Dit artikel uit Contracteren is gepubliceerd door Boom juridisch en is bestemd voor anonieme bezoeker

Artikel

Verwerkersovereenkomsten in de praktijk

Mr. M.S. van der Jagt*

1. Inleiding

1.1 Introductie

Het was niet te missen, 25 mei 2018, de datum waarop de Algemene verordening gegevensbescherming (AVG)[1] in werking is getreden. Veel bedrijven stuurden nog diezelfde dag hun aangepaste privacybeleid rond. Privacystatements op websites zijn niet meer weg te denken. Privacy werd het gesprek van de dag, bijna alsof het vóór de AVG niet bestond. Dat terwijl bedrijven onder de Wet bescherming persoonsgegevens (Wbp) toch ook al allerlei verplichtingen op het gebied van privacy hadden. Het grote verschil was dat de Autoriteit Persoonsgegevens (AP) de bevoegdheid kreeg om veel hogere boetes op te leggen bij schending van de AVG (tot het hoogste van € 20 miljoen of 4% van de wereldwijde jaaromzet van een onderneming) dan op grond van de Wbp mogelijk was (tussen € 120.000 en € 500.000). De vrees bij bedrijven voor die boetes is niet ongegrond gebleken. De AP heeft sinds de inwerkingtreding van de AVG al vijftien keer een boete opgelegd van € 400.000 of hoger.[2]

Een van de verplichtingen die uit de AVG volgt, is dat partijen die persoonsgegevens door anderen laten verwerken (zoals bijvoorbeeld het geval is bij een bedrijf dat zijn salarisadministratie extern heeft uitbesteed) met die verwerkers een verwerkersovereenkomst moeten sluiten waarin allerhande privacygerelateerde onderwerpen geregeld moeten worden. Deze verplichting is opgenomen in artikel 28 lid 3 AVG. De AP is bevoegd om boetes op te leggen wegens schending van deze verplichting, ook al heeft de AP van die bevoegdheid tot op heden nog geen gebruik gemaakt.

1.2 Doelstelling

In de praktijk merk ik dat nog altijd lang niet alle bedrijven hun verwerkersovereenkomsten op orde hebben, of dat bij het inschakelen van nieuwe leveranciers überhaupt over het hoofd wordt gezien dat een verwerkersovereenkomst nodig is. Als een verwerkersovereenkomst wordt gesloten, dan is dat vaak pas na afloop van een onderhandeltraject waarbij intensief over de details van de hoofdovereenkomst is gesproken. De verwerkersovereenkomst wordt dan behandeld als een bijzaak, waar vooral niet al te ingewikkeld over gedaan moet worden.

Dit artikel is bedoeld om handvatten te geven bij het opstellen van en onderhandelen over verwerkersovereenkomsten. Dat hoeft gelukkig niet (altijd) ingewikkeld te zijn. De AVG geeft in artikel 28 AVG zelf al een soort checklist van wat er in de verwerkersovereenkomst moet staan. Daarnaast zijn er binnen verschillende branches modelovereenkomsten ontwikkeld, en ook zijn er online legio documentengenerators te vinden waar na het invullen van een vragenlijst een contract uit komt rollen. Ter gelegenheid van dit artikel heb ik enkele daarvan op kwaliteit en bruikbaarheid beoordeeld.

In dit artikel behandel ik eerst de vraag wanneer een verwerkersovereenkomst verplicht is, en vervolgens wat daar in hoort te staan, bezien vanuit enerzijds het perspectief van de verwerkingsverantwoordelijke en anderzijds dat van de verwerker. Ten slotte bespreek ik enkele online documentengenerators en modelovereenkomsten om te bekijken of daar in de praktijk kostbare tijd mee te besparen valt.

* Mr. M.S. van der Jagt is advocaat IE/IT & privacy bij Griffiths Advocaten.

1 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene verordening gegevensbescherming).

2 https://autoriteitpersoonsgegevens.nl/nl/publicaties/boetes-en-sancties.

doi: 10.5553/Contr/156608932022024004005

Dit artikel uit Contracteren is gepubliceerd door Boom juridisch en is bestemd voor anonieme bezoeker

2. Wanneer is een verwerkersovereenkomst verplicht?

Voor sommigen is het misschien een open deur, maar laten we beginnen bij de basis. Ik stipte hiervoor al aan dat een verwerkersovereenkomst verplicht is op het moment dat de ene organisatie (de verwerkingsverantwoordelijke) een andere organisatie (de verwerker) inschakelt om persoonsgegevens te verwerken.[3] Bijvoorbeeld door de salarisadministratie extern uit te besteden, zoals hiervoor al genoemd, of door het inschakelen van een clouddienst om klantgegevens in de cloud op te slaan.

De verantwoordelijke is degene die het doel en de middelen van de verwerking vaststelt. De verwerker verwerkt persoonsgegevens *ten behoeve van* de verantwoordelijke, en dus niet *voor zichzelf*. Soms is het lastig te bepalen welke partij de verwerkingsverantwoordelijke is en welke de verwerker, en een partij kan ook beide zijn. Ik illustreer dit aan de hand van twee voorbeelden.

1. Een advocatenkantoor dat een ICT-dienstverlener inschakelt weet zelf bijvoorbeeld vaak weinig van ICT en kan dan nauwelijks meepraten over de concrete middelen die worden ingezet. Daardoor kan het lijken alsof de ICT-dienstverlener in de onderlinge samenwerking het doel en de middelen van de verwerking bepaalt, maar dat is niet zo. Het advocatenkantoor behoudt de beslissingsmacht en is daarmee dus de verantwoordelijke, althans voor zover het data van het advocatenkantoor betreft die door de ICT-dienstverlener worden verwerkt. De ICT-dienstverlener zal daarnaast ook persoonsgegevens van bijvoorbeeld de contactpersoon bij het advocatenkantoor verwerken, maar dat doet de ICT-dienstverlener dan weer ten behoeve van zijn eigen bedrijfsvoering en ten aanzien daarvan is hij zelf de verwerkingsverantwoordelijke.
2. Een loodgieter die wordt ingehuurd door een vereniging van eigenaren om lekkages binnen een appartementencomplex te verhelpen zal daarbij persoonsgegevens van de bewoners verwerken, maar doet dat op eigen verantwoordelijkheid. De opdracht van de vereniging ziet niet op het verwerken van persoonsgegevens en de loodgieter is dus geen verwerker.

Op de website van de AP is een handige voorbeeldlijst te vinden van veelvoorkomende situaties en welke partij daarbij de verantwoordelijke of de verwerker is.[4]

Meestal wordt de verwerkersovereenkomst als een bijlage bij een hoofdovereenkomst gevoegd. Het is niet verplicht om het op die manier te doen. De bepalingen die in de verwerkersovereenkomst opgenomen moeten worden, kunnen ook rechtstreeks in de hoofdovereenkomst gezet worden. Dat heeft als voordeel dat alle bepalingen over bijvoorbeeld geheimhouding en aansprakelijkheid bij elkaar op dezelfde plek staan en niet verdeeld zijn over meerdere documenten. Nadeel is dat de hoofdovereenkomst gelijk een stuk langer wordt en dat de bepalingen die met persoonsgegevens te maken hebben dan vaak juist op verschillende plekken in de hoofdovereenkomst terechtkomen. De vrij herkenbare structuur die verwerkersovereenkomsten meestal met dank aan de AVG-'checklist' hebben, kan verloren kan gaan als de bepalingen in de hoofdovereenkomst zelf verwerkt worden.

3. Wat staat er in een verwerkersovereenkomst? De AVG-'checklist'

3.1 De checklist

De AVG stelt in artikel 28 de volgende onderdelen verplicht om op te nemen in een verwerkersovereenkomst:

- onderwerp en duur verwerking;
- aard en doel verwerking;
- soort persoonsgegevens en categorieën betrokkenen;
- rechten en plichten verwerkingsverantwoordelijke;
- verplichting verwerker om uitsluitend persoonsgegevens te verwerken op schriftelijke instructies van de verantwoordelijke;
- vertrouwelijkheid/geheimhouding;
- technische en organisatorische maatregelen;
- inschakelen van subverwerkers;
- uitoefening rechten van betrokkenen;
- beveiliging, datalekmeldplicht en medewerking bij gegevensbeschermingseffectbeoordeling (DPIA);
- vernietiging of teruggave persoonsgegevens bij einde overeenkomst;
- audits.

Deze verplichte onderdelen worden in de praktijk vaak aangevuld met enkele standaardclausules, zoals clausules over aansprakelijkheidsbeperking, vrijwaring, contractuele boetes en rechts- en forumkeuze.

3.2 Onderwerp en duur, aard en doel van de verwerking, soort persoonsgegevens en categorieën van betrokkenen

Voor de eerste verplichte onderdelen van de verwerkersovereenkomsten kan vaak aangesloten worden bij een omschrijving van de samenwerking die in de hoofdovereenkomst al opgenomen zal zijn. Bij soorten persoonsgegevens kan natuurlijk gedacht worden aan NAW-gegevens (naam, adres, woonplaats) en telefoonnummers, maar ook aan minder voor de hand liggende gegevens zoals bijvoorbeeld IP-adressen. Categorieën van betrokkenen kunnen bijvoorbeeld klanten, werknemers, websitebezoekers, abonnees of patiënten zijn.

3 De AVG is niet van toepassing op de verwerking van persoonsgegevens door natuurlijke personen voor privégebruik, zie art. 2 lid 2 sub c AVG.

4 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/verantwoordelijke-en-verwerker.

doi: 10.5553/Contr/156608932022024004005

Dit artikel uit Contracteren is gepubliceerd door Boom juridisch en is bestemd voor anonieme bezoeker

Voorzichtigheid moet worden betracht indien bijzondere categorieën persoonsgegevens worden verwerkt, zoals gegevens met betrekking tot iemands gezondheid of politieke opvattingen.[5] In dat geval geldt een verwerkingsverbod, tenzij wordt voldaan aan een van de uitzonderingen zoals opgenomen in artikel 9 AVG. Ook kan sprake zijn van verwerking van persoonsgegevens van kwetsbare betrokkenen, zoals minderjarigen. In dat geval kunnen strengere eisen gesteld worden aan de te nemen beveiligingsmaatregelen. Zo werd juist het feit dat het gezondheidsgegevens van minderjarigen betrof bijvoorbeeld genoemd in het besluit van de AP om een boete van € 12.000 op te leggen aan een orthodontiepraktijk die de beveiliging van de website niet op orde had.[6]

3.3 Rechten en plichten verantwoordelijke en verplichting verwerker om uitsluitend persoonsgegevens te verwerken op schriftelijke instructies van de verantwoordelijke

Vaak worden de rechten en plichten over en weer in een van de eerste contractsbepalingen in het algemeen uiteengezet, als algemene uitgangspunten bij de samenwerking. Daarbij kan dicht worden aangesloten bij de letterlijke tekst van de AVG. De meer specifieke verplichtingen volgen dan in de bepalingen daarna.

Hoewel het doel van de verwerking meestal al in de hoofdovereenkomst zal zijn opgenomen, is het van belang om duidelijk te maken dat uitsluitend de verwerkingsverantwoordelijke het doel van de verwerking bepaalt en instructies ten aanzien daarvan aan de verwerker kan geven. Een algemene verwijzing naar de hoofdovereenkomst kan ruimte voor interpretatie opleveren over de wijze waarop de persoonsgegevens worden verwerkt teneinde aan het doel uit de hoofdovereenkomst te voldoen. Hierna wordt een voorbeeldclausule weergegeven:

- 1.1 Verwerkingsverantwoordelijke bepaalt het doel van de verwerking, het soort persoonsgegevens dat verwerkt wordt en de categorieën betrokkenen ten aanzien waarvan persoonsgegevens verwerkt worden.
- 1.2 Verwerker verwerkt de persoonsgegevens uitsluitend op basis van schriftelijke instructies van Verwerkingsverantwoordelijke, tenzij de verwerking noodzakelijk is om te voldoen aan een op Verwerker rustende wettelijke verplichting. In dat geval stelt Verwerker Verwerkingsverantwoordelijke voorafgaand aan de verwerking in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving verbiedt.
- 1.3 Verwerkingsverantwoordelijke zal Verwerker uitsluitend instructies geven die in lijn zijn met toepasselijke wet- en regelgeving inzake gegevensbescherming, waaronder de AVG. Verwerker stelt Verwerkingsverantwoordelijke onmiddellijk in kennis indien een instructie naar zijn mening inbreuk oplevert op voornoemde wet- en regelgeving.

Sommige verwerkers willen de gegevens die zij ontvangen toch zelf graag gebruiken om te analyseren hoe hun product gebruikt wordt en om hun product aan de hand daarvan verder te kunnen ontwikkelen. Denk daarbij bijvoorbeeld aan software. Dit kan een knelpunt opleveren, omdat de verwerkingsverantwoordelijke de persoonsgegevens niet voor dat doel verzameld heeft.

De Franse Autoriteit Persoonsgegevens (CNIL) heeft een richtlijn gepubliceerd waarin voorwaarden uiteengezet zijn waaronder dergelijk hergebruik is toegestaan.[7] Aangenomen wordt dat de Nederlandse AP er eenzelfde visie op na houdt, omdat EU-verordeningen zoals de AVG rechtstreekse werking hebben en de Franse en Nederlandse toezichthouder dus binnen hetzelfde Europese kader werken.[8] Het hergebruik is volgens de richtlijn van de Franse toezichthouder alleen toegestaan als de verwerkingsverantwoordelijke daar toestemming voor geeft, en die toestemming mag de verwerkingsverantwoordelijke alleen geven als het hergebruik verenigbaar is met het doel waarvoor de gegevens zijn verzameld. Bij het bepalen van de verenigbaarheid moet bijvoorbeeld rekening gehouden worden met de mogelijke gevolgen van de voorgestelde verwerking voor de betrokkenen en het bestaan van passende waarborgen, waaronder encryptie of pseudonimisering.

