Artikel

Data, de Wet bescherming bedrijfsgeheimen en het contractenrecht

Mr. drs. M. Kool*

1. Inleiding

40 De Wet bescherming bedrijfsgeheimen (Wbbg) is inmiddels ruim twee jaar van kracht. De wet¹ kent aan rechtmatige houders van bedrijfsgeheimen bepaalde vorderingsrechten toe waarmee kan worden opgetreden tegen inbreuken op die bedrijfsgeheimen. Op vordering van de houder van een bedrijfsgeheim kan bijvoorbeeld een verbod worden opgelegd tot staking van of verbod op het gebruik van een bedrijfsgeheim. De Wbbg kan een aanvulling vormen op bescherming door middel van intellectuele eigendomsrechten (IE-rechten), of een alternatief bieden. Dit laatste kan spelen als men (nog) niet voor bescherming door middel van een IE-recht in aanmerking komt, bijvoorbeeld ingeval men nog niet klaar is met de ontwikkeling van een uitvinding (en het al dan niet nog onzeker is of de uitvinding octrooieerbaar is). Maar ook als men – om de openbaarheid te mijden – (nog) niet in aanmerking wil komen voor bescherming door middel van een IE-recht, kan een beroep op de Wbbg mogelijk uitkomst bieden.² Dit artikel gaat

over het scenario dat een onderneming ‘iets’ heeft wat commerciële waarde heeft, maar waarop helemaal geen IE-rechten – noch andere eigendomsrechten – van toepassing lijken te kunnen zijn: data. Door de Wbbg in de contractspraktijk slim te benutten kunnen data alsnog beter worden beschermd. Dit artikel geeft daarvoor enkele concrete tips.³

2. Kwalificatie bedrijfsgeheim

Er zijn veel soorten informatie en knowhow die kunnen kwalificeren als ‘bedrijfsgeheim’. Artikel 1 Wbbg bepaalt dat een bedrijfsgeheim ‘informatie’ is die voldoet aan de volgende cumulatieve voorwaarden (geparafraseerd):

1. de informatie moet geheim zijn, in haar geheel dan wel in de juiste samenstelling en ordening van haar bestanddelen, niet algemeen bekend of gemakkelijk toegankelijk voor degenen binnen de kringen van personen die zich gewoonlijk bezighouden met dergelijke informatie;
2. de informatie moet handelswaarde bezitten omdat zij geheim is; en
3. de informatie moet, door degene die daar rechtmatig over beschikt, zijn onderworpen aan redelijke maatregelen (gezien de omstandigheden) om deze geheim te houden.

* Mr. drs. M. Kool is advocaat bij The Data Lawyers B.V.

1. Die zijn oorsprong kent in het TRIPS-verdrag en een implementatie vormt van de Richtlijn (EU) 2016/943 betreffende de bescherming van niet-openbaar gemaakte knowhow en bedrijfsinformatie (bedrijfsgeheimen) tegen het onrechtmatig verkrijgen, gebruiken en openbaar maken daarvan.
2. Zoals de memorie van toelichting bij de Wbbg het verwoordt: ‘Zo begint menig IE-recht met een geheim: het plot van een auteur, schetsen van een nieuw model auto, onderzoeksresultaten met betrekking tot een nieuw medicijn of plannen ten aanzien van een nieuw merkproduct. In gevallen waar bescherming van knowhow en informatie door IE-rechten (nog) niet mogelijk of gewenst is, voldoet deze knowhow en informatie misschien wel aan de voorwaarden voor de bescherming als

bedrijfsgeheim’ (MvT Kamerstukken II 2017/18, 34821, nr. 3, onder 1.3.1, p. 5).

3. Voor meer algemene informatie, achtergronden en historie van de Wbbg verwijs ik naar het artikel ‘Wet bescherming bedrijfsgeheimen’ in Onderneming en Financiering (2018/4), van Oostwouder, Thonen en mijzelf.

De memorie van toelichting geeft verschillende voorbeelden van informatie die een bedrijfsgeheim kan zijn, waaronder fabricagemethoden, recepturen, handelsgegevens, informatie over klanten en leveranciers, bedrijfsplannen of marktonderzoek en marktstrategieën.

In de huidige tijdsgeest en dus ook in de rechtspraak is er veel aandacht voor het beschermen van (digitale) ‘data’ en/of ‘big data’ vanwege de commerciële waarde die ze vertegenwoordigen. In feite gaat de Wbbg ook over het beschermen van data. Het begrip ‘data’ is immers informatie,⁴ of zuiverder: data geplaatst in een context krijgt betekenis en wordt informatie.⁵ De hiervoor gegeven voorbeelden van informatie die een bedrijfsgeheim kan zijn, vinden veelal hun oorsprong in data. Met big data worden – al dan niet ongeordende, ruwe – grote verzamelingen van data bedoeld.⁶ Big data worden doorgaans gebruikt om analyses te maken, denk bijvoorbeeld aan Spotify en Netflix, die op basis van alle gebruikersdata voorspellingen kunnen maken over wat een specifieke gebruiker waarschijnlijk goede muziek of een goede serie zal vinden. Ook big-datasets kunnen voldoen aan de vereisten van artikel 1 Wbbg.

3. Data en het goederenrecht

De Wbbg is voor de houder van data belangrijk, omdat datasets (1) vaak niet in aanmerking komen voor bescherming door IE-rechten, en (2) door het goederenrecht niet sluitend lijken te worden beschermd. De meest voor de hand liggende IE-rechten (ad 1) – het auteursrecht en het databankenrecht – zullen slechts in uitzonderingsgevallen toepasbaar zijn op datasets als zodanig.⁷ Er is daarom doorgaans geen exclusief recht op een dataset, waarmee het ieder ander kan worden verboden om de dataset te gebruiken zonder toestemming van degene die de dataset heeft samengesteld. Dit maakt het uitdagend(er) om hier een economisch verdienmodel op te baseren.

Daarnaast (ad 2) zijn de meeste juridische auteurs⁸ het erover eens dat ‘data’ geen ‘goed’ is in de zin van artikel 3:1 van het Burgerlijk Wetboek (BW) (namelijk geen zaak⁹ en geen vermogensrecht¹⁰). De consequentie is dat er in goederenrechtelijke zin geen ‘eigendom’ op data bestaat.¹¹ Degene die beschikt over een dataset (of andersoortige digitale informatie) lijkt dan ook geen beroep te kunnen doen op de wettelijke bepalingen die een (goederenrechtelijke) eigenaar van een zaak wél ten dienste staan, zoals bijvoorbeeld het op de voet van artikel 5:2 BW opeisen van de zaak indien een ander de zaak zonder recht houdt.

Ik merk op dat er naast het IE-recht en het goederenrecht evenwel nog een breder ‘grondrechtelijk eigendomsbegrip’ is op de voet van artikel 1 van het Europees Verdrag voor de Rechten van de Mens (EVRM) en artikel 17 van het Europees Handvest. Van Engelen zet in een recent artikel¹² uiteen dat ‘feitelijke beschikkingsmacht’ (zoals het hebben/houden van data) rechtens gerespecteerd wordt als ‘eigendom’. In feite is de Wbbg ook een uitwerking van dit grondrecht: het geeft de houder (grondrechtelijke eigenaar) van een bedrijfsgeheim het recht om op te treden tegen derden die niet rechtmatig houder zijn van het bedrijfsgeheim. Een van de conclusies van Van Engelen is echter ook dat dit grondrecht op gespannen voet staat met het ‘veronderstelde gesloten goederenrechtelijke systeem’.¹³

Dit alles wringt in de praktijk wel eens met het (financiële) belang dat aan bepaalde data kan worden gehecht. Vaak zal de houder van de data vinden dat hij ‘eigenaar’ is en dat hij exclusief gerechtigd is tot de data, maar een andere partij dan de eerstbedoelde houder kan dat ook vinden.¹⁴

Een eenvoudig voorbeeld om deze theoretische overwegingen wat inzichtelijker te maken. Een ziekenhuis koopt een MRI-scanner bij een grote leverancier. Zodra de MRI-scanner in gebruik is, genereert het apparaat data. Voor de hand liggend is dat er patiëntgegevens worden verzameld.¹⁵ Maar daarnaast worden er ook data verzameld over het uitvoeren van de scans zelf: het is bijvoorbeeld mogelijk om op basis van die data te analy-

4. Of: ‘gegevens’ volgens de Dikke van Dale.

5. Th.C.J.A. van Engelen, De vrijheid om over data en informatie te beschikken, *Maandblad voor Vermogensrecht* 2020/7/8, p. 308.

6. Ruitinga gaat in haar artikel ‘Big data: vatbaar voor (faillissements)beslag’ (*Maandblad voor Vermogensrecht* 2019/6 p. 197-206) dieper in op de definitie van ‘big data’ (zie vooral paragraaf 2 van dit artikel). Er is geen eenduidige definitie van big data en Ruitinga ziet big data in navolging van de Koninklijke Nederlandse Akademie van Wetenschappen als een variant van data.

7. Zie eveneens Ruitinga 2019, paragraaf 4.1 en 4.2. Kort samengevat: voor een databankrecht is bijvoorbeeld vereist dat sprake is van een ‘systematische en methodische ordening’ van data (art. 1 lid 1 sub a Databankenwet). Daar is vaak sowieso geen sprake van bij big data. Verder moet de ‘verkrijging, de controle of de presentatie van de inhoud’ van de databank in kwalitatief of kwantitatief opzicht getuigen van een ‘substantiële investering’ (zie eveneens art. 1 lid 1 sub a Databankenwet). Het verkrijgen van de data mag bijvoorbeeld geen ‘bijproduct’ zijn van andere activiteiten (anders is er geen substantiële investering gedaan in de verkrijging), maar dat is het vaak wel. Onder het auteursrecht worden ‘werken’ beschermd die een ‘eigen oorspronkelijk karakter’ hebben en ‘het persoonlijk stempel van de maker’ dragen (art. 1 Auteurswet). Dat is bij feitelijke gegevens (zoals data) doorgaans niet het geval.

8. Bijv. T.F.E. Tjong Tjin Tai, Data in het vermogensrecht, WPNR 2015/7085; T.F.E. Tjong Tjin Tai, Een goederenrechtelijke benadering van databestanden, NJB 2018/1242; E. Verheul, Revindicatie van data in de cloud, *Ars Aequi* 2018/0578; Ruitinga 2019, paragraaf 3.

9. Art. 3:2 BW.

10. Art. 3:6 BW. Volledigheidshalve: zou er wel een IE-recht toepasselijk zijn op een dataset, dan is dat wel een vermogensrecht.

11. Eigendom is in ons goederenrechtelijk systeem alleen mogelijk ten aanzien van zaken, art. 5:1 BW.

12. Van Engelen 2020, p. 308-313.

13. Van Engelen 2020, p. 312.

14. Het moge duidelijk zijn dat het mij in dit artikel vooral gaat om data en informatie die niet vrijelijk beschikbaar zijn (of zouden moeten zijn), maar over data die ter beschikking staan aan één of enkele partijen.

