niet was gebeurd).

Algemene Voorwaarden

Geen IT-procedure, maar wel relevant voor de IT-praktijk is het arrest van de Hoge Raad over de toepassing van de "bekendheidsuitzondering". De bekendheidsuitzondering houdt in dat een wederpartij zich niet op vernietigbaarheid van een beding in de algemene voorwaarden kan beroepen, wanneer zij ten tijde van het sluiten van de overeenkomst met dat beding bekend was of geacht kon worden bekend te zijn. De Hoge Raad heeft overwogen dat dit ook geldt wanneer de wederpartij niet door toedoen van de gebruiker, maar op een andere wijze bekend is geworden met (een beding in) de algemene voorwaarden. Een verruiming van de bekendheidsuitzondering dus.

Zorgplicht

De afnemer van een te ontwikkelen platform mocht verwachten dat het platform bij de lancering een acceptabele prestatie zou leveren en niet dat dan pas duidelijk zou zijn dat hiervoor een complete rebuild noodzakelijk was. Dit gold volgens de rechtbank Rotterdam ook indien de architectuur van het platform als gevolg van door de afnemer gewenste wijzigingen niet meer zou hebben voldaan. De IT-leverancier had in dat geval op een eerder

tijdstip duidelijk moeten waarschuwen. Het feit dat in de overeenkomst de *agile/scrum*-methode was overeengekomen, deed daaraan niet af. De IT-leverancier was de bij uitstek deskundige partij als het gaat om de architectuur van het platform. Als deze redelijkerwijs kon zien aankomen dat de afnemer wensen had die de functionaliteit in zodanige mate zou aantasten dat die niet meer zou functioneren, rustte er een waarschuwingsplicht op de IT-leverancier.

Ook het hof Arnhem-Leeuwarden overwoog dat een waarschuwingsplicht op de IT-leverancier rustte, indien deze van mening was dat de afnemer zich inschikkelijker had moeten opstellen voor wat betreft zijn eisen aan de (standaard)software. Deze waarschuwingen hadden voldoende concreet in de projectovereenkomst moeten worden opgenomen. De ten tijde van het project geuite waarschuwingen voor budgetoverschrijdingen achtte het hof niet meer van invloed te zijn geweest op de gerechtvaardigde verwachtingen van de afnemer bij aanvang van de overeenkomst. Het hof baseerde deze verwachtingen onder meer op de betaalde voor-analyse die als doel had om “een juiste calculatie en een passend contractvoorstel aan te bieden.” Volgens het hof mocht de afnemer er daarom van uitgaan dat de IT-leverancier concreet in kaart had gebracht wat de afnemer nodig had en ook dat de calculatie binnen redelijke marges zou zijn. Met het herijken van de afspraken na de Go Live datum had de afnemer geen afstand gedaan van het recht om zich te beroepen op de gerechtvaardigde verwachtingen die hij bij het aangaan van de overeenkomst had. Uit de overwegingen van het hof lijkt te volgen dat dit oordeel mede is ingegeven door het feit dat de afspraken werden herijkt op een moment dat er al aanzienlijke (meer)kosten waren gemaakt en de ingeschatte projectduur al was uitgelopen.

Een afnemer deed een tevergeefs beroep op falend projectmanagement, omdat volgens de rechtbank Oost-Brabant het project gedeeltelijk was vertraagd door oorzaken die in de risicosfeer van de afnemer lagen. Daarnaast was de tijd voor het project erg kort, wat de afnemer zich volgens de aanbestedingsdocumenten ook had gerealiseerd. Met dit oordeel week de rechtbank af van bestendige rechtspraak over de zorgplicht van IT-leveranciers. Het zou logischer zijn geweest als de rechtbank in haar overwegingen had meegenomen dat de afnemer een adviesbureau had ingeschakeld dat gespecialiseerd was in de begeleiding van lokale overheden bij IT-projecten. Deskundigheid van afnemers is immers een omstandigheid die meeweegt bij de beoordeling van een beroep op de zorgplicht.

