ICT Projecten

Inhoudsopgave

Inleiding

ICT-projecten mislukken vaak. Te vaak. Iedereen kent de koppen uit de krant over mislukte overheidsprojecten zoals de modernisering van de Gemeentelijke Basisadministratie, de OV-chipkaart etc. Ook in de private sector mislukken ICT-projecten met grote regelmaat.

Het marktonderzoeksbureau Standish Group International voert sinds 1994 door middel van case studies onderzoek uit naar het slagen en falen van ICT-projecten. De onderzochte projecten worden ingedeeld in drie categorieën: geslaagd, mislukt en problematisch. 'Geslaagd' betekent dat het project binnen de planning en begroting is afgesloten. 'Mislukt' betekent dat het systeem niet in gebruik is genomen. De categorie 'problematische' projecten zijn niet 'mislukt' of 'geslaagd', maar duurden langer dan gepland, kosten meer dan gebudgetteerd en bieden minder functionaliteit en/of kwaliteit dan overeengekomen of verwacht. Volgens recente cijfers van Standish Group International mislukt 31,1% van de ICT-projecten en is slechts 16,2% van de projecten geslaagd. Dat wil zeggen dat slechts 16,2% van de projecten op tijd en binnen de begroting is afgerond en de beoogde functionaliteiten en kwaliteit bevat.

De Clercq begeleidt al bijna 25 jaar ICT-projecten, zowel aan de kant van de aanbieders (de ICT-leveranciers) als de afnemers (de opdrachtgever van een ICT-project). Ook worden wij regelmatig ingeschakeld door partijen in een project dat is mislukt of dreigt te mislukken. Door onze ruime ervaring in projecten en door een jarenlange analyse van afgesloten of afgebroken ICT-projecten zijn de faalfactoren van ICT-projecten ons bekend. Dit is de reden dat wij graag onze kennis en ervaring delen met onze cliënten en relaties door middel van bijeenkomsten en publicaties. Ter gelegenheid van ons seminar over ICT-projecten in november 2022, leek het ons goed onze publicaties te bundelen in dit boekje. Wij hopen je hiermee een beknopt naslagwerk te bieden met aandachtspunten voor ICT-projecten en contracten.

Wij wensen iedereen veel leesplezier toe. Eventuele suggesties of aanvullingen uit de praktijk zijn uiteraard van harte welkom. Laten we met elkaar proberen ICT-projecten succesvoller te maken.

Natascha H.A. van Duuren
Partner IT, IE & Privacy De Clercq
November 2022

1. Twee valkuilen bij (inschrijven op) een ICT-overheidsopdracht

Misschien vraag je je wel eens af wat de grootste valkuil is bij inschrijven op een (IT-)aanbesteding. Als inschrijver wil je die valkuilen immers vermijden en als aanbestedende dienst zijn dit juist aspecten waarover je duidelijkheid wil geven in de aanbestedingsdocumentatie. Helderheid hierover kan voor beide spelers discussie voorkomen. Onafgebroken zien wij afgelopen jaren dat de grootste valkuil voor inschrijvers eenvoudige vergissingen zijn. Een andere valkuil is het leerstuk van rechtsverwerking.

Eerste valkuil: vergissingen

Denk bij eenvoudige vergissingen aan een vergeten vinkje in het Uniform Europees Aanbestedingsdocument (UEA). Maar ook gedacht kan worden aan meer bewuste gemaakte vergissingen. Zoals het bewust niet invullen van de vraag in het UEA wie als onderaannemer zal optreden, aangezien die informatie al wordt verstrekt op een andere plek in de inschrijving (in een bijlage met de veelzeggende naam 'Verklaring onderaannemer'). Hoe ga je als inschrijver of aanbestedende dienst om met die situatie? Sluit je als aanbestedende dienst genadeloos die inschrijver uit? Gooi je als inschrijver meteen de handdoek in de ring? Of bestaat recht op herstel van de inschrijving?

Herstel van het Uniform Europees Aanbestedingsdocument?

Ten aanzien van het UEA was de jurisprudentie over het algemeen zeer terughoudend. Illustratief voor die terughoudendheid is een uitspraak van de Rechtbank Den Haag uit 2019 waarin een inschrijver vergeten was één vraag te beantwoorden. Dit was voor risico van de inschrijver: de inschrijver is verantwoordelijk voor het indienen van de juiste en volledig ingevulde stukken en dient daarmee zorgvuldig om te gaan.

In december 2021 deed het Hof Arnhem-Leeuwarden een baanbrekende uitspraak waarin wij met succes de inschrijver bijstonden. De inschrijver had een vraag in de UEA onbeantwoord gelaten. Het betrof de vraag of de inschrijver haar belastingen en sociale premies had voldaan. De aanbestedende dienst was glashelder: herstel van het UEA is niet toegestaan. Het Hof oordeelde dat objectief kan worden vastgesteld hoe deze (onbeantwoorde) vraag beantwoord had moeten worden. In de verificatiefase kan de aanbestedende dienst immers een bewijsstuk vragen waaruit objectief blijkt of het 'herstelde en nagekomen' antwoord juist is geweest. De aanbestedende dienst moest daarom toestaan dat de inschrijver de ingediende UEA aanvulde.

Bijzonder was dat het Hof zelfs toestond dat meerdere(!) ontbrekende antwoorden werden aangevuld, zoals ook de onbeantwoorde vraag welke partij als onderaannemer zou optreden. Veelzeggend voor de welwillendheid is de overweging van het Hof:

> **"***Hierbij moet worden bedacht dat fouten zelden alleen komen, en de beginselen van gelijkheid en transparantie niet verlangen dat een inschrijver daarop wordt afgerekend.***"**

Daarmee lijkt de rechtspraak zoekende naar een meer menselijke maat in het aanbestedingsrecht. Het is niet langer ondenkbaar dat meerdere ontbrekende antwoorden in het UEA alsnog mogen worden ingevuld. Die beweging naar minder formalisme komt overeen met de wens van de wetgever die ook initiatieven neemt in de zoektocht naar minder formalisme.

Ontbrekende formulieren?

Je kunt denken 'één zwaluw maakt nog geen zomer', maar niet alleen het Hof Arnhem-Leeuwarden heeft het afgelopen jaar die menselijke maat laten zien. Ook lagere rechters laten die beweging zien, bijvoorbeeld in een geschil over de mega-aanbesteding Road2021 voor datacenterdienstverlening.

Leverancier Protinus was daarbij als vijfde geëindigd. Zij wilde alsnog tot de raamovereenkomst toetreden en had daarvoor een haakje gevonden. Zij richtte haar pijlen op de inschrijving van Computacenter. Bij de inschrijving van Computacenter ontbrak namelijk het formulier met de veelzeggende naam – 'onderaannemers'. Duidelijk was wel wie de onderaannemer zou worden, want de onderaannemer was opgevoerd in het UEA. Kort samengevat oordeelt de rechter dat het 'level playing field' niet is geschaad. Op basis van het UEA was duidelijk wie de onderaannemer zou worden. Dat het formulier 'Onderaannemers' volledig ontbrak, is niet relevant volgens het Hof: de informatie die het formulier beoogde te verkrijgen is opgenomen, elders in de inschrijving. Ook in deze uitspraak toont het Hof zich vergevingsgezind jegens een inschrijver die een menselijke fout maakt. Wat ons betreft een goede ontwikkeling, zolang de beginselen van het aanbestedingsrecht – waaronder met name gelijke behandeling en transparantie – niet worden geschonden.

Te klein lettertype?

Dat roept de vraag op hoe sterk die wens tot minder formalisme is. Wat als je, bijvoorbeeld in een plan van aanpak, een te klein lettertype hanteert? De Haagse voorzieningenrechter trok daar de grens en sloot die inschrijving uit, met als toelichting dat die eis tot gevolg moet hebben dat alle inschrijvers evenveel ruimte ter beschikking hebben. Maakt het aantal gehanteerde woorden dan nog uit? Nee, volgens de rechter is het niet relevant of de meer beschikbare ruimte ook daadwerkelijk is gebruikt. Een formele insteek dus, ondanks dat het niet gebruiken van de extra verkregen ruimte een

zeer sterke aanwijzing is voor een (herstelbare) vergissing. In deze kwestie was de rechtbank duidelijk nog niet toe aan minder formalisme.

Waar ligt de grens?

De Europese wetgeving die ten grondslag ligt aan de Nederlandse Aanbestedingswet bevat al jaren de mogelijkheid om – onder omstandigheden – fouten door inschrijvers te laten herstellen.[1] Die mogelijkheid wordt ingekleurd door rechters. De lijn die wij afgelopen jaren in de rechtspraak zagen, zouden wij samenvatten als 'fouten zijn voor rekening van de inschrijver'.

Het afgelopen jaar is een duidelijke beweging zichtbaar waarbij men zoekt naar ruimte om herstel mogelijk te maken. Om de grens van het 'herstelbare' te bepalen wordt aansluiting gezocht bij de doelstelling van een aanbesteding: het openstellen van overheidsopdrachten voor mededinging. Om dit doel te bereiken moet een aanbestedende dienst onderzoeken of een vormfout zich voor herstel leent. Een inschrijving die alle informatie bevat, alleen niet op de juiste plaats, mag worden hersteld (aldus het Hof Arnhem-Leeuwarden). Uitsluiting om die reden schaadt namelijk eerder de mededinging dan dat dit de mededinging bevordert.

Wanneer volgt dan nog uitsluiting? Als herstel zou leiden tot ongelijke behandeling of schending van het transparantiebeginsel. Daarvan is sprake als niet objectief kan worden aangetoond wat het ontbrekende antwoord, ten tijde van de inschrijving, zou zijn geweest. Dan wordt de aanvulling, verduidelijking of verbetering namelijk gezien als een nieuwe inschrijving. Dat is de niet te overschrijden grens waarbij een fout voor rekening van de inschrijver blijft.

Foutieve beantwoording vraag UEA?

Komende jaren zal blijken hoe bestendig die lijn tot het toestaan van herstel is. Recent maakte een voorzieningenrechter nog een terugtrekkende beweging in een kwestie waarin de inschrijver in zijn UEA een vraag foutief had beantwoord. Het betrof de vraag of de inschrijver de afgelopen drie jaar een positief eigen vermogen had. Een inschrijver gaf hierop aan 'ja', terwijl zij kort daarna ontdekte dat uit haar jaarrekening blijkt dat zij geen positief eigen vermogen had. Een vergissing.

De inschrijver ontdekt de fout zelf en stuurde direct de aanbestedende dienst een brief waarin zij deze vergissing aangaf. De aanbestedende dienst sluit vervolgens de inschrijver uit en geeft daarbij aan dat ook nog eens sprake is van een valse verklaring(!). Dit heeft grote gevolgen voor toekomstige inschrijvingen, aangezien die inschrijver dan bij toekomstige inschrijvingen – gedurende drie jaar – zal moeten melden dat zij in het verleden is uitgesloten wegens een valse verklaring op grond van artikel 2.87 onder h Aw.

[1] Artikel 56 lid 3 van Richtlijn 2014/24/EU.

Het oordeel

De rechter oordeelt in een korte overweging dat de verklaring feitelijk onjuist is en dat de inschrijver zich voor het indienen beter had moeten vergewissen van de (on)juistheid van haar inschrijving.[2] Het bezwaar van de inschrijver, inhoudende dat geen sprake zou zijn van een valse verklaring, wordt afgewezen.

Ontbrekende argumenten

Opvallend is dat in het vonnis geen aandacht wordt besteed aan relevante jurisprudentie die door het Europese Hof is gewezen. Vermoedelijk is dit door de inschrijver niet aangedragen. Uit een uitspraak van het Europese Hof blijkt namelijk dat 'opzet' niet is vereist, maar wel dat sprake moet zijn van "nalatigheid van een zekere ernst".[3] Aangezien de inschrijver de fout in haar UEA zelf heeft gemeld en kennelijk geen kwade bedoeling had, ligt het in de rede dat aan voornoemd criterium in ieder geval zou worden getoetst.

Ook is geen verwijzing te lezen naar de Gids Proportionaliteit waarin is opgenomen dat deze uitsluitingsgrond terughoudend moet worden toegepast en dat deze is bedoeld voor kwesties waarin de integriteit ter discussie staat (p. 37). Het is dus zeer de vraag of alle relevante argumenten in deze kwestie naar voren zijn gebracht en hoe maatgevend dit oordeel is. In de rechtspraak zagen wij een lijn die is samen te vatten als 'fouten zijn voor rekening van de inschrijver'. Inmiddels is een duidelijke beweging zichtbaar waarbij wordt gezocht naar ruimte om herstel mogelijk te maken. We hebben gezien dat voor nu een inschrijving die alle informatie bevat, alleen niet op de juiste plaats, mag worden hersteld.

Tweede valkuil: een te beperkte proactieve houding

Een andere valkuil wordt gevormd door het formalistische karakter van aanbestedingen. Aanbestedingsdocumenten zijn doorvlochten met rechtsverwerkingsclausules, bijvoorbeeld dat een inschrijver – na het uiten van bezwaren die door de aanbestedende dienst worden afgewezen – nog voor de sluitingstermijn van de inschrijving een procedure moet starten. Doet die inschrijver dat niet, dan mag hij niet meer klagen.

Inschrijvers zijn zich vaak niet bewust van de omvang van de proactieve houding die van hen wordt verlangd rond de rechtsverwerking, ofwel het formalistische karakter van aanbestedingen. Het adagium 'wie zwijgt, stemt toe' geldt dan en heeft tot gevolg dat menig klagende inschrijver zijn recht om te klagen heeft verwerkt. Ook aanbestedende diensten doen met regelmaat pas een beroep op rechtsverwerking nadat zij door hun raadslieden op die (juridische) mogelijkheid zijn gewezen. Voor beide kanten geldt

[2] Rb. Oost-Brabant 6 juni 2022, ECLI:NL:RBOBR:2022:2473.
[3] HvJEU, 4 mei 2017, ECLI:EU:C:2017:338, C-387/14, r.o. 71.

partijen zich vaak laten leiden door de inhoud van de discussie en daarbij de formele verweren uit het oog verliezen.

In een aanbesteding op het gebied van IT leidden bezwaren van inschrijver Protinus niet tot wijziging van de aanbestedingsdocumenten. De inschrijver schreef vervolgens gewoon in. Pas nadat duidelijk was dat die inschrijver niet had gewonnen, besloot zij alsnog een procedure te starten. De rechtbank, en aansluitend het Hof, wijzen alle vorderingen af: de clausule is toelaatbaar.

Interessant is wel dat het Hof expliciet aangeeft dat zo'n rechtsverwerkingsclausule (inhoudende dat men moet procederen voor het indienen van de inschrijving op straffe van verval van recht) in *bepaalde* omstandigheden niet is toegestaan. Het Hof geeft een aantal voorbeelden:

1. een aanbesteding met een beperkte waarde waarop wordt ingeschreven door het midden- en kleinbedrijf, en
2. een aanbesteding van een grote opdracht waarbij wordt getoetst aan subjectieve en daarmee minder goed controleerbare criteria waarbij de vrees bestaat dat de gerechtelijke procedure doorwerkt in de latere beoordeling.

In beide gevallen kan in de regel niet van inschrijvers worden geëist dat zij al vóór het indienen van hun inschrijving hun bezwaren tegen een aanbesteding aan de rechter in kort geding voorleggen. Het hof zet dus de deur op een kier naar minder formalisme. Deze uitspraak laat helder zien dat het leerstuk van rechtsverwerking ook voor ervaren inschrijvers nog steeds een valkuil kan zijn en dat ondanks het formele karakter er toch twee uitzonderingen zijn om die valkuil zonder kleerscheuren te passeren.

De Clercq *takeaways*

- Een eerste valkuil die zich voor kan doen bij inschrijvingen op IT-aanbestedingen zijn vergissingen in de aangeleverde stukken. In beginsel is een inschrijver namelijk verantwoordelijk voor het indienen van de juiste en volledig ingevulde stukken ten aanzien van het UEA. Echter, in 2021 bepaalde het Hof dat een aanbestedende dienst moet toestaan dat een inschrijver de ingediende UEA op een later moment aanvult. Dit past in een bredere trend, waarin de rechtspraak op zoek lijkt naar meer menselijke maat in aanbestedingsprojecten. Tegelijkertijd zit er nog steeds wel een grens aan deze minder formalistische houding. Zo oordeelde de rechter dat het hanteren van een te klein lettertype alsnog kan resulteren in uitsluiting van de inschrijving, aangezien alle inschrijvers evenveel ruimte moeten hebben.
- Ondertussen is er ook een duidelijke beweging zichtbaar waarbij men zoekt naar ruimte om herstel mogelijk te maken. Een aanbestedende dienst moet hiertoe – gelet met het doel van de aanbesteding in het achterhoofd – onderzoeken of een

vormfout zich voor herstel leent. Geen herstel is mogelijk als dit leidt tot ongelijke behandeling of schending van het transpiratiebeginsel. Dergelijke gevallen leiden dus alsnog tot uitsluiting. Gebleken is dat ontbrekende informatie in een inschrijving niet fataal hoeft te zijn en dat een aanbestedende dienst niet zomaar tot uitsluiting kan en mag overgaan.

- Een tweede valkuil bij IT-aanbestedingen is een verminderd proactieve houding van inschrijvers. Want ondanks dat uit rechtspraak blijkt dat in de regel niet van inschrijvers kan worden geëist dat zij al vóór het indienen van hun inschrijving hun bezwaren tegen een aanbesteding aan de rechter in kort geding voorleggen en dus ook hier de rechter de deur op een kier lijkt te zetten naar minder formalisme, is rechtsverwerking ook voor ervaren inschrijvers nog steeds een valkuil. Gelukkig zijn er twee uitzonderingen om deze valkuil zonder kleerscheuren te passeren.

2. Private ICT-aanbesteding

Private partijen zijn – in tegenstelling tot aanbestedende diensten – niet verplicht een opdracht te 'plaatsen' door middel van een aanbestedingsprocedure. Vaak heerst de gedachte dat private partijen geen enkele rekening hoeven te houden met het aanbestedingsrecht. Die gedachte is echter een onjuist. Wanneer een private partij vrijwillig een aanbestedingsprocedure start, is zij – zelfs indien zij het geen aanbesteding noemt – gehouden het spel volgens bepaalde regels te spelen. Zo kan het voorkomen dat uiteindelijk de opdracht moet worden gegund aan de partij die niet de voorkeur heeft. In de afgelopen tien jaar zijn er veel ontwikkelingen geweest ten aanzien van private aanbestedingen. De Hoge Raad heeft zich diverse malen uitgelaten over juridische vraagstukken ten aanzien van private aanbestedingen[4] en vele malen vaker is hierover geprocedeerd bij lagere rechters. Wanneer je als 'private' opdrachtgever meerdere partijen vraagt te offreren, dan is alertheid dus geboden.

Een (private) aanbesteding?

Een eerste vraag is wanneer sprake is van een private aanbesteding. Wellicht denk je op die weg eenvoudig te kunnen wegblijven bij dat mijnenveld. Het antwoord op die vraag is helaas niet eenduidig. De voorzieningenrechter van de Rechtbank Den Haag overwoog bijvoorbeeld al in 2012 dat dit afhankelijk zal zijn van de omstandigheden van het geval. De gebruikte termen in de offerteaanvraag zijn daarbij niet leidend, maar slechts een indicatie. Wanneer een private opdrachtgever een aantal bedrijven vraagt te offreren en dit een aanbesteding noemt, hoeft dus geen sprake te zijn van een aanbesteding. Maar ook andersom kan een offerteaanvraag toch als aanbesteding worden aangemerkt, zelf als geen enkele keer het woord 'aanbesteding' in de documenten of correspondentie voorkomt.

Ook relevante aspecten om te beoordelen of sprake is van een private aanbesteding, zijn de omvang van de private partij, de omvang van de relevante markt, en de verwachtingen die zijn gewekt ten aanzien van de te volgen procedure (denk aan in hoeverre dit aansluit bij een aanbestedingsprocedure).[5] Van belang is ook wat gebruikelijk is binnen de kring waartoe de inschrijvers behoren en dus hetgeen partijen van elkaar mochten verwachten.[6]

[4] Hoge Raad 4 april 2003, ECLI:NL:HR:2003:AF2830; Hoge Raad 3 mei 2013, ECLI:NL:HR:2013:BZ2900; Hoge Raad 8 juli 2016, ECLI:NL:HR:2016:1484.
[5] Hof Arnhem-Leeuwarden 2 juli 2013, ECLI:NL:GHARL:2013:4715, JAAN 2013, p. 149 (PG Goutum/Smederij, r.o. 6.4.
[6] Rb. Den Haag 30 januari 2015, ECLI:NL:RBDHA:2015:926, r.o. 4.4.

Wanneer bij het opvragen van offertes wordt aangegeven wat de beoordelingsprocedure zal inhouden en wat de gunningscriteria zijn, dan zal al snel sprake zijn van een private aanbesteding.[7] Een beoordelingsprocedure en vooraf bekendgemaakte gunningscriteria zijn immers essentieel kenmerken van een 'aanbesteding'. Het vervolgens niet gunnen van de opdracht op onvoorziene gronden is dan toegestaan, maar brengt wel de verplichting mee om de schade te vergoeden die de beoogde winnaar lijdt.[8]

De grondslag

Dat brengt ons bij het juridische kader. Hoe kan een private onderneming onbewust in aanraking komen het aanbestedingsrecht? De grondslag hiervoor is niet de Aanbestedingswet. De daarin opgenomen procedures gelden immers voor aanbestedende diensten en dat zijn private opdrachtgevers niet.

De sleutel zit in de precontractuele redelijkheid en billijkheid. Die redelijkheid en billijkheid kunnen ertoe leiden dat de algemene beginselen van het aanbestedingsrecht van toepassing worden op een private aanbesteding. Wat zijn die beginselen die via deze achterdeur naar binnen komen? Het gaat het om:

- het *gelijkheidsbeginsel*, ook wel het non-discriminatiebeginsel (op grond waarvan inschrijvers op een gelijke en niet-discriminerende wijze moeten worden behandeld);
- het *transparantiebeginsel* (op grond waarvan aan inschrijvers een bepaalde mate van transparantie moet worden geboden, bijvoorbeeld ten aanzien van de te hanteren gunningscriteria of de motivering van de gunningsbeslissing); en
- het *proportionaliteitsbeginsel* (op grond waarvan bijvoorbeeld te stellen eisen in verhouding moeten staan tot de aard en omvang van de opdracht).

Een praktisch gevolg is dat bijvoorbeeld niet de winnende inschrijver mag worden gepasseerd (zonder schadeplichtigheid). Iets wat overigens KLM – als private onderneming – wel deed toen zij op zoek was naar een nieuwe leverancier voor schoonmaakdiensten. Die zaak kwam uiteindelijk bij de Hoge Raad.[9] Dat arrest bevat de uitgangspunten die in latere jurisprudentie zijn uitgewerkt.[10] De kern daarvan lees je hierna.

De kern

In de kern kan als algemeen uitgangspunt worden gehanteerd dat de beginselen van het aanbestedingsrecht van toepassing zijn als het een private opdrachtgever betreft die:

[7] Rb. Limburg 19 juni 2018, ECLI:NL:RBLIM:2018:5956, (Monsdal/Daelzicht), r.o. 4.3.
[8] Rb. Limburg 19 juni 2018, ECLI:NL:RBLIM:2018:5956, (Monsdal/Daelzicht).
[9] Hoge Raad 3 mei 2013, ECLI:NL:HR:2013:BZ2900, NJ 2013, p. 572 (KLM/CCC).
[10] Hof Arnhem-Leeuwarden 2 juli 2013, ECLI:NL:GHARL:2013:4715, (PG Goutum/Smederij); Hof Den Haag, 30 september 2014, ECLI:NL:GHDHA:2014:3028.

- een *kleine* speler is op de relevante markt van de opdracht én deze zich in de offerteaanvraag uitdrukkelijk heeft verbonden aan de beginselen van het aanbestedingsrecht; of
- een *grote* speler is op de relevante markt van de opdracht én de beginselen van het aanbestedingsrecht niet uitdrukkelijk zijn uitgesloten of daarvan is afgeweken.

Relevant is echter om te realiseren dat het Hof Den Haag in het eerder genoemde voorbeeld van KLM nog een voorbehoud lijkt te maken, inhoudende dat de vrijheid om de beginselen buitenwerking te stellen uitzondering kan leiden als de bijzondere omstandigheden van het geval meebrengen dat naar maatstaven van redelijkheid en billijkheid die buitenwerkingstelling onaanvaardbaar zou zijn.[11]

De Clercq *takeaways*

Uit de huidige stand van zaken in de jurisprudentie kunnen een aantal adviezen worden gedestilleerd. Private opdrachtgevers zouden erop moeten letten om:

- transparant te communiceren met de partijen bij wie aanvraag voor een offerte wordt neergelegd;
- in de aanbestedingsvoorwaarden uitdrukkelijk aan te geven of de beginselen van het aanbestedingsrecht van toepassing zijn op de offerteaanvraag;
- desgewenst de toepasselijkheid van de beginselen van het aanbestedingsrecht uit te sluiten;
- heldere voorbehouden te maken, zoals:
    - het recht om bij onduidelijkheden een redelijke uitleg te mogen geven;[12]
    - een beding dat pas een overeenkomst tot stand komt bij ondertekening van de te gunnen overeenkomst; en
    - het recht om zonder schadeplichtigheid over te gaan tot beëindiging van het offertetraject.

[11] Hoge Raad 3 mei 2013, ECLI:NL:HR:2013:BZ2900 (KLM) en later Hof Den Haag 4 november 2014 ECLI:NL:GHDHA:2014:3501 (KLM).
[12] Rb. Den Haag 30 januari 2015, ECLI:NL:RBDHA:2015:926, r.o. 4.4.

3. Een DPIA: wanneer is het verplicht en hoe pak je dat aan?

Het uitvoeren van een zogenoemde gegevensbeschermingseffectbeoordeling — vaak beter bekend onder de Engelstalige naam Data Protection Impact Assessment (DPIA) — is voor iedere organisatie verplicht op grond van de Europese privacywet, wanneer de beoogde verwerking van persoonsgegevens een 'hoog privacy risico' kent. Een DPIA is in feite een (schriftelijk) onderzoek waarin de voorgenomen verwerking wordt getoetst aan de toepasselijke privacywet- en regelgeving. DPIA's moeten aan bepaalde eisen voldoen en zullen binnen een organisatie een bepaald proces behoren te doorlopen. Voor het uitvoeren ervan zijn diverse modellen beschikbaar.

Wanneer verplicht?

Een DPIA is wettelijk verplicht voor alle verwerkingen van persoonsgegevens die waarschijnlijk een hoog risico met zich meebrengen.[13] Doorgaans gebeurt dat vooraf, hetgeen in beginsel ook moet.[14] Voor een aantal verwerkingen is vastgesteld dat het uitvoeren van een DPIA altijd verplicht is.[15] Hierbij kan worden gedacht aan profilering, het gebruik van monitoring, cameratoezicht, zwarte lijsten, het (op grote schaal) verwerken van bijzondere persoonsgegevens[16] of gevoelige gegevens[17], het delen van deze gegevens in samenwerkingsverbanden, het samenvoegen van datasets of het gebruik van nieuwe technologische of organisatorische oplossingen.[18]

De verplichting tot het (laten) uitvoeren van een DPIA ligt bij de verwerkingsverantwoordelijke. Wie is nu de 'verwerkingsverantwoordelijke'? De 'verwerkingsverantwoordelijke' bepaalt de doeleinden waarvoor en de middelen

[13] Artikel 35(1) Algemene Verordening Gegevensbescherming (AVG).

[14] Artikel 35(1) en overweging 90 AVG. Uiteraard is het ook relevant om voor verwerkingen waarvoor DPIA's verplicht zijn en die reeds zijn gestart alsnog een DPIA uit te voeren, mocht dat nog niet zijn gedaan.

[15] Deze verwerkingen zijn aangemerkt als hoog risico in de 'Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679', zoals laatstelijk gewijzigd en vastgesteld op 4 april 2017 van de Artikel 29-Werkgroep (tegenwoordig: European Data Protection Board) en *Stct.* 2019, nr. 64418.

[16] Dit zijn gegevens die iets zeggen over iemands ras, etnische afkomst, politieke, religieuze of levensbeschouwelijke opvattingen, seksuele leven en lidmaatschap van een vakbond. Daarnaast omvat dit genetische gegevens, biometrische gegevens en gezondheidsgegevens. Zie ook artikel 9(1) AVG. Het Burgerservicenummer wordt vaak ook onder deze categorie gegevens geschaard, vanwege de zeer beperkte voorwaarden waaronder deze mag worden verwerkt. Zie ook artikel 87 AVG jo artikel 46 Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG).

[17] Dit zijn gegevens die niet zijn aangemerkt als bijzondere persoonsgegevens in de AVG, maar die in het maatschappelijk verkeer wel als gevoelig worden beschouwd zoals: gegevens over iemands beroepsprestaties, financiële of economische situatie, persoonlijke voorkeuren of interesses, privé problematiek, betrouwbaarheid of gedrag, locatie of verplaatsingen, gegevens uit persoonlijke documenten en inloggegevens.

[18] Zie ook overweging 89 en 91 AVG.

waarmee persoonsgegevens worden verwerkt. Als uw onderneming/organisatie dus beslist *waarom* en *hoe* persoonsgegevens moeten worden verwerkt, is zij de verwerkingsverantwoordelijke. Indien er een verwerker in het spel is, is deze verplicht conform afspraken uit de verwerkersovereenkomst de verwerkingsverantwoordelijke bij de DPIA te ondersteunen.

Uitvoering

Voor het uitvoeren van een DPIA dient een organisatie zelf een model en/of methode te kiezen of te creëren. Er zijn verschillende modellen in omloop. Modellen die bijvoorbeeld (ter inspiratie) zouden kunnen worden gebruikt:

- NOREA (zeer uitgebreid en daarmee bijv. geschikt voor zeer risicovolle verwerkingen);
- CNIL (afkomstig van de Franse privacytoezichthouder en beschikbaar gesteld samen met tooling om het DPIA-proces digitaal te kunnen doorlopen en diverse uitleg);
- Criteria samengesteld door de Artikel 29-Werkgroep (met name geschikt ter inspiratie voor het creëren van een eigen DPIA-model);
- ICO (afkomstig van de Engelse privacytoezichthouder, een kort en bondig model dat kan worden gebruikt voor 'light' DPIA's).

Veel organisaties kiezen ervoor om niet alleen voor verplichte verwerkingen een DPIA uit te voeren, maar ook voor verwerkingen waarvan nog niet vaststaat of sprake is van een (hoog) privacy risico of waarbij de organisatie een groot belang heeft. Om die reden worden binnen organisaties vaak twee modellen gebruikt: één model voor de verwerkingen waarvoor een DPIA verplicht is (zoals het migreren van de gehele digitale omgeving naar de Cloud) en één light model voor de minder risicovolle verwerkingen of voor verwerkingen waarvan de risico's nog niet goed zijn te overzien (zoals voor het in gebruik nemen van een nieuwe evenemententool).

Benodigde personen en functies

Voor het schrijven van een DPIA zijn in ieder geval personen nodig met kennis over:

1. Het project/proces/systeem waarop de DPIA ziet;
2. De organisatie van de verwerkingsverantwoordelijke;
3. De privacywet- en regelgeving;
4. De techniek en mogelijke technische en organisatorische beveiligingsmaatregelen; en
5. De werkwijze/het product van de verwerker, wanneer de verwerking door een verwerker wordt uitgevoerd.

Veelal wordt een projectteam samengesteld om een DPIA uit te voeren, waarbij iedere expertise om input wordt gevraagd. De Clercq wordt vaak gevraagd onderdeel uit te maken van dit projectteam.

Tijdstip van starten en termijnen
Qua doorlooptijd, duurt een volledige DPIA gemiddeld drie maanden. Dit komt, doordat vanuit verschillende hoeken expertise benodigd is en vaak meerdere afstem-, review- en adviesrondes nodig zijn voordat een DPIA definitief is. Light DPIA's kosten gemiddeld twee weken, omdat hier minder diep op alle risico's en eisen wordt ingezoomd.

Als een DPIA ziet op een in te kopen product, is het raadzaam om reeds in de uitvraag informatie over informatiebeveiliging en privacy op te vragen. Zodra dit binnen is, zou een light DPIA kunnen worden uitgevoerd. Op die manier kan bij de keuze voor een product namelijk al rekening worden gehouden met informatiebeveiliging en privacy. Als de keuze voor een product eenmaal vaststaat, kan een volledige DPIA worden uitgevoerd. Op die manier werkt de privacy- en informatiebeveiligingstoets zo min mogelijk vertragend, maar kan wel aan wettelijke eisen worden voldaan.

Een vergelijkbare strategie is raadzaam voor nieuwe ideeën of plannen binnen een organisatie. Als deze in hoofdlijnen bekend zijn, kan al een light toets worden uitgevoerd om te verifiëren of aan alle relevante elementen is gedacht. Daarbij kan op die manier al de hoogte van het risico in kaart worden gebracht. Als vervolgens de plannen concreet zijn, kan de volledige DPIA worden uitgevoerd.

Verplichte adviezen
Als binnen de organisatie van de verwerkingsverantwoordelijken een Functionaris voor gegevensbescherming (FG) is aangesteld, is het verplicht om deze FG om advies te vragen over de DPIA. De FG is vervolgens vrij om te bepalen of hij/zij wel/geen advies wil geven en in welke vorm. Gegeven FG-advies moet aan de DPIA worden toegevoegd. Indien het advies van de FG niet wordt opgevolgd, dient gemotiveerd te worden vastgelegd waarom niet.

Als uit de DPIA grote privacyrisico's naar voren komen die niet kunnen worden verminderd, is een voorafgaande raadpleging van de Autoriteit Persoonsgegevens (AP, de Nederlandse privacytoezichthouder) vereist. De AP verschaft vervolgens ook advies, en kan al haar bevoegdheden (denk aan het instellen van onderzoeken en nemen van corrigerende maatregelen) uitoefenen.

In voorkomend geval, moet ook de mening van betrokkenen of hun vertegenwoordigers worden gevraagd (bijv. middels een enquête). Zo kan bijvoorbeeld de mening van medewerkers worden gevraagd wanneer de DPIA ziet op een medewerkersonderzoek, of de mening van een consumentenorganisatie wanneer de DPIA ziet op het opbouwen van klantprofielen. De verkregen meningen moeten worden vastgelegd in de DPIA. Als de verwerkingsverantwoordelijke besluit om niet naar de mening van betrokkenen te

vragen en/of de uitkomst daarvan niet op te volgen, moet dit eveneens gemotiveerd worden vastgelegd.

DPIA-beleid

Om het DPIA-proces te borgen is het belangrijk dat binnen de organisatie van de verwerkingsverantwoordelijke wordt vastgelegd:

- Waar risicovolle verwerkingen binnen de organisatie dienen te worden gemeld;
- Wanneer het uitvoeren van een DPIA verplicht is;
- Welke medewerkers bij het uitvoeren van een DPIA worden betrokken, wie verantwoordelijk is en hoe de route naar de FG werkt;
- Welk DPIA-model moet worden gebruikt, en waar dit te vinden is;
- Waar de DPIA moet worden opgeslagen en geregistreerd; en
- Hoe wordt geborgd dat de DPIA periodiek wordt geüpdatet.

De Clercq *takeaways*

- Zorg dat voor alle verwerkingen waarvoor een DPIA verplicht is, een DPIA wordt gedaan.
- Kies of creëer een DPIA-model dat aansluit bij de organisatie, en gebruik bij voorkeur twee DPIA-modellen (één uitgebreide versie voor verplichte zaken en één light versie voor overige zaken waarvoor een voorafgaand privacy- en informatiebeveiligingsonderzoek gewenst is).
- Zorg dat in de DPIA of in een separaat assessment wordt getoetst of passende technische en organisatorische maatregelen zijn genomen en bekijk of het mogelijk is om met (aanvullende) beveiligingsmaatregelen de privacy risico's te verminderen.
- Stel voor iedere DPIA een team samen van personen met de benodigde expertise, betrek hierbij (indien relevant) de verwerker en vraag (indien relevant) om advies van de FG, de AP en/of de mening van de betrokkenen.
- Stel een DPIA-beleid op waarin wordt gespecificeerd hoe, door wie en op welke manier binnen de organisatie wordt omgegaan met de DPIA-verplichting en maak duidelijke afspraken over DPIA's met verwerkers.

4. Privacy en Security by Design: wat is dat precies?

Cyberaanvallen en datalekken staan bovenaan de lijst met risico's die bestuurders het meeste zorgen baren. Dit is niet zonder reden. Datalekken zijn aan de orde van de dag en cyberaanvallen nemen steeds meer toe. 'Privacy by Design', 'Privacy by Default' en 'Security by Design' zijn begrippen die in dit kader vaak worden gebruikt. Wat betekenen deze begrippen precies en wat betekenen deze begrippen concreet voor organisaties en bedrijven?

Wat is 'Privacy by Design'?

Het begrip Privacy by Design is al in de jaren 90 geïntroduceerd door Canadese privacy toezichthouder Ann Cavoukian. Zij was van mening dat niet alleen technische, maar ook organisatorische en fysieke maatregelen tijdens de volledige levenscyclus (van begin tot eind), essentieel zijn voor het behoud van privacy.

Inmiddels zijn de beginselen van Privacy by Design in onze wet- en regelgeving verankerd. Zo leggen onze Algemene Verordening Gegevensbescherming (AVG) Privacy by Design (artikel 25 lid 1 AVG) en Privacy by Default (artikel 25 lid 2 AVG) als verplichting op, ook al worden deze termen niet expliciet genoemd. De verplichting blijft helaas wat abstract en is weinig concreet.

Artikel 25 lid 1 AVG noemt slechts twee concrete verplichtingen:

1. Dataminimalisatie: alleen strikt noodzakelijke gegevens verzamelen; en
2. Pseudominiseren: ervoor zorgen dat de persoonsgegevens niet meer aan specifieke betrokkene kunnen worden gekoppeld.[19]

Verder bevat de AVG een aantal afzonderlijke bepalingen met verplichtingen die nauw samenhangen met Privacy by Design en Privacy by Default. Je kunt het ook anders stellen: om te kunnen voldoen aan deze verplichtingen is het noodzakelijk Privacy by Design toe te passen:

1. Encryptie; of
2. Bewaren.[20]

Uitleg in de praktijk

De vraag is: Hoe moeten deze (deels abstracte) verplichtingen in de praktijk worden uitgevoerd? Welk houvast hebben bedrijven en organisaties daarbij?

[19] Artikel 5 lid 1 sub c AVG resp. artikel 4 lid 5 AVG.
[20] Artikelen 6 lid 4 sub e en 32 lid 1 sub a AVG resp. artikel 5 lid 1 sub e AVG.

In 2015, al voor invoering van de AVG, heeft ENISA in haar rapport '*Privacy and Data Protection by Design – from policy to engineering*' getracht een brug te bouwen tussen "the legal framework" en "the available technologies implementation measures". Vier jaar later heeft de EDPD-richtlijnen gepubliceerd over de toepassing van data protection by design en default. Ondanks de goedbedoelde pogingen bieden de richtlijnen niet het houvast die zij beoogden te bieden. Bestudering van de richtlijnen leidt mijns inziens tot de conclusie dat slechts een aantal voorbeelden en handvatten wordt gegeven, maar dat de richtlijnen toch vrij abstract blijven. Hetzelfde geldt voor het eerder verschenen ENISA-rapport.

Wie is verantwoordelijk voor een juiste toepassing van Security by Design

Op grond van de AVG is Privacy & Security by Design een verplichting van de verwerkingsverantwoordelijke (in veel gevallen de opdrachtgever). De praktijk is echter, dat verwerkingsverantwoordelijken software niet zelf ontwikkelen en dat door de opdrachtgever vaak te weinig eisen worden gesteld aan de beveiliging. Dit heeft tot gevolg dat kwetsbaarheden in de software vaak pas aan het licht komen in de gebruiksfase, soms pas op het moment dat er bijvoorbeeld een cyberincident plaatsvindt. Dat is uiteraard een onwenselijke zaak.

Accountability

Ondanks het feit dat de wet- en regelgeving en aanwezige richtlijnen helaas vrij abstract blijven, is het van belang te realiseren dat de AVG uitgaat van 'accountability'. Dit betekent dat organisaties zullen moeten documenteren op welke wijze zij aan de AVG voldoen. Ook aan Privacy en Security by Design. Voldoet een organisatie niet aan haar documentatieplicht, dan kan zij door de Autoriteit Persoonsgegevens op de vingers worden getikt.

De Clercq *takeaways*

- Documenteer op welke wijze aan de verplichting van Privacy & Security by Design is voldaan.
- Bij een gebrek aan concrete handvatten voor de concrete invulling van Privacy & Security by Design doen organisaties en bedrijven er vooralsnog goed aan de bestaande richtlijnen/baselines te volgen.
- Deze bestaande richtlijnen/baselines dienen uiteraard te worden aangevuld met een risicoanalyse op organisatieniveau.
- Stel ook concrete eisen aan externe developers en aanbieders, zodat ook zij privacy 'van het begin tot het eind' borgen in hun producten.

5. Soorten IT-contracten

Leveranciers van IT-producten en IT-diensten maken gebruik van veel verschillende soorten contracten. Veel van die contracten zijn ontleend aan de Anglo-Amerikaanse rechtspraktijk. Denk aan een *Service Level Agreement*, een *End User License Agreement* of een *Software-as-a-Service* overeenkomst. Deze contractvormen komen als zodanig niet voor in het Nederlands recht en moeten daarom worden ingepast in ons burgerlijk recht. Bij het opstellen van een IT-contract moet dus steeds een 'vertaalslag' worden gemaakt. Waarom dit belangrijk is wordt uitgelegd in dit hoofdstuk.

IT-contracten in de praktijk

In de praktijk wordt gebruikgemaakt van allerlei soorten benamingen bij het sluiten van een overeenkomst ter zake IT-producten en IT-diensten. Veelgebruikte benamingen zijn onder meer:

- Softwareontwikkelingsovereenkomst
- Support- en onderhoudsovereenkomst
- End User License Agreement
- SaaS-overeenkomst
- Samenwerkingsovereenkomst
- Service Level Agreement
- IT-outsourcingsovereenkomst

Koop, huur en opdracht

Het Burgerlijk Wetboek geeft algemene regels voor de totstandkoming, de rechtsgevolgen en de ontbinding van overeenkomsten (Titel 5 Boek 6 BW). Daarnaast bevat het BW specifieke regels die gelden voor een beperkt aantal bij naam genoemde bijzondere overeenkomsten (Boek 7 en 7A BW). Geen van de hierboven genoemde benamingen zul je als zodanig in het BW aantreffen. Er is bijvoorbeeld geen bijzondere regeling voor een SLA of voor een EULA. Wel bevat het BW bijzondere regelingen voor koop, huur en opdracht.[21]

Een overeenkomst op basis waarvan hardware wordt aangeschaft geldt als een koopovereenkomst. Dat zal niet verbazen. Maar ook de aankoop van een licentie voor gebruik van standaardsoftware wordt onder omstandigheden gezien als een overeenkomst waarop de koopregels van toepassing zijn. Dit is het geval als tegen betaling een licentie voor onbepaalde duur wordt verkregen op

[21] Artikel 7:1 BW, resp. artikel 7:201 BW, resp. artikel 7:400 BW.

standaardcomputerprogrammatuur. Het doet er daarbij niet toe of de software ter beschikking wordt gesteld op een gegevensdrager of via download.[22]

Een softwareontwikkelingsovereenkomst, een SaaS-overeenkomst of een support- en onderhoudsovereenkomst zullen dan weer vaak kwalificeren als een overeenkomst van opdracht. Er wordt immers een prestatie geleverd, anders dan op grond van een arbeidsovereenkomst, en deze prestatie bestaat uit iets anders dan het vervaardigen van een fysiek werk, het bewaren van spullen, het uitgeven van werken of het vervoeren van personen of zaken. Bij hostingdiensten of IaaS-diensten zou mogelijk sprake kunnen zijn van huur.[23]

Overeenkomsten kunnen ook een combinatie zijn van verschillende in de wet genoemde overeenkomsten. Zo kan een outsourcingsovereenkomst deels zien op de aanschaf van hardware en deels op het leveren van IT-diensten. Er is dan sprake van een combinatie van koop en opdracht.

Dwingend recht

Sommige regels in het BW zijn van dwingend recht. Dit betekent dat contractpartijen niet de vrijheid hebben om contractueel van die regels af te wijken. Is een contractuele afspraak gemaakt in strijd met dwingend recht dan blijft de contractuele afspraak buiten toepassing.

Dwingendrechtelijke regels beogen vaak de rechtspositie van een 'zwakke' contractpartij te beschermen. Zo mag een consument-opdrachtgever een aangegane overeenkomst van opdracht te allen tijde opzeggen. Dat opzegrecht kan niet contractueel ten nadele van de consument worden beperkt.[24] Ook in de kooptitel en de huurtitel zijn veel regels opgenomen die de consument-koper/huurder beschermen en waarvan niet ten nadele van de consument mag worden afgeweken.

Regelend recht

Interessanter voor de IT-praktijk zijn de regels die van regelend recht zijn. Zulke regels zijn van toepassing, tenzij partijen daarover onderling een afwijkende afspraak hebben gemaakt. Bij het opstellen van een IT-contract is het belangrijk om rekening te houden met dit regelend recht, want juist deze regels kunnen belangrijke gevolgen hebben voor de rechtspositie van partijen.

[22] Hoge Raad 27 april 2012, ECLI:NL:HR:2012:BV1301 (*Hulskamp/De Beeldbrigade*).
[23] J.L. Jonker & J.A. Bal, 'Toepasselijkheid huurtitel 7.4 BW op IT', *Computerrecht* 2015/124.
[24] Artikelen 7:413 en 7:408 BW.

Neem bijvoorbeeld de vergoeding van onkosten. Een opdrachtnemer heeft op grond van de wet recht op vergoeding van loon en onkosten.[25] Een opdrachtgever die met zijn IT-beheerder alleen een uurloon afspreekt, kan gemakkelijk denken dat geen onkosten vergoed hoeven te worden. Het contract zegt immers alleen iets over vergoeding van een uurloon en niets over onkosten. Niets is echter minder waar. Als vergoeding van onkosten niet expliciet is uitgesloten in de overeenkomst kan de IT-beheerder op grond van artikel 7:406 BW met recht betogen dat hij ook onkosten in rekening mag brengen. Als opdrachtgever is het dus zaak in het contract op te nemen dat de opdrachtnemer in het kader van de geleverde diensten alleen recht heeft op de vergoedingen waarin de overeenkomst expliciet voorziet.

Een ander voorbeeld. Wanneer IT-diensten worden gecontracteerd voor meerdere groepsmaatschappijen is het van belang rekening te houden met artikel 7:407 lid 1 BW. Dit artikel zegt dat als een opdracht wordt gegeven door twee of meer personen gezamenlijk, zij hoofdelijk verbonden zijn tegenover de opdrachtnemer. Dit is niet altijd wenselijk of de bedoeling. Het is in dat geval zaak duidelijk vast te leggen (i) welke entiteit namens de groep optreedt als opdrachtgever en (ii) dat uitsluitend deze entiteit verantwoordelijk is voor de nakoming van de (betalings)verplichtingen uit hoofde van de overeenkomst. Deze twee voorbeelden illustreren dat de inhoud van een IT-contract steeds beoordeeld moet worden in relatie tot het toepasselijk recht. Het is niet voldoende om alleen naar de inhoud van het contract zelf te kijken.

Entire agreement clause

In veel IT-contracten is ten slotte een *entire agreement clause* opgenomen. In goed Nederlands ook wel een 'vierhoekenbepaling' genoemd. Zo'n bepaling beoogt, kort samengevat, de inhoud van de overeenkomst strikt te beperken tot datgene dat op papier staat en waaronder partijen hun handtekening hebben gezet. Een interessante vraag is of met het opnemen van een entire agreement clause ook in één klap al het regelend recht buitenspel gezet kan worden.

De uitleg van een overeenkomst wordt beheerst door de zogenaamde *Haviltex*-formule.[26] Volgens deze formule is de subjectieve partijbedoeling bepalend voor de uitleg van een contractvoorwaarde. Volgens de Hoge Raad is ook een entire agreement clause onderhevig aan deze uitlegformule, zodat steeds aan de hand van de omstandigheden van het geval moet worden beoordeeld wat partijen concreet voor ogen hebben gehad bij het opnemen van zo'n bepaling.[27]

[25] Artikel 7:406 BW.
[26] Hoge Raad 13 maart 1981, NJ 1981, 635 (*Ermes/Haviltex*).
[27] Hoge Raad 5 april 2013, ECLI:NL:HR:2013:BY8101 (*Lundiform/Mexx*).

Volgens de Hoge Raad beogen partijen doorgaans met een entire agreement clause te bewerkstelligen dat zij niet gebonden zijn aan vóór de contractsluiting gemaakte andersluidende mondelinge of schriftelijke afspraken. Ook staat de clausule, aldus de Hoge Raad, niet zonder meer eraan in de weg dat voor de uitleg van de in de overeenkomst vervatte bepalingen betekenis wordt toegekend aan verklaringen die zijn afgelegd tijdens de onderhandelingen. Gelet op deze benadering zal het opnemen van een entire agreement clause er in de regel niet toe leiden dat regelend recht daarmee automatisch buiten toepassing blijft.

De Clercq *takeaways*

- De inhoud van een overeenkomst wordt niet alleen bepaald door de tekst van een contract, maar ook door het samenstel aan wettelijke regels die op dat type contract van toepassing is. Bij het opstellen van een IT-contract moet daarmee rekening worden gehouden. Schakel daarom een contractjurist in.
- Voor de gemiddelde IT-overeenkomst is geen bijzondere regeling getroffen in het Burgerlijk Wetboek. Vaak is echter sprake van een koopovereenkomst, een overeenkomst van opdracht, een huurovereenkomst, of een combinatie daarvan.
- Een entire agreement clause is onderhevig aan de *Haviltex*-toets en leidt er niet automatisch toe dat geen enkele betekenis wordt toegekend aan verklaringen afgelegd vóór contractsluiting of de toepasselijkheid van aanvullende rechtsregels waarover partijen niet hebben onderhandeld.

6. Software en intellectueel eigendomsrecht

Veel softwareontwikkelaars vragen zich af hoe zij hun software kunnen beschermen. Dit is uiteraard een relevante vraag aangezien de ontwikkeling van software een langdurig en kostbaar traject kan zijn. Ook voor organisaties die software laten ontwikkelen is dit een relevante vraag. Ook zij zullen hun software willen beschermen. Voor hen is het daarbij eerst van belang te weten wie de rechthebbende van de intellectuele-eigendomsrechten op de software is en – indien deze rechten niet bij hen rusten – (in veel gevallen) deze rechten willen verwerven. In dit hoofdstuk zal dan ook kort worden beschreven welke intellectuele-eigendomsrechten op software kunnen rusten, welke handelingen zijn vereist om bescherming te krijgen en wie de rechthebbende is.

Auteursrecht

Een van de voornaamste IE-rechten die bij software aan de orde is, is het auteursrecht. Het auteursrecht beschermt werken op het gebied van letterkunde, wetenschap en kunst. In de Auteurswet worden computerprogramma's en het voorbereidend materiaal daarvan expliciet genoemd als werken die auteursrechtelijk beschermd kunnen zijn. Om voor auteursrechtelijke bescherming in aanmerking te komen moet sprake zijn van een 'eigen en oorspronkelijk karakter', dat 'het stempel van de maker draagt'. Dit houdt in dat het werk niet is ontleend aan dat van een ander en het werk het resultaat is van creatieve keuzes.

De auteursrechtelijke bescherming voor software is echter wel beperkt. Alleen de uitwerking of vormgeving van de software is namelijk beschermd, zoals de bron- en objectcode en het design. Ook voorbereidend ontwerpmateriaal (zoals het functioneel en technisch ontwerp, flow charts en datamodellen) kan voor bescherming in aanmerking komen. Dit is alleen het geval indien het voorbereidend materiaal kan leiden tot een computerprogramma. Het auteursrecht strekt zich niet uit tot de functionaliteit als zodanig van de software. De (technische) functionaliteit, de programmeertaal en de aan de software ten grondslag liggende ideeën en beginselen zijn dus niet beschermd.

Het auteursrecht ontstaat door de creatie als zodanig. Er zijn geen formele vereisten, zoals een aanvraag of registratie. Voor ontwikkelaars is het dan ook verstandig alle stappen in de ontwikkeling te documenteren, dateren en archiveren zodat kan worden aangetoond wanneer, waarop precies en bij wie de auteursrechten zijn ontstaan.

Octrooirecht

Over het octrooieren van software is veel te doen. De vraag of software kan worden geoctrooieerd is relevant omdat het auteursrecht slechts beperkte bescherming biedt. Zoals zojuist besproken, beschermt het auteursrecht immers niet het achterliggende

idee/de functionaliteit. Hoewel software als zodanig wettelijk is uitgesloten, staat de deur voor het verkrijgen van een octrooi toch open als sprake is van software met een 'technisch karakter'. Dit houdt in dat het een bijdrage moet leveren aan de oplossing van een technisch probleem. Anders dan het auteursrecht moet een octrooi worden aangevraagd en is verlening door een octrooi verlenende instantie vereist. Een octrooi kent een beschermingsduur van maximaal 20 jaar.

Knowhow bescherming

Een andere manier om ontwikkelde software te beschermen is door middel van geheimhouding. De bescherming van knowhow was in Nederland tot voor kort niet geregeld in specifieke regelgeving. Sinds oktober 2018 kennen we echter de Wet bescherming bedrijfsgeheimen ('Wbb'). Deze wet regelt wat er onder bedrijfsgeheim wordt verstaan, tegen welke inbreuken op een bedrijfsgeheim kan worden opgetreden en welke handhavingsmaatregelen en procedureregels er daarbij gelden.

De Wbb verstaat onder bedrijfsgeheim informatie die aan de volgende voorwaarden voldoet:

1. de informatie mag niet algemeen bekend zijn bij of algemeen toegankelijk zijn voor personen binnen de kringen die zich gewoonlijk bezighouden met dergelijke informatie;
2. de informatie moet handelswaarde hebben; en
3. er moeten redelijke maatregelen zijn getroffen om de informatie geheim te houden.

Om als onderneming een beroep te kunnen doen op de Wbb is het echter wel noodzaak dat beschermingsmaatregelen worden genomen om de informatie geheim te houden (anders kwalificeert de informatie simpelweg niet als 'bedrijfsgeheim' onder de Wbb). Die maatregelen bestaan uit zowel technische, organisatorische als contractuele beschermingsmaatregelen. Gedacht kan worden aan het opnemen van geheimhoudingsbepalingen in (handels)contracten en arbeidsovereenkomsten, de toegang beperken tot bepaalde sleutelfiguren in de onderneming, fysieke beveiliging en digitale beschermingsmaatregelen zoals encryptie. Het opstellen van een intern beleid zal daarbij essentieel zijn.

Merk- en handelsnaamrecht

Tot slot kan naast bescherming van de software zelf, ook gedacht worden aan het beschermen van de handelsnaam of de naam of het logo waaronder het product/dienst op de markt zal worden gebracht. Indien een goede naam wordt opgebouwd en waarde wordt gecreëerd, zit dit immers ook in de handelsnaam of naam van het product. De handelsnaam waaronder een onderneming wordt gedreven is beschermd door de Handelsnaamwet. Handelsnaamrechten ontstaan automatisch door het gebruik van de

handelsnaam, bijvoorbeeld op het internet, in reclame-uitingen en op briefpapier en facturen. Om een handelsnaam zo goed mogelijk te beschermen is het van belang deze ook te registreren als merk. Voor merkenrechtelijke bescherming is registratie vereist. De registratie beslaat vervolgens een bepaald gebied, bijvoorbeeld de Benelux of de EU. Indien de naam of het logo van het product/dienst afwijkt van de handelsnaam, is het belangrijk ook daar merken voor aan te vragen. Hiermee kan worden voorkomen dat andere partijen met dezelfde naam aan de haal gaan.

Wie is nu de rechthebbende van het intellectueel eigendomsrecht?

Hoofdregel

Als het om IE-bescherming van software gaat, gaat het met name over het auteursrecht. In het auteursrecht is de hoofdregel dat de maker van het werk auteursrechthebbende is.

Werkgever vs. Werknemer

Hier bestaan wel uitzonderingen op. Een veel voorkomende uitzondering is de ontwikkeling in dienstverband. Als de software in dienstverband wordt gemaakt, dan geldt de werkgever als de rechthebbende. Daarvoor is wel vereist dat het ontwikkelen van de software plaatsvindt in het kader van de normale uitoefening van de werkzaamheden van de werknemer. Valt het ontwikkelen van software buiten het takenpakket, dan kan de werknemer mogelijk zelf auteursrechthebbende zijn. Ook is van belang dat het werkgeversauteursrecht enkel op gaat als sprake is van een gezagsverhouding in arbeidsrechtelijke zin. Het geldt dus niet voor externen zoals freelancers of stagiaires. Om eventuele onzekerheid te voorkomen zouden werkgevers in de (arbeids)overeenkomst met een programmeur kunnen opnemen dat het auteursrecht aan de werkgever toekomt en ook wordt overgedragen. Met freelancers e.d. dient dit sowieso contractueel te worden afgesproken/

Opdrachtgever vs. opdrachtnemer

In de relatie opdrachtgever opdrachtnemer ligt het auteursrecht op software in beginsel bij de opdrachtnemer als maker van de software. Het is daarbij niet relevant dat de software uitdrukkelijk in opdracht van de opdrachtgever wordt ontwikkeld en voor de opdrachtgever op maat wordt gemaakt. Ook het feit dat de opdrachtgever de kosten draagt maakt geen verschil. Zonder nadere afspraken liggen de auteursrechten in beginsel bij de opdrachtnemer. Er bestaat echter nog wel een escape. Als een rechtspersoon de software als van haar afkomstig openbaar maakt (bij de eerste openbaarmaking en zonder daarbij de ontwikkelaar als maker te vermelden), wordt die rechtspersoon als auteursrechthebbende aangemerkt (tenzij deze openbaarmaking onrechtmatig is). Hoewel in sommige gevallen dus ook zonder contractuele afspraken het auteursrecht aan de opdrachtgever zou kunnen toekomen, heeft een uitdrukkelijke overdracht sterk de voorkeur omdat dit zekerheid biedt.

Samenwerkingsverband

Indien software door meerdere personen of bedrijven gezamenlijk wordt ontwikkeld, kan sprake zijn van gezamenlijk (ondeelbaar) auteursrecht. Dit is het geval als meerdere partijen een oorspronkelijke bijdrage aan de ontwikkeling van de software hebben geleverd. Dit kan anders zijn als die verschillende bijdragen als zodanig zijn aan te wijzen en gescheiden kunnen worden. In dat geval zullen de verschillende partijen een zelfstandig auteursrecht hebben op het door hun gemaakte deel. Denk bijvoorbeeld aan de situatie dat de graphical user interface kan worden onderscheiden van de onderliggende code.

Einde samenwerkingsverband

Indien sprake is van gezamenlijk auteursrecht, hebben de ontwikkelaars elkaars medewerking nodig voor de exploitatie van het auteursrecht. Wel kan ervoor worden gekozen om hier bij overeenkomst van af te wijken. Regelmatig zie je dat er bij samenwerkingsverbanden die geen rechtspersoon zijn (zoals een vof of een maatschap) na ontbinding problemen ontstaan als er geen afspraken zijn gemaakt over de in samenwerking ontwikkelde software. Ook als één partij software inbrengt om vervolgens door de vof te laten exploiteren, levert dit na ontbinding vaak problemen op. Er moet dan ook duidelijk worden afgesproken wie welke rechten krijgt en wat er na het einde van de vof met de rechten gebeurt.

Overdracht

Als van tevoren duidelijk is aan wie de auteursrechten moeten toekomen, is het belangrijk dat de auteursrechten worden overgedragen. Bijvoorbeeld als het voor opdrachtgever en opdrachtnemer duidelijk is dat de auteursrechten op het op maat gemaakte programma aan de opdrachtgever moet toekomen. Het is niet voldoende dat partijen afspreken dat de auteursrechten aan de opdrachtgever zullen toekomen. Er dient echt expliciet een overdracht te worden afgesproken. De overdracht van auteursrechten moet plaatsvinden bij akte, oftewel een schriftelijk ondertekend stuk.

Licentie

Een andere mogelijkheid om gebruik te maken van software waarvan je oorspronkelijk niet zelf rechthebbende bent, is het verkrijgen van een licentie voor het gebruik. Indien de rechten maar aan één partij toekomen, zal het duidelijk zijn van wie een licentie moet worden verkregen. Echter, software is vaak maatwerk waar verschillende partijen aan hebben bijgedragen, of waarbij tevens gebruik wordt gemaakt van open source software (ook voor het gebruik van open source software gelden bepaalde voorwaarden). In dat geval zal het moeilijk te duiden zijn van wie allemaal een licentie nodig is om rechtmatig gebruik van de software te kunnen maken of welk gebruik onder de open source licenties

precies is toegestaan. Het is belangrijk om dit goed uit te zoeken of de licentiegever in te laten staan voor eventuele claims van derden.

De Clercq *takeaways*

- Let op, de auteursrechten op software liggen in beginsel bij de softwareontwikkelaar als maker van de software.
- Als de rechten bij bijvoorbeeld de opdrachtgever of bij een samenwerkingsverband moeten komen te liggen, is het belangrijk om daar schriftelijke afspraken over te maken.
- Zorg dat je als onderneming een beroep kan doen op de Wet bescherming bedrijfsgeheimen ('Wbb'). Daarvoor is het noodzakelijk dat beschermingsmaatregelen worden genomen om de informatie (de software) geheim te houden. Denk bijvoorbeeld aan het opnemen van geheimhoudingsbepalingen in (handels)contracten en arbeidsovereenkomsten, de toegang beperken tot bepaalde sleutelfiguren in de onderneming, fysieke beveiliging en digitale beschermingsmaatregelen zoals encryptie. Het opstellen van een intern beleid zal daarbij essentieel zijn.

7. Afspraken maken over kwaliteit

Software en IT-diensten spelen een steeds belangrijker rol in onze samenleving. Het is dus essentieel dat goede afspraken worden gemaakt over de kwaliteit van programmatuur en IT-diensten. Toch vinden veel organisaties dit lastig. In de praktijk wordt vooral gekeken naar functionaliteit en kosten, maar wordt relatief weinig stilgestaan bij andere uiterst relevante aspecten voor het functioneren van software en IT-diensten, zoals beveiliging, onderhoudbaarheid en service levels. Dat kan en moet anders.

Wanneer is software goed?

Goed contracteren over de kwaliteit van de software begint met een gemeenschappelijk referentiekader voor de beoordeling van die kwaliteit. Een goed vertrekpunt is ISO/IEC 25010. Deze norm bevat een raamwerk voor de beoordeling van de kwaliteit van ICT-systemen, waaronder programmatuur.

ISO/IEC 25010 maakt onderscheid tussen verschillende kwaliteitsaspecten, zoals betrouwbaarheid, veiligheid, snelheid, gebruiksgemak en onderhoudbaarheid. Niet alle aspecten zullen steeds in gelijke mate van belang zijn voor de klant. Wie software koopt om deze zelf door te ontwikkelen zal daaraan andere eisen stellen dan een klant die een standaard SaaS-dienst afneemt. Voor de eerste zal de onderhoudbaarheid van de software bij uitstek van belang zijn en voor de laatste zal vooral de functionele scope, de beschikbaarheid en het gebruiksgemak ertoe doen.

ISO/IEC 25010 houdt hiermee rekening en benadert het probleem van de kwaliteit van software daarom vanuit het perspectief van de betrokken stakeholders. Softwarekwaliteit volgens ISO/IEC 25010 is: "the degree to which the system satisfies the stated and implied needs of its various stakeholders and provides value".

Meetbare prestaties

Een referentiekader alleen is uiteraard niet genoeg. Dat referentiekader zal vervolgens vertaald moeten worden naar specifieke kwaliteitsafspraken.[28] ISO/IEC 25010 voorziet in indicatoren en meetvoorschriften voor het meetbaar maken van kwaliteitskenmerken, maar bevat geen concrete prestatienormen. De norm beschrijft met andere woorden wel *hoe* de responstijd van een systeem gemeten kan worden, maar niet *wat* de responstijd in een concrete toepassing moet zijn. Dit zal logischerwijs afhangen van het type applicatie en het doel waarvoor de applicatie wordt ingezet.

[28] W.F.R. Rinzema en F.B. Melis, 'Hoe kan de kwaliteit van ICT systemen juridisch meetbaar worden gemaakt?', *Computerrecht* 2014/150.

Van belang is dus dat voor ieder systeem wordt uitgewerkt welke kwaliteit concreet van een kwaliteitskenmerk verwacht mag worden. Dat kan worden gedaan door een specifieke norm op te nemen, bijvoorbeeld dat de responstijd maximaal drie seconden mag zijn. Of – iets algemener – dat een webapplicatie in ieder geval zal beschermen tegen de meest kritieke beveiligingsrisico's volgens de OWASP Top 10. Maar ook kan worden gedacht aan verwijzing naar relevante benchmarks. Zo bestaat er een door TÜV gecertificeerde methode waarbij het kwaliteitskenmerk onderhoudbaarheid wordt getoetst op basis van een benchmarkmodel.

Het is overigens niet nodig om steeds voor alle aspecten van ISO/IEC 25010 concreet en meetbaar uit te werken welke kwaliteit daarvan verwacht mag worden. Vaak kan worden volstaan met uitwerking voor die eigenschappen die voor de betreffende toepassing bij uitstek relevant zijn.

Geen afspraken, geen kwaliteit?

Goede afspraken maken over softwarekwaliteit is dus mogelijk en belangrijk, maar gebeurt lang niet altijd. In de praktijk wordt dikwijls volstaan met het maken van geen of slechts summiere afspraken op dit onderwerp. Een interessante vraag is wat dit betekent voor de klant als de kwaliteit niet aan de verwachtingen voldoet. Staat de klant dan per definitie met lege handen? Het antwoord daarop luidt: nee, niet per se.

Ook wanneer geen expliciete afspraken zijn gemaakt over softwarekwaliteit mag een klant in veel gevallen een minimaal kwaliteitsniveau verwachten. Belangrijk in dat verband is de aard van de overeenkomst. Bij de verwerving van software wordt gebruikgemaakt van twee typen in het Burgerlijk Wetboek genoemde overeenkomsten: i) men *koopt* een licentie op standaardsoftware of ii) men geeft *opdracht* tot ontwikkeling van maatwerksoftware of het ter beschikking stellen van software als dienst (SaaS, PaaS, IaaS).

Koop en conformiteit

In de kooptitel is een regeling opgenomen over conformiteit.[29] Het onderwerp van een koopovereenkomst moet de eigenschappen bezitten die de koper op grond van de overeenkomst mocht verwachten, waaronder de eigenschappen die voor normaal gebruik nodig zijn en waarvan de koper de aanwezigheid niet behoefde te betwijfelen. De conformiteitsregeling impliceert dus dat een afnemer recht heeft op een zeker minimum aan kwaliteit.[30]

[29] Artikel 7:17 BW.

[30] Zie bijvoorbeeld: Rb. Rotterdam 20 november 2019, ECLI:NL:RBROT:2019:9175 (*Joulz/Siemens*); Rb. Utrecht 28 januari 2009, ECLI:NL:RBUTR:2009:BH2449 (*KMD/Intaal*); Rb. Den Bosch 13 april 2005, ECLI:NL:RBSHE:2005:AX3067 (*Steinz/Kluwer*).

Maar let op: professionele partijen kunnen contractueel afwijken van artikel 7:17 BW. Een 'as is' bepaling kan worden beschouwd als zo'n afwijkende bepaling. De strekking van een dergelijke bepaling is dat de software door de klant wordt geaccepteerd in de staat waarin deze afgeleverd wordt, met inbegrip van alle zichtbare en onzichtbare gebreken. Voor professionele partijen kan dit betekenen dat het niet mogelijk is een beroep te doen op de conformiteitsregeling, tenzij dit onaanvaardbaar zou zijn naar maatstaven van redelijkheid en billijkheid. Het is voor afnemers dus zaak alert te zijn op een dergelijke 'as is' bepaling.

Zorg van een goed opdrachtnemer

De overeenkomst op basis waarvan maatwerkprogrammatuur wordt ontwikkeld of op basis waarvan software als dienst ter beschikking wordt gesteld geldt als een overeenkomst van opdracht.[31] De opdrachttitel kent geen conformiteitseis zoals de kooptitel die kent. Wel is de opdrachtnemer verplicht om de zorg van een goed opdrachtnemer in acht te nemen.[32] Meer concreet betekent dit dat de ICT-leverancier de software moet ontwikkelen c.q. ter beschikking moet stellen als een *redelijk bekwaam en redelijk handelend* vakgenoot.

Wat betekent deze laatste norm voor de kwaliteitseisen die aan software gesteld mogen worden? Dat hangt allereerst af van de (beroeps)normen die gelden in de ICT. In de meeste sectoren zien beroepsnormen in de eerste plaats op gedrag en pas in de tweede plaats op de inhoudelijke kwaliteit van de werkzaamheden. Denk aan de gedragsregels die van toepassing zijn op de advocatuur. Deze regels zien vooral op de opstelling van de advocaat richting de cliënt en niet zozeer op de juridisch-inhoudelijke kwaliteit van de verrichte werkzaamheden. Dergelijke gedragsnormen zijn dus niet erg behulpzaam.

Iets soortgelijks is helaas zichtbaar in de jurisprudentie over de zorgplicht van ICT-leveranciers. In verreweg de meeste gevallen waarin een schending van een zorgplicht door een ICT-dienstverlener wordt aangenomen, gaat het om schending van een informatie- of waarschuwingsplicht.[33] Dat wil zeggen: de ICT-dienstverlener schiet tekort in zijn rol als adviseur of projectleider. Zo is aangenomen dat een IT-leverancier zijn zorgplicht kan schenden wanneer hij slecht projectmanagement levert,[34] de klant inadequaat informeert over de voortgang van een project,[35] nalaat de klant te

[31] Artikel 7:400 BW.
[32] Artikel 7:401 BW.
[33] P.G. van der Putt & C.A.M. van de Bunt, 'Bijzondere zorgplichten van IT-leveranciers', *Computerrecht* 2018/160.
[34] Hof 's-Hertogenbosch 3 november 2015, ECLI:NL:GHSHE:2015:4428 (*Tweesteden Ziekenhuis/Alert*).
[35] Rb. Amsterdam 18 januari 2017, ECLI:NL:RBAMS:2017:228 (*CGI/Staalbankiers*).

waarschuwen over de gevolgen van diens wijzigingsvoorstellen,[36] of onvoldoende waarschuwt over een risicovolle back-upstructuur.[37]

Toch kunnen ook kwaliteitsaspecten langs de band van de zorgplicht worden meegewogen bij de uitleg van een overeenkomst. Zo oordeelde de rechtbank Amsterdam in 2019 dat een ICT-leverancier zijn zorgplicht had geschonden door een CRM-systeem op te leveren dat voortdurend foutmeldingen gaf, vaak niet beschikbaar was en bovendien bewerkelijk was in het gebruik.[38]

Service Level Agreement

Omdat de zorgplicht van een IT-leverancier een relatief vage norm is die bovendien vooral ziet op gedrag en minder op kwaliteit, is het bij IT-dienstverlening gebruikelijk dat partijen een Service Level Agreement (SLA) sluiten. In de SLA wordt de zorgplicht voor wat betreft het kwaliteitsaspect als het ware nader ingekleurd en worden concrete afspraken gemaakt over de kwaliteit die de klant van de dienstverlening mag verwachten. Onderwerpen die in de SLA in ieder geval niet mogen ontbreken zijn:

- Beschikbaarheid van de dienst;
- Procedures ten aanzien van gepland en ongepland (nood)onderhoud;
- Bereikbaarheid en reactietijd van de service desk;
- Procedures (en soms oplostijd) bij foutmeldingen;
- Procesafspraken ten aanzien van de roadmap van de IT-leverancier en het beschikbaar maken van updates en nieuwe versies; en
- Service kredieten voor het geval het serviceniveau niet wordt gehaald.

Een bijzonder aandachtspunt bij het onderhandelen over een SLA is de zogenaamde *exclusieve remedie* clausule. Een dergelijke clausule heeft de strekking dat de remedies van de klant bij schending van de SLA beperkt zijn tot een specifieke sanctie, meestal vergoeding van een service krediet. Kwaliteitsafspraken kunnen nog zo concreet en 'streng' zijn opgesteld, maar als de sanctie op overtreding weinig voorstelt, dan hebben de afspraken nog altijd relatief weinig waarde. Onder omstandigheden zal het goedkoper zijn voor de leverancier om te wanpresteren.

De Clercq *takeaways*

- Een goed vertrekpunt bij het maken van afspraken over softwarekwaliteit is om overeen te komen dat software zal voldoen aan (relevante aspecten van) ISO/IEC 25010. Idealiter worden de belangrijkste kenmerken vervolgens concreet en meetbaar uitgewerkt in het contract.

[36] SGOA 7 januari 2014, vonnis 22 (*Nieuwe softwareapplicatie en daaraan gekoppeld een nieuwe website*).
[37] Rb. Amsterdam 14 november 2018, ECLI:NL:RBAMS:2018:10124 (*O'Cliance*), zie in dit kader ook hoofdstuk 8.
[38] Rb. Amsterdam 18 december 2018, ECLI:NL:RBAMS:2019:9635 (*Smart Connections/All Safe*).

- Voor het maken van meer specifieke kwaliteitsafspraken kan worden aangesloten bij relevante normenkaders en benchmarks. Denk aan ISO/IEC 27001 voor algemene informatiebeveiliging, ISO/IEC 27017 voor de beveiliging van clouddiensten, de OWASP Top 10 voor de beveiliging van webapplicaties, ITIL voor dienstverlening, of het door TÜV gecertificeerde benchmarkmodel voor onderhoudbaarheid.
- Denk bij het formuleren van een SLA goed na over de aard van de service levels: is de leverancier daadwerkelijk verplicht om een specifiek resultaat te bereiken of moet deze enkel een bepaalde inspanning leveren? Kan de leverancier een beroep doen op overmacht? Hoe verhoudt de SLA zich tot de wettelijke zorgplicht van de IT-leverancier?
- Afnemers moeten in het bijzonder alert zijn op 'as is' bepalingen in softwarecontracten en 'exclusieve remedie' clausules in SLA's. Deze clausules kunnen de rechten en verhaalsmogelijkheden van afnemers sterk beperken. Voor leveranciers zijn zulke bepalingen juist gunstig.

8. Informatiebeveiligingsaspecten

De gevolgen van gebrekkige informatiebeveiliging kunnen enorm zijn, zo is anno 2022 genoegzaam bekend. In 2017 werd scheepvaartgigant Maersk slachtoffer van een ransomware aanval. Als gevolg daarvan kon wekenlang geen transport of overslag van containers plaatsvinden. Schade: 300 miljoen dollar aan gemiste omzet. Dichter bij huis werd de Universiteit Maastricht in 2019 aangevallen door cybercriminelen. Studenten en medewerkers konden wekenlang niet meer bij hun bestanden en kregen pas weer toegang tot de systemen nadat de universiteit twee ton aan losgeld had betaald. Waar informatiebeveiliging vroeger nog weleens een ondergeschoven kindje was bij het maken van een IT-contract, is dat niet langer het geval (althans dat zou niet meer het geval mogen zijn). Dit hoofdstuk belicht enkele belangrijke punten van aandacht.

Wettelijke beveiligingsverplichtingen

Voordat een klant afspraken kan maken met een leverancier over informatiebeveiliging moet de klant in kaart hebben gebracht welke informatiebeveiligingseisen op zijn eigen organisatie van toepassing zijn. Deze eisen zal hij normaal gesproken immers moeten doorleggen aan de leverancier. De belangrijkste wet- en regelgeving wordt hier kort genoemd.

Algemene verordening gegevensbescherming (AVG)

Iedere verwerkingsverantwoordelijke is op grond van artikel 32 AVG verplicht om passende technische en organisatorische beveiligingsmaatregelen te treffen ter beveiliging van persoonsgegevens. De keuze voor beveiligingsmaatregelen moet gebaseerd zijn op een risicoanalyse en de doeltreffendheid van de getroffen voorzieningen moet regelmatig worden geëvalueerd. Voor inbreuken in verband met persoonsgegevens geldt voorts een meldplicht bij de Autoriteit Persoonsgegevens (AP) en/of richting betrokkenen.[39]

Wet beveiliging netwerk- en informatiesystemen

De Wet beveiliging netwerk- en informatiesystemen (Wbni) is van toepassing op aanbieders van essentiële diensten, andere vitale aanbieders en digitale dienstverleners. De essentiële diensten en andere vitale aanbieders worden bij wet aangewezen. Denk aan netbeheerders van het hoogspanningsnet of houders van een vergunning op grond van de Kernenergiewet. De digitale dienstverleners worden niet specifiek bij wet aangewezen. Wel geldt voor hen een omvangvereiste.[40] Is de Wbni van toepassing, dan

[39] Artikelen 33 en 34 AVG.

[40] Namelijk: meer dan 50 medewerkers en een omzet van meer dan EUR 10 miljoen per jaar, zie artikel 1 Wbni jo. Artikel 16 lid 11 NIB-richtlijn.

is de aanbieder verplicht passende beveiligingsmaatregelen te treffen en moeten incidenten worden gemeld bij het Nationaal Cyber Security Centrum (NCSC) of een andere nader aangewezen instantie.

Sectorale wet- en regelgeving
In sectorale wet- en regelgeving kunnen aanvullende eisen zijn gesteld op het gebied van informatiebeveiliging. Zo moet een zorgaanbieder voldoen aan NEN 7510 en NEN 7512 wanneer hij gebruikmaakt van een zorginformatiesysteem of een elektronisch uitwisselingssysteem waarop hij is aangesloten.[41] Een verzekeraar die IT-voorzieningen wil uitbesteden aan een clouddienstverlener mag dit alleen doen wanneer is voldaan aan specifieke richtlijnen.[42] Ook deze sectorale wet- en regelgeving moet dus in kaart worden gebracht.

Standaarden en normen
Wanneer de toepasselijke eisen in beeld zijn gebracht is het zaak deze in het contract op te nemen. Zowel de AVG als de Wbni bevat een open norm voor wat betreft de eisen die aan informatiebeveiliging gesteld moeten worden. Voor het doorleggen van zulke verplichtingen kan allereerst worden verwezen naar de norm zelf en kan aanvullend op onderdelen een concretere uitwerking worden opgenomen.

Garanties en certificaten
Een IT-leverancier moet garanties kunnen bieden ten aanzien van beveiliging. Vraag daarom relevante certificaten en auditverklaringen op en laat deze beoordelen door een deskundige. Vergeet niet om ook de scope en de verklaring van toepasselijkheid van een certificering te checken. Een ISO/IEC 27001-certificering die alleen ziet op een ontwikkelomgeving is niet per se relevant voor een transactie waarbij alleen beheer- en supportdiensten worden afgenomen.

Inmiddels is de Cyberbeveiligingsverordening van kracht. Deze verordening schept een Europees kader voor de certificering van cyberbeveiliging. Met deze certificaten kunnen fabrikanten en aanbieders het beveiligingsniveau van hun IT-producten, -diensten en -processen aantonen. De certificeringsregelingen zullen op Europees niveau worden opgesteld, maar de uitgifte van certificaten en handhaving en toezicht zal plaatsvinden op nationaal niveau. Op Europees niveau wordt op het moment onder meer gewerkt aan certificeringsregelingen voor IT-beveiligingsproducten en clouddiensten.

Verwerkersovereenkomst niet voldoende
Op basis van de AVG zijn partijen onder omstandigheden verplicht om afspraken met elkaar te maken over de beveiliging van persoonsgegevens. Deze afspraken worden dan

[41] Artikel 3 Besluit elektronische gegevensverwerking door zorgaanbieders.
[42] Artikel 27d Besluit prudentiële regels Wft.

vastgelegd in een zogenaamde verwerkersovereenkomst.[43] Van belang is op te merken dat de verwerkersovereenkomst doorgaans alleen ziet op de verwerking van persoonsgegevens en niet op de verwerking van andere type data. Dit betekent dat de afspraken in de verwerkersovereenkomst niet noodzakelijkerwijs van toepassing zijn op die toepassingen waarbij geen persoonsgegevens worden verwerkt. Het is daarom zaak dat ook in het lichaam van de overeenkomst adequate afspraken worden opgenomen over informatiebeveiliging.

Zorg van een goed opdrachtnemer

Bij IT-dienstverlening is vaak sprake van een overeenkomst van opdracht. In zulke gevallen dient de opdrachtnemer – zoals besproken in hoofdstuk 7 – zorg te dragen voor een goede uitvoering van de opdracht. Deze zorgplicht kan ook vergaande consequenties hebben voor de aansprakelijkheid van een IT-dienstverlener bij beveiligingsgebreken. IT-leveranciers moeten ernstig rekening houden met deze zorgplicht bij het aannemen van een opdracht en bij de uitvoering daarvan.

In 2018 oordeelde de rechtbank Amsterdam dat een klant die opdracht geeft tot levering van een 'totaalpakket' – bestaand uit de aanleg en het beheer en onderhoud van een bedrijfsnetwerk – mag verwachten dat een adequate beveiliging in de vorm van een firewall en adequate back-upstructuur is inbegrepen. Hoewel de IT-leverancier aan de klant had voorgesteld om extra beveiligingsmaatregelen te treffen in de vorm van een firewall en andere back-upstructuur, was dit volgens de rechtbank onvoldoende. De IT-leverancier had de opdracht wegens onuitvoerbaarheid moeten weigeren, alternatieven moeten aandragen, of indringend en herhaaldelijk moeten waarschuwen over de risico's.[44]

Computervredebreuk

Hacken is strafbaar. Wie slachtoffer wordt van een cyberaanval moet daarom ook overwegen om aangifte te doen van computervredebreuk (o.a. artikel 138ab, 138b, 138c, 350 en 350a Sr). Hoewel de pakkans bij digitale criminaliteit wellicht niet heel groot lijkt, kan het doen van aangifte toch belangrijk zijn. Al is het maar om naar de buitenwereld te tonen dat jouw organisatie slachtoffer is geworden van een ernstig misdrijf. Het doen van aangifte kan ook een verzekeringsvoorwaarde zijn.

De Clercq *takeaways*

- Ga als afnemer na welke beveiligingseisen op grond van de wet gelden voor jouw organisatie en leg deze verplichtingen door aan geselecteerde IT-leveranciers.
- Een IT-leverancier moeten garanties kunnen bieden ten aanzien van beveiliging. Vraag daarom relevante certificaten en auditverklaringen op, laat deze

[43] Artikel 28 lid 3 AVG en zie hoofdstuk 9 hierna voor meer informatie.
[44] Rb Amsterdam 14 november 2018, ECLI:NL:RBAMS:2018:10124 (*O'Cliance*).

beoordelen door een deskundige en vergeet niet ook de scope van een certificering te toetsen.

- Leg afspraken over informatiebeveiliging niet uitsluitend vast in de verwerkersovereenkomst (die immers alleen ziet op de verwerking van een specifieke categorie data, namelijk persoonsgegevens), maar ook in het lichaam van de overeenkomst.
- De overeenkomst op basis waarvan IT-diensten worden verleend kwalificeert vaak als een overeenkomst van opdracht zodat de IT-dienstverlener de zorg van een goed opdrachtnemer in acht moet nemen. Dit kan betekenen dat op de IT-dienstverlener een vergaande waarschuwingsplicht rust, ook ten aanzien van beveiligingsrisico's. Het niet in acht nemen van deze waarschuwingsplicht kan leiden tot aansprakelijkheid.

9. De verwerkersovereenkomst

Er is bijna geen IT-project voor te stellen waarbij geen persoonsgegevens worden verwerkt. Op het moment dat persoonsgegevens worden verwerkt, zijn zowel de verwerkingsverantwoordelijke als de verwerker op grond van artikel 28 AVG verplicht om een verwerkersovereenkomst op te stellen. Naleving van deze wettelijke verplichting is van belang, al is het maar dat omdat het enkele feit dat geen verwerkersovereenkomst is gesloten kan leiden tot een boete van de Autoriteit Persoonsgegevens. Wanneer ben je nu 'verwerkingsverantwoordelijke' of 'verwerker' en welke eisen worden aan een verwerkersovereenkomst gesteld?

Rolverdeling – verwerkingsverantwoordelijke of verwerker?

Op het moment dat er verschillende partijen betrokken zijn bij een verwerking van persoonsgegevens, gaat de AVG uit van een rolverdeling. Een van de belangrijke begrippen bij deze rolverdeling is de verwerkingsverantwoordelijke. Dit is de partij die het doel en de middelen van het gebruik van persoonsgegevens bepaalt.[45] Een ander belangrijk begrip is verwerker. Een verwerker verwerkt de persoonsgegevens ten behoeve van de verwerkingsverantwoordelijke.[46] Een voorbeeld van een verwerker is een salarisadministratiekantoor. Ook een SaaS-dienstaanbieder of hostingprovider die persoonsgegevens verwerkt kwalificeert (in beginsel) als verwerker. (Er kan ook nog sprake zijn van een gezamenlijke verantwoordelijkheid, maar dat laten we omwille van het geven van een helder en beknopt overzicht buiten beschouwing).

Het is van belang dat partijen zich bewust zijn van hun rol. De AVG stelt immers verschillende wettelijke eisen aan de invulling van deze rollen. In de praktijk blijkt echter dat het niet altijd eenvoudig is de juiste rol te kwalificeren. Het risico dat partijen in dat geval lopen is dat zij te veel of juiste te weinig verplichtingen op zich nemen. In het eerste geval trekken zij meer verantwoordelijkheid (en uiteindelijk ook meer kans op aansprakelijkheid) naar zich toe dan noodzakelijk. In het tweede geval voldoen zij niet aan hun wettelijke verplichtingen. In beide gevallen is dit niet zonder risico.

De verwerkersovereenkomst

Het sluiten van een verwerkersovereenkomst tussen verwerkingsverantwoordelijke en verwerker(s) is wettelijk verplicht. Een wijdverbreid misverstand is dat alleen de verwerkingsverantwoordelijke de verplichting heeft zorg te dragen voor een verwerkersovereenkomsten. Dit is niet juist. Deze wettelijke verplichting rust zowel op de verwerkersverantwoordelijke als op de verwerker. Welke afspraken moeten nu worden

[45] Artikel 4 sub 7 AVG.
[46] Artikel 4 sub 8 AVG.

opgenomen in een verwerkersovereenkomst? De volgende zaken dienen in ieder geval te worden geregeld:

- Het onderwerp en de duur van de verwerking;
- De aard en het doel van de verwerking;
- Het soort persoonsgegevens en de categorieën van betrokkenen; en
- De rechten en verplichtingen van de verwerkingsverantwoordelijke.

Bepalingen ten aanzien van verwerker

Daarnaast moet de overeenkomst:

- Bepalen dat de persoonsgegevens uitsluitend verwerkt mogen worden op basis van de schriftelijke instructies van verwerkingsverantwoordelijke;[47]
- Waarborgen dat de personen die betrokken zijn bij de verwerking vertrouwelijkheid in acht nemen;[48]
- Waarborgen dat verwerker zorg zal dragen voor afdoende beveiliging van de persoonsgegevens (in lijn met artikel 32 AVG);[49]
- Bepalen dat verwerker de verwerkingshandelingen niet zonder meer overdraagt aan sub-verwerkers;[50]
- Bepalen dat verwerker de verwerkingsverantwoordelijke bijstand verleent (al dan niet in de vorm van informatie) bij het nakomen van de verplichtingen die voortvloeien uit de AVG;[51] en
- Bepalen of de verwerker de gegevens wist of terugbezorgt aan de verwerkingsverantwoordelijke na afloop van de verwerkingsdiensten.[52]

Het staat partijen vrij om deze zaken gedetailleerder te regelen. Zo kunnen partijen bijvoorbeeld specifieke voorwaarden afspreken waaronder verwerker zijn verwerkingsdiensten wel uit mag besteden aan sub-verwerkers. Ook is het gebruikelijk een lijst op te nemen van de beveiligingsmaatregelen die ten minste verwacht worden van de verwerker.

Aanvullende bepalingen

Naast de bepalingen die op grond van de wet in ieder geval moeten worden opgenomen in een verwerkersovereenkomst, is het raadzaam om bepalingen op te nemen over aansprakelijkheid en vrijwaring. Hoe gaan partijen om met een boete die opgelegd worden door de Autoriteit Persoonsgegevens als sprake is van niet-naleving van de AVG? Ook is het raadzaam nadere (procedure)afspraken te maken over datalekken. Hoe te handelen in geval van een datalek? Bij wie en hoe moet een datalek worden gemeld? Welke informatie moet in dat geval worden gedeeld, etc.?

[47] Artikel 28 lid 3 sub a AVG.
[48] Artikel 28 lid 3 sub b AVG.
[49] Artikel 28 lid 3 sub c AVG.
[50] Artikel 28 lid 3 sub d AVG.
[51] Artikel 28 lid 3 sub e, f en h AVG.
[52] Artikel 28 lid 3 sub g AVG.

De Clercq *takeaways*

- De AVG maakt onderscheid tussen partijen op basis van hun onderlinge rolverdeling. Als verwerkingsverantwoordelijke wordt aangemerkt de partij die het doel en de middelen van het gebruik van persoonsgegevens bepaalt. De verwerker is de partij die de persoonsgegevens verwerkt ten behoeve van de verwerkingsverantwoordelijke.
- Er zijn echter situaties denkbaar waarin de posities van partijen niet duidelijk afgebakend zijn. Het is dus van belang dat grote zorgvuldigheid in acht wordt genomen bij het bepalen van de positie van partijen. Dit om te voorkomen dat te weinig of juist te veel verantwoordelijkheid wordt genomen.
- Zowel de verwerkingsverantwoordelijke als de verwerker zijn op grond van artikel 28 AVG verplicht zorg te dragen voor een verwerkersovereenkomst. Deze verwerkersovereenkomst bevat in elk geval bepalingen over het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen en de rechten en verplichtingen van de verwerkingsverantwoordelijke.
- Partijen kunnen onderling overeenkomen om deze zaken gedetailleerder en preciezer af te spreken. Ten aanzien van een aantal onderwerpen is dit zeker raadzaam.

10. Contracteren met Amerikaanse partijen

Contracteren met Amerikaanse clouddienstverleners is een heet hangijzer. Dit heeft alles te maken met enerzijds, de dominante positie van Amerikaanse spelers op de wereldwijde markt voor IT-dienstverlening en anderzijds, met de strenge Europese wetgeving inzake de doorgifte van persoonsgegevens. Onder welke voorwaarden kan nog wél gebruik worden gemaakt van Amerikaanse clouddienstverleners? Een overzicht en update.

Het Internet is Amerikaans

In veel opzichten is het Internet een Amerikaanse uitvinding. In de jaren '60 was het Amerikaanse ministerie van Defensie op zoek naar een manier waarmee haar wereldwijd gestationeerde personeel informatie kon uitwisselen, ongeacht waar dat personeel zich bevond en ongeacht het type apparaat waarop werd gewerkt. Dat systeem werd ARPANET en ARPANET werd uiteindelijk het Internet.

Nog altijd is veel van de huidige Internet infrastructuur ontworpen en aangelegd door Amerikaanse bedrijven. Dat geldt voor de hardware (HP, Apple, Dell), de chips (Intel, Qualcomm) en voor routers en modems (Cisco, Juniper). Ook de markt voor web-diensten en platforms voor e-mail en cloudopslag is hoofdzakelijk in handen van enkele grote Amerikaanse spelers (Google, Oracle, Amazon, Microsoft). Gevolg is dat Europese organisaties en bedrijven voor hun IT-wensen in veel gevallen zijn aangewezen op Amerikaanse partijen.

Europese beperkingen

Sinds 1981 bestaat in Europa een bijzonder rechtsregime voor de verwerking en doorgifte van persoonsgegevens.[53] Dit rechtsregime, dat inmiddels is vastgelegd in hoofdstuk V van de AVG stelt beperkingen aan de vrije doorgifte van persoonsgegevens. Onder de AVG kunnen persoonsgegevens namelijk vrijelijk circuleren binnen de Europese Economische Ruimte (EER), maar is de doorgifte van persoonsgegevens aan een land of gebied buiten de rechtsmacht van een van de EER-lidstaten alleen toegestaan als aan strenge eisen wordt voldaan. De Europese wetgever heeft daarmee willen voorkomen dat het rechtsbeschermingsniveau dat de AVG beoogt te garanderen eenvoudig omzeild zou kunnen worden door dataverwerkingen te verplaatsen naar het buitenland.

[53] In 1981 komt binnen de Raad van Europa het Verdrag inzake gegevensbescherming tot stand. Dit verdrag – dat overigens nog steeds van kracht is – vormt in veel opzichten de blauwdruk van de AVG.

Doordat veel computerkracht en dataverwerking sinds de jaren '10 is verplaatst van lokale PC's naar centrale servers van clouddienstverleners, is de regeling over internationale doorgiften flink in belang toegenomen.

Wanneer is sprake van een doorgifte?

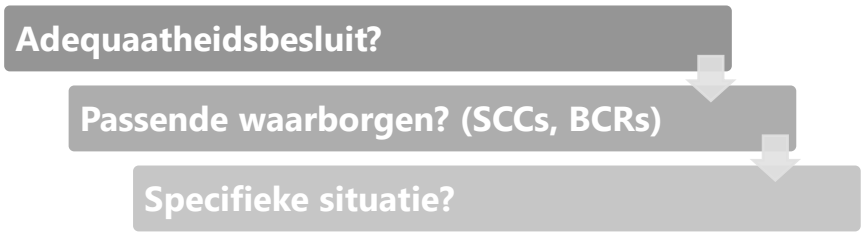
In onderstaand overzicht zijn enkele voorbeelden opgenomen van situaties waarin wel of geen sprake is van een internationale doorgifte.

Wel een doorgifte		Geen doorgifte	
Financemedewerker stuurt vanuit Nederland een rapportage naar een accountant in de VS	✓	Publicatie van persoons-gegevens op Internet[54]	✗
Sales-medewerker maakt vanuit Nederland gebruik van een in de VS gehoste CRM-applicatie	✓	Routering van IP-packets tussen twee eindpunten in de EER	✗
Nederlandse IT-dienstverlener deelt persoonsgegevens met een sub-verwerker in de VS	✓	HR-medewerker benadert vanuit de VS de in Nederland gehoste HRM-database van zijn werkgever[55]	✗

Getrapte systematiek

Is sprake van een internationale doorgifte, dan moet worden beoordeeld of de doorgifte is toegestaan. Dit regime kent een 'getrapte' systematiek. Biedt een land buiten de EER naar het oordeel van de Europese Commissie een passend beschermingsniveau, dan mogen persoonsgegevens zonder meer worden doorgegeven aan dat land op basis van het desbetreffende adequaatheidsbesluit, anders zijn passende waarborgen nodig.[56] De belangrijkste passende waarborgen in de praktijk zijn de door de Europese Commissie vastgestelde standaardcontractbepalingen (SCCs)[57] en bindende bedrijfsvoorschriften (BCRs). Is ook geen sprake van passende waarborgen, dan is een doorgifte in enkele specifieke situaties onder strenge voorwaarden alsnog toegestaan.[58]

[54] HvJEU 6 november 2003, ECLI:EU:C:2003:596 (*Lindqvist*).
[55] EDPB Guidelines 05/2021 on the interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, adopted on 18 November 2021, pag. 5.
[56] Artikel 45 resp. 46 AVG.
[57] Uitvoeringsbesluit (EU) 2021/914 van 4 juni 2021 betreffende standaardcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen.
[58] Artikel 49 AVG.



Schrems I en II

Voor de Verenigde Staten is tot tweemaal toe een adequaatheidsbesluit afgegeven door de Europese Commissie. Het eerste besluit was beter bekend onder de naam *Safe Harbor* en het tweede besluit als het *Privacy Shield*. Beide besluiten werden in respectievelijk 2015 (*Schrems I*)[59] en 2020 (*Schrems II*)[60] door het Hof van Justitie van de Europese Unie (HvJEU) ongeldig verklaard. Volgens het HvJEU resulteren de afspraken die in beide instrumenten zijn gemaakt namelijk niet in een beschermingsniveau voor persoonsgegevens dat in grote lijnen overeenkomt met het beschermingsniveau in de Unie. De Europese Commissie had de adequaatheidsbesluiten daarom niet mogen afgeven.

Het 'tekort' aan bescherming in de Verenigde Staten schuilt volgens het Europees hof in het feit dat de bevoegdheden van Amerikaanse inlichtingendiensten te ruim zijn geformuleerd. Het gaat daarbij ten eerste om wetgeving die inlichtingendiensten de bevoegdheid geeft informatie betreffende niet-Amerikanen op te vorderen bij aanbieders van internetdiensten en telecommunicatiebedrijven (FISA 702). Ten tweede gaat het om de bevoegdheid om te tappen op onderzeese kabels op de Atlantische bodem, en deze gegevens te verzamelen en te bewaren voordat zij in de Verenigde Staten aankomen (E.O. 12333). Deze wetgeving bevat naar Europese maatstaven onvoldoende waarborgen om ervoor te zorgen dat zulke ingrijpende bevoegdheden alleen worden ingezet als dat strikt noodzakelijk is, aldus het Europees Hof.

Het Privacy Shield is dood, leve de SCCs?

Het *Privacy Shield* is dus niet meer bruikbaar als doorgifte instrument. De vraag dient zich vervolgens aan of het mogelijk is om zonder problemen over te schakelen op de 'tweede trap', de passende waarborgen. Helaas ligt dit lastig. In *Schrems II* oordeelde het HvJEU namelijk ook dat de SCC's en andere passende waarborgen genoemd in artikel 46 AVG niet in een vacuüm opereren. Bedrijven die persoonsgegevens willen doorgeven op basis van deze instrumenten moeten van geval tot geval beoordelen of de waarborgen daadwerkelijk effectief zijn. Soms zijn aanvullende waarborgen nodig.

[59] HvJEU 6 oktober 2015, ECLI:EU:C:2015:650 (*Schrems I*).
[60] HvJEU 16 juli 2020, ECLI:EU:2020:559 (*Schrems II*).

Dit oordeel is begrijpelijk. SCCs veranderen immers niets aan de bevoegdheden van Amerikaanse inlichtingendiensten. Niets in de SCCs staat eraan in de weg dat de NSA data opvordert op grond van FISA 702 of dat de CIA onderzeese kabels aftapt op grond van E.O. 12333. Het zou raar zijn als een doorgifte wegens die ruime bevoegdheden niet gebaseerd kan worden op een adequaatheidsbesluit, maar nog wel steeds op de SCCs die daar geen enkele waarborg tegen bevatten.

CLOUD Act

In 2013 werd Microsoft door een Amerikaanse rechter bevolen om e-mails die waren verzonden via haar e-mailplatform (hotmail.com, msn.com, outlook.com) af te staan in verband met een onderzoek naar illegale drugshandel. De e-mails in kwestie lagen opgeslagen op servers in Dublin, Ierland. Microsoft meende dat de Amerikaanse rechter geen bevoegdheid had om een bevel uit te vaardigen ter zake data die buiten de VS lagen opgeslagen en weigerde aan het bevel gehoor te geven.

In eerste en tweede instantie kreeg Microsoft ongelijk, maar in hoger beroep bij het Second Circuit Court werd Microsoft in juli 2016 in het gelijk gesteld.[61] Volgens het Second Circuit Court waren er onvoldoende aanknopingspunten om aan te nemen dat de wet waarop het bevel was gebaseerd "extraterritoriale" werking toekwam. Terwijl de zaak vervolgens diende bij het Hooggerechtshof, nam het Congres een nieuwe wet aan, de *Clarifying Lawful Overseas use of Data Act* (CLOUD Act). Zoals de titel tot uitdrukking brengt, verduidelijkte deze wet dat een gerechtelijk bevel ook kan zien op data die ligt opgeslagen op servers buiten de Verenigde Staten.

Op basis van de CLOUD Act kunnen Amerikaanse rechtshandhavingsinstanties dus data invorderen die in het bezit is van Amerikaanse IT-leveranciers, ongeacht waar die gegevens zich bevinden. Dit risico kan worden gemitigeerd door goede afspraken te maken over encryptie en over het beoordelen en aanvechten van informatieverzoeken.

De Clercq *takeaways*

Effectief betekent voorgaande dat ten minste de navolgende attentiepunten de revue moeten passeren wanneer wordt overwogen gebruik te maken van een clouddienstverlener in de Verenigde Staten:

- Doorgifte van persoonsgegevens aan een clouddienstverlener in de Verenigde Staten die toegang moet kunnen hebben tot de gegevens in niet-versleutelde toestand is sinds *Schrems II* (haast) niet meer mogelijk. Ook niet wanneer gebruik wordt gemaakt van de SCCs.
- Wel bestaat er nog ruimte voor doorgifte van persoonsgegevens aan Amerikaanse clouddienstverleners wanneer de persoonsgegevens: (i)

[61] *Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp*., No. 14-2985, 2016 WL 3770056 (2d Cir. July 14, 2016).

gepseudonimiseerd; of (ii) versleuteld zijn waarbij in het laatste geval de cryptografische sleutels onder beheer van de data-exporteur binnen de EER dienen te blijven.

- De grote clouddienstverleners bieden inmiddels vrijwel allemaal de mogelijkheid aan om contractueel overeen te komen dat klantdata uitsluitend worden opgeslagen op servers binnen de EER. Let erop dat een dergelijke optie doorgaans alleen geldt voor opslag van klantdata at-rest en niet voor (i) klantdata in-transit; (ii) meta-data; en (iii) data die wordt verwerkt in het kader van support. In toenemende mate zetten clouddienstverleners stappen om ook zulke data binnen de EER te houden.[62]
- Ook als klantdata at-rest in de EER is opgeslagen, kunnen Amerikaanse IT-dienstverleners op grond van de CLOUD Act nog steeds worden verplicht om deze gegevens aan Amerikaanse overheidsinstanties over te dragen. Dit risico kan worden gemitigeerd door goede afspraken te maken over encryptie en over het beoordelen en aanvechten van informatieverzoeken.
- Voer een data protection impact assessment (DPIA) uit om ervoor te zorgen dat bovenstaande punten de revue passeren en dat een gedocumenteerde risicoafweging is gemaakt.[63]

[62] Zie: https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/.
[63] Zie in dit kader ook hoofdstuk 3.

11. Outsourcing van IT

Uitbesteden is nog steeds hot is. Uit een recent onderzoek blijkt dat de Nederlandse IT-outsourcingmarkt zal blijven groeien.[64] Bijna de helft van de respondenten geeft aan dat ze de komende twee jaar in een hoger tempo te zullen uitbesteden. Dit is momenteel het hoogste niveau in Europa. De plannen om te insourcen zijn gehalveerd, van 16% naar 8%. De financiële dienstverleningssector voorspelt de meeste outsourcinggroei: 64% van de organisaties is van plan meer uit te besteden. De hoofdredenen om te gaan outsourcen zijn: focus op kernactiviteiten, terugdringen van IT-kosten en verbetering van de IT-ondersteuning. Door outsourcing kan je focussen op waar je sterk in bent en ondersteunende taken, zoals IT, overdragen aan partijen die dáár sterk in zijn en ook schaal in hebben. Door die schaal kunnen deze partijen meer kwaliteit leveren tegen lagere kosten. Toch zijn er ook bedrijven die aarzelen of juist gas willen terugnemen. Die aarzeling is niet onbegrijpelijk. IT-outsourcing blijft complex. Ook vanuit juridisch oogpunt.

Scope van de uitbesteding

Vaak ontbreekt bij uitbesteders een feitelijk beeld van de scope. Wat wil je precies uitbesteden? Dit is immers de kern van de outsourcingsovereenkomst. Zonder een feitelijk beeld van de scope is goede onderhandeling over de prijs en oplevertermijn niet mogelijk, hetgeen vaak leidt tot langdurige onderhandelingen, die er uiteindelijk op neerkomen dat een dienstverlener gedwongen wordt om (als gevolg van de onduidelijke scope) te veel marge in te bouwen.

Iedere outsourcing valt of staat met teamwork

Voorts gebeurt het nog steeds regelmatig dat niet alle disciplines en stakeholders (zoals HR, finance en legal) op tijd bij het proces worden betrokken. Dit terwijl iedere outsourcing valt of staat met teamwork dat wordt geleverd. Zo zal bijvoorbeeld vanuit HR moeten worden aangegeven of er sprake is van een overgang van onderneming, als gevolg waarvan werknemers van rechtswege in dienst komen van de dienstverlener.

Juridische pitfalls

Onvoldoende oog voor (de complexiteit van) toepasselijke wet- en regelgeving is één voorbeeld van een juridische pitfall bij outsourcing. Onvoldoende oog voor eventuele beperkingen in licentievoorwaarden is een andere bekende juridische pitfall. In licentievoorwaarden van softwareleveranciers zijn immers vaak beperkingen opgenomen die outsourcing niet toestaan. Handelen in strijd met deze voorwaarden kan bedrijven duur komen te staan.

[64] Zie: https://whitelane.com/netherlands-2021/.

Verdere pitfalls zijn bijvoorbeeld:

- geen heldere en meetbare service levels voor het gewenste niveau van dienstverlening;[65]
- onvoldoende aandacht voor het borgen van de continuïteit van de dienstverlening. Wat gebeurt er in geval van calamiteiten? Is er een regeling omtrent disaster recovery en business continuity?;
- onvoldoende oog voor compliance met voorschriften en regelgeving. In gereguleerde markten zal bijvoorbeeld rekening moeten worden gehouden met de richtlijnen over outsourcing. Zo hebben De Nederlandse Bank en Autoriteit Financiële Markten uitgebreide richtlijnen; en
- het ontbreken van een exitprocedure die de continuïteit van de dienstverlening waarborgt in de situatie dat partijen uit elkaar gaan.[66]

Vertrouwen

Bij het onderhandelen over en vastleggen van de afspraken zijn vertrouwen en begrip van elkaars positie en belangen nodig. Zo is het voor de outsourcende partij van belang dat de diensten mee moeten kunnen groeien met haar bedrijfsvoering. Er zullen dan ook changeprocedures overeengekomen moeten worden. Ook voor de dienstverlener is flexibiliteit van belang, nu hij de mogelijkheid moet hebben om de overeengekomen dienstverlening te kunnen aanpassen aan nieuwe ontwikkelingen in de techniek. De outsourcende partij zal zich bij de onderhandelingen bovendien moeten realiseren dat zij bedrogen uit kan komen als zij een contract aangaat waar geen of weinig marge in zit. De dienstverlener zal begrijpelijkerwijs tijdens de uitvoering van het contract alsnog op zoek gaan naar (meer) marge.

De Clercq *takeaways*

- Bereid een outsourcing goed voor en wees alert op de valkuilen, zodat de voordelen van outsourcing verzilverd kunnen worden.
- Zorg dat je eerst een feitelijk beeld van de scope van de outsourcing hebt. Wat wil je precies uitbesteden en wat wil je ermee bereiken?
- Breng vervolgens het juridisch kader in beeld. Met welke wet- en regelgeving hebben we te maken en op welke wijze bepaalt deze wet- en regelgeving de randvoorwaarden van de uitbesteding
- Zorg ook voor een goed exitscenario. Leg de afspraken vooraf vast op het moment dat de relatie nog goed is. Afspraken maken over hoe partijen uit elkaar gaan is lastiger op het moment dat partijen besloten hebben om uit elkaar te gaan en/of sprake is van een conflict.

[65] Zie in dit kader ook hoofdstuk 7.
[66] Zie in dit kader ook hoofdstuk 13.

12. Exoneraties voor schade

Een van de belangrijkste onderwerpen waarover wordt onderhandeld tijdens contractonderhandelingen is het onderwerp aansprakelijkheid. De belangen van partijen staan op dit punt vaak lijnrecht tegenover elkaar. De leverancier wil zijn aansprakelijkheid zoveel mogelijk beperken terwijl de klant er juist belang bij heeft dat de leverancier ruimhartig aansprakelijkheid aanvaardt. Dit hoofdstuk belicht enkele aandachtspunten.

Grondslagen voor aansprakelijkheid

Het Nederlandse recht kent diverse grondslagen op basis waarvan een IT-leverancier aansprakelijk gesteld kan worden voor schade. De bekendste grondslagen zijn wanprestatie en onrechtmatige daad.[67] Naast deze algemene leerstukken kent de wet nog enkele bijzondere regelingen voor aansprakelijkheid, zoals voor de producent van een gebrekkige zaak of wegens overtreding van de AVG.[68] Voor de IT-leverancier is het van belang dat een contractuele beperking van zijn aansprakelijkheid duidelijk maakt dat de exoneratie geldt ongeacht de grondslag voor aansprakelijkheid.

Directe en indirecte schade

In veel IT-contracten wordt een onderscheid gemaakt tussen directe en indirecte schade. Aansprakelijkheid van de leverancier voor indirecte schade is dan geheel uitgesloten en aansprakelijkheid voor directe schade is beperkt tot de (jaarlijkse) opdrachtwaarde, al dan niet vermenigvuldigd met een factor 2 of 3.

Wie in het Burgerlijk Wetboek (BW) zoekt naar de betekenis van de begrippen 'directe' en 'indirecte' schade zoekt tevergeefs. Die begrippen komen niet in ons wetboek voor en zijn overgewaaid uit de Anglo-Amerikaanse rechtspraktijk. Het onderscheid tussen directe en indirecte schade naar Anglo-Amerikaans recht is terug te voeren op de uitspraak *Hadley vs. Baxendale* uit 1854.[69] Grofweg betekent directe schade het soort schade dat onder normale omstandigheden het gevolg is van een bepaalde tekortkoming. Het begrip indirecte schade verwijst naar schade die alleen voorzienbaar is gelet op de specifieke (bijzondere) situatie van de klant.[70]

Nu dit onderscheid naar Nederlands recht geen vastomlijnde betekenis heeft, doen partijen die deze begrippen willen gebruiken in een contract waarop Nederlands recht

[67] Artikel 6:74 BW resp. artikel 6:162 BW.
[68] Artikel 6:185 e.v. BW resp. artikel 82 AVG.
[69] Hadley vs. Baxendale (1854), 9 Ex. 341, 156 Eng. Rep. 145.
[70] Mr. J.W.A. Dousi, 'Exoneraties voor indirecte schade. Over de uitleg van dit boilerplate-beding naar Nederlands en Anglo-Amerikaans recht', *Contracteren* maart 2017, nr.1.

van toepassing is, er goed aan deze begrippen te verduidelijken. Het contract moet dan definiëren wat onder ieder van deze begrippen wordt verstaan.

Een alternatief is dat helemaal geen gebruik wordt gemaakt van deze leenbegrippen en dat gewoon wordt aangesloten bij de terminologie in het ons burgerlijk recht. Het BW stelt dat vermogensschade kan bestaan uit geleden verlies en uit gederfde winst (artikel 6:96 lid 1 BW). Verder kan vermogensschade bestaan uit de redelijke kosten die worden gemaakt ter voorkoming of beperking van schade, ter vaststelling van schade en aansprakelijkheid en ter verkrijging van voldoening buiten rechte (artikel 6:96 lid 2 BW). Een IT-leverancier kan bijvoorbeeld in zijn voorwaarden opnemen dat aansprakelijkheid voor gederfde winst is uitgesloten en dat aansprakelijkheid voor geleden verlies en de hierboven genoemde redelijke kosten is beperkt tot de (jaarlijkse) opdrachtwaarde.

Garanties en vrijwaringen

Verwant aan de aansprakelijkheden zijn de garanties en vrijwaringen in een contract. De begrippen 'garantie' en 'vrijwaring' zijn naar Nederlands recht geen vastomlijnde juridische begrippen. Onder een garantie wordt doorgaans verstaan een versterkte verbintenis die geen bevrijdend overmacht verweer toelaat. De IT-leverancier is bij schending van een garantie dus schadeplichtig, zelfs als sprake is van overmacht. Een vrijwaring ziet volgens verkeersopvattingen op het afdekken van een specifiek risico (bijvoorbeeld een claim van een derde wegens auteursrechtinbreuk) dat ten tijde van contractsluiting voorzienbaar was, maar waarvan onzeker was of dit risico zich ook zou manifesteren. Een vrijwaringsverplichting wordt in de literatuur getypeerd als een vordering tot nakoming, zodat de regels van het schadevergoedingsrecht niet van toepassing zijn.[71]

Voorgaande betekent – maar let op, veel hangt af van de specifieke bewoordingen in het contract – dat een exoneratie in de regel wel van toepassing is op een geschonden garantieverplichting, maar niet op een vrijwaringsverplichting. Leveranciers moeten dus terughoudend zijn met het aanvaarden van garanties en (vooral) vrijwaringen.

Ongedaanmaking

Bij het opstellen van een exoneratiebeding moet ook rekening worden gehouden met het onderwerp ontbinding en ongedaanmaking. Wordt een overeenkomst ontbonden wegens een wanprestatie dan ontstaan over en weer zogenaamde ongedaanmakingsverbintenissen.[72] Gevolg daarvan kan zijn dat de leverancier ontvangen betalingen moet terugbetalen aan de klant ('ongedaanmaken'). Net als de verplichting om een klant te vrijwaren geldt de verplichting om een ontvangen prestatie

[71] R.-J. Tjittes, *Commercieel Contractenrecht*. Deel I: totstandkoming en inhoud, Den Haag: Boom Juridische Uitgevers, 2018, pag. 417-419, 464-465.
[72] Artikel 2:265 BW resp. artikel 6:271 BW.

ongedaan te maken in beginsel niet als een verplichting tot het vergoeden van schade, zodat een exoneratie daarop in veel gevallen niet van toepassing zal zijn.

Onaanvaardbare exoneraties

Ten slotte is van belang dat een eenmaal overeengekomen beperking van aansprakelijkheid ook in rechte afdwingbaar is. Een exoneratie blijft buiten toepassing wanneer de bepaling naar maatstaven van redelijkheid en billijkheid onaanvaardbaar is.[73] Dit wordt ook wel de beperkende werking van de redelijkheid en billijkheid genoemd.

Bij de beoordeling of een exoneratiebeding naar maatstaven van redelijkheid en billijkheid onaanvaardbaar is, moet rekening worden gehouden met tal van omstandigheden, zoals: de zwaarte van de schuld, de aard en de verdere inhoud van de overeenkomst waarin het beding voorkomt, de maatschappelijke positie en de onderlinge verhouding van partijen, de wijze waarop het beding is tot stand gekomen, en de mate waarin de wederpartij zich de strekking van het beding bewust is geweest. Veel hangt dus af van de omstandigheden van het geval.[74]

In beginsel houdt een contractuele voorwaarde overeengekomen tussen professionele partijen stand. Ook een vergaande exoneratie of een exoneratie van een kernverplichting houdt in beginsel stand.[75] Slechts in uitzonderlijke omstandigheden wordt in IT-zaken toepassing gegeven aan de beperkende werking van de redelijkheid en billijkheid. Voor wat betreft exoneraties is dit vooral het geval (i) bij opzet of bewuste roekeloosheid van de IT-leverancier die zich op de exoneratie beroept;[76] en (ii) wanneer de klant een relatieve leek is op het gebied van de ingekochte IT-prestatie, partijen niet specifiek hebben onderhandeld over de exoneratie en de exoneratie tot gevolg heeft dat alle redelijkerwijs te verwachten schade is uitgesloten.[77]

De Clercq *takeaways*

- Het Nederlandse recht kent diverse grondslagen op basis waarvan een IT-leverancier aansprakelijk gesteld kan worden voor schade. Voor de IT-leverancier is het van belang dat de exoneratiebepaling duidelijk maakt dat de exoneratie geldt ongeacht de grondslag voor aansprakelijkheid.
- De begrippen directe en indirecte schade zijn ontleend aan de Anglo-Amerikaanse rechtspraktijk en hebben naar Nederlands recht geen vastomlijnde betekenis. Het is daarom zaak in het contract te definiëren wat onder deze

[73] Artikel 6:248 lid 2 BW.
[74] Hoge Raad 9 mei 1967, NJ 1967/261 (*Saladin/HBU*).
[75] Rb. Den Haag 14 maart 2018, ECLI:RBDHA:2018:3094 (*BrightContact/Belastingdienst*), r.o. 4.15; Hof Den Haag 27 september 2016, ECLI:NL:GHDHA:2016:2690 (*Alhra/ITC*), r.o. 5.2.
[76] Hoge Raad 5 september 2008, ECLI:NL:HR:2008:BD2984 (*Telfort/Scaramea*), r.o. 3.5.
[77] Rb. Rotterdam 10 februari 2016, ECLI:NL:RBROT:2016:1016 (*NBK/GreenCat*), r.o. 4.9, bevestigd in Hof Den Haag 21 november 2017, ECLI:NL:GHDHA;2017;3239 (*NBK/GreenCat*), r.o. 9.

begrippen moet worden verstaan. Alternatief is dat wordt aangesloten bij gangbare schadebegrippen in het Burgerlijk Wetboek.

- Nauw verwant aan het onderwerp aansprakelijkheid zijn afspraken over garanties, vrijwaringen en ongedaanmakingsverbintenissen. Voor leveranciers is het zaak terughoudend te zijn met het geven van garanties en vrijwaringen. Voorts is het voor IT-leveranciers aan te raden om expliciet op te nemen dat een exoneratie ook van toepassing is op een geschonden garantieverplichting, vrijwaringsverplichting en ongedaanmakingsverbintenis.
- Een exoneratie tussen professionele partijen houdt in beginsel stand, ook wanneer het een kernverplichting betreft. Slechts in uitzonderlijke omstandigheden wordt in IT-zaken toepassing gegeven aan de beperkende werking van de redelijkheid en billijkheid.

13. Contractmanagement: met een contract in handen is de kous af, toch?

Na ondertekening van een contract belandt deze vaak in een la en wordt er pas weer uitgehaald op het moment dat er een geschil is ontstaan. Ook raken contracten regelmatig zoek. Niet alleen in het bedrijfsleven, maar ook bij de overheid. Uit de uitkomsten van het onderzoek van de Tijdelijke Commissie ICT-projecten bij de overheid (commissie Elias) bleek dat het contractmanagement bij de overheid regelmatig tekortschiet. En dit is vaak niet zonder gevolgen.

Wat is contractmanagement nu precies?
ICT Contractmanagement is het managen van een overeenkomst na het sluiten van de overeenkomst. Het doel van contractmanagement is het daadwerkelijk realiseren van de doelstellingen van de overeenkomst. Om deze doelstellingen te realiseren dient toezicht te worden gehouden op de prestaties en op de naleving van de (financiële) afspraken.

Het kan ook noodzakelijk zijn de overeenkomst tijdens de looptijd aan te passen. Bijvoorbeeld aan wijzigingen in de organisatie of omgeving. Of partijen komen tot gewijzigde inzichten die aanpassingen in het contract vergen. Daarnaast blijkt geregeld dat contractafspraken onvoldoende concreet zijn en hiaten en onduidelijkheden bevatten.

Contractmanagement omvat dan ook de volgende werkzaamheden:

- Het bewaken van de nakoming van afspraken (niet alleen door de wederpartij, maar ook door de eigen organisatie);
- Het monitoren van de kwaliteit van de diensten;
- Het aanpassen van de overeenkomst aan de hand van wijzigingen;
- Het ondernemen van actie in het geval de contractpartij de contractuele afspraken niet nakomt.

Governance
In een goed contract is een duidelijke governance afgesproken. De verschillende overlegstructuren zijn beschreven (veelal op strategisch, tactisch en operationeel niveau) en beschreven is hoe escalatie dient plaats te vinden in geval van een probleem. Deze governanceafspraken zijn vaak vastgelegd in een Dossier Afspraken en Procedures (DAP). Het is belangrijk deze governance ook daadwerkelijk te volgen. Er zijn diverse uitspraken van rechters bekend waarin het niet volgen van de overeengekomen escalatieprocedure keihard werd afgestraft. Dit is begrijpelijk. Op het moment dat partijen afspraken maken over hoe te handelen in geval van een probleem, moeten ze erop kunnen vertrouwen

dat deze afspraken ook daadwerkelijk gevolgd worden als een probleem zich voordoet. Een voorbeeld: als in het contract is vastgelegd dat de IT-leverancier in de gelegenheid moet worden gesteld een verbeterplan op te leveren, dan kan de afnemer deze stap niet overslaan en de IT-leverancier in gebreke stellen.

SLA

In een SLA worden afspraken gemaakt over de kwaliteit van de diensten in de vorm van servicelevels. Het is belangrijk om deze servicelevels voortdurend te monitoren, te rapporteren en te evalueren, anders blijft de SLA een papieren tijger. Bovendien is het lastig om – vaak als de maat écht vol is – actie te ondernemen op het niet-nakomen van servicelevels als deze situatie in de weken, maanden of zelfs jaren daarvoor werd gedoogd. Ook hier is het van belang goed te kijken welke procedureafspraken zijn gemaakt en deze procedure ook daadwerkelijk te volgen.

Meerwerk

Meerwerkgeschillen vormen een klassiek probleem tussen leverancier en opdrachtgever bij ICT-contracten. Ook deze geschillen kunnen worden voorkomen door goed contractmanagement. Welke afspraken zijn er in het contract gemaakt over meerwerk? Wanneer is sprake van meerwerk? Welke procedures dienen te worden gevolgd om meerwerk te mogen verrichten? En wat zijn de consequenties indien deze procedures niet zijn gevolgd?

Bijhouden contractdossier

Het komt vaak genoeg voor dat het contractdossier niet op orde of incompleet is. Dit met alle gevolge van dien. Contracten staan niet op zich. Voor de uitleg en betekenis komt het namelijk niet alleen aan op het getekende contract, maar ook op alle informatie die tussen partijen is uitgewisseld. Denk daarbij aan presentaties die zijn gehouden, projectverslagen, presentaties, e-mails en soms ook alle conceptversies die voor het sluiten van de overeenkomst over en weer zijn gegaan. In het kader van professioneel contractmanagement zal een compleet contractdossier moeten worden aangelegd en bijhouden. Zo zullen notulen en verslagen moeten worden gemaakt van de overleggen op diverse niveaus en zal een actie- en besluitenlijst moeten worden bijgehouden.

Organisatorische inbedding van contractmanagement

Goed contractmanagement begint bij een goede organisatorisch inbedding. In sommige organisaties wordt contractmanagement als deeltaak bij een al bestaande afdeling neergelegd die meerdere contracten managen. Bij grotere contracten worden een of meerdere contractmanagers voor één contract aangewezen of wordt het contractmanagement uitbesteed aan een externe partij. Waar de verantwoordelijkheid ook wordt belegd, de expertise van de projectmanager(s) is van grote invloed op de efficiëntie en effectiviteit van het contractmanagement. Daarnaast is het van belang dat

men zich bewust is van het feit dat verschillende stakeholders betrokken zijn bij de uitvoering van een overeenkomst. Zowel intern als extern. Heldere communicatie naar alle stakeholders, zowel intern- als extern-gericht, is daarom van cruciaal belang.

De Clercq *takeaways*

- Met een contract in handen is de kous vaak niet af.
- Contractmanagement is een manier om grip te houden op de juiste nakoming van de contractuele afspraken en de overeengekomen actie te ondernemen in die gevallen waarin de IT-leverancier zich niet aan de afspraken houdt.
- Op het moment dat een IT-leverancier zich niet aan de afspraken houdt, dienen de overeengekomen procedures te worden gevolgd. Het overslaan van een of meerdere stappen kan de afnemer duur komen te staan.
- Zorg dat het contractdossier altijd up-to-date is. Op het moment dat er geen overzicht is over de gemaakte afspraken, is het niet mogelijk te sturen op de juiste nakoming van een contract en is het ook niet mogelijk een partij aan te spreken op grond van niet-nakoming.

14. Het belang van licentiemanagement

Organisaties gebruiken veel verschillende computerprogramma's. Meestal betreft dat software, die ze niet zelf hebben ontwikkeld en op basis van een gebruiks- of licentieovereenkomst gebruiken. Licentiemanagement is dan ook een noodzakelijk kwaad, maar vormt voor veel organisaties tevens een zorg. Regelmatig zijn licentieovereenkomsten bijvoorbeeld onvindbaar binnen een organisatie. Zij lopen hierdoor onnodig grote compliancerisico's en/of betalen onnodig veel geld aan licenties die zij (soms allang) niet meer gebruiken.

Oorzaken non-compliance

Uit diverse onderzoeken blijkt wat de belangrijkste oorzaken zijn van non-compliance. Allereerst wijt men dit aan de onbegrijpelijkheid van licentieovereenkomsten. Ook de complexiteit van de IT-omgeving is een belangrijke oorzaak. Tot slot worstelen veel organisaties met het overzicht houden over wat geïnstalleerd is en wat nu daadwerkelijk gebruikt wordt. Hoe groter de organisatie en hoe meer verschillende softwareproducten worden gebruikt, hoe lastiger het blijkt dit overzicht te behouden.

Geen eenduidigheid in licentievoorwaarden

Allereerst de onbegrijpelijkheid van licentievoorwaarden. Veel organisaties worstelen daarmee. Dit is niet verwonderlijk. Er zijn in de praktijk immers vele soorten licenties, die leveranciers ook weer verschillend uitwerken. Dit zorgt voor vragen als "heb ik de juiste hoeveelheid licenties?" en "pas ik de licenties goed toe?". Indien een licentievergoeding in rekening wordt gebracht per gebruiker is het bijvoorbeeld van belang vast te stellen of hiermee gedoeld wordt op concurrent users (gelijktijdige gebruikers), names users (benoemde gebruikers) of Adminstrator/read only user (bepaald type user). Indien wordt afgerekend per werkplek is de vraag of wordt uitgegaan van de werknemer (met soms meerdere devices) of iedere computer als aparte werkplek geldt? Ook is het van belang hoe wordt omgegaan met installatie op virtuele servers.

Open source

Een wijdverbreid misverstand is dat bij open source software licentieperikelen niet of nauwelijks meer aan de orde zouden zijn. Dit is niet het geval. Ook het gebruik van open source software is gebonden aan licentievoorwaarden. Bij sommige open source licenties ben je bijvoorbeeld verplicht om de naam van de oorspronkelijke maker te vermelden. Je hoeft jouw aanpassingen en toevoegingen zelf niet openbaar te maken. Bij andere open source licenties is het wel verplicht jouw wijzigingen en verbeteringen in de originele broncode openbaar maken. Dan zijn er ook nog open source licenties die je verplichten om ook de code die jij zelf ontwikkelt met behulp van de broncode openbaar

te maken voor anderen. Ook schending van open source licentievoorwaarden kan dus aan de orde zijn en kan zelfs leiden tot een rechtszaak.

Overige valkuilen

De meeste licentievoorwaarden verbieden het door derden laten gebruiken van de software. In geval van outsourcing is dit een belangrijk issue en kan een dergelijke bepaling grote consequenties hebben voor de business case. Verder geldt dat softwarelicenties regelmatig op naam van een rechtspersoon zijn aangeschaft, terwijl het feitelijk gebruik door een andere of meerdere rechtspersonen plaatsvindt. Bijvoorbeeld indien een centrale inkoopafdeling is ingericht bij een aparte rechtspersoon of de holding van de groep. Ook dit kan voor vervelende (financiële) verrassingen zorgen tijdens een audit door de leverancier.

Goede voorbereiding audit

Een goede voorbereiding begint eigenlijk al tijdens de contractonderhandelingen over de licentieovereenkomst. Iedere term in de licentieovereenkomst dient voor de afnemer helder te zijn. De praktijk leert immers dat iedere leverancier zijn eigen interpretatie aan bepaalde termen geeft. Uiteraard dient daarbij rekening te worden gehouden met toekomstplannen van de afnemer. Veel leveranciers verwijzen naar hun licentievoorwaarden op de website. Dit betekent dat zij deze gemakkelijk kunnen wijzigen. Het is daarom zaak de licentievoorwaarden te printen en als bijlage aan het contract te hechten. Eenzijdige wijzigingen door de leverancier dienen te worden uitgesloten.

Nog onvoldoende aandacht voor licentiemanagement

Licentiemanagement blijft binnen veel organisaties een punt van zorg. Er is onvoldoende overzicht over de in gebruik zijnde softwareapplicaties, geen overzicht over het feitelijk gebruik van de applicaties en de door leveranciers gehanteerde licentievoorwaarden zijn vaak onbegrijpelijk en bovendien aan wijzigingen onderhevig. Ondanks de financiële gevolgen die een audit kan hebben en de imagoschade die de organisatie op kan lopen, is er binnen veel organisaties nog onvoldoende aandacht voor licentiemanagement. Dit terwijl veel leed kan worden voorkomen door voldoende aandacht te besteden aan de (uitleg) van licentievoorwaarden tijdens de contractonderhandelingen en het centraal inkopen en beheren van licentiecontracten binnen de organisatie.

De Clercq *takeaways*

- Elke organisatie dient een actueel overzicht te hebben van de software die de organisatie in huis heeft en de regels die daarvoor gelden (wat zijn de gebruiksrechten en -beperkingen?). Licentiemanagement dient centraal belegd te zijn in de organisatie zodat één persoon of één afdeling een totaaloverzicht heeft en zich eindverantwoordelijk voelt;

- Het vooraf samenstellen van een auditteam zorgt ervoor dat na een aankondiging van een audit deskundig en snel kan worden geopereerd. Na een eventuele audit (en na de eventuele corrigerende maatregelen) dient erop worden toegezien dat de leverancier een document opstelt waarin hij verklaart dat de organisatie op dat moment compliant is.

15. Een ICT-geschil: wat nu?

Met regelmaat loopt een ICT-project niet zoals verwacht, zo is algemeen bekend. Vooral over mislukte ICT-projecten binnen de overheid is veel te doen geweest,[78] maar er is reden om te denken dat het ICT-projecten binnen de private sector niet veel beter vergaat. De kans is dus groot dat een afnemer of leverancier van ICT-prestaties vroeg of laat te maken krijgt met een geschil. Dit hoofdstuk belicht enkele aandachtspunten waarmee in dat geval rekening gehouden moet worden.

Remedies bij niet-nakoming

Op grond van de wet beschikt een teleurgestelde klant over verschillende remedies, zoals het vorderen van nakoming, schadevergoeding, opschorting van de eigen verplichtingen, verrekening of ontbinding van de overeenkomst.[79] Voor de meeste van deze remedies geldt de voorwaarde dat sprake moet zijn van een tekortkoming aan de kant van de leverancier. Bij een geschil is het dus allereerst zaak te beoordelen in hoeverre sprake is van een tekortkoming. Regelmatig zien wij in de praktijk dat er een verschil bestaat tussen hetgeen in de beleving van de klant is afgesproken en hetgeen feitelijk (aantoonbaar) is afgesproken. Voorkomen moet worden dat de klant er met gestrekt been ingaat terwijl de leverancier de afspraken blijkt te zijn nagekomen.

Inspannings- of resultaatsverbintenis?

Voor de beoordeling of sprake is van een tekortkoming is de aard van de verbintenis van groot belang. Bij een inspanningsverplichting kan immers worden volstaan met het leveren van een zekere inspanning en bij een resultaatsverbintenis is de schuldenaar gehouden een specifiek resultaat te behalen. Juist in IT-zaken is dit onderscheid relevant. Bij een mislukt IT-project is immers vaak sprake van een relatief omvangrijk en ingewikkeld feitencomplex. De oorzaak voor het mislukken van een project is vaak moeilijk eenduidig vast te stellen. Zowel technische, organisatorische, bestuurlijke als communicatieve factoren kunnen daarbij een rol spelen.

Nu de oorzaak voor het falen van een project moeilijk eenduidig is vast te stellen, is cruciaal wat de aard is van de verbintenis en wie ter zake de bewijslast – en dus het bewijs*risico* – draagt in het licht van artikel 150 Rv. Is sprake van een resultaatsverbintenis, dan kan de opdrachtgever in beginsel volstaan met het leveren van bewijs dat het afgesproken resultaat is uitgebleven. Het is dan aan de opdrachtnemer om aan te tonen dat sprake is van overmacht dan wel schuldeiserverzuim. Is slechts sprake van een

[78] Parlementair onderzoek naar ICT Projecten bij de overheid, TK 2014-2015 33 326, nr. 5.
[79] Artikelen 3:296 BW, resp. artikel 6:74 BW, resp. artikelen 6:52 en 6:262 BW, resp. artikel 6:127 BW resp. artikel 6:265 BW.

inspanningsverbintenis aan de kant van de opdrachtnemer dan zal de opdrachtgever moeten aantonen dat de opdrachtnemer heeft nagelaten de overeengekomen inspanning te leveren. Dit is doorgaans een zeer zware opgave. In enkele recente uitspraken slaagt de opdrachtgever bijvoorbeeld niet in het leveren van zulk bewijs.[80]

De zorgplicht als reddingsboei?

Wanneer duidelijke resultaatafspraken ontbreken dan kan de zorgplicht voor de teleurgestelde klant nog als 'reddingsboei' fungeren. Veel IT-prestaties worden – zoals al eerder genoemd – geleverd op basis van een overeenkomst van opdracht, waardoor de IT-leverancier de zorg van een goed opdrachtnemer in acht moet nemen. Ter opfrissing: concreet betekent dit dat de IT-leverancier zich moet opstellen als een redelijk bekwaam en redelijk handelend vakgenoot.[81]

Door de jaren heen is er een levendige IT-zorgplichtjurisprudentie ontstaan.[82] In verreweg de meeste gevallen waarin een schending van een zorgplicht door een IT-dienstverlener wordt aangenomen, is sprake van een schending van een informatie- of waarschuwingsplicht. Maar ook kwaliteitsaspecten kunnen langs de band van de zorgplicht worden meegewogen bij de uitleg van een overeenkomst.[83] De zorgplichtjurisprudentie is zeer casuïstisch van aard. Het is dus zaak aan de hand van het dossier zorgvuldig te beoordelen of mogelijk een zorgplicht is geschonden.

Acceptatietestprocedure

Een ander belangrijk aandachtspunt bij een dreigend geschil is de acceptatietestprocedure. Veel softwaretoepassingen worden door de leverancier opgeleverd aan de klant, waarna de klant de toepassing gedurende een zekere periode kan testen om te beoordelen of de applicatie voldoet aan hetgeen is afgesproken. Een dergelijke procedure wordt bijvoorbeeld beschreven in artikel 36 van de NLdigital Voorwaarden en in de artikelen 11 en 59 van de ARBIT-2022.

Een IT-systeem geldt vaak als geaccepteerd (i) als de klant de testperiode laat verstrijken zonder een testrapport op te leveren; (ii) nadat fouten die tijdig binnen de testperiode zijn gerapporteerd door de leverancier zijn hersteld; of (iii) op het moment van ingebruikname van de software (dat laatste geldt niet op grond van de ARBIT-2022). Nadat de software eenmaal is geaccepteerd kunnen gebreken die de klant redelijkerwijs

[80] Rb. Amsterdam 31 maart 2021, ECLI:NL:RBAMS:2021:2008 (*Webs Inbound/Scanmar*); en Hof Den Haag 7 september 2021, ECLI:NL:GHDHA:2021:1720 (*MR2/Result XL*).
[81] Hof Den Haag 8 maart 1984, *Computerrecht* 1984 afl. 2 (p. 29) (*RBC/ Brinkers*), bekrachtigd door HR 11 april 1986, *Computerrecht* 1986 afl. 3 (p. 174) (*RBC/Brinkers*).
[82] Voor een overzicht van de IT-zorgplichtjurisprudentie, zie: P.G. van der Putt & C.A.M. van de Bunt, 'Bijzondere zorgplichten van IT-leveranciers', *Computerrecht* 2018/160; en P.G. van der Putt & C.A.M. van de Bunt, 'Update Nederlandse zorgplicht-jurisprudentie', *Computerrecht* 2021/207.
[83] Rb. Amsterdam 18 december 2019, ECLI:NL:RBAMS:2019:9635 (*Smart Connections/All Safe*); Rb. Rotterdam 2 maart 2022, ECLI:NL:RBROT:2022:1641 (*Dream Bid/DPDK*), r.o. 4.13.

had kunnen ontdekken tijdens de testperiode in beginsel niet meer worden tegengeworpen aan de leverancier. Het is als afnemer dus zaak om de acceptatietestprocedure goed voor te bereiden, daarover afspraken te maken met de leverancier, en om de termijn voor het rapporteren van fouten goed in het oog te houden.

Verzuim en ingebrekestelling

Is sprake van een tekortkoming, dan bestaat nog niet automatisch een recht op schadevergoeding of ontbinding van de overeenkomst. Daarvoor is ook 'verzuim' nodig. De hoofdregel is dat het verzuim intreedt nadat een ingebrekestelling is verstuurd waarin een redelijke termijn voor herstel is geboden en welke termijn niet is gehaald. In opvallend veel ICT-geschillen wordt deze stap echter overgeslagen. Partijen corresponderen weliswaar veel, maar een (goede) ingebrekestelling ontbreekt in het dossier. De klant zal in dat geval een beroep moeten doen op een van de uitzonderingen op de hoofdregel dat voor verzuim een ingebrekestelling nodig is.

Fatale termijnen

Geen ingebrekestelling is nodig wanneer een fatale termijn is geschonden (artikel 6:83 onderdeel a BW). De hoofdregel is dat een *overeengekomen* termijn voor nakoming in beginsel fataal is (fataal, tenzij).[84] Het enkel eenzijdig stellen van een termijn is echter niet voldoende. Een go-livedatum die in projectverband wordt gehanteerd geldt om die reden nog niet automatisch als een fatale termijn.[85] Daarvoor is nodig dat deze datum *als opleverdatum* met de leverancier is afgesproken, in de zin dat laatstgenoemde gehouden is ervoor te zorgen dat ingebruikname van het systeem uiterlijk op een bepaalde datum mogelijk is.

In de overeenkomst kan overigens van het 'fataal, tenzij' uitgangspunt worden afgeweken. Zo is in de NLdigital Voorwaarden opgenomen dat oplevertermijnen in beginsel steeds gelden als streefdata en dat het enkele missen van deze termijnen niet zal leiden tot verzuim. Het fatale karakter van een termijn moet in dat geval dus uitdrukkelijk uit de overeenkomst blijken (niet-fataal, tenzij). In IT-projecten wordt verder regelmatig afgeweken van de oorspronkelijke planning of worden geen consequenties verbonden aan het overschrijden van een termijn. Dit kan ertoe lijden dat een termijn zijn fatale karakter verliest (de 'doormodderdoctrine').[86]

[84] T&C BW, commentaar op artikel 6:83 BW, aantekening 2. Zie ook: Hoge Raad 4 oktober 2002, ECLI:NL:HR:2002:AE4358 (*Fraanje/Götte*).
[85] Hof Amsterdam 9 juli 2013, ECLI:NL:GHAMS:2013:2121 (*Tycobuilding/Inter Access*).
[86] P.G. van der Putt, 'Update Nederlandse IT-wanprestatiejurisprudentie', *Computerrecht* 2019/214, para. 4.

Nakoming blijvend onmogelijk?

Verzuim is niet vereist wanneer nakoming blijvend onmogelijk is. De gedachte daarachter is dat het geen zin heeft een hersteltermijn te geven als nakoming toch niet mogelijk is. Door de Hoge Raad is bepaald dat indien sprake is van levering van een zaak en die zaak dermate ondeugdelijk is opgeleverd dat herstel slechts mogelijk is door opnieuw te beginnen, de prestatie als definitief verricht moet worden beschouwd.[87] In IT-zaken is daarom wel erkend dat nakoming blijvend onmogelijk is als het systeem dermate ondeugdelijk is dat in feite een volledige herbouw nodig is om het systeem aan de overeengekomen eisen te laten voldoen.[88] In dat geval is dus geen ingebrekestelling nodig.

Redelijkheid en billijkheid

Ten slotte kan het verzuim ook intreden op grond van de redelijkheid en billijkheid.[89] Hiervoor kan bijvoorbeeld aanleiding bestaan wanneer de IT-leverancier niet of niet toereikend reageert op een verzoek van de klant om binnen een redelijke termijn toe te zeggen dat hij binnen een gestelde, eveneens redelijke, termijn zal nakomen.[90] Of om zich binnen een redelijke termijn uit te laten over de wijze waarop en de termijn waarbinnen hij door de klant omschreven gebreken in de uitvoering van de overeenkomst zal herstellen.[91]

De Clercq *takeaways*

- Op grond van de wet beschikt een teleurgestelde klant over verschillende remedies, zoals het vorderen van schadevergoeding, opschorting van de eigen verplichtingen, of ontbinding van de overeenkomst.
- Voor de meeste van deze remedies geldt de voorwaarde dat sprake moet zijn van een tekortkoming aan de kant van de leverancier. Bij een geschil is het dus allereerst zaak zorgvuldig te beoordelen in hoeverre sprake is van een tekortkoming.
- Bij het maken van die beoordeling is een belangrijk aandachtspunt of sprake is van een inspannings- of resultaatsverbintenis. De positie van de klant is over het algemeen lastig bij een inspanningsverbintenis, maar de zorgplicht kan mogelijk fungeren als reddingsboei.
- Is een acceptatietestprocedure overeengekomen, dan is het belangrijk dat de klant de procedureregels volgt en de leverancier binnen de afgesproken termijn op de hoogte stelt van gebreken.

[87] Hoge Raad 22 mei 1981, NJ 1982, 59.
[88] Hof Amsterdam 14 februari 2012, ECLI:NL:GHAMS:2012:4473 (*Waterdrinker/SAP*); Hof Amsterdam 20 oktober 2020, ECLI:NL:GHAMS:2020:2749 (*Equihold/Capgemini*).
[89] Hoge Raad 4 oktober 2002, ECLI:NL:HR:2002:AE4358 (*Fraanje/Götte*).
[90] Hoge Raad 11 oktober 2019, ECLI:NL:HR:2019:1581 (*Fraanje/Alukon*).
[91] Hoge Raad 11 oktober 2019, ECLI:NL:HR:2019:1581 (*Fraanje/Alukon*).

- Voor schadevergoeding en ontbinding is niet alleen een tekortkoming nodig maar doorgaans ook verzuim. In de regel moet de klant hiervoor een ingebrekestelling versturen.

16. Beoordeling van inschrijvingen

Bijzondere aandacht verdient de beoordeling van de inschrijving. Dat maakt namelijk het verschil tussen het winnen of verliezen van de aanbesteding. Uiteraard moet de voorgenomen gunningsbeslissing gemotiveerd worden en moet een standstill-termijn in acht worden genomen alvorens definitief mag worden gegund. Dat laatste geeft de verliezende inschrijver(s) de mogelijkheid om de beslissing aan de rechter voor te leggen. De mogelijke bezwaren tegen de voorgenomen gunningsbeslissing zijn oneindig. Van onmogelijk (veronderstelde) prijzen van de winnende inschrijver tot fouten in de berekening van de score. Zeer regelmatig ziet het bezwaar (ook) op de wijze waarop de beoordelingscommissie de inschrijving heeft beoordeeld. Om die reden staan wij iets uitvoeriger stil bij beoordelingscommissies.

Beoordelingscommissies

Beoordelingscommissies zijn soms noodzakelijk. Niet alle goederen en diensten kunnen worden beoordeeld op basis van objectieve kenmerken. Knelpunt bij beoordelingscommissies is vaak de aanvaardbaarheid van die beoordeling. Inzicht in de hoofden van de leden van de commissie is niet mogelijk en daarom schort het aan de objectieve controleerbaarheid van een beoordeling. Om die reden pleit(t)en wij ervoor beoordelingscommissies alleen in te zetten in die gevallen dat het echt noodzakelijk is. Uiteraard ervaart vooral de verliezende inschrijver het gebrek aan controleerbaarheid. Waarom werd zijn inschrijving bijvoorbeeld als ‘goed’ en niet als ‘zeer goed’ beoordeeld?

Uitgangspunt

Uitgangspunt is dat de beoordelingscommissie een ruime beoordelingsvrijheid heeft, zolang hij maar transparant handelt en inschrijvers gelijk behandelt. Deze verplichtingen brengen mee (i) dat het voor inschrijvers duidelijk moet zijn wat van hen wordt verwacht, (ii) dat de inschrijvingen aan de hand van een zo objectief mogelijk systeem moeten worden beoordeeld en (iii) dat de gunningsbeslissing zodanig inzichtelijk moet worden gemotiveerd dat de afgewezen inschrijvers kunnen toetsen op welke wijze de beoordeling heeft plaatsgevonden.[92]

In de meeste zaken gaat het om de vraag of de beoordelingscommissie juist heeft gehandeld. De lijn daarin is dat de rechter terughoudend het handelen toetst. Rechters achten zich niet deskundig in de te beoordelen materie. Dat vond ook de Rechtbank Den Haag in een zaak die Actacom Nederland tegen een onderwijsinstelling had aangespannen na de aanbesteding van (o.a.) beheer en onderhoud van een datacentrum. De rechter vond het niet aan hem om te beoordelen of de inschrijving moest worden

[92] Hof Den Haag 30 oktober 2018, ECLI:NL:GHDHA:2018:2878.

beoordeeld als 'goed' of 'zeer goed'.[93] Inmiddels mag de *inhoud* van de beoordeling – wat ons betreft – niet meer het speerpunt van een procedure zijn, tenzij apert sprake is van een duidelijk onjuist oordeel. Dat ligt anders bij een gebrekkige motivering, waarover later meer. Kansrijker is het om te procederen over meer procedurele aspecten. Aan de hand van een aantal noemenswaardige uitspraken van het afgelopen jaar lichten wij dit nader toe.

Drie of vier beoordelaars?

Bij de aanbesteding van een DMS (Document Management System) zouden de inschrijvers punten toebedeeld krijgen van vier beoordelaars. Als gevolg van het uitvallen van de vierde beoordelaar besloot de aanbestedende dienst, Eindhoven Airport, de beoordeling te laten plaatsvinden door de resterende drie beoordelaars. Gelijke behandeling was daarmee gewaarborgd. Alle drie de inschrijvers werden immers op dezelfde wijze beoordeeld, zo dacht men. De rechter ging hier niet in mee. Door het ontbreken van de vierde beoordelaar was de beoordelingswijze op een essentieel onderdeel gewijzigd. Dat is niet toegestaan en de verliezende inschrijver (Advantive) kreeg gelijk:

> *"Er hebben zich niet alleen slechts drie personen gebogen over de inschrijvingen, ook heeft er na het individueel door de beoordelaars toekennen van de cijfers een overleg plaatsgevonden met slechts drie in plaats van vier personen, die gezamenlijk tot een definitieve score zijn gekomen."*[94]

Van belang is om te realiseren dat het hierbij ging om de samenstelling van de commissie. Als een beoordelingscommissie zich – onaangekondigd – laat bijstaan door een adviseur, dan wijzigt dit strikt genomen niet de samenstelling van de commissie. De rechter oordeelde dan ook het laten bijstaan door een adviseur is toegestaan.[95] Een adviseur is immers geen beoordelaar en is geen onderdeel van een beoordelingscommissie. Dit is anders indien de adviseur feitelijk als onderdeel gaat functioneren van de commissie door bijvoorbeeld punten toe te kennen of de doorslag geeft bij onverdeeldheid binnen een beoordelingscommissie. Wees dus alert op de feitelijke rol die een adviseur heeft bij de beoordeling.

Ondeskundige beoordelaars?

Een ander aspect dat niet de inhoudelijke beoordeling raakt, is de samenstelling van een beoordelingscommissie. De leden dienen deskundig te zijn en die deskundigheid wordt in beginsel aangenomen. Echter, een directeur financiën is niet de aangewezen persoon

[93] Rb. Den Haag 11 december 2018, ECLI:NL:RBDHA:2018:14593 en zie ook: https://www.declercq.com/kennisblog/aanbesteding-ict-oplossingen-in-de-onderwijswereld/.
[94] Rb. Oost-Brabant, 16 november 2018, ECLI:NL:RBOBR:2018:5690.
[95] Rb. Den Haag 11 december 2018, ECLI:NL:RBDHA:2018:14593.

om een inhoudelijk oordeel te geven over de kwaliteit van een inschrijving waaraan ieder financieel aspect ontbreekt, zo oordeelde de rechter.[96] Belangrijk is dus dat je kritisch bent op de samenstelling van de beoordelingscommissie. Wie nemen plaats en zijn zij deskundig?

Souplesse en beoordelingscommissies

Wellicht denk je na het lezen van deze highlights van het afgelopen jaar dat alleen klachten over procedurele aspecten succes kunnen hebben. Wees gerust, weliswaar is duidelijk dat procedurele klachten meer succes hebben, maar ook kan het lonen een inhoudelijke beoordeling aan te vechten. Voorwaarde is dat de beoordelingscommissie niet in redelijkheid tot haar oordeel heeft kunnen komen. De bewijslast daarvan rust op de inschrijver.

Toen een beoordelingscommissie overwoog dat "wanneer de eisen strikt gehanteerd zouden worden de inschrijver niet voor gunning in aanmerking zou komen", maar dat "met enige souplesse een aantal blokkerende issues overkomen kunnen worden" en dat daarom het op een subonderdeel het oordeel 'matig' werd toegekend (in plaats van onvoldoende), was de rek er bij de rechter wel uit.[97] Dat oordeel van de beoordelingscommissie was ontoelaatbaar.

Dat was ook het geval toen een beoordelingscommissie (negatieve) ervaringen van een andere opdrachtgever meewoog in haar beoordeling. Hiermee werd een nieuw element aan de beoordeling toegevoegd dat niet in de aanbestedingsstukken was voorzien en waar de inschrijvers ook niet over waren geïnformeerd. Een dodelijke fout![98] Overigens hoeven ervaringen van andere opdrachtgevers niet geheel buiten beschouwing te worden gelaten, daarvoor wordt dan echter meestal plaats ingeruimd in de (eerdere) selectiefase, waar "technische bekwaamheid en beroepsbekwaamheid" dan met referentie-opdrachten kan worden onderbouwd.

Baanbrekend

Op grond van het voorgaande kunnen we concluderen dat rechters de handelwijze van beoordelingscommissies behoorlijk terughoudend toetsen. In een op 13 juni 2019 gepubliceerde uitspraak greep de rechtbank Amsterdam echter hard in.[99] Waar ging het om? De gemeente Amsterdam had een aanbesteding 'Scannen en Printen' uitgeschreven op basis van de Best Value benadering. Bij 'Best Value' wordt niet in detail voorgeschreven aan welke voorwaarden de inschrijving moet voldoen, maar wordt de inschrijvers zoveel mogelijk ruimte geboden voor een eigen invulling van de aanbieding.

[96] Rb. Midden-Nederland 27 juli 2018, ECLI:NL:RBMNE:2018:3579.
[97] Rb. Den Haag 17 oktober 2018, ECLI:NL:RBDHA:2018:12401.
[98] Hof Den Haag 30 oktober 2018, ECLI:NL:GHDHA:2018:2878.
[99] Rb. Amsterdam 9 mei 2019, ECLI:NL:RBAMS:2019:4206.

Net als bij iedere gunningsbeslissing geldt ook bij Best Value procurement dat de gunningsbeslissing moet worden gemotiveerd. Dat is immers vastgelegd in de Aanbestedingswet (Aw).[100] De verliezende inschrijver vond dat de gunningsbeslissing onvoldoende was gemotiveerd. Zij stelde dat het volstrekt onduidelijk was waarom haar inschrijving op verschillende onderdelen 'maar' met een zes werd beoordeeld. De mededeling dat haar beantwoording onvoldoende SMART was, was volgende de inschrijver onvoldoende concreet.

De rechtbank herhaalde eerst de standaardoverweging die de afgelopen jaren in de jurisprudentie is neergezet: de rechter heeft slechts een beperkte beoordelingsruimte. Echter, daarna nam de Rechtbank Amsterdam een andere afslag en oordeelde:

> *"(...) dat indien sprake is van zodanige onjuistheden of onduidelijkheden in de motivering van de gunningsbeslissing dat redelijk handelende en redelijk deskundige beoordelaars deze niet mochten laten ontstaan en de aanbesteder deze niet voor zijn rekening mocht nemen, plaats is voor ingrijpen door de rechter. Voor rechterlijk ingrijpen is dus niet slechts aanleiding in geval van evidente onjuistheden."*

Dat was hier het geval. De verliezende inschrijver was in casu namelijk niet in staat om de wijze van beoordeling te toetsen. Daarmee was de motiveringsplicht geschonden. De gegeven motivering, dat 'beantwoording onvoldoende smart is' kon niet door de beugel. Dit veronderstelde namelijk een nadere motivering *waarom* zulks onvoldoende was. Die nadere motivering ontbrak. De gemeente Amsterdam moest daarom overgaan tot herbeoordeling door een nieuwe beoordelingscommissie.

Deze uitspraak dwingt aanbestedende diensten om zeer zorgvuldig te kijken naar hun motivering, ook waar het een oordeel van haar beoordelingscommissie betreft. Ondanks dat het slechts één uitspraak betreft, hechten wij veel waarde aan de overwegingen van de rechtbank. De rechter die de zaak behandelde is namelijk de voormalig vicepresident van Hoge Raad, die de laatste jaren voor zijn pensioen nog eens 'eenvoudige' rechter wilde zijn.

De Clercq *takeaways*

- De omstandigheid dat beoordelingscommissies vaak de doorslag geven bij het bepalen van de winnende inschrijver en het feit dat beoordelen mensenwerk blijft, maakt dat ook komende jaren wij uitspraken verwachten over het handelen en de samenstelling van beoordelingscommissies verwachten. Het blijft simpelweg een essentieel aspect bij veel aanbestedingen. En zeker bij IT-

[100] Artikel 2.130 Aw.

aanbestedingen, waar het vaak aankomt op de beoordeling van kwalitatieve criteria.

- Aan de beoordeling door deskundigen is een zekere mate van subjectiviteit nu eenmaal inherent, hoezeer ook wordt getracht die te objectiveren. Ongetwijfeld zal ook het aantal procedures over de motivering van de gunningsbeslissing een stijgende lijn vertonen. Wij verwachten ook dat, na de uitspraak van de Rechtbank Amsterdam, rechters vaker zullen ingrijpen.

17. Vormen van geschilbeslechting

Is er een geschil en blijkt – zelfs na tussenkomst van advocaten – een onderlinge oplossing niet mogelijk, dan is hulp van buitenaf nodig. Die hulp komt in verschillende vormen. De drie belangrijkste daarbij zijn mediation, de overheidsrechter of arbitrage.

Mediation
Alvorens te kiezen voor arbitrage of de overheidsrechter, zou een logische overweging altijd mediation moeten zijn. Wellicht is die overweging kort – bijvoorbeeld omdat het geschil te principieel of complex is – toch is het wijs die overweging te maken. Ten opzichte van de andere mogelijkheden is mediation namelijk goedkoper, sneller en houden partijen zelf de regie. Regie over de vraag of een volgende bijeenkomst zinvol is. En belangrijker: regie over de vraag of de oplossing die op tafel komt aanvaardbaar is. Bij de overheidsrechter en arbitrage geven partijen de besluitvorming volledig uit handen.

In de (IT)-praktijk is de inzet van mediation beperkt. Vaak is de materie complex, omvangrijk en verschillen de zienswijze van partijen principieel. De opdrachtgever vindt bijvoorbeeld dat de code slecht is geschreven, terwijl de opdrachtnemer nog nooit zulke mooie code heeft gezien. Ook zijn de belangen financieel vaak dusdanig dat 'middelen' geen reële optie is. Dat zijn belangrijke verschillen met dossiers waarin mediation populair is, zoals arbeidsgeschillen of burenruzies.

Overheidsrechter
Als partijen de beslissing over hun conflict uit handen durven geven, dan is de overheidsrechter geen vreemde keuze. De juridische kwaliteit is uitstekend, de rechter behandelt de zaak voor een transparant vast bedrag aan griffierechten, en er is altijd de mogelijkheid van hoger beroep bij het Hof. Er is zelfs een mogelijkheid tot cassatie bij de Hoge Raad. Bij arbitrage zijn die mogelijkheden beperkter of soms geheel afwezig.

Nadeel is echter dat de gemiddeld doorlooptijd lang is en dat specifieke technische IT-kennis ontbreekt. Vooraf is onduidelijke welke rechter de zaak zal behandelen en of die rechter beschikt over (basis) IT-kennis. Zo maakte ik mee dat het voor een oudere rechter onbegrijpelijk was wat een .zip-bestand was. Dat dit bestand een bepaalde omvang had (rechtermuisknop eigenschappen) was helemaal niet uit te leggen. De rechter kan zich weliswaar laten voorlichten door een te benoemen IT-deskundige, maar dat is uiteindelijk aan de rechter, kost veel tijd en is bovenal kostbaar.

Maken partijen geen afwijkende afspraken, dan staat de weg naar de overheidsrechter altijd open. In veel algemene voorwaarden wordt ook uitdrukkelijk voor de overheidsrechter gekozen. Zo bepalen de Algemene Rijksvoorwaarden bij IT-overeenkomsten 2018 (ARBIT-2018) dat de rechtbank Den Haag bevoegd is om over geschillen te oordelen. Dat laat zien dat de rijksoverheid veel vertrouwen heeft in overheidsrechtspraak.

Arbitrage

Belangrijk voordeel is dat bij arbitrage meer technische deskundigheid kan worden gewaarborgd. Zeker wanneer partijen zelf hun arbiters selecteren, is deskundigheid een gegeven. Een veel geziene samenstelling is een arbitraal college bestaande uit twee materiedeskundigen onder leiding van een voorzitter die vaak een ervaren jurist of rechter is. Die samenstelling maakt het mogelijk om tot een hoogwaardig inhoudelijk correct oordeel te komen, waarbij sneller een oordeel kan worden gevormd omdat vaak geen deskundigen hoeven te worden aangezocht. Die materiedeskundigen zijn immers onderdeel van het arbitrale college.

Voordeel is verder dat – afhankelijk van het te benaderen arbitrage-instituut – de procedure flexibeler is dan die bij de overheidsrechter. Ook vertrouwelijkheid is vaak een belangrijke beweegreden. Uitspraken van de overheidsrechter zijn openbaar en verschijnen veelal op rechtspraak.nl, terwijl partijen bij arbitrage vertrouwelijk kunnen afspreken. Dat voorkomt aandacht van de media, reputatieschade en geeft partijen de mogelijkheid om bedrijfsvertrouwelijke informatie tijdens de procedure naar voren te brengen zonder dat een concurrent in de zaal meeluistert.

De samenstelling brengt ons echter ook bij een nadeel. Personen die in de markt als deskundig bekend staan, hanteren bij arbitrage commercieel verantwoorde uurtarieven. Bij een arbitraal college bestaande uit drie arbiters, zijn er dus drie personen die ieder nauwgezet het dossier bestuderen, de zitting(en) voorbereiden en het vonnis schrijven. Die kwaliteit komt dus met een prijskaartje, terwijl bij overheidsrechtspraak de kosten vaak vele malen lager liggen omdat de te betalen griffierechten niet kostendekkend zijn. Vaak zijn de administratiekosten bij een arbitrage al hoger dan het griffierecht bij de rechtbank, zulks nog zonder de kosten van de arbiters.

Belangrijk om te realiseren is dat de mogelijkheden bij arbitrage omvangrijk zijn. Zo behandelende wij afgelopen jaren bijvoorbeeld geschillen waarbij partijen geen arbitrage-instituut wilde benaderen. De advocaten maken in zo een geval procesafspraken over de te voeren procedure en laten zich daarbij wellicht inspireren door de wetgeving die bij de overheidsrechter geldt of door een arbitragereglement. Er zijn echter ook instituten die de administratie rondom een arbitrage verzorgen en een register aan beschikbare arbiters kennen. Een van de bekendste voor de IT-branche de

stichting Geschillenoplossing Organisatie & Automatisering, het SGOA. Deze stichting wordt bijvoorbeeld in de NLdigital voorwaarden aangewezen als bevoegd arbitraal collega.

De Clercq *takeaways*

- Een eerste mogelijkheid die overwogen moet worden bij een aanhoudend geschil is mediation. Mediation is namelijk goedkoper, sneller en autonomer dan de andere mogelijkheden. Complexiteit en verschillen in zienswijze zorgen er echter voor dat mediation niet de meest gekozen weg is bij IT-geschillen.
- De tweede mogelijkheid is de overheidsrechter. Hierbij is de juridische kwaliteit vaak hoger en er zijn vaak meerdere beroepsmogelijkheden, dit is niet zo bij arbitrage. De nadelen zijn echter dat de doorlooptijd vaak lang is en dat specifieke technische IT-kennis vaak ontbreekt.
- De laatste mogelijkheid is arbitrage. Hierbij is het eerste grote voordeel dat er veel technische deskundigheid kan worden gewaarborgd. Daarnaast is ook de procedure flexibeler en kan vertrouwelijkheid beter worden gewaarborgd. De keerzijde van de deskundigheid is echter wel dat dit vaak resulteert in een hoog prijskaartje.

Auteurs

Aan dit boek hebben meegeschreven:

Natascha van Duuren
advocaat / partner IT, IE & Privacy
n.vanduuren@declercq.com
+31654983766

Jeroen van Helden
advocaat IT, IE & Privacy
j.vanhelden@declercq.com
+31628536054

Michelle Wijnant
advocaat IT, IE & Privacy
m.wijnant@declercq.com
+31612628121

Menno de Wijs
advocaat, IT en Aanbestedingsrecht
m.dewijs@declercq.com
+31641194880

DE CLERCQ
Advocaten • Notariaat

Leiden: Hoge Rijndijk 306
Den Haag: WTC The Hague,
Prinses Margrietplantsoen 33

info@declercq.com +31 71 58 15 300