15. Het gaat hier om persoonsgegevens waarop onder meer de Algemene verordening gegevensbescherming (AVG; Verordening (EU) 2016/679) van toepassing is. De mogelijkheid om deze persoonsgebonden gegevens vrijelijk te gebruiken (waaronder te vercommercialiseren) is door privacywetgeving begrensd.

seren hoeveel patiënten er per uur of per dag door de MRI-scanner kunnen.¹⁶ Zulke informatie is bruikbaar om zorgprocessen optimaal in te richten. Die informatie is niet alleen interessant voor het ziekenhuis dat de MRI-scanner heeft gekocht, maar zeker ook voor de leverancier van de MRI-scanner én voor concurrenten van de leverancier. Het ziekenhuis en de leverancier zijn partij bij een onderlinge koopovereenkomst. Zoals hierna zal worden toegelicht, kan het van belang zijn om in die koopovereenkomst iets te regelen over de data die de MRI-scanner genereert.

Het is – in de situatie van het voorbeeld, waarin het ziekenhuis de MRI-scanner heeft gekocht – namelijk geen vanzelfsprekendheid dat de leverancier na de levering van de MRI-scanner nog toegang heeft tot de bedoelde data. Wil de leverancier er toch zeker van zijn dat hij de gebruiksdata van de MRI-scanner kan bemachtigen, dan doet de leverancier er goed aan om dat schriftelijk overeen te komen met het ziekenhuis. Bijvoorbeeld door overeen te komen dat de leverancier het apparaat (al dan niet op afstand) periodiek mag uitlezen op gebruiksdata.

Het ziekenhuis heeft er op zijn beurt ook belang bij om bij overeenkomst iets te regelen over de data die de MRI-scanner genereert, mits het die data natuurlijk wil kunnen gebruiken. In het gegeven voorbeeld is het ziekenhuis eigenaar van de ‘gegevensdrager’ (de MRI-scanner) en kan het om die reden ook de feitelijke macht uitoefenen over de zich daarop bevindende data. ‘Eigenaar’ van die data is het ziekenhuis in goederenrechtelijke zin echter niet. Stel dat de leverancier van de MRI-scanner op een dag onderhoud komt plegen aan het apparaat en tijdens dat onderhoud alle data over het gebruik van de MRI-scanner kopieert op een eigen gegevensdrager en vervolgens (met goede intenties) verwijdt uit het geheugen van de MRI-scanner om dat geheugen op te schonen. Los van eventuele strafrechtelijke of contractuele implicaties of complicaties op het gebied van persoonsgegevensbescherming: gevoelsmatig is het ziekenhuis dan toch iets ‘verloren’ waar het ‘recht’ op had. Het terugvorderen op de voet van artikel 5:2 BW lijkt niet mogelijk, of is ten minste onzeker.

Omdat het goederenrecht hier geen zekerheid biedt, zal het ziekenhuis de data zo goed mogelijk moeten beschermen door middel van het contractenrecht. In relatie tot de leverancier van het apparaat die onderhoud komt plegen en op die manier toegang krijgt tot de data, zal het ziekenhuis dan bijvoorbeeld moeten bedingen dat de leverancier de data niet mag verwijderen. En misschien wil het ziekenhuis wel meer dan dat: bijvoorbeeld dat de leverancier de data ook geheim moet houden. Als het ziekenhuis alleen een koopovereenkomst sluit met de leverancier (en het onderhoud bijvoorbeeld zelf wil gaan doen), dan zal hiervoor voor het ziekenhuis minder

noodzaak zijn. Maar een onderhoudsovereenkomst die het ziekenhuis met betrekking tot het apparaat sluit (met de leverancier of een derde), verdient dus wel een clause over de gebruiksdata.

De inhoud van de Wbbg leidt overigens waarschijnlijk wel tot complicaties voor de leverancier in het gegeven voorbeeld. Onder de Wbbg krijgen bedrijfsgeheimen (waaronder in de vorm van data) geen goederenrechtelijke status. Bedrijfsgeheimen zijn ook geen nieuw IE-recht onder de Wbbg; er zijn op bedrijfsgeheimen dan ook alsnog geen exclusieve rechten komen te rusten door de invoering van de Wbbg. De scope van de Wbbg is beperkt tot het optreden tegen het gebruik van *onrechtmatig verkregen* bedrijfsgeheimen. Artikel 2 Wbbg bepaalt dat het verkrijgen van een bedrijfsgeheim zonder toestemming van de houder van het bedrijfsgeheim onrechtmatig is wanneer het bedrijfsgeheim is verkregen door middel van (1) onbevoegde toegang tot of het zich onbevoegd toe-eigenen of kopiëren van documenten, voorwerpen, substanties, materialen of elektronische bestanden waarover de houder van het bedrijfsgeheim rechtmatig beschikt en die het bedrijfsgeheim bevatten of waaruit het bedrijfsgeheim kan worden afgeleid, en (2) andere gedragingen die, gezien de omstandigheden, worden beschouwd als strijdig met eerlijke handelspraktijken.

Het is verdedigbaar dat de data die de leverancier van de MRI-scanner (in het voorbeeld hiervoor) meeneemt, onderdeel uitmaken van de knowhow van zijn technologie. De data kunnen in feite vanuit het perspectief van zowel het ziekenhuis als de leverancier heel goed in aanmerking komen voor de kwalificatie ‘bedrijfsgeheim’. Als er geen ‘eigenaar’ is van deze data, als het ziekenhuis het contractueel niet heeft verboden en de data kwalificeren niet als persoonsgegevens: waarom zou de leverancier de data dan níét ‘mee mogen nemen’?¹⁷ Het ziekenhuis zou hier best kunnen aanvoeren dat alleen hij rechtmatige houder was van het bedrijfsgeheim (zijnde de betreffende data) en dat de leverancier zich dat bedrijfsgeheim onbevoegd heeft toegeëigend. Het ziekenhuis heeft namelijk geen expliciete toestemming gegeven voor de toe-eigening.

De Wbbg kent bepaalde vorderingsrechten toe aan de rechtmatige houder van een bedrijfsgeheim die goed van pas kunnen komen wanneer iemand onrechtmatig met data aan de haal gaat. Het gaat dan bijvoorbeeld om de volgende vorderingen:

1. De rechter kan staking van of verbod van het gebruik of (verdere) openbaarmaking van het bedrijfsgeheim bevelen.
2. De rechter kan gehele of gedeeltelijke vernietiging bevelen van documenten en elektronische bestanden die op onrechtmatige wijze het bedrijfsgeheim bevatten, of kan bevelen dat deze documenten en/of bestanden aan de houder van het bedrijfsgeheim worden overhandigd.

16. Niet alleen de ‘netto’ tijd van de scan is relevant, maar ook de tijd die de gemiddelde patiënt nodig heeft om de kamer te betreden, op de scan te gaan liggen, enzovoort. Voor zover de gegevens hierbij (indirect) herleidbaar blijven tot een patiënt, is ook hierop de AVG van toepassing.

17. Zie hierover ook Van Engelen 2020, p. 308-313.

3. Voor zover daar niet al andere grondslagen voor waren: de Wbbg regelt ook dat de houder van een bedrijfsgeheim schadevergoeding kan vorderen van de inbreukmaker die wist of behoorde te weten dat hij onrechtmatig een bedrijfsgeheim verkreeg, gebruikte of openbaar maakte. De rechter kan de schadevergoeding op een forfaitair bedrag vaststellen.

Écht vernieuwend is de Wbbg voor houders van vertrouwelijke informatie hiermee niet. De hiervoor beschreven vorderingen konden vóór de inwerkingtreding van de Wbbg ook al worden ingesteld als onrechtmatige-daadvordering.¹⁸ De winst zit wellicht vooral in twee aspecten. Ten eerste biedt de Wbbg een heel duidelijke mogelijkheid om documenten en/of bestanden te laten *overhandigen* aan de houder van het bedrijfsgeheim, terwijl er eerder geen duidelijke juridische regeling was voor revindicatie van databestanden.¹⁹ Data die voldoen aan de kwalificatie van een bedrijfsgeheim en waarover de oorspronkelijke houder de beschikking heeft verloren, kunnen aldus via de Wbbg worden teruggevorderd. Ten tweede heeft het concept ‘bedrijfsgeheim’ expliciete wettelijke ‘erkenning’ gekregen in de Wbbg. Daarmee kan de contractspraktijk dan weer haar voordeel doen door de bescherming van bedrijfsgeheimen contractueel extra te waarborgen. In paragraaf 4 volgen hiervoor enkele concrete tips. Maar toch nog even kort terug naar het gegeven voorbeeld. Het moge duidelijk zijn dat de leverancier van de MRI-scanner – als deze na verkoop van het apparaat toegang wenst tot de gebruiksdata – daarvoor *in ieder geval* contractuele afspraken zal moeten maken. Voor het ziekenhuis is de nood – zeker de vorderingsrechten en revindicatiemogelijkheid uit de Wbbg als vangnet – wellicht minder hoog vanwege de feitelijke macht over de data. Om echter gebruik te kunnen maken van de Wbbg als vangnet moeten de data wél kwalificeren als een bedrijfsgeheim van het ziekenhuis. En juist voor dat laatste element zijn de tips in de volgende paragraaf ook van belang.

4. De Wbbg contractueel benutten

Geschillen tussen contractspartijen over wie gerechtigd is tot bedrijfsgeheimen (waaronder data) kunnen in veel gevallen worden voorkomen door goede contractuele afspraken, behoudens uiteraard gevallen waarin een derde onrechtmatig met de bedrijfsgeheimen aan de haal gaat. Terug naar het voorbeeld van het ziekenhuis en de leverancier van de MRI-scanner. Als de leverancier belang heeft bij de gebruiksdata van de MRI-scanner, dan zal de leverancier normaal gesproken contractueel

proberen te bedingen dat hij die data mag uitlezen voor eigen gebruik. Vindt de leverancier dat die data cruciale knowhow zijn waarmee hij zijn technologie en services kan verbeteren (lees: data die de leverancier op de een of andere manier te gelde wil kunnen maken), dan wil de leverancier wellicht ook contractuele beperkingen opleggen aan het gebruik of zelfs de enkele inzage van die data door het ziekenhuis zelf. Dit soort afspraken werd ook voor de inwerkingtreding van de Wbbg al veelvuldig gemaakt.

De Wbbg geeft nu kaders voor de invulling van wat er nodig is om te kunnen spreken van een ‘bedrijfsgeheim’. En omdat de Wbbg is gebaseerd op een Europese richtlijn,²⁰ zijn die kaders binnen de interne markt van de Europese Unie ook nog eens gelijk. In de inleiding van dit artikel is het eerste artikel van de Wbbg al geciteerd, waarin staat aan welke drie voorwaarden informatie moet voldoen om een bedrijfsgeheim te zijn. De informatie moet geheim zijn, handelswaarde bezitten en zijn onderworpen aan redelijke maatregelen ter geheimhouding. Het is nuttig om deze voorwaarden te benoemen in contractuele afspraken over bedrijfsgeheimen, waaronder data. Nog los van het feit dat de derde voorwaarde vaak toch al zal vergen dat contractuele regelingen getroffen worden rondom bedrijfsgevoelige informatie. Het contractueel overeenkomen van geheimhouding is immers een manier – en vaak de meest voor de hand liggende manier – om de voorwaarde van het nemen van ‘redelijke maatregelen tot geheimhouding’ in te vullen.