De CNIL noemt zelf het voorbeeld van een verwerker die gegevens wil hergebruiken om zijn cloudcomputingdiensten te verbeteren. Dit hergebruik zou als verenigbaar met de oorspronkelijke verwerking kunnen worden beschouwd, mits passende waarborgen worden geboden, zoals anonimisering.[9] Anderzijds zou het hergebruik voor commerciële acquisitie nauwelijks voldoen aan de 'verenigbaarheidstoets', aldus de CNIL.

Als de verenigbaarheidstoets leidt tot toestemming aan de verwerker om de persoonsgegevens te hergebruiken, dan is de hiervoor genoemde contractsbepaling een goede plek om die toestemming in op te nemen. Daarbij kan dan benadrukt worden dat de verwerker ten aanzien

5 De volledige opsomming staat in art. 9 lid 1 AVG. Het gaat hierbij om persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens, gezondheidsgegevens, gegevens met betrekking tot iemand seksueel gedrag of seksuele gerichtheid. Art. 10 AVG geeft een apart regime voor persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen.

6 https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-boete-orthodontiepraktijk-vanwege-onbeveiligde-patientenwebsite.

7 www.cnil.fr/fr/sous-traitants-la-reutilisation-de-donnees-confiees-par-un-responsable-de-traitement.

8 www.ictrecht.nl/blog/persoonsgegevens-gebruiken-voor-analyse-en-ontwikkeling-wat-mag-een-verwerker.

9 NB Bij correcte uitvoering zijn de gegevens na anonimiseren onomkeerbaar niet meer te herleiden tot een persoon, waarna de AVG daarop niet meer van toepassing is. Om de persoonsgegevens te kunnen anonimiseren zal de verwerker die persoonsgegevens echter voor zijn eigen doeleinden moeten verwerken (verzamelen, opslaan, bewerken enz.). Dat gebeurt doorgaans voor een ander doeleinde dan waarvoor de verwerkingsverantwoordelijke de verwerker heeft ingeschakeld. Daar heeft de verwerker dus ook al toestemming van de verwerkingsverantwoordelijke voor nodig.

doi: 10.5553/Contr/156608932022024004005

Dit artikel uit Contracteren is gepubliceerd door Boom juridisch en is bestemd voor anonieme bezoeker

van dit hergebruik de verwerkingsverantwoordelijke is. Ook kan worden opgenomen wie van beide partijen de betrokkenen informeert over de doorgifte van gegevens voor dit doel, en de mogelijkheid van betrokkenen om daar bezwaar tegen te maken.

3.4 Vertrouwelijkheid/geheimhouding

In de verwerkersovereenkomst moet worden opgenomen dat de verwerker waarborgt dat de personen die toegang hebben tot de persoonsgegevens aan een contractuele of wettelijke geheimhoudingsplicht zijn gebonden. Meestal zal het hierbij gaan om werknemers van de verwerker. In dat geval volgt de geheimhoudingsplicht al uit de eisen van goed werknemerschap, zoals opgenomen in artikel 7:611 van het Burgerlijk Wetboek (BW).[10] Daarnaast kan een geheimhoudingsbeding in de arbeidsovereenkomst zijn opgenomen.

Uitzendkrachten en freelancers zijn niet aan artikel 7:611 BW gebonden, omdat zij niet in dienst zijn bij de verwerker. In die gevallen moet de geheimhouding dus apart geregeld worden.

De verwerkingsverantwoordelijke kan verlangen dat de geheimhoudingsverplichting van de verwerker versterkt wordt met een boeteclausule in de zin van artikel 6:91 BW, als stok achter de deur om de geheimhoudingsverplichting adequaat na te komen. Daar kan met name aanleiding voor zijn als er gewerkt wordt met bijzondere persoonsgegevens, waarbij geheimhouding van het grootste belang is. Een knelpunt bij het overeenkomen van zo'n boeteclausule is – zoals ook het geval is bij zulke clausules in Non Disclosure Agreements – dat de verwerkingsverantwoordelijke deze kan misbruiken, onder meer doordat de geheimhoudingsverplichtingen gewoonlijk heel ruim zijn omschreven en er in de boeteclausule meestal geen onderscheid wordt gemaakt tussen grote en kleine overtredingen; verwerkers zullen daardoor in de praktijk vrijwel steeds proberen de toevoeging van een boeteclausule tegen te houden.

3.5 Technische en organisatorische maatregelen

Een verwerkingsverantwoordelijke mag alleen verwerkers inschakelen die voldoende garanties bieden met betrekking tot het toepassen van passende technische en organisatorische maatregelen, zodat de verwerking aan de eisen van de AVG voldoet en de rechten van betrokkenen gewaarborgd zijn. Daarbij moet rekening worden gehouden met de stand van de techniek en de uitvoeringskosten tegenover de aard, omvang en context van de verwerkingsdoeleinden en in dat verband de mogelijke risico's voor de rechten en vrijheden van personen.

Meestal wordt deze verplichting in algemene zin opgenomen in de verwerkersovereenkomst, waarbij dan verwezen wordt naar een bijlage waarin de specifiek toegepaste maatregelen opgesomd staan. Daarbij kan het bijvoorbeeld gaan om pseudonimisering en versleuteling van persoonsgegevens, tweefactorauthenticatie, bijhouden van logbestanden zodat gecontroleerd kan worden wie toegang tot bepaalde gegevens heeft gehad, regelmatig back-ups maken en regelmatig testen van de doeltreffendheid van de beveiliging.