Eveneens een tevergeefs beroep op de zorgplicht deed een afnemer die stelde dat zijn hosting-dienstverlener niet de juiste server had geadviseerd en hem niet had ontzorgd. De rechtbank Gelderland overwoog dat de overeenkomst tot (enkel) het leveren van twee managed servers niet inhield dat de hostingprovider de afnemer tevens van advies moest voorzien over de vraag welke server het beste paste bij de webshop en ook niet dat hij de afnemer moest ontzorgen. Hierbij speelde mee dat de afnemer niet had weersproken dat de geleverde server geschikt was voor de webshop en dat de traagheid van de webshop werd veroorzaakt door problemen in onder meer de code van de webshop.

Het hof Arnhem-Leeuwarden overwoog dat geen sprake was van schending van de zorgplicht, omdat de IT-leverancier regelmatig inzicht had gegeven in de status en voortgang van het project. De afnemer had tijdens de vele werksessies de mogelijkheid gehad om vragen te stellen en zijn input was verwerkt. Ook kon de afnemer de werkzaamheden volgen via een server. De algemene stelling dat de werksessies geen inzicht hadden gegeven in de voortgang, was volgens het hof onvoldoende om te concluderen dat de IT-leverancier was tekortgeschoten in zijn informatieplicht. Ook hier leek wederom een rol te spelen dat de afnemer zelf min of meer deskundig was. Het hof overwoog namelijk dat de afnemer zelf ook software ontwikkelde en als professional mocht worden geacht inzicht te hebben in de (problemen bij) ontwikkelprocessen.

Inspanningsverbintenis

Een bepaling in de algemene voorwaarden dat sprake is van een inspanningsverbintenis, kan een indicatie zijn voor wat er is afgesproken. Of inderdaad sprake is van een inspanningsverbintenis vereist uitleg van de overeenkomst, waarbij alle omstandigheden van het concrete geval van beslissende betekenis zijn en moeten worden gewaardeerd naar maatstaven van redelijkheid en billijkheid. Volgens de rechtbank Rotterdam bevatte de offerte geen afspraken of toezeggingen, maar slechts een opsomming van posten en werkzaamheden, die te weinig concreet waren om een bepaald eindresultaat te kunnen omschrijven. Ook was geen oplevering op een bepaalde datum overeengekomen, wat eveneens duidde op een inspanningsverbintenis. Volgens de rechtbank had de afnemer nauwkeuriger moeten stellen welke inspanning zij van de IT-leverancier had mogen verwachten, anders dan alleen een te behalen resultaat.

Exit

Een ontwikkelingsovereenkomst voor een webshop is door de rechtbank Oost-Brabant aangevuld, omdat deze een leemte bevatte ten aanzien van een exitregeling. Daarbij nam de rechtbank het voor de webshop betaalde bedrag in aanmerking evenals de correspondentie tussen partijen. Uit de correspondentie tussen partijen bleek namelijk dat zij

de noodzaak van een exitregeling voor ogen hadden gezien. De IT-leverancier had daarin, weliswaar onder voorwaarden, aangeboden om tot migratie van de webshop over te gaan. De IT-leverancier kon dan niet, voor het eerst in kort geding onder verwijzing naar zijn algemene voorwaarden, het standpunt innemen dat van een verplichting om medewerking te verlenen aan migratie geen sprake was. Indien de IT-leverancier deze uitleg van zijn algemene voorwaarden voorstond, dan had hij zijn afnemer daar bij aanvang van de overeenkomst, maar in ieder geval bij het voorstel van de afnemer om de overeenkomst te beëindigen, op moeten wijzen. Het beroep van de IT-leverancier op opschorting kon eveneens niet slagen. Afgezien daarvan was het volgens de rechtbank de vraag of een opschorting gerechtvaardigd was, gelet op het belang van de afnemer bij migratie van de webshop en het feit dat de afnemer het overgrote deel van de eenmalige kosten al had voldaan.

Back-ups

De rechtbank Rotterdam oordeelde dat een deskundigenbericht nodig was om vast te kunnen stellen of de IT-leverancier verantwoordelijk kon worden gehouden voor het ontbreken van back-ups na een ransomware-aanval. De enkele omstandigheid dat de IT-leverancier het back-up proces zou monitoren, betekende volgens de rechtbank namelijk niet dat de IT-leverancier zelf back-ups diende te maken van alle software (en de maatwerksoftware die een derde aan het ontwikkelen was). Ook het enkele feit dat de aanval zich had voorgedaan, betekende niet dat de IT-leverancier was tekortgeschoten in het voldoende waarborgen van de veiligheid van de IT-systemen van de afnemer. Tot slot was het ook niet voldoende dat de destijds aanwezige beveiliging beter had kunnen worden ingericht. De afnemer zag echter geen heil in een deskundigenbericht: de oude IT-omgeving was niet meer beschikbaar en de afnemer meende dat al vaststond dat de IT-leverancier was tekortgeschoten in de nakoming van zijn verplichtingen. De rechtbank respecteerde dit standpunt en gelastte geen deskundigenbericht. Dat had wel tot gevolg dat de afnemer niet was geslaagd in zijn bewijslevering en alle vorderingen werden afgewezen.

De rechtbank Overijssel overwoog inzake een geschil over back-ups, dat het feit dat de IT-leverancier een volledige IT-infrastructuur had aangelegd en het onderhoud en beheer daarvan verzorgde, betekende dat de IT-leverancier een totaalpakket zou leveren. De IT-leverancier had vervolgens onvoldoende gemotiveerd betwist dat dit tevens inhield dat hij diende te zorgen voor een adequate IT-beveiliging van de gegevens van zijn afnemer. Dat de IT-leverancier de hosting van de server had uitbesteed aan een derde, deed daaraan niet af. De IT-leverancier werd veroordeeld tot vergoeding van de schade met betrekking tot het verlies van de data op de FTP-server. In de vrijwaringsprocedure (ten aanzien van de ingeschakelde derde) werd geoordeeld dat de derde niet was tekortgeschoten ten aanzien van de FTP-server. Er waren geen afspraken gemaakt over het maken van back-ups van de FTP-server. Bovendien was de derde slechts host van een SQL-server en had hij de FTP-server slechts beschikbaar gesteld zonder te weten wat de afnemer daarop plaatste.

Garanties

De rechtbank Oost-Brabant overwoog dat een beroep op de garantie dat de software compleet en gebruiksklaar was, naar maatstaven van redelijkheid en billijkheid onaanvaardbaar was. Volgens de rechtbank had de afnemer het risico aanvaard dat de applicatie nog niet compleet en nog niet volledig gebruiksklaar was. De afnemer had er namelijk zelf voor gekozen om snel live te gaan zonder de acceptatieprocedure te volgen.

Verzuim

In een geschil tussen een appontwikkelaar en een winkel heeft de rechtbank Noord-Holland geoordeeld dat er geen sprake was van een fatale termijn voor oplevering. De afgesproken data waren volgens de rechtbank streefdata. Daarnaast bleek volgens de rechtbank niet dat de appontwikkelaar de nieuwe opleverdata had aanvaard als fatale termijn, waardoor geen sprake was van een bindende afspraak. Bij een agile ontwikkelmethode ligt het ook minder voor de hand dat partijen een fatale datum voor oplevering overeenkomen, aldus de rechtbank.

De rechtbank Oost-Brabant overwoog dat de inkoopvoorwaarden van de afnemer een strikter criterium hanteerden voor het begrip “fatale termijn” dan het criterium dat op basis van HR-jurisprudentie (Fraanje/Götte) geldt. Om die reden hadden de woorden “fatale termijn” uitdrukkelijk in de overeenkomst moeten worden vermeld, of er had in ieder geval duidelijk moeten worden gemaakt dat het ging om een termijn die bij overschrijding automatisch verzuim zou opleveren. Alleen de term “uiterlijk” was hiervoor onvoldoende.

Opschorting en ontbinding

Het hof Amsterdam bracht in een geschil over de beëindiging van een samenwerkingsovereenkomst in herinnering dat voor een gerechtvaardigd beroep op opschorting een opeisbare vordering vereist is. De opschortende partij had echter niet gesteld welke specifieke verplichting op zijn contractspartner zou hebben gerust. Dit klemde volgens het hof des te meer omdat ook niet was gebleken dat de opschortende partij aan zijn contractspartner concreet had gemeld aan welke eisen deze moest voldoen om weer recht op betaling te krijgen.

De rechtbank Rotterdam herinnerde de afnemer eraan dat deze niet van zijn betalingsverplichtingen

werd bevrijd door de gestelde onvolledigheid of ondeugdelijkheid van de prestaties van de IT-leverancier. Daarvoor is immers ontbinding van de overeenkomst vereist en dat was niet gebeurd.

In de al eerdergenoemde zaak bij het hof Arnhem-Leeuwarden (waarschuwingsplicht) had een afnemer eveneens zijn betalingsverplichtingen opgeschort, zonder de overeenkomst te ontbinden. De afnemer ontbond echter na de memoriewisseling, comparitie en tussenarrest, alsnog de overeenkomst. Het hof overwoog dat de omstandigheid dat de afnemer in de hoger beroepsprocedure al een memorie van grieven had genomen, niet maakte dat de afnemer de overeenkomst op dat moment niet buitengerechtelijk mocht ontbinden. Het hof oordeelde dat de IT-leverancier alle betaalde facturen moest terugbetalen.

Geldvordering in kort geding

De voorzieningenrechter in Amsterdam wees een geldvordering (gedeeltelijk) toe. Het spoedeisend belang was volgens de voorzieningenrechter gelegen in het feit dat de betalingstermijnen al enige tijd verstreken waren. Met “enige tijd” werd respectievelijk drie en vier maanden bedoeld. De voorzieningenrechter achtte het verweer van de afnemer dat partijen stilzwijgend waren overeengekomen dat de afnemer te laat mocht betalen, niet aannemelijk. Het structureel te laat betalen betekende niet dat dit was overeengekomen of een bestendig gebruik was geworden.

Opzegging

De rechtbank Den Haag oordeelde dat sprake was van ongerechtvaardigde verrijking door opzegging van een samenwerkingsovereenkomst tot ontwikkeling en exploitatie van een webinarplatform. Door de opzegging was iedere aanspraak van de opgezegde partij op mogelijk rendement van zijn tijdsinvestering in het platform tenietgedaan. Volgens de rechtbank druiste dat niet alleen in tegen de aard en inhoud van de (door uitleg vastgestelde) afspraken tussen partijen, maar was tevens zondermeer sprake van strijd met de redelijkheid en billijkheid.

Het hof Arnhem-Leeuwarden overwoog dat een IT-leverancier rechtmatig de overeenkomst had opgezegd. De IT-leverancier had een gewichtige reden in de zin van artikel 7:408 lid 2 BW vanwege het verlies van vertrouwen in de afnemer. Deze liet telkens facturen onbetaald en liet na vele pogingen om uit de impasse te geraken, niets meer van zich horen.

Elektronische handtekening

In een geschil over de betaling van een factuur voor licenties en hardware, was niet aangetoond dat de onderliggende overeenkomst en het bestelformulier door de afnemer waren ondertekend. Er was niet gesteld dat sprake was van een gekwalificeerde elektronische handtekening. De rechtbank Noord-Holland onderzocht daarom of de methode die voor ondertekening was gebruikt, voldoende betrouwbaar was. Dat was niet het geval, omdat de handtekening was gezet op een tablet die een werknemer van de IT-leverancier bij zich droeg in een omgeving die door de IT-leverancier of een door hem ingeschakelde partij werd beheerd. Wat er vervolgens met de handtekening gebeurde, was onvoldoende te controleren, aldus de rechtbank.

Thuiskopievergoeding cloudopslagdiensten

Het Hof van Justitie van de EU heeft zich uitgesproken over de vergoeding voor het maken van privékopieën door cloudopslagdiensten, in Nederland bekend als de thuiskopievergoeding. Op grond van richtlijn 2001/29 kunnen lidstaten een nationale regeling treffen omtrent het reproduceren van auteursrechtelijk beschermde werken, bijvoorbeeld het opslaan van muziek op een mobiele telefoon. Een Oostenrijkse rechtbank had het Hof verzocht om zich uit te laten over de vraag of het privégebruik van cloudopslagdiensten onder de reikwijdte valt van richtlijn 2001/29. Het Hof kwam tot de conclusie dat het uploaden van content naar een aan de gebruiker ter beschikking gestelde opslaglocatie, zoals een server, een reproductie is. Ook oordeelde het Hof dat een dergelijke server een ‘drager’ is zoals bedoeld in de richtlijn. Het staat lidstaten daarom vrij een nationale regeling te treffen op grond waarvan cloudopslagdiensten een compensatie moeten betalen voor het opslaan van auteursrechtelijk beschermde privékopieën door natuurlijke personen.

Meer weten?

Neem contact op met ons team IT&IT-outsourcing:

Annemarie Bolscher

Ernst-Jan Louwers

Frank Rutgers

Sven van Dooren

Pieter de Laat