De ‘redelijke maatregelen tot geheimhouding’ zijn natuurlijk net als ‘de informatie moet handelswaarde bezitten’ en ‘de informatie moet geheim zijn’ vrij open normen. Dat betekent dat wanneer een geschil ontstaat rondom de vraag of er een bedrijfsgeheim is geschonden, de rechtsstrijd in potentie nogal omvangrijk kan worden. Het vergt wat van de eiser om aannemelijk te maken dat zijn bedrijfsgeheim ook echt geheim is en handelswaarde bezit en dat de eiser redelijke maatregelen heeft genomen ter bescherming van zijn bedrijfsgeheim.²¹ De gedaagde heeft op zijn beurt haast eindeloze mogelijkheden om zijn verweer in te kleden

18. De Wbbg bevat wel – voor Nederlandse begrippen – nieuwe vorderingsrechten, maar die vind ik minder zinvol voor het bestek van dit artikel, bijv. art. 9 van de Wbbg over het ‘namen and shamen’ van de inbreukmaker.

19. Meer hierover Tjong Tjin Tai 2018.

20. Richtlijn (EU) 2016/943 betreffende de bescherming van niet-openbaar gemaakte knowhow en bedrijfsinformatie (bedrijfsgeheimen) tegen het onrechtmatig verkrijgen, gebruiken en openbaar maken daarvan.

21. In Duitsland is onlangs een uitspraak gedaan door het gerechtshof van Stuttgart (19 november 2020, 2 U 575/19) waarin een aantal algemene handvatten wordt geboden om vast te stellen of in een specifiek geval redelijke maatregelen zijn genomen ter bescherming van een bedrijfsgeheim: (1) de aard en waarde van het bedrijfsgeheim, (2) het belang van het bedrijfsgeheim voor de onderneming, (3) de R&D-kosten van het bedrijfsgeheim, (4) de omvang van de onderneming die ‘eigenaar’ van het geheim is, (5) de gebruikelijke beveiligingsmaatregelen van de onderneming, (6) de manier waarop de geheime informatie is ‘gelabeld’, en (7) bepalingen in contracten met werknemers en professionele contractspartijen (‘business partners’). Het is aannemelijk dat een Nederlandse rechter min of meer dezelfde handvatten in overweging zal nemen in zijn beoordeling over ‘redelijke maatregelen’. Zie over de Duitse uitspraak ook een korte blog van V. Wettner, Keeping trade secrets secret: The Stuttgart Court of Appeal on the protection of an undertaking’s most valuable information, te vinden via www.wilmerhale.com (februari 2021).

op die drie onderwerpen. Dat is voor de houder van een bedrijfsgeheim niet efficiënt en het risico op een geschil dat zo ‘uit de hand loopt’ kan beter zo veel mogelijk worden beperkt. In de situatie dat een derde onrechtmatig inbreuk maakt op een bedrijfsgeheim is dat wellicht niet goed mogelijk, maar tussen contractspartijen kan veel toekomstig leed wel degelijk worden vermeden met de Wbbg als kapstok.

Om mogelijke toekomstige geschillen met (al dan niet voormalige) contractspartijen over bedrijfsgeheimen zo veel mogelijk in te kaderen kunnen concrete bepalingen overeengekomen worden die zijn afgestemd op de voorwaarden die de Wbbg aan bedrijfsgeheimen stelt. Zulke bepalingen kunnen worden opgenomen in allerlei soorten overeenkomsten. Direct voor de hand liggend is de *letter of intent* (LOI) of de *non disclosure agreement* (NDA), maar in de praktijk bevatten bijna alle overeenkomsten wel enige geheimhoudingsbepalingen (al dan niet versterkt met een boeteclausule om het belang van het bedrijfsgeheim nog meer te benadrukken). Deze bepalingen kunnen met behulp van de Wbbg net wat verder worden aangescherpt.

Zo kunnen contractspartijen bijvoorbeeld met elkaar overeenkomen dat zij erkennen (of vaststellen) dat bepaalde informatie – die wordt uitgewisseld of die de ene partij voor de uitvoering van het contract van de andere partij ontvangt – een bedrijfsgeheim is in de zin van artikel 1 Wbbg, dat zij erkennen dat deze informatie handelswaarde bezit, en dat zij overeenkomen dat – met het overeenkomen van geheimhoudingsbepalingen tussen hen en met eventueel door hen ingeschakelde derden – redelijke maatregelen zijn genomen ter bescherming van het bedrijfsgeheim.

Vooraf op de voorwaarde dat de informatie ‘handelswaarde’ moet bezitten is naar mijn mening winst te behalen. Partijen kunnen hieromtrent namelijk een vaststellingsovereenkomst en bewijsovereenkomst sluiten (als onderdeel van de geheimhoudingsbepaling in het contract). De wettelijke basis hiervoor is te ontleen aan artikel 153 van het Wetboek van Burgerlijke Rechtsvordering (Rv) en artikel 7:900 BW. Op basis van deze artikelen kunnen partijen bij een overeenkomst ter voorkoming van een toekomstig geschil iets gezamenlijk ‘vaststellen’ (ook als dit van de werkelijk bestaande rechtstoestand afwijkt) en bepalen dat het wettelijk bewijsrecht hierop niet van toepassing is, zodat er later ook geen tegenbewijs mag worden geleverd van de vastgestelde rechtstoestand.

Concreet: partijen kunnen in hun contract vastleggen dat zij vaststellen dat de uitgewisselde informatie handelswaarde vertegenwoordigt en dat daartegen geen tegenbewijs is toegestaan. Dat zou doorgaans moeten werken indien de contractuele wederpartij een professionele partij is.²²

22. Consumenten worden in dit geval beschermd door art. 6:236 BW (zwarte lijst).

Ook met het oog op de andere twee voorwaarden die artikel 1 Wbbg aan een ‘bedrijfsgeheim’ stelt, zou ik het opnemen van een vaststellingsovereenkomst en bewijsovereenkomst in de geheimhoudingsbepalingen ten minste in overweging nemen. Oftewel: het is raadzaam om op te nemen dat partijen vaststellen dat de uitgewisselde informatie geheim is en dat daartegen geen tegenbewijs is toegestaan, en om op te nemen dat de houder van het bedrijfsgeheim redelijke maatregelen heeft genomen ter bescherming van het bedrijfsgeheim en dat ook daartegen geen tegenbewijs is toegestaan. Hier kan het algemeen maatschappelijk belang dat de waarheid in rechte aan het licht moet komen onder omstandigheden wel beperkingen aanleggen.²³ Datzelfde geldt voor artikel 6:248 lid 2 BW; een contractuele bepaling kan – in uitzonderlijke gevallen – buiten toepassing blijven indien deze naar maatstaven van redelijkheid en billijkheid onaanvaardbaar is.

Zoals wel vaker, geldt ook hier eigenlijk dat naarmate partijen concreter zijn in hun overeenkomst, de kans op een succesvol beroep op de bepalingen in die overeenkomst groter zal zijn.²⁴ De contractuele vaststelling dat de houder van een bedrijfsgeheim redelijke maatregelen heeft genomen om het bedrijfsgeheim te beschermen wordt sterker naarmate de houder in het contract toelicht welke maatregelen – naast de geheimhoudingsbepalingen in het contract zelf – hij zoal heeft genomen.²⁵ Volledigheidshalve onderstreep ik toch ook even een open deur: de geheimhoudingsbepalingen zelf worden uiteraard ook sterker naarmate men concreter is over welke informatie precies als bedrijfsgeheim wordt gezien en vertrouwelijk moet worden behandeld. Dit pleit ervoor om niet zomaar een standaard-NDA uit de kast te trekken, maar echt even de tijd te nemen om te beschrijven welke informatie er in een concreet geval wordt gedeeld en waarmee de ontvanger uiterst vertrouwelijk om moet gaan. Als een slang die zich in zijn eigen staart bijt: naarmate een NDA concreter is, zal de NDA ook eerder bijdragen aan de overtuiging dat er redelijke maatregelen zijn genomen om een bedrijfsgeheim te beschermen.

Is dit nodeloos ingewikkeld? Dat kan. In het voorbeeld van het ziekenhuis en de leverancier van de MRI-scanner kunnen de afspraken over de gebruiksdata die de MRI-scanner genereert vast eenvoudiger worden verwoord. Als het ziekenhuis na de aanschaf van de MRI-

23. HR 10 april 2009, ECLI:NL:HR:2009:BG9470, NJ 2010/471: vooral als een overeenkomst niet met expliciete bewoordingen een bewijsovereenkomst bevat.

24. Een uitgebreider pleidooi voor het gebruik van de bewijsovereenkomst is te lezen in M. Uijen, *Münchhausen revisited: de bewijsovereenkomst als instrument voor contractenmakers*, *Contracteren* 2017/1, p. 19.

25. De contractuele ‘ontvanger’ die wordt gevraagd om te erkennen dat er redelijke maatregelen zijn genomen, zal dit waarschijnlijk ook willen weten voordat de handtekening wordt gezet en het recht op tegenbewijs wordt weggegeven. Voor wat betreft digitale bescherming van bedrijfsgeheimen kan bijvoorbeeld worden gedacht aan certificeringen voor informatiebeveiliging: ‘Partijen stellen vast dat zolang A beschikt over certificaat X, A redelijke maatregelen heeft genomen om de “informatie” te beschermen en dat daartegen geen tegenbewijs mogelijk is.’

scanner verder geen interesse heeft in doorlopende uitwisseling van gebruiksdata met de leverancier, kan bijvoorbeeld in de koopovereenkomst van de scanner worden opgenomen dat het ziekenhuis is verboden om de gebruiksdata voor bepaalde doeleinden te gebruiken of te delen met derden (onder wie concurrenten van de leverancier). De leverancier krijgt de data dan zelf niet, maar kan zo wellicht voorkomen dat de informatie door anderen gebruikt kan worden (waaronder het ziekenhuis zelf). Heeft de leverancier bij een ander ziekenhuis meer ‘geluk’ en kan hij daar wel data verzamelen, ook dan kan hij contractueel beperkingen opleggen aan het gebruik van die data door het ziekenhuis zonder naar de Wbbg te verwijzen. In zekere zin zijn dit dan meer ‘ad hoc’-afspraken. Indien een onderneming echter een duidelijk beleid wil voeren rondom ‘haar’ data – en dat is wel aan te bevelen als het waardevolle data betreft, gelet op de eis om ‘redelijke maatregelen’ te nemen ter bescherming van bedrijfsgeheimen –, dan is het wel aan te bevelen om stelselmatig met contractspartijen overeen te komen dat het een bedrijfsgeheim/bedrijfsgeheimen betreft. Nog beter is het als al die contractspartijen dat schriftelijk erkennen. Voorbeeld: de leverancier van het ziekenhuis creëert een eenvoudigere bewijspositie voor zichzelf op het moment dat alle ziekenhuizen waaraan de leverancier levert bereid zijn om contractueel te erkennen dat de gebruiksdata van de MRI-scan bedrijfsgeheim van de leverancier zijn. De moeite om het zaadje voor die bewijspositie in zijn overeenkomsten te creëren, lijkt vrij klein. Daarmee is overigens niet gezegd, dat de leverancier niet ook andere maatregelen zou moeten nemen om zijn bedrijfsgeheimen (data) te beschermen.²⁶

5. Reverse engineering

Een ander aspect van de Wbbg dat voor de contractspartij relevant is, is het onderwerp *reverse engineering*. Het is namelijk volgens artikel 3 lid 1 sub b Wbbg in beginsel niet onrechtmatig als een bedrijfsgeheim wordt verkregen door middel van ‘observatie, onderzoek, demontage of testen van een product of voorwerp’ (reverse engineering) dat ter beschikking van het publiek is gesteld of op een rechtmatige manier in het bezit is van degene die de informatie verwerft. Het ziekenhuis in het voorbeeld mag de MRI-scanner dus helemaal uit elkaar halen om te kijken hoe het apparaat werkt en kan zo bedrijfsgeheimen van de leverancier bemachtigen: op rechtmatige wijze. Tenzij de leverancier in de overeenkomst met het ziekenhuis heeft bepaald dat reverse engineering niet is toegestaan; dat mag de leverancier volgens artikel 3 lid 1 sub b Wbbg namelijk bedingen.

In verhouding tot het onderwerp ‘data’ en ‘datasets’ is reverse engineering echter minder relevant. Het is minder goed voorstelbaar dat iemand door middel van

reverse engineering probeert een dataset te bemachtigen. Daarnaast ziet de definitie van reverse engineering op producten en voorwerpen en is daarmee minder goed toepasbaar op data. Daarom slechts kort het volgende. Artikel 3 lid 1 aanhef en sub b Wbbg geeft aan dat het niet onrechtmatig is om een bedrijfsgeheim te verkrijgen door middel van reverse engineering, te weten door: ‘observatie, onderzoek, demontage of testen van een product of voorwerp dat ter beschikking van het publiek is gesteld of dat op een rechtmatige manier in het bezit is van degene die de informatie verwerft en die niet gebonden is aan een rechtsgeldige verplichting het verkrijgen van het bedrijfsgeheim te beperken’.

Het is onder de Wbbg toegestaan om deze vrijheid contractueel weer uit te sluiten, dus om op te nemen dat de contractspartner *niet* aan reverse engineering mag doen. Daarbij meen ik overigens dat bedrijfsgeheimen weliswaar rechtmatig kunnen worden *verkregen* door middel van reverse engineering, maar dat dat niet zonder meer betekent dat de op die wijze ontdekte bedrijfsgeheimen door de ontdekker verder openbaar gemaakt of gebruikt mogen worden, ook als daar contractueel niets over is bepaald. In het genoemde artikel-lid van de Wbbg staat letterlijk alleen dat ‘verkrijging’ van een bedrijfsgeheim door middel van reverse engineering niet onrechtmatig is. Op andere plaatsen in de Wbbg is nu juist ook expliciet geregeld dat kan worden opgetreden tegen het ‘gebruik’ en de ‘openbaarmaking’ van bedrijfsgeheimen.²⁷ Hoe dan ook, het kan om iedere discussie uit te sluiten zinvol zijn om in contracten beperkingen te stellen aan reverse engineering juist omdat de wet reverse engineering in beginsel toestaat. Een leverancier van een product of dienst (hardware zoals een MRI-scanner, maar ook software) zal daarom doorgaans contractueel bedingen dat het de afnemer niet is toegestaan om aan reverse engineering te doen. In het voorbeeld van het ziekenhuis zou ik als leverancier ook in de overeenkomst opnemen dat het ziekenhuis het verbod op reverse engineering ook moet opleggen aan eventuele derde partijen (zoals concurrenten van de leverancier) waaraan het ziekenhuis de opdracht geeft om onderhoud te plegen aan de MRI-scanner.

6. Contractuele beperkingen voor anderen dan oorspronkelijke houders van bedrijfsgeheimen

Interessant is dat iemand die door middel van reverse engineering een bedrijfsgeheim ontdekt, ‘op rechtmatige wijze’ over dat bedrijfsgeheim komt te ‘beschikken’.²⁸

26. Denk aan digitale beveiliging, maar dat valt verder buiten het bestek van dit artikel.

27. Zie bijv. art. 2 Wbbg.

28. Behalve natuurlijk als diegene daarmee handelt in strijd met een contractuele verplichting om niet aan reverse engineering te doen.

Verkrijging van een bedrijfsgeheim door reverse engineering is immers volgens de wet niet onrechtmatig. Daarmee voldoet die persoon vervolgens aan de definitie van ‘houder van het bedrijfsgeheim’ zoals opgenomen in artikel 1 Wbbg. De ‘houder van het bedrijfsgeheim’ is: ‘iedere natuurlijke persoon of rechtspersoon die rechtmatig over een bedrijfsgeheim beschikt’. Dit is niet alleen toepasbaar op een hobbyist die aan reverse engineering doet. Ook andere natuurlijke personen en rechtspersonen die bedrijfsgeheimen niet onrechtmatig (dus rechtmatig) verkrijgen, kwalificeren volgens de letterlijke tekst van de wet als houder. Dus: de licentienemer die op de hoogte gebracht wordt van een bedrijfsgeheim van de licentiegever ten behoeve van de uitvoering van de licentieovereenkomst. En: werknemers die in de uitoefening van hun werkzaamheden kennis vergaren die als bedrijfsgeheim kwalificeert. Maar (waarschijnlijk) ook: de curator die kennisneemt van bedrijfsgeheimen van een failliete onderneming. In het in dit artikel steeds aangehaalde voorbeeld: het ziekenhuis komt als eigenaar van de MRI-scanner waarschijnlijk ook rechtmatig over de gebruiksdata van – en andere knowhow over – de MRI-scanner te beschikken. Als de leverancier (of zelfs een derde) in verband met onderhoud aan de MRI-scanner de gebruiksdata uitleest en er daardoor over komt te beschikken, dan lijkt dat ook niet zonder meer onrechtmatig.

De houder van het bedrijfsgeheim is nu echter juist degene die in feite centraal staat in de gehele Wbbg: *die* krijgt namelijk het recht om op te treden tegen inbreuken op het bedrijfsgeheim. De rechter kan op vordering van de ‘houder van het bedrijfsgeheim’ maatregelen nemen tegen een inbreukmaker.²⁹ De houder van het bedrijfsgeheim kan bijvoorbeeld ook schadevergoeding vorderen van de inbreukmaker.³⁰ Dat levert in potentie processuele chaos op.

Het is maar zeer de vraag of de redenering dat alle rechtmatige verkrijgers van bedrijfsgeheimen ook houders van die bedrijfsgeheimen worden in de zin van de Wbbg, een juiste uitleg van de Wbbg is en/of dit in alle gevallen gehonoreerd zal worden in de rechtszaal. Ik kan mij zo’n uitleg ten aanzien van reverse engineering in ieder geval minder goed voorstellen dan bij bijvoorbeeld een licentienemer. Maar die uitleg volgt wél uit de letterlijke wettekst. Zolang daarover echter geen duidelijkheid is verschaft door het Hof van Justitie van de Europese Unie (of er ten minste richting is gegeven door nationale rechters), is het temeer van belang om (desgewenst) contractueel aandacht te besteden aan dit onderwerp. Ook in het geval er gecontracteerd wordt over het delen van data/een dataset. De oorspronkelijke ‘houder’ van de data moet zich realiseren dat iedereen met wie hij de data vrijwillig deelt ook een ‘houder’ van het bedrijfsgeheim wordt.³¹ Wil de oorspronkelijke houder de regie in handen houden voor wat betreft de pro-

cesvoering tegen inbreuken op het bedrijfsgeheim en bij het vorderen van en onderhandelen over schadevergoeding, dan zal hij dat contractueel moeten regelen met partijen met wie hij bedrijfsgeheimen deelt. In bijvoorbeeld licentieovereenkomsten is dat overigens (al dan niet ten aanzien van IE-rechten) op zich al een veel geziene bepaling.³²

Ook vanuit het oogpunt van een mogelijk toekomstig faillissement van een contractuele wederpartij is het verstandig voor de houder van een bedrijfsgeheim (waaronder data) om contractueel goede afspraken te maken over de rechten op het bedrijfsgeheim. Afspraken die het goederenrechtelijk eigenaarschap zo veel mogelijk benaderen en waarbij wordt bepaald dat degene met wie de data worden gedeeld, die data bijvoorbeeld slechts ‘houdt’ voor zijn opdrachtgever.³³ Zij het dat bij gebrek aan richtinggevende jurisprudentie nog onduidelijk is of de curator van een gefailleerde opdrachtnemer de data dan inderdaad niet te gelde zou mogen maken ten gunste van de boedel.³⁴

7. Conclusie

Zijn bepaalde data (in potentie) veel geld waard en/of zijn er andere redenen om data geheim te willen of moeten houden, dan is dat een gedegen beschermingsbeleid waard. Een van de belangrijkste pijlers daarvan – en juist een pijler waarop een onderneming zelf veel invloed kan uitoefenen – is een goede contractuele bescherming van die data. Schuw daarbij de Wet bescherming bedrijfsgeheimen vooral niet, zeker niet wanneer contractspartijen zich in verschillende EU-staten bevinden waar nu gelijkkluidende wettelijke definities gehanteerd worden.³⁵ De Wbbg biedt zinvolle (en grensoverschrijdende) handvatten om duidelijke afspraken te maken over de contractuele rechten en plichten met betrekking tot datasets. Omdat de Wbbg toch ook wel enkele ‘mazen’ of ten minste ‘aandachtspunten’ kent in bijvoorbeeld het begrip ‘houder’, kan het zelfs broodnodig zijn om bij het opstellen van contractuele bepalingen over datasets aandacht te besteden aan de Wbbg om

29. Zie art. 5 en 6 Wbbg.

30. Zie art. 8 Wbbg.

31. Zolang het geheim niet met zoveel personen wordt gedeeld dat niet meer van een geheim kan worden gesproken.

32. Meer tips voor het opstellen van contracten met het oog op de bescherming van bedrijfsgeheimen zijn te vinden in J.L. Naves, Contracteren over data, Tijdschrift overeenkomst in de rechtspraak 2018/4, p. 37-41. In paragraaf 3.2 van Naves’ artikel staat een zevental tips om ‘data’ die tussen partijen worden uitgewisseld contractueel te beschermen. Deze tips zijn niet alleen toepasbaar op ‘data’, maar op alle vormen van bedrijfsgeheimen die worden uitgewisseld tussen contractspartijen (voor zover daartussen al een onderscheid te maken is).

33. Maak in de overeenkomst dus duidelijk dat het de bedoeling van de contractspartijen is om een situatie te creëren die zo veel mogelijk gelijk is aan het goederenrechtelijke houderschap. Zie ook Van Engelen 2020, p. 312.

34. Idem: Van Engelen noemt als voorbeeld het faillissement van de hostingprovider als ‘houder’ van data voor een opdrachtgever. Los van de contractuele component om data zo veel mogelijk te beschermen.

35. De Wbbg is immers de implementatie van Richtlijn (EU) 2016/943 betreffende de bescherming van niet-openbaar gemaakte knowhow en bedrijfsinformatie (bedrijfsgeheimen) tegen het onrechtmatig verkrijgen, gebruiken en openbaar maken daarvan.

eventuele lacunes te ondervangen. Met enige creativiteit kan van die nood ook nog een deugd gemaakt worden door bijvoorbeeld toekomstige discussies over de vraag óf bepaalde data wel kwalificeren als bedrijfsgeheim bij voorbaat contractueel te elimineren.