Het opnemen van een algemene garantie van de verwerker aan de verwerkingsverantwoordelijke, die inhoudt dat de verwerker passende maatregelen zal treffen, lijkt onvoldoende in het licht van de eigen verantwoordelijkheid van de verwerkingsverantwoordelijke op dit vlak, die duidelijker naar voren komt in de tekst van artikel 32 AVG ('treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen'). De AP beveelt dan ook aan om de specifieke maatregelen in een bijlage vast te leggen.[11]

In de praktijk verlangen sommige verwerkers omgekeerd een vrijwaring van de verwerkingsverantwoordelijke die inhoudt dat de verwerkingsverantwoordelijke de opgesomde maatregelen als passend heeft beoordeeld en de verwerker schadeloos stelt voor zover de maatregelen toch niet passend mochten blijken te zijn. Hoewel het vaak de verwerker zelf is die de specifieke technische en organisatorische maatregelen vaststelt, blijft het immers ook aan de verantwoordelijke om een passend beschermingsniveau te waarborgen. Een verwerker zal geen verantwoordelijkheid of aansprakelijkheid willen dragen voor de eventuele financiële consequenties (waaronder boetes) als de getroffen maatregelen achteraf niet passend blijken te zijn geweest. Dit kan een knelpunt in de onderhandelingen opleveren als het bij de verwerkingsverantwoordelijke aan de specifieke deskundigheid ontbreekt om bepaalde maatregelen op adequaatheid te beoordelen. De AP beveelt in zo'n geval aan om in ieder geval na overleg vast te leggen welke risico's er door de verwerker dienen te worden gemitigeerd of uiteen te zetten met welke maatregelen men dat doet.[12]

Zowel verwerker als verwerkingsverantwoordelijke moet zich bovendien realiseren dat de stand van de techniek aan verandering onderhevig is. Maatregelen die vandaag passend zijn, zijn dat over een jaar misschien al niet meer. Het verdient dan ook aanbeveling om een bepaling op te nemen die inhoudt dat partijen periodiek zullen evalueren of de getroffen maatregelen nog altijd passend zijn. De verwerkingsverantwoordelijke zal niet zelden proberen te bereiken dat de verwerker de maatregelen spontaan up-to-date houdt, terwijl de verwerker er meestal naar streeft om het initiatief daarvoor bij de verwerkingsverantwoordelijke te laten.

In de praktijk zijn diverse certificeringen ontwikkeld aan de hand waarvan verwerkers kunnen aantonen dat zij een passend beschermingsniveau bieden. Internatio-

10 HR 26 oktober 2012, ECLI:NL:HR:2012:BW9244, r.o. 3.5.1: 'In beginsel dient een werknemer, uit hoofde van goed werknemerschap als bedoeld in art. 7:611 BW, ten opzichte van zijn werkgever loyaliteit en discretie te betrachten. Dit houdt mede in dat hij bijzonderheden over de bedrijfsvoering van de werkgever voor zich moet houden.'

11 Autoriteit Persoonsgegevens, Werkende verwerkersovereenkomsten. Onderzoek naar de toepassing in de private sector, 2019, p. 20.

12 Idem.

doi: 10.5553/Contr/156608932022024004005

Dit artikel uit Contracteren is gepubliceerd door Boom juridisch en is bestemd voor anonieme bezoeker

naal gaat het daarbij bijvoorbeeld om ISO 27001.[13] Specifiek voor de zorg zijn de nationale normen NEN 7510, NEN 7512 en NEN 7513 ontwikkeld.[14] Een certificering doet echter geen afbreuk aan de verantwoordelijkheid van de verwerkingsverantwoordelijke, zo bepaalt artikel 42 lid 4 AVG. Een verwerkingsverantwoordelijke kan dus niet blind vertrouwen op een dergelijke certificering, maar zal zich er ook van moeten vergewissen wat een dergelijke certificering inhoudt en of daarmee in gegeven omstandigheden een passend beschermingsniveau wordt bevestigd.

3.6 Inschakelen van subverwerkers (en doorgifte naar andere landen)

Een verwerker mag bij zijn dienstverlening aan de verwerkingsverantwoordelijke geen andere verwerkers (subverwerkers) inschakelen zonder voorafgaande toestemming van de verwerkingsverantwoordelijke. Het is dus van belang om in de verwerkersovereenkomst op te nemen op welke manier die toestemming gegeven wordt. Zo kan er specifieke toestemming voor het inschakelen van bepaalde subverwerkers gegeven worden, waarbij die subverwerkers bij naam worden genoemd. Voor het inschakelen van andere subverwerkers moet dan nog apart toestemming gevraagd worden. Meestal wordt hierover afgesproken dat de verwerkingsverantwoordelijke zijn toestemming niet op onredelijke gronden zal weigeren. Een voorbeeldbepaling ziet er als volgt uit:

- 2.1 Verwerker mag bij het uitvoeren van de Overeenkomst alleen met voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke een subverwerker inschakelen. Deze toestemming wordt niet zonder redelijke grond geweigerd.
- 2.2 Verwerkingsverantwoordelijke geeft hierbij toestemming voor het inschakelen van de in Bijlage 2 opgenomen subverwerkers.

Een algemene toestemming voor het inschakelen van subverwerkers is ook mogelijk. De verantwoordelijke moet dan wel de mogelijkheid worden geboden om bezwaar te maken tegen het inschakelen van een nieuwe subverwerker, zo volgt uit artikel 28 lid 2 AVG. Er wordt dan meestal een bepaling opgenomen die inhoudt dat de verwerker minimaal een x-aantal dagen voor aanvang van de werkzaamheden door de subverwerker de verantwoordelijke op de hoogte zal stellen van het voornemen om deze subverwerker in te schakelen, waarna de verwerkingsverantwoordelijke de mogelijkheid krijgt om daar bezwaar tegen te maken.

De verwerker die een subverwerker inschakelt, is op grond van artikel 28 lid 4 AVG verplicht om op zijn beurt een verwerkersovereenkomst met de subverwerker te sluiten waarin minimaal dezelfde verplichtingen zijn opgenomen als in de verwerkersovereenkomst tussen de verwerker en de verwerkingsverantwoordelijke. Deze verplichting wordt meestal expliciet in de verwerkersovereenkomst overgenomen. Daarbij is het mogelijk om de verantwoordelijke een recht op inzage in de subverwerkersovereenkomsten toe te kennen. Het is niet noodzakelijk om dat apart te benoemen, omdat dit ook al volgt uit de algemene informatieplicht van de verwerker aan de verwerkingsverantwoordelijke zoals opgenomen in artikel 28 lid 3 sub h AVG. Een voorbeeldbepaling kan er volgt uitzien:

- 2.3 Indien Verwerker met inachtneming van het bepaalde in dit artikel een subverwerker inschakelt om ten behoeve van Verwerkingsverantwoordelijke verwerkingsactiviteiten te verrichten, worden aan deze subverwerker bij een overeenkomst minimaal dezelfde verplichtingen inzake gegevensbescherming opgelegd als die welke in deze Verwerkersovereenkomst zijn opgenomen.
- 2.4 Verwerker biedt Verwerkingsverantwoordelijke op eerste verzoek inzage in de verwerkersovereenkomsten(en) die hij met subverwerker(s) heeft gesloten.

Een punt van aandacht bij het inschakelen van subverwerkers is de doorgifte van persoonsgegevens aan andere landen. Hostingpartijen zoals Amazon AWS en Google Cloud werken bijvoorbeeld vaak met servers die in het buitenland staan, waardoor persoonsgegevens over de grens verwerkt worden. Doorgifte van persoonsgegevens aan derde landen is op grond van artikel 45 AVG alleen toegestaan als dat land een passend beschermingsniveau biedt. Dit houdt in dat het land een niveau van bescherming van de grondrechten en de fundamentele vrijheden biedt dat in grote lijnen overeenkomt met het niveau dat binnen de EU wordt gewaarborgd.[15] Doorgifte van persoonsgegevens aan andere landen binnen de EU is dus toegestaan.

Voor een aantal landen buiten de EU, zoals Canada, Japan, Nieuw-Zeeland, Zwitserland en het Verenigd Koninkrijk, heeft de Europese Commissie zogenoemde adequaatheidsbesluiten[16] genomen waarin is vastgesteld dat die landen een passend beschermingsniveau bieden. De volledige lijst kan ingezien worden op de website van de Europese Commissie.[17] Grote afwezige op de lijst adequaatheidsbesluiten zijn de Verenigde Staten. Tot tweemaal toe zijn adequaatheidsbesluiten ten aanzien van de VS ongeldig verklaard door het Europees Hof van Justitie (HvJ EU) in de Schrems I- en Schrems II-uitspraken.[18]

Bestaat ten aanzien van een bepaald land geen adequaatheidsbesluit, dan kan gebruik worden gemaakt van

13 www.iso.org/isoiec-27001-information-security.html.

14 Deze NEN-normen zijn door het ministerie van Volksgezondheid, Welzijn en Sport afgekocht en daardoor gratis beschikbaar op www.nen.nl/.

15 HvJ EU 6 oktober 2015, C-362/13 (Schrems I), r.o. 73.

16 Op grond van art. 45 AVG kan een doorgifte van persoonsgegevens aan een derde land of een internationale organisatie plaatsvinden wanneer de Commissie heeft besloten dat het derde land, een gebied of één of meerdere nader bepaalde sectoren in dat derde land, of de internationale organisatie in kwestie een passend beschermingsniveau waarborgen. Dergelijke besluiten door de Europese Commissie worden adequaatheidsbesluiten genoemd.

17 https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

18 HvJ EU 6 oktober 2015, C-362/13 (Schrems I); HvJ EU 16 juli 2020, C-311/18 (Schrems II).

doi: 10.5553/Contr/156608932022024004005

Dit artikel uit Contracteren is gepubliceerd door Boom juridisch en is bestemd voor anonieme bezoeker

de door de Europese Commissie opgestelde standaard contractsbepalingen (artikel 46 lid 2 sub c AVG), waarmee in beginsel tussen partijen onderling alsnog de benodigde passende waarborgen worden gegeven. Gebruik van de standaard contractsbepalingen is echter niet voldoende, mede omdat de lokale wet contractuele bepalingen kan overrulen. Partijen moeten per geval beoordelen of de wet of praktijk in het derde land afbreuk doet aan de doeltreffendheid van de waarborgen. Als dat zo is, zijn aanvullende waarborgen nodig.[19] Naar aanleiding van Schrems II heeft de European Data Protection Board (EDPB) aanbevelingen gepubliceerd voor dergelijke aanvullende waarborgen.[20]

In de praktijk wordt in verwerkersovereenkomsten meestal expliciet vermeld dat het doorgeven van persoonsgegevens buiten de EU niet is toegestaan. Met name bij sommige subverwerkers die hosting en cloudopslag verzorgen is dat echter niet altijd haalbaar. Gaat het om verwerking in een land ten aanzien waarvan geen adequaatheidsbesluit bestaat, dan is het raadzaam om de aanbevelingen van de EDPB erop na te slaan.

3.7 Rechten van betrokkenen

Op grond van de AVG hebben betrokkenen (de natuurlijke personen van wie de persoonsgegevens worden verwerkt) onder andere het recht op inzage (artikel 15 AVG), rectificatie (artikel 16 AVG) en gegevenswissing[21] (artikel 17 AVG). Deze rechten kunnen uitgeoefend worden tegenover de verwerkingsverantwoordelijke. De verwerker is verplicht om de verantwoordelijke, voor zover mogelijk, bij de uitvoering hiervan te assisteren.

Bij de aanvang van de samenwerking is vaak nog niet te voorspellen hoe vaak betrokkenen van hun rechten gebruik zullen willen maken en hoe tijdrovend het voor de verwerker zal zijn om zijn medewerking te verlenen. Vanuit de verwerker bezien is het daarom raadzaam om een bepaling op te nemen die inhoudt dat de uren en kosten die door de verwerker gemaakt worden in verband met het verlenen van deze bijstand vergoed worden door de verantwoordelijke tegen een vooraf bepaald tarief. De verantwoordelijke zal juist verlangen dat de verwerker deze werkzaamheden uitvoert als onderdeel van de totale deal, en dus zonder daarvoor extra kosten in rekening te brengen. Kunnen partijen het niet eens worden over de kosten, dan is het mogelijk om een min of meer neutrale bepaling op te nemen waarin wordt afgesproken dat de verantwoordelijke de kosten in redelijkheid zal vergoeden.

3.8 Beveiliging, datalekmeldplicht en medewerking bij gegevensbeschermingseffectbeoordeling (DPIA)

In de verwerkersovereenkomst moet opgenomen worden dat de verwerker verplicht is om de verwerkingsverantwoordelijke bijstand te verlenen bij de nakoming van diens verplichtingen uit hoofde van de artikelen 32 tot en met 36 AVG. Daarbij gaat het om het treffen van beveiligingsmaatregelen (hiervoor al besproken), het melden van datalekken, en de gegevensbeschermingseffectbeoordeling, beter bekend onder de Engelse afkorting DPIA (Data Protection Impact Assessment). Een DPIA is verplicht als de verwerking waarschijnlijk een hoog risico voor de betrokkenen oplevert en moet in dat geval voorafgaand aan de verwerking door de verwerkingsverantwoordelijke uitgevoerd worden.

Speciale aandacht gaat uit naar de datalekmeldplicht. Op grond van artikel 33 lid 2 AVG is de verwerker verplicht om de verantwoordelijke 'zonder onredelijke vertraging' te informeren zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens (datalek). De verantwoordelijke is (uitzonderingen daargelaten)[22] op grond van artikel 33 lid 1 AVG verplicht om een datalek uiterlijk 72 uur nadat hij er kennis van heeft genomen aan de AP te melden. De AP vat het niet tijdig doen van een melding op als een ernstige overtreding van de AVG en heeft hiervoor al enkele boetes uitgedeeld.[23]

De 72 uur die de verantwoordelijke heeft om te melden gaan in principe lopen vanaf het moment dat de verwerker hem op de hoogte heeft gesteld van het datalek. Dat is het moment dat de verantwoordelijke kennis heeft van het datalek, aldus de EDPB.[24]

In verwerkersovereenkomsten wordt de termijn van 72 uur die de verantwoordelijke heeft om melding te doen echter vaak 'opgeknipt' en verdeeld over de verwerker en de verwerkingsverantwoordelijke. De verwerker moet dan bijvoorbeeld binnen 36 uur na ontdekking melden aan de verwerkingsverantwoordelijke, waarbij men ervan uitgaat dat de verantwoordelijke dan zelf nog 36 uur over heeft om de melding te doen. Als er nog subverwerkers bij betrokken zijn, wordt het soms nog krapper. De 36 uur die de verwerker heeft, wordt dan weer gedeeld met de subverwerker, waardoor beide partijen nog maar 18 uur overhouden om de meldingen te doen. Hoe korter

19 Schrems II, r.o. 134.

20 EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, https://edpb.europa.eu.

21 Bekend geworden als 'het recht om vergeten te worden', dat bijvoorbeeld ook ingeroepen kan worden tegen zoekmachines om zoekresultaten die naar verouderde informatie verwijzen te verwijderen. Zie in dit verband HvJ EU 13 mei 2014, C-131/12 (Google Spain).

