centrum informatiebeveiliging en privacybescherming

Privacyafspraken bij ketensamenwerking

6 september 2020

Titel	**Privacyafspraken bij ketensamenwerking**
Datum	**September 2020**
Status	**Versie 1.1 definitief**
Regime	Becommentarieerde praktijk (voor uitleg zie https://cip-overheid.nl/totstandkoming)
Opdrachtgever	Centrum Informatiebeveiliging en Privacybescherming
Realisatie	CIP-werkgroep 'Ketens en verwerkersovereenkomsten' (2017)
Hoofdauteur	Ruben Tienhooven (BDO)
Adviezen	Marcel Koers (CIP)
Eerste verschijningsdatum	12 februari 2018 (versie 1.0)
Review 2020	Ruud de Bruijn (2020) 'Nieuwe CIP Huisstijl en tekstuele aanpassingen'
Documentnaam	Privacyafspraken bij ketensamenwerking v1.1.docx

Considerans

CIP-producten steunen op kennis van professionals uit verschillende organisaties actief in het CIP-netwerk, zowel uit de overheid als de markt.

Opmerkingen en aanvullingen kun je melden op cip-overheid.nl/contact.

Voorwoord

Risico en aansprakelijkheid kun je onder de moderne wetgeving niet zomaar wegwerken door naar anderen te wijzen. Werken in ketens vereist daarom afspraken met alle ketenbetrokkenen. En als je verstandig bent dan maak je die afspraken waterdicht.
Dit document gaat over dergelijke afspraken in het licht van de nieuwe Europese privacywetgeving. Het analyseert de privacy problematiek in ketenstructuren en geeft mogelijke oplossingen, niet in de laatste plaats in de vorm van een opzet voor een modelovereenkomst.

Totstandkoming van dit document

Dit document is het product van de inbreng en slagvaardigheid van professionals, die bij elkaar een breed palet van organisaties uit het CIP-netwerk bijeen hebben gebracht in de bijeenkomsten van de werkgroep 'Ketens en verwerkersovereenkomsten' onder voorzitterschap van Ad Kint (UWV/CIP) en Robert van Vianen (BDO). De informatie die tijdens deze bijeenkomsten is aangedragen en bediscussieerd over ketenbrede privacyafspraken, is werkendeweg opgeschreven en herhaaldelijk gereviewd door deelnemers van de werkgroep.
Zonder anderen te kort te willen doen zijn bij de totstandkoming van deze productie in het bijzonder te noemen: Ruben Tienhooven (BDO), Robert van Vianen (BDO), Helmer Berkhoff (BDO), Bart de Goeij (Privacy Management Partners), Désirée Galavazi (Kamer van Koophandel), Shirley Antonius (Gemeente Almere), Jo Stoffels (Gemeente Brunssum), Alex Davis (NVWA), Ad Kint (UWV/CIP), Marcel Koers (UWV/CIP) en Tady Slebioda (UWV/CIP).
Ruben Tienhooven (BDO) is de hoofdauteur van dit document. Aan de eindredactiefase heeft ook het CIP-redactieteam bijgedragen.

De deelnemers aan de Werkgroep Ketens en Verwerkersovereenkomsten (2017) zijn:

Shirley Antonius	Gemeente Almere
Remy van den Boom	IND
Roger Coenen	Gemeente Heerlen
Alex Davis	NVWA
Lex van Elshout	Thuisvester
Désirée Galavazi	Kamer van Koophandel
Bart de Goeij	Privacy Management Partners
Johannes Homan	Gemeente Amsterdam
Ad Kint	UWV/CIP
Evelien van Meerkerk	Gemeente Alkmaar
Ted Mos	Ministerie van Justitie DJI
Franziska Sigrist	Boven IJ Ziekenhuis
Tady Slebioda	CIP
Jo Stoffels	Gemeente Brunssum
Ruben Tienhooven	BDO
Robert van Vianen	BDO
Peter van der Zwan	Servicekantoor Ipse de Bruggen

Bij de versie 1.1

Het document is redactioneel gereviewed (tekst en lay-out) en hier en daar licht aangepast. De inhoud van versie 1.0 is nergens wezenlijk veranderd.

Inhoudsopgave

1. Inleiding

Nog maar weinig organisaties die opereren in de dienstverlening, de handel of de productie drijven hun zaak volledig zelfstandig, zonder externe afhankelijkheden. Globalisering, de vergaande modulering van bedrijfsprocessen vanwege de noodzakelijke specialisaties en het outsourcen daarvan zijn hierbij bepalende factoren. Beperking tot kerncompetenties en risicospreiding spelen eveneens mee.
Maar 'risico' en 'aansprakelijkheid' kun je onder de moderne wetgeving niet zomaar wegwerken door te outsourcen. Werken in ketens vereist daarom afspraken met alle ketenbetrokkenen. En als je verstandig bent dan maak je die afspraken waterdicht. De Europese privacywetgeving is bij uitstek zo'n 'moderne' wet. Zij gaat zelfs nog wat verder door expliciet ook privacybelangen van de 'burger/betrokkene' een zwaar gewicht toe te kennen en expliciet maatregelen ter bescherming ervan in de wet op te nemen én: het maken van ketenafspraken hierover verplicht te stellen.

1.1 Privacy in ketens

Per 25 mei 2018 geldt de Algemene Verordening Gegevensbescherming (AVG) en moeten organisaties de AVG hebben geïmplementeerd in hun organisatie en hun gegevensverwerkingen[1]. In de praktijk maken veel organisaties deel uit van een keten(s) met andere organisaties bij het leveren van bepaalde producten of diensten of bij het nastreven van een gezamenlijk maatschappelijk doel. Bij gegevensverwerkingen zijn meerdere interne afdelingen betrokken, maar daarnaast veelal ook externe partijen. Vooral wanneer bij de gegevensverwerking meerdere partijen betrokken zijn kunnen complexe ketens ontstaan, waarbij in iedere schakel aandacht voor het beschermen van de privacy aanwezig moet zijn. In ketens kan sprake zijn van complexe afhankelijkheden en wisselende relaties tussen de partijen. Het is van groot belang dat er voor dergelijke situaties duidelijke afspraken bestaan om incidenten te voorkomen en zo nodig op te lossen. Allereerst dienen de in de keten betrokken partijen in beeld te zijn. Vervolgens moet gekeken worden naar zowel de eigen wettelijke verantwoordelijkheden, als de verantwoordelijkheden die onderling verdeeld moeten worden. De AVG maakt onderscheid tussen partijen in de rol van *verwerkingsverantwoordelijke* en die van *verwerker*.

1.2 Hoe in de praktijk het borgen van privacy in ketens wordt ervaren

De AVG heeft veel regels over de bescherming van persoonsgegevens. In de verordening staan ook bepalingen die zien op verhoudingen tussen bepaalde organisaties. In de praktijk wordt echter ervaren dat de bepalingen geen concrete handvatten bieden, waardoor organisaties die met ketensamenwerkingen te maken krijgen een groot grijs gebied ervaren.

1.3 Dialoog als fundament van een keten

Het uitgangspunt bij een ketensamenwerking moet zijn dat er duidelijke informatiekanalen en aanspreekpunten zijn, zodat een dialoog gevoerd kan worden over de wijze van samenwerking en gegevensuitwisseling. Door een goede dialoog kan een sterke samenwerking in de keten ontstaan. Dit document staat uitgebreid stil bij de problemen die er kunnen zijn in ketens. Een veel voorkomende schakel binnen ketens is die tussen *verwerkingsverantwoordelijke en verwerker*. Het is in deze verhouding wettelijk verplicht om schriftelijke afspraken te maken over de verwerking van persoonsgegevens. In de praktijk wordt daar dikwijls invulling aan gegeven door het afsluiten van een verwerkersovereenkomst[2]. We zullen uitgebreid aandacht besteden aan de inhoud van zo'n verwerkersovereenkomst.

[1] De verordening is al van kracht per 25 mei 2016, maar kent een 'grace period' van twee jaar: overtredingen kunnen worden vastgesteld, maar leiden nog niet tot boetes.
[2] Overheidspartijen onderling sluiten juridisch gezien geen overeenkomsten; zij maken afspraken.

Ook waar sprake is van een relatie tussen *twee verwerkingsverantwoordelijken* moet, om aan de AVG-verplichtingen te voldoen, de verdeling van verantwoordelijkheden duidelijk zijn.

1.4 Handreiking

Deze handreiking biedt handvaten om tot ketenafspraken te komen. Hiertoe worden eerst de in de AVG gebruikte termen voor partijen in een keten (verwerkingsverantwoordelijke en verwerker) beschreven en vervolgens de relaties tussen deze partijen (hoofdstuk 2). Deze relaties vormen de verschillende typen van schakels die in een keten kunnen voorkomen. Op basis van deze typen van schakels wordt gekeken naar ketens, zoals die in de praktijk worden ervaren.
Om te komen tot afspraken om in een keten grip op privacy te krijgen stellen wij als best practice het nemen van 6 stappen voor. Deze 6 stappen worden beschreven in hoofdstuk 3. Om een succes te maken van deze stappen gelden 11 aandachtspunten (hoofdstuk 4).
Dit document is een handreiking in de vorm van een best practice, inclusief een Model bewerkersovereenkomst, en is bedoeld om de afspraken en daarmee de werking van de keten mogelijk te maken en te versterken. Wij hopen dat ons werk u inspireert en aanzet om de dialoog aan te gaan met organisaties in ketens, en actief met deze informatie aan de slag te gaan met het sterker maken van de keten en het waarborgen van de belangen van de betrokkenen.

1.5 Naslagliteratuur

Bij de totstandkoming van deze handreiking is gebruik gemaakt van de volgende bronnen:

- **De AVG**
  De (Nederlandse) tekst van de verordening is te vinden via de link: http://www.privacy-regulation.eu/nl
- **De Tekstuitgave Privacyverordening**
  Aangezien de wetsartikelen niet altijd voor zich spreken is bij het schrijven van dit document onder meer gebruik gemaakt van de "Tekstuitgave Privacyverordening" (niet vrijelijk beschikbaar): https://www.bju.nl/juridisch/catalogus/tekstuitgave-privacyverordening-1;
- **De Privacy Baseline van het CIP**
- In de "Privacy Baseline" is de AVG samengevat in 13 criteria onderverdeeld in een PDCA cyclus met Beleid, Uitvoeren en Controle; vrijelijk beschikbaar op de CIP-site: https://www.cip-overheid.nl/;
- **Factsheet verwerkersovereenkomsten gemeenten**
  Ook is gebruik gemaakt van de "Factsheet verwerkersovereenkomsten" van de Informatiebeveiligingsdienst (IBD); beschikbaar op https://www.ibdgemeenten.nl/wp-content/uploads/2017/03/20170314-factsheet-verwerkersovereenkomsten-v1.00-2.pdf;
- **Model verwerkersovereenkomst ARVODI en ARBIT**
  Algemene Rijksvoorwaarden voor het verstrekken van opdrachten tot het verrichten van diensten en Algemene Rijksvoorwaarden bij IT-overeenkomsten (resp. bijlage 2 en 3)
  https://www.pianoo.nl/document/9596/model-verwerkersovereenkomst-arvodi.
  https://www.pianoo.nl/document/12027/model-verwerkersovereenkomst-arbit.

2. Verschillende soorten ketens

Ketens ontstaan door afhankelijkheden tussen partijen. Om de verschillende soorten van ketens te kunnen benoemen is het van belang dat duidelijk is welke rollen de verschillende partijen hebben in het kader van de AVG.

2.1 Rollen in ketens

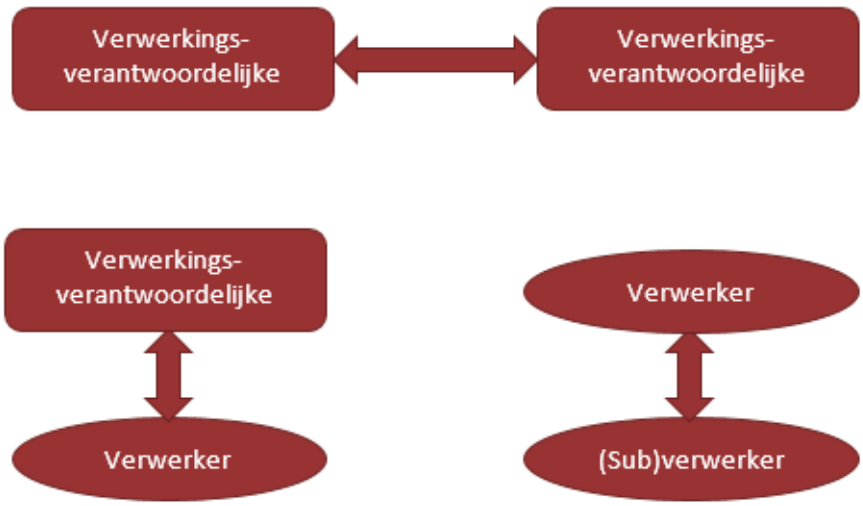
De AVG kent slechts 2 rollen: de verwerkingsverantwoordelijke en de verwerker. Om duidelijk te krijgen wat het verschil is tussen beiden volgen hier de volledige definities, zoals gehanteerd in de AVG:

- Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het wettelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.
- Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Dit betekent dat (in tegenstelling tot een verwerker) een verwerkingsverantwoordelijke, alleen of samen met anderen, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. Een verwerker kan en mag persoonsgegevens alleen verwerken namens een verwerkingsverantwoordelijke.

2.2 Schakels in ketens

Met de rol van verwerkingsverantwoordelijk en die van verwerker kunnen binnen een keten de volgende drie soorten schakels worden gevormd:



1. **De schakel tussen twee verwerkingsverantwoordelijken**:
   Omdat verwerkingsverantwoordelijken zelf, al dan niet in samenspraak met anderen in de keten, hun doel van en hun middelen voor de verwerking van persoonsgegevens vaststellen, is hier in feite sprake van een horizontale keten gebaseerd op gelijkwaardigheid. De afhankelijkheid blijft beperkt tot het kunnen realiseren van de eigen doelen en de gemeenschappelijke doelen. De inzet van de middelen bepalen zij zelf.

   NB: wanneer de inzet van middelen door een partij zelf bepaald wordt, dan is deze partij een verwerkingsverantwoordelijke en geen verwerker; óók wanneer de financiering ervan door een andere verwerkingsverantwoordelijke plaatsvindt.
2. **De schakel tussen verwerkingsverantwoordelijke en verwerker**:
   Wanneer een verwerker namens een verwerkingsverantwoordelijke de verwerking uitvoert en de middelen door de verwerkingsverantwoordelijke bepaald worden, dan spreken we van een verticale keten, waarin een hiërarchische relatie bestaat.
3. **De schakel tussen twee verwerkers**:
   Een partij die namens een andere verwerker werkzaamheden uitvoert doet kan dit op zijn beurt ook weer doen als verwerker. Deze verwerker duiden we in dit document aan als *subverwerker* om het onderscheid met een verwerker te kunnen aangeven. De AVG kent echter alleen de rol van verwerker en niet die van subverwerker.

2.3 Ketens zoals die in de praktijk worden ervaren

Ketens kunnen in diverse vormen bestaan. Niet alleen grote of kleine organisaties zitten met elkaar in een keten; de praktijk wijst uit dat organisaties van alle formaten met elkaar in een keten kunnen zitten. Hier zullen enkele voorbeelden van ketens behandeld worden.

2.3.1 Keten met één gezamenlijk doel en meerdere partijen met eigen verantwoordelijkheden

In een keten met één gezamenlijke doelstelling en meerdere partijen die elk een eigen taak hebben, kan de verdeling van wat onder de eigen verantwoordelijkheid gebeurt en wat onder een "gemeenschappelijke verantwoordelijkheid" valt vragen oproepen. Bij de overheid komt dit soort ketens regelmatig voor.

Binnen de overheid is vaak sprake van een maatschappelijk doel dat het beste door gezamenlijke inspanning gerealiseerd kan worden. Voorbeelden hiervan zijn:

- de samenwerking tussen gemeenten en zorginstellingen in het sociaal domein en
- de samenwerking rond het Veiligheids-huis, waarbij onder meer gemeenten, OM, zorgpartijen en Reclassering betrokken kunnen zijn.

De keten kan als volgt worden weergegeven:

De verdeling van verantwoordelijkheden kan eenvoudig worden bepaald aan de hand van de beantwoording van de vraag hoe de doelbinding is vastgesteld. Om persoonsgegevens in een keten te mogen verwerken is doelbinding vereist met een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel. Het gerechtvaardigde doel moet een rechtsgrond kennen die is vastgesteld bij het recht dat op de verwerkingsverantwoordelijke van toepassing is[3]. Voor iedere verwerkingsverantwoordelijke in de keten die de gegevens verwerkt moet dit recht vastgesteld zijn.
De rechten daarvoor kunnen op verschillende manieren tot stand komen:

1. Voor iedere ketenpartner geldt een eigen verwerkingsgrondslag die bij de (wettelijke) taakstelling van de betreffende organisatie hoort.
2. Binnen de gezamenlijke doelstelling zijn de verwerkingsgrondslagen van de betreffende organisaties wettelijk vastgelegd.
3. Een combinatie van beiden.

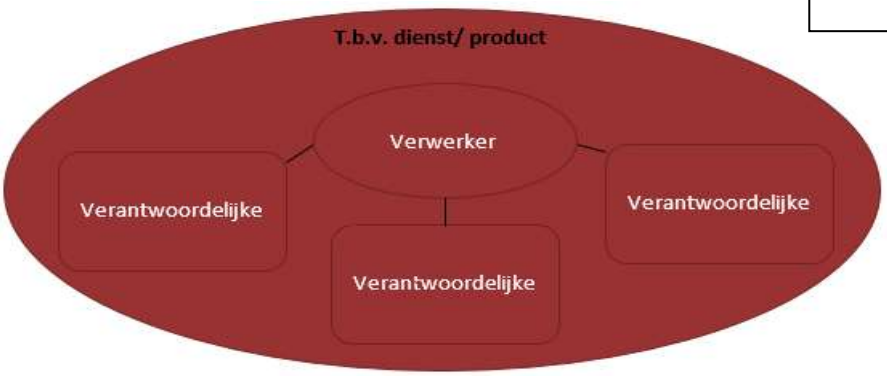
Als duidelijk is welke taken door de verschillende partijen uitgevoerd moeten worden, kunnen afspraken gemaakt worden over de samenwerking. Wanneer het recht niet is vastgesteld of zelfs ontbreekt bij een ketenpartij, dan is samenwerking op basis van de daarvoor benodigde persoonsgegevens niet toegestaan.

2.3.2 Keten met één gezamenlijk doel en partijen die geen eigen verantwoordelijkheid nemen

In een variant op bovengenoemd model kan het ook voorkomen dat er één of meerdere partijen hun eigen verantwoordelijkheid niet zien of willen nemen als onderdeel van een gezamenlijke doel-/taakstelling. Hierdoor voelen deze partijen zich slechts (deels) aansprakelijk voor overