VAST | VERZEKERINGSRECHT AANSPRAKELIJKHEID SCHADE EN TOEZICHT

Aandachtspunten bij het sluiten van verwerkersovereenkomsten

VAST 2021 / P-010
1 april 2021

Vaak stellen dienstverleners bij het contracteren graag hun eigen templates beschikbaar, zo ook wat betreft de verwerkersovereenkomst. Deze zal echter doorgaans in het voordeel van de dienstverlener zijn opgesteld, en het is daarbij nog maar de vraag of het template aan de wettelijke vereisten voldoet. Verder heerst bij sommige dienstverleners de gedachte dat een verwerkersovereenkomst een standaardovereenkomst is die slechts hoeft te worden ondertekend en bijgevoegd bij de hoofdovereenkomst; maar niets is minder waar. Over de vereisten die gelden voor verwerkersovereenkomsten is daarbij het afgelopen jaar veel guidance gepubliceerd door de toezichthouders. Daardoor is nu duidelijker hoe de wettelijke kaders van de AVG geïnterpreteerd moeten worden. En wat blijkt? Er is minder ruimte dan tot nu toe vaak werd aangenomen.

In deze bijdrage gaan we in op de aandachtspunten bij het sluiten van een verwerkersovereenkomst. Nu de verzekeraar meestal als verwerkingsverantwoordelijke kan worden aangemerkt, gaan we daarbij uit van deze positie. Wat zijn de must-haves en wat de nice-to-haves? We gaan in op de onderhandelingsruimte en de redenen waarom het meestal niet verstandig is om akkoord te gaan met standaardverwerkersovereenkomsten van de wederpartij. Dit aan de hand van de recente ontwikkelingen en nadere guidance op dit vlak.

Wanneer een verwerkersovereenkomst?

Bij de relatie tussen een verzekeraar en tussenpersoon of gevolmachtigd agent zullen beide partijen vaak als verwerkingsverantwoordelijke kwalificeren. Ook bij pensioenovereenkomsten die werkgevers aangaan ten behoeve van hun werknemers, zijn de werkgever en de verzekeraar (en in voorkomende gevallen de tussenpersoon) zelfstandig verwerkingsverantwoordelijke. Dan hoeft geen verwerkersovereenkomst te worden gesloten. Maar wat als je als verzekeraar een dienstverleningsovereenkomst afsluit met bijvoorbeeld een IT-dienstverlener zoals de aanbieder van een clouddienst of een hosting service provider? Afhankelijk van de rol van de dienstverlener, is een verwerkersovereenkomst in dat geval wel vereist. Dit is in lijn met artikel 28 van de Algemene Verordening Gegevensbescherming (AVG) en artikel 7.9.1 van de Gedragscode Verwerking Persoonsgegevens Verzekeraars (versie 26 juni 2018).

Nadere guidance verwerkersovereenkomsten

Het afgelopen jaar hebben de Europese privacytoezichthouders druk aan de weg getimmerd op het gebied van verwerkersovereenkomsten. Over welke guidance hebben we het dan? En welke guidance kun je waarvoor het best gebruiken? In de eerste plaats hebben de Europese privacytoezichthouders zoals verenigd in de European Data Protection Board (EDPB) in september 2020 nieuwe guidelines ter consultatie ingediend over de begrippen (gezamenlijk) verwerkingsverantwoordelijke en verwerker, waarin ook op de inhoudelijke vereisten voor verwerkersovereenkomsten wordt ingegaan (Guidelines 07/2020). Diezelfde maand heeft de Autoriteit Persoonsgegevens het onderzoeksrapport 'Werkende verwerkersovereenkomsten'

gepubliceerd. Daarin worden onder meer specifieke bepalingen uit verwerkersovereenkomsten geciteerd, waarbij de Autoriteit Persoonsgegevens deze heeft gekwalificeerd als 'Do' of 'Don't'. Een praktisch referentiekader voor de praktijk, alhoewel het verre van een volledig kader biedt. Gelukkig is er op dit vlak nog meer gepubliceerd het afgelopen jaar.

In de tweede plaats zijn er twee Europese privacytoezichthouders geweest die zelf een modelverwerkersovereenkomst hebben opgesteld, in lijn met artikel 28(8) AVG. Het betreft de Deense en Sloveense toezichthouder. De Deense versie van Datatilsynet is publiekelijk toegankelijk in het Engels (zie website EDPB). Alhoewel duidelijk is dat het stuk niet is opgesteld door juristen die zelf werkzaam zijn in een contractpraktijk, kan het handig zijn om naar dit stuk te verwijzen in geval van discussie. Het stuk is opgesteld in het kader van het coherentiemechanisme van de AVG. Dit houdt kort gezegd in dat de andere Europese toezichthouders ook hun zegje hebben kunnen doen over de conceptversie, waarna de Deense toezichthouder nog het een en ander heeft aangepast. Aldus mag worden aangenomen dat teksten uit dit stuk – mits op juiste wijze toegepast – ook in Nederland compliant zijn. Een makkelijk model is het overigens niet: met name de Annexen zijn bijzonder uitgebreid. Deze annexen vormen de eigenlijke kern van een verwerkersovereenkomst waarin staat beschreven waarop de verwerking precies ziet.

In de derde plaats zijn er de 'standaardbepalingen voor contracten tussen verwerkingsverantwoordelijken en verwerkers in de EU' zoals door de Europese Commissie gepubliceerd, welke een bron van inspiratie kunnen vormen bij het opstellen of reviewen van verwerkersovereenkomsten (Ares(2020)6654429). Deze zijn beduidend behapbaarder, maar met name werkbaarder wanneer wordt opgetreden als verwerker. Aangezien het hier nog slechts de conceptversie betreft is het wanneer hieruit wordt geput raadzaam om de opinie van de EDPB en de EDPS over deze conceptbepalingen erbij te pakken (EDPB-EDPS Joint Opinion 1/2021). Daaruit blijkt wat de Europese privacytoezichthouders belangrijke onderwerpen vinden, en hoever bepaalde grenzen vanuit praktische overwegingen kunnen worden opgerekt. Ook de EDPB-opinies over de conceptversies van de modelcontracten van de Deense en Sloveense toezichthouder, zijn hiervoor zeer bruikbaar (Opinion 14/2019 en Opinion 17/2020).

Genoeg bronmateriaal dus om uit te putten. Maar wat zijn enkele kernpunten die hieruit naar voren komen, die nuttig zijn om te weten voor de praktijk?

Keuze verwerker

Voorafgaand aan het sluiten van de verwerkersovereenkomst dient een verwerker te worden geselecteerd. Een verwerkingsverantwoordelijke mag slechts gebruikmaken van een verwerker die voldoende technische en organisatorische maatregelen heeft genomen. De verwerkingsverantwoordelijke dient zich ervan te vergewissen dat de verwerking voldoet aan de vereisten uit de AVG en dat de rechten van de betrokkenen afdoende zijn gewaarborgd. In de praktijk komt het erop neer dat de verwerker relevante documentatie zal moeten overleggen die de verwerker daadwerkelijk kan aantonen. Denk hierbij bijvoorbeeld aan een privacystatement, gebruikersvoorwaarden, verwerkingsregisters, een informatiebeveiligingsbeleid, (externe) auditrapporten en relevante certificeringen (ISO 27000, NEN enzovoort). Dit zijn immers de enige waarborgen waar een verwerkingsverantwoordelijke daadwerkelijk rekening mee kan houden bij de beoordeling. Een verantwoordelijke zal daarnaast bij het beoordelen van de waarborgen van een verwerker in ieder geval rekening moeten houden met de expertise van de verwerker, de betrouwbaarheid en de middelen waarover de verwerker beschikt. Verder kan de reputatie van de

verwerker in de markt volgens de EDPB ook een rol spelen. Alhoewel verzekeraars vaak al een standaardproces voor vendor due diligence geïntegreerd zullen hebben in hun dagelijkse praktijk, kan het nuttig zijn deze procedure nog eens opnieuw te beoordelen in het licht van voornoemde specifieke punten zoals genoemd in de nadere guidance van de privacytoezichthouders. In dat kader kunnen ook de processors checklist en de information security checklist van de Information Commissioner's Office (ICO) in de UK, van pas komen.

One-pagers volstaan niet

Overeenkomsten waarin slechts de bepalingen uit artikel 28(2-4) AVG worden herhaald, volstaan niet. Partijen dienen uit te werken hoe zal worden voldaan aan de verplichtingen opgesomd in dat artikel. Op wat voor manier zal de verwerker bijstand verlenen aan de verwerkingsverantwoordelijke? Hoe zal de verwerker handelen wanneer deze zelf privacyverzoeken van individuen ontvangt (zoals een inzageverzoek) binnen de reikwijdte van de verwerkersovereenkomst? En hoe zal uitvoering worden gegeven aan het auditrecht van de verwerkingsverantwoordelijke? Om de overzichtelijkheid van de verwerkersovereenkomst toch te bewaken, kunnen dergelijke onderwerpen deels ook worden uitgewerkt in de bijlagen. Zowel de EDPB guidance als de modelverwerkersovereenkomst van Datatilsynet bevatten daarbij voorbeelden van de informatie die kan worden ingevuld. Hieruit blijkt dat voor het specificeren van de persoonsgegevens niet afdoende is als alleen de hoofdcategorie wordt vermeld: het is niet afdoende als alleen wordt aangegeven of al dan niet bijzondere categorieën persoonsgegevens overeenkomstig artikel 9 AVG en/of gevoelige persoonsgegevens in de zin van artikel 10 en 87 AVG worden verwerkt. Voorbeelden van omschrijvingen van persoonsgegevens die wel afdoende specifiek zijn, zijn: naam, e-mailadres, telefoonnummer, adres, nationaal identificatienummer, betaalgegevens, lidmaatschapsnummer en type lidmaatschap. Indien ook bijzondere of gevoelige gegevens worden verwerkt, dient het typte te worden gespecificeerd. Denk aan 'gegevens opgenomen in het patiëntendossier' of 'gegevens over lidmaatschap van een vakbond'.

Doorgifte

Een verwerkersovereenkomst dient informatie te bevatten over de vereisten voor doorgiftes die gelden voor de verwerker. Voor het legitimeren van doorgifte van persoonsgegevens naar buiten de Europese Economische Ruimte (EER; de EU-lidstaten plus Liechtenstein, Noorwegen en IJsland) gelden additionele vereisten, op basis van hoofdstuk V van de AVG. Van doorgifte is ook sprake als de persoonsgegevens toegankelijk kunnen zijn vanuit een land buiten de EER, zonder dat zij daar zelf staan opgeslagen. Tot voor kort bestond in dat kader het Privacy Shield voor doorgifte naar de Verenigde Staten (VS). Daarnaast vormden drie varianten van de zogeheten Standard Contractual Clauses (SCC's) een andere valide en relatief gemakkelijke optie voor het legitimeren van doorgiftes. Hierin is verandering gekomen sinds de Schrems II uitspraak van het Hof van Justitie van de Europese Unie (C-311/18), waarin het Privacy Shield ongeldig is verklaard en de rechtmatigheid van het gebruik van de doorgifte-SCC's ter discussie is komen te staan. Uit nadere guidance van de EDPB is duidelijk geworden dat de doorgifte-SCC's an sich niet volstaan. Naast een bepaling over doorgifte is het daarom raadzaam om de verwerker aanvullende informatie te laten specificeren. In de eerste plaats dient te worden aangegeven of de wet- en regelgeving in de landen waarnaar de persoonsgegevens zullen worden doorgegeven mogelijk in de weg staan aan de effectiviteit van de doorgifte-SCC's. Dit is bijvoorbeeld het geval voor de VS, alwaar overheidsinstanties zich onder omstandigheden toegang tot de persoonsgegevens kunnen verschaffen in weerwil van het gegevensbeschermingskader dat de doorgifte-SCC's beogen te bieden. Om een verwerker dit te laten beoordelen, kan gebruik worden gemaakt van een standaard questionnaire, waarbij de verwerker bijvoorbeeld dient aan te geven dat deze is ingevuld door een advocaat gespecialiseerd in het recht in desbetreffende jurisdictie. Indien blijkt dat in desbetreffend land het gegevensbeschermingskader niet afdoende wordt gewaarborgd, dient de

verwerker ook aan te geven of en, zo ja, welke additionele maatregelen zijn genomen in lijn met desbetreffende guidance van de EDPB. Indien ook subverwerkers mogen worden ingeschakeld, dient voornoemde informatie ook hiervoor in kaart te worden gebracht. Daarbij dient met betrekking tot de subverwerkers ook verdere informatie te worden opgenomen.

Subverwerkers en medewerkers

Subverwerkers mogen alleen met algemene of specifieke toestemming van de verwerkingsverantwoordelijke worden ingeschakeld. Inmiddels is duidelijk dat het verschil tussen algemene of specifieke toestemming beperkt is. In beide gevallen dient een lijst van subverwerkers te worden bijgevoegd waarvoor op het moment van ondertekening van de verwerkersovereenkomst toestemming wordt verleend. In het Deense model moet daarvoor worden ingevuld: volledige juridische naam van de subverwerker, KvK-nummer, adres en de verwerking waarvoor de subverwerker wordt ingeschakeld. Het verschil tussen algemene en specifieke toestemming voor het inschakelen van subverwerkers zit hem in de uitleg die mag worden gegeven aan het stilzitten van de verwerkingsverantwoordelijke wanneer de verwerkers nieuwe of andere subverwerkers willen inschakelen tijdens de contractstermijn. Bij specifieke toestemming is hiervoor opnieuw toestemming en dus een actieve handeling van de verwerkingsverantwoordelijke vereist. Bij algemene toestemming hoeft de verwerkingsverantwoordelijke alleen tijdig te worden geïnformeerd over de beoogde wijziging. Indien de verwerkingsverantwoordelijke vervolgens geen bezwaar maakt, kan de wijziging doorgang vinden. In dat kader beveelt de Autoriteit Persoonsgegevens aan dat de verwerkersovereenkomst ook afspraken bevat over de wijze van het maken van bezwaar. Denk aan het opnemen van een termijn voor het maken van bezwaar en het opnemen van criteria voor het afwijzen van een verwerker. Naar onze mening zullen laatstgenoemde criteria echter niet te restrictief mogen zijn, omdat dan de betekenis van de mogelijkheid van bezwaar zoals vereist door artikel 28(2) AVG te zeer wordt uitgehold.

Subverwerkersovereenkomsten dienen dezelfde verplichtingen inzake gegevensbescherming te bevatten als die zijn opgenomen in de verwerkersovereenkomst. Dit mag functioneel worden geïnterpreteerd. Indien een subverwerker slechts voor een specifiek onderdeel van de verwerking wordt ingeschakeld hoeven bepalingen uit de verwerkersovereenkomst die daarvoor niet relevant zijn, niet te worden opgenomen in de subverwerkersovereenkomst. Wel is in de Deense SCC met betrekking tot subverwerkers opgenomen dat de verwerkingsverantwoordelijke moet kunnen controleren of de verwerker inderdaad aan de subverwerkers dezelfde verplichtingen inzake gegevensbescherming heeft opgelegd. Daartoe mag de verwerkingsverantwoordelijke in het Deense model de gesloten subverwerkersovereenkomsten opvragen. Wel mogen bepalingen over '*business related issues that do not affect the legal data protection content*' worden weggelaten. Tot slot bevat het Deense model een verplichting voor de verwerker om met subverwerkers een third-party beneficiary clause op te nemen om te regelen dat de verwerkingsverantwoordelijke nakoming van de subverwerkersovereenkomst kan vorderen in geval van faillissement van de verwerker.

Ten aanzien van medewerkers van een verwerker die zijn betrokken bij de verwerking van de persoonsgegevens, heeft de EDPB in de eerste plaats aangegeven dat moet worden opgelet dat dit niet te beperkt is gedefinieerd (opinie re SCC Deense privacytoezichthouder). Alleen '*werknemers*' volstaat niet; '*personen die onder het gezag staan van de verwerker*' of '*personen direct of indirect in dienst van de verwerker*' is dan mogelijk een passender definiëring. Verder dient de verwerker aan te kunnen tonen dat deze personen aan een passende geheimhoudingsverplichting zijn

onderworpen en alleen op need-to-know-basis toegang krijgen tot de persoonsgegevens (opinie re SCC Sloveense privacytoezichthouder). Dit onder meer om het risico op datalekken te verminderen.

Datalekken

Op grond van de AVG dienen datalekken door de verwerker zonder onredelijke vertraging aan de verwerkingsverantwoordelijke te worden gemeld. De EDPB raadt aan hier een specifieke maximumtermijn aan te koppelen, in lijn met de algemene praktijk. Wat dan een passende termijn is, staat echter vaak ter discussie. Veelal mikken verwerkingsverantwoordelijken op 24 uur en verwerkers op 48 tot zelfs 72 uur. In de conceptversie van de Europese Commissie werd hierover de knoop alvast doorgehakt door een termijn van 48 uur vast op te nemen in de SCC. De EDPB geeft in haar opinie over deze SCC met de EDPS echter aan dat een passende termijn zal afhangen van de specifieke situatie, en dat deze daarom toch beter door partijen zelf kan worden bepaald. De Autoriteit Persoonsgegeven raadt in dat kader aan om als doelstelling te nemen dat de termijn zo kort mogelijk dient te zijn.

Het is raadzaam om in de verwerkersovereenkomst op te nemen dat het niet aan de verwerker is om te bepalen of een (mogelijk) datalek gemeld moet worden aan de bevoegde toezichthouder (zie EDPB-opinie over de Deense SCC). Daarbij is het raadzaam om bijvoorbeeld in een bijlage op te nemen welke informatie precies met betrekking tot het datalek moet worden gemeld. Daarbij kan worden aangehaakt bij de informatie die moet worden verstrekt op grond van het meldingsformulier voor datalekken zoals gehanteerd door de Autoriteit Persoonsgegevens zelf, alsook de informatie die andere mogelijk bevoegde toezichthouders vereisen.

Audits en inspecties

Vaak wordt het bereik van auditmogelijkheden door verwerkers beperkt. In de opinie over de Deense SCC heeft de EDPB echter duidelijk aangegeven dat het auditrecht niet mag worden beperkt tot bijvoorbeeld de faciliteiten van de verwerker. De verwerkingsverantwoordelijke (of auditor) moet bij audits toegang kunnen krijgen tot alle plekken, faciliteiten en systemen die worden gebruikt voor de verwerking. In dat kader heeft de EDPB ook duidelijk gemaakt dat zowel de verwerker als diens eventuele subverwerkers geaudit moeten kunnen worden. Dit laatste vormt in de praktijk vaak een struikelblok omdat dit door de verwerker dan ook in diens overeenkomst met desbetreffende subverwerker moet zijn opgenomen. Alhoewel bepalingen kunnen worden geïntroduceerd op grond waarvan de auditor aan bepaalde kwalificaties moet voldoen of dat de verwerker een auditor mag voorstellen, dient de verwerkingsverantwoordelijke hierover uiteindelijk de eindbeslissing te nemen.

Wat soms ontbreekt in verwerkersovereenkomsten is welke rechten en plichten partijen toekomen na afloop van de audit. Vaak is iets opgenomen in de trant van dat de verwerker die aanpassingen zal doorvoeren die vereist zijn om het adequate beveiligingsniveau te kunnen bieden zoals overeengekomen in de bepaling over beveiliging (en bijbehorende bijlage). In de opinie over de conceptversie van de Deense SCC vereist de EDPB echter dat ook de verwerkingsverantwoordelijke moet kunnen verzoeken dat maatregelen worden doorgevoerd naar aanleiding van de resultaten van de audit. In de SCC's van de Deense toezichthouder wordt daarvoor in de bepaling over audits en inspecties verwezen naar twee bijlagen waarin procedurebeschrijvingen dienen te worden opgenomen voor audits bij de verwerker en – indien van toepassing – bij subverwerkers. De voorbeelden die zijn voor-ingevuld zijn zeer uitgebreid en kunnen inspiratie bieden voor de praktijk.

Einde verwerking

Na afloop van de verwerkingsdiensten moeten de persoonsgegevens worden gewist of terugbezorgd aan de verwerkingsverantwoordelijke, en bestaande kopieën dienen te worden verwijderd. Bij voorkeur wordt deze keuze vooraf gemaakt, maar de verwerkersovereenkomst moet wel de mogelijkheid bevatten voor de verwerkingsverantwoordelijke om hierover van gedachte te veranderen. Indien de verwerkingsverantwoordelijke ervoor kiest om de persoonsgegevens door de verwerker te laten wissen, dient de verwerker ervoor zorg te dragen dat dit op beveiligde wijze geschiedt, ook met het oog op artikel 32 AVG. Daarbij dient de verwerker aan de verwerkingsverantwoordelijke te bevestigen wanneer het wissen van de gegevens is voltooid. Daarbij raden de privacytoezichthouders aan om de afspraken hieromtrent zo concreet mogelijk te maken. Denk aan de termijn waarbinnen dit gebeurt en de impact die dit heeft op de normale bedrijfsvoering. Indien de persoonsgegevens worden terugbezorgd kan de verwerkersovereenkomst vereisten bevatten over het bestandsformaat waarin zij dienen te worden aangeleverd en hoe de persoonsgegevens dienen te zijn beveiligd.

Aanbevelingen voor de praktijk

Voorgaande bevat reeds concrete handvatten voor de praktijk, waarbij nader is ingezoomd op enkele kernonderwerpen bij het uitonderhandelen van verwerkersovereenkomsten. Meer op hoofdlijnen kunnen de volgende aanbevelingen voor de praktijk worden gedestilleerd:

1. Beoordeel of het vendor due dilligence proces voldoet aan de nadere guidance van de Europese privacytoezichthouders.
2. Beoordeel of eigen modelverwerkersovereenkomsten voldoen aan de nadere guidance van de Europese privacytoezichthouders en pas aan waar nodig.
3. Maak bij het reviewen van modelverwerkersovereenkomsten gebruik van de nadere guidance van de Europese privacytoezichthouders: (i) ter beoordeling van de compliance van de inhoud daarvan maar ook (ii) als referentiekader en argument bij de contractonderhandelingen hierover.

Keywords

AVG
Privacy
Verwerker
Verwerkersovereenkomst
Verwerkingsverantwoordelijke

Auteur(s)

Vonne Laan

Advocaat privacyrecht en partner bij The Data Lawyers

LinkedIn

Joep Bakker

Paralegal privacy- en IT-recht bij The Data Lawyers

LinkedIn