22 Er hoeft geen melding plaats te vinden als het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

23 De PVV Overijssel kreeg op 16 juni 2020 een boete van € 7500 opgelegd omdat volledig was nagelaten melding te doen van een datalek. Bij het verzenden van een e-mailuitnodiging waren 101 e-mailadressen voor alle geadresseerden zichtbaar. Booking.com kreeg op 10 december 2020 een boete van € 475.000 voor het 22 dagen te laat melden van een datalek waarbij o.a. creditcardgegevens door hackers waren buitgemaakt. Zie www.autoriteitpersoonsgegevens.nl/nl/nieuws/boete-pvv-overijssel-vanwege-niet-melden-datalek; www.autoriteitpersoonsgegevens.nl/nl/nieuws/boete-bookingcom-voor-te-laat-melden-datalek.

24 WP250 rev.1, 6 februari 2018, Guidelines on Personal data breach notification under Regulation 2016/679 – onderschreven door de EDPB, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052. Zie ook Engelfriet & De Vos, Handboek ICT-contracten, Utrecht: Ius Mentis 2020, p. 417.

doi: 10.5553/Contr/156608932022024004005

Dit artikel uit Contracteren is gepubliceerd door Boom juridisch en is bestemd voor anonieme bezoeker

de termijn wordt, hoe meer dit tot een discussiepunt tijdens de onderhandelingen kan leiden, zeker als de meldplicht wordt versterkt met een boeteclausule.
De hierna nog te bespreken documentengenerator van Rocket Lawyer gaat zelfs uit van een standaardtermijn van slechts 4 uur om een datalek te melden aan de verwerkingsverantwoordelijke, op straffe van een boete die per uur dat er te laat gemeld wordt met 2% verhoogd wordt.
Dit 'opknippen' van de termijn van 72 uur is toelaatbaar, maar niet nodig. Wel moet in het oog gehouden worden dat de verwerker zonder onredelijke vertraging de verantwoordelijke moet informeren. Het is niet ongebruikelijk om daar een termijn van bijvoorbeeld 24 of 48 uur te noemen, tenzij bijvoorbeeld de aard en omvang van het datalek een snellere melding vereisen.

3.9 Vernietiging of teruggave persoonsgegevens bij einde overeenkomst

Na afloop van de verwerkingsdiensten moet de verwerker de persoonsgegevens aan de verwerkingsverantwoordelijke teruggeven en/of wissen, naar keuze van de verwerkingsverantwoordelijke. De meest logische plek om deze verplichting op te nemen is in een algemene clausule met betrekking tot de duur en beëindiging van de overeenkomst. De duur zal altijd gelijk moeten zijn aan die van de hoofdovereenkomst, want zolang er persoonsgegevens verwerkt worden is er een verwerkersovereenkomst nodig. De verwerkersovereenkomst kan dus niet los opzegbaar zijn ten opzichte van de hoofdovereenkomst.
De verwerkingsverantwoordelijke kan specifieke instructies aan de verwerker geven over de wijze waarop de vernietiging of teruggave moet plaatsvinden. De verantwoordelijke kan bijvoorbeeld verlangen dat de verwerker de persoonsgegevens in een ander formaat retourneert dan waarin ze zijn aangeleverd. Het is dan wel gebruikelijk dat dit gebeurt tegen vergoeding van de redelijke kosten daarvan.

3.10 Audits

De verwerker is verplicht om de verwerkingsverantwoordelijke alle informatie ter beschikking te stellen om de nakoming van zijn verplichtingen uit hoofde van de verwerkersovereenkomst aan te tonen en om in dat verband zijn medewerking te verlenen aan audits door of namens de verwerkingsverantwoordelijke.
Meestal wordt in de verwerkersovereenkomst afgesproken hoe vaak de verwerkingsverantwoordelijke een audit uit kan laten voeren, door wie, en voor wiens rekening de kosten van een dergelijke audit komen. Een voorbeeld van dergelijke bepalingen luidt als volgt:

- 3.1 Verwerker stelt op eerste verzoek van Verwerkingsverantwoordelijke alle informatie ter beschikking die nodig is om aan te tonen dat de verplichtingen uit hoofde van deze overeenkomst zijn nagekomen.
- 3.2 Verwerker is verplicht zijn medewerking te verlenen aan namens Verwerkingsverantwoordelijke uit te voeren audits. Verwerkingsverantwoordelijke zal maximaal 1 maal per jaar een audit laten uitvoeren, tenzij Verwerkingsverantwoordelijke gerede aanleiding heeft om te twijfelen aan de nakoming van de verplichtingen door Verwerker.
- 3.3 Een audit als bedoeld in dit artikel wordt uitgevoerd door een onafhankelijke auditor en vindt plaats op kosten van Verwerkingsverantwoordelijke, tenzij uit de audit volgt dat Verwerker tekort is geschoten in de nakoming van zijn verplichtingen.

3.11 Aansprakelijkheid

De verwerking van persoonsgegevens kan vele complexe aansprakelijkheidsvraagstukken oproepen. Op grond van de AVG hebben de verwerkingsverantwoordelijke en verwerker ieder eigen verplichtingen en daarmee samenhangende individuele aansprakelijkheidsrisico's, maar tegelijkertijd is het heel goed mogelijk dat ze alle twee voor dezelfde onvolkomenheden bij de verwerking worden aangesproken (door de AP of betrokkenen).[25]
Aangezien er geen algemene verzekeringsplicht bestaat voor dat soort aanspraken, blijken beide partijen in de praktijk een sterke neiging te voelen om de risico's naar de ander te verleggen.
Meestal is er in de hoofdovereenkomst al een bepaling opgenomen met betrekking tot de aansprakelijkheid van partijen over en weer. Het is aan te bevelen om erbij stil te staan of die bepaling zich ook leent om in de verwerkersovereenkomst naar te verwijzen. Dat is niet altijd het geval.
Vaak is de aansprakelijkheid in de hoofdovereenkomst namelijk over en weer gemaximeerd tot een bepaald bedrag, waarbij bijvoorbeeld aansluiting wordt gezocht bij het totaal in een contractjaar gefactureerde bedrag, maar waarbij geen rekening is gehouden met de hoogte van een eventuele door de AP op te leggen boete. De maximale boete die de AP kan opleggen bedraagt ingevolge artikel 83 AVG € 20.000.000 of 4% van de totale wereldwijde jaaromzet van een onderneming, en zou dus veel hoger kunnen zijn dan de aansprakelijkheidslimiet die in de hoofdovereenkomst is opgenomen.
Dit leidt in de praktijk vaak tot een discussie over de aansprakelijkheidslimiet. Een partij die een boete opgelegd krijgt als gevolg van een doen of nalaten van de andere partij, zal die andere partij volledig aansprakelijk willen stellen voor die boete, ongeacht de limiet die in de hoofdovereenkomst is opgenomen. Als de aansprakelijkheidsclausule uit de hoofdovereenkomst overeenkomstig van toepassing zou zijn verklaard, dan zou dat dus (afhankelijk van de exacte bewoordingen van de clausule) niet altijd kunnen.
De vrees voor een eventuele boete die de AP aan de verwerkingsverantwoordelijke zou kunnen opleggen als ge-

25 Vanwege het feit dat verwerkingsverantwoordelijke en verwerker ieder een eigen rol hebben, betreft het daarbij geen hoofdelijke aansprakelijkheid. Zie echter art. 82 AVG: de verwerkingsverantwoordelijke is op grond van lid 2 in beginsel aansprakelijk voor alles wat er fout gaat bij de verwerking, tenzij hij aantoont dat 'hij op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit' (lid 3). Verder bepaalt art. 82 lid 4 AVG dat gezamenlijke verwerkingsverantwoordelijken of verwerkers ieder altijd 'voor de gehele schade' aansprakelijk zijn.

doi: 10.5553/Contr/156608932022024004005

Dit artikel uit Contracteren is gepubliceerd door Boom juridisch en is bestemd voor anonieme bezoeker

volg van een doen of nalaten door de verwerker, is daarom vaak aanleiding voor verwerkingsverantwoordelijken om in de verwerkersovereenkomst niet aan te sluiten bij de aansprakelijkheidslimiet uit de hoofdovereenkomst, maar juist een uitzondering op die limiet te bedingen in verband met eventuele boetes van de AP.
Vanuit de verwerker bezien kan een dergelijk verzoek tot ongelimiteerde aansprakelijkheid gepareerd worden door te wijzen op de verantwoordelijkheid van de verwerkingsverantwoordelijke om de verwerker te voorzien van de juiste instructies teneinde aan de AVG te (kunnen) voldoen, en de auditmogelijkheden die de verantwoordelijke toekomen om te controleren of de verwerker aan zijn verplichtingen voldoet. Daarmee biedt de wet de verantwoordelijke al voldoende mogelijkheden om zich ervan te verzekeren dat de AVG niet door de verwerker wordt overtreden, zo kan de verwerker betogen. Het begrip 'verwerkings*verantwoordelijke*' is natuurlijk ook niet voor niets zo gekozen.
Andersom kan de verwerker ook weer van de verwerkingsverantwoordelijke verlangen dat een ongelimiteerde aansprakelijkheid geldt voor eventuele boetes die aan de verwerker zouden kunnen worden opgelegd als gevolg van het nakomen van de instructies van de verwerkingsverantwoordelijke.

4. Documentengenerators

4.1 Divers aanbod online documentengenerators

Als in Google wordt gezocht op 'verwerkersovereenkomst' of 'verwerkersovereenkomst opstellen', dan komt een aantal advertenties naar boven van partijen die contracten aanbieden via documentengenerators, te weten DAS, ICTRecht, Rocket Lawyer en Wonder Legal. De eerste twee zullen bij de gemiddelde lezer van dit tijdschrift wel bekend zijn. Rocket Lawyer is een van oorsprong Amerikaans online juridische dienstverlener die in Nederland een samenwerking heeft met Sdu.[26] Wonder Legal is een website die wordt uitgegeven door een Frans IT-bedrijf en waarmee contracten op te stellen zijn op basis van modellen die door advocaten en juristen zijn geschreven, zo is te lezen in de algemene voorwaarden.[27]
DAS en ICTRecht bieden een verwerkersovereenkomst aan voor € 65 exclusief btw, Rocket Lawyer biedt een abonnementsdienst aan voor € 39,90, met een gratis proefperiode van zeven dagen, en Wonder Legal biedt een verwerkersovereenkomst aan voor € 39,99 exclusief btw. In alle gevallen wordt gewerkt met een vragenlijst die door de gebruiker ingevuld moet worden. Ik analyseer in het navolgende kort deze standaardovereenkomsten.

4.2 Rocket Lawyer en Wonder Legal

Ik begin met het bekijken van de goedkoopste opties, want we blijven natuurlijk wel zuinige Hollanders. Wat opvalt is dat bij Wonder Legal en Rocket Lawyer nauwelijks iets hoeft te worden ingevuld. Bij Wonder Legal ben je na het invullen van de partijnamen in vijf klikken bij het einde van het document. Bij Rocket Lawyer lukt het in zeven klikken, maar ben je vooral bezig met het invullen van boetebedragen. In beide gevallen rolt er uiteindelijk een overeenkomst uit waar je zelf nog allerlei bijlagen aan moet toevoegen, zoals een overzicht van het onderwerp en van duur, aard en doel van de verwerking, soort persoonsgegevens en categorieën van betrokkenen en de getroffen technologische en organisatorische maatregelen. In geen van beide gevallen wordt gevraagd namens welke partij de overeenkomst opgesteld wordt. Het model van Rocket Lawyer lijkt uit te gaan van de verwerkingsverantwoordelijke, gezien de daarin opgenomen boeteclausules en de forumkeuze die automatisch op de vestigingsplaats van de verwerkingsverantwoordelijke komt te staan.
Deze twee modellen leiden dus weliswaar binnen een paar muisklikken tot een overeenkomst, maar zijn nauwelijks op maat gesneden, houden geen rekening met de hoedanigheid van degene die de overeenkomst opstelt, en er is nog aanvullend werk nodig voor het opstellen van de benodigde bijlagen.

4.3 DAS en ICTRecht

De vragenlijsten van DAS en ICTRecht zijn daarentegen allebei zéér uitgebreid en overigens identiek. Dat lijkt geen toeval, want nader onderzoek leert dat beide partijen gebruikmaken van de documentengenerator van het legal tech platform JuriBlox, opgericht door de eigenaren van ICTRecht.[28]
Alle aspecten die in de verwerkersovereenkomst opgenomen moeten worden, komen in de vragenlijst aan bod, met daarbij allerlei varianten van bepalingen om uit te kiezen en allerlei extra opties waar partijen zelf misschien nog niet aan gedacht hadden.
Iemand die de uitgebreide vragenlijst moet invullen, zou dit wel wat veel werk kunnen vinden en misschien niet goed in staat zijn om sommige vragen zelf te beantwoorden, ondanks de toelichting die bij elke vraag wordt gegeven. Wie er zelf niet uitkomt, kan tegen bijbetaling een half uurtje telefonisch sparren met een jurist. Al met al zou dat tegen een redelijk tarief tot een solide verwerkersovereenkomst moeten leiden, zij het zonder advies op maat.

4.4 Documentengenerators als oplossing? Het hangt zoals altijd af van de omstandigheden van het geval.

Juist zo'n advies op maat is van belang om te kunnen bepalen welke specifieke risico's er in een bepaalde situatie spelen en hoe de belangen van partijen daarbij het beste gewaarborgd kunnen worden. Een verwerkers-

26 www.rocketlawyer.com/nl/nl.
27 www.wonder.legal/nl/.
28 https://juriblox.nl/succesverhalen/klanten-das-genereren-juridische-documenten-zelf.

doi: 10.5553/Contr/156608932022024004005

Dit artikel uit Contracteren is gepubliceerd door Boom juridisch en is bestemd voor anonieme bezoeker

overeenkomst opstellen via een documentengenerator lijkt daarom een prima oplossing voor eenvoudigere verwerkingen waar niet al te veel risico's bij komen kijken, maar in andere situaties blijft een advies op maat onontbeerlijk. Daarbij kan een modelovereenkomst natuurlijk wel als startpunt genomen worden.

5. Modelovereenkomsten

In diverse branches zijn modelverwerkersovereenkomsten ontwikkeld. Deze modelovereenkomsten hebben als voordeel dat ze specifiek zijn toegesneden op de branche waarin de persoonsgegevens verwerkt worden.

- Zo hebben de Brancheorganisaties Zorg gezamenlijk de BoZ modelverwerkersovereenkomst opgesteld voor de zorg, gratis online beschikbaar met toelichting.[29] Hierin wordt er rekening mee gehouden dat er sprake is van het verwerken van gezondheidsgegevens, inclusief de in de zorg geldende kwaliteitsnormen.
- Binnen het onderwijs hebben de PO-raad, VO-raad en MBO-raad een privacyconvenant gesloten namens alle aangesloten schoolbesturen.[30] Bij het convenant hoort een modelverwerkersovereenkomst. Verwerkers die diensten aan de aangesloten scholen willen aanbieden, kunnen toetreden tot het convenant en moeten de afspraken uit het convenant dan in hun verwerkersovereenkomsten opnemen. Daarvoor kan de modelovereenkomst gebruikt worden. Ook SURF, een samenwerkingsverband van Nederlandse universiteiten, hogescholen, universitaire medische centra, mbo-instellingen en onderzoeksinstellingen, heeft een modelverwerkersovereenkomst opgesteld.[31]
- Voor rijksoverheidsorganisaties heeft de overheid modelverwerkersovereenkomsten opgesteld die aansluiten bij de diverse sets algemene voorwaarden die door de overheid worden gehanteerd (ARBIT, ARVODI en ARIV).[32] In het algemeen geldt bij aanbestedingen door de overheid dat deze documenten vaststaan en dat een verwerker eigenlijk geen onderhandelruimte heeft.
- Branchevereniging NL Digital heeft een verwerkersovereenkomst opgesteld die achter een inlog gratis beschikbaar is voor leden.[33]
- Als onderdeel van het Horizon 2020 EU financieringsprogramma voor onderzoek en innovatie heeft het Zwitserse bedrijf Proton Technologies AG de website GDPR.eu ontwikkeld, een kennisdatabank voor AVG-compliance. Daar is een Engelse template voor een verwerkersovereenkomst te vinden die zeer summier en slechts in algemene termen de vanuit de AVG verplichte onderdelen opsomt.[34] Hoewel gefinancierd door de EU betreft dit geen officieel EU/EC-model. Als basisdocument is het wel een handzaam model, echter is aan te bevelen om het model aan te vullen met informatie over de specifieke casus waarvoor het model gebruikt wordt, zoals een omschrijving van technische en organisatorische beveiligingsmaatregelen.

Over het algemeen kunnen modelovereenkomsten die door brancheverenigingen zijn ontwikkeld goed als uitgangspunt worden genomen. Daarbij is het van belang om in het oog te houden vanuit welke partij bezien (verantwoordelijke dan wel verwerker) het model met name ontwikkeld zal zijn. Dit zal vooral te merken zijn in de bepalingen over kosten, aansprakelijkheid en boeteclausules.

6. Conclusie

Het opstellen van verwerkersovereenkomsten kan op het eerste gezicht ingewikkeld lijken, maar is dat in de basis eigenlijk niet. Aan de hand van de verplichte onderdelen die in artikel 28 AVG genoemd staan, kan de overeenkomst opgesteld en ingevuld worden. Er kan een modelovereenkomst als startpunt gebruikt worden, zeker wanneer een specifiek branchemodel beschikbaar is. Voor wie het allemaal dan toch nog duizelt, biedt een documentengenerator met een half uurtje telefonisch sparren wellicht soelaas. Daarmee is dan de belangrijke eerste stap gezet.

De tweede stap, het onderhandelen over de concrete uitwerking van ieders contractuele verplichtingen bij de verwerking van persoonsgegevens, levert in de praktijk daarentegen nog aardig wat botsingen op. Wat niet helpt, is dat alles door de dreiging van potentieel draconische boetes nog eens extra op scherp wordt gezet. Pasklare oplossingen voor contractenmakers zijn er daardoor bijna per definitie niet – de onderhandelingen over verwerkersovereenkomsten zijn in hoge mate een *zero sum game* waarbij elk van de partijen gedwongen wordt een zeer zorgvuldige risicoafweging te maken. Wel is er een lijstje met veelvoorkomende knelpunten te formuleren: bijzondere aandacht is vereist bij de allocatie van verantwoordelijkheid voor het vaststellen van de te treffen technische en organisatorische maatregelen, (sub)verwerkers die persoonsgegevens voor eigen doeleinden willen gebruiken, doorgifte naar derde landen, 'opgeknipte' termijnen voor het melden van datalekken en aansprakelijkheidsbeperkingen.

29 www.brancheorganisatieszorg.nl/nieuws_list/modelverwerkersovereenkomst-voor-de-zorgsector.

30 www.privacyconvenant.nl.

31 www.surf.nl/surf-juridisch-normenkader-cloudservices.

32 www.rijksoverheid.nl/documenten/publicaties/2018/01/25/model-verwerkersovereenkomst-avg.

33 www.nldigital.nl/avg-verwerkersovereenkomst.

34 https://gdpr.eu/data-processing-agreement.

doi: 10.5553/Contr/156608932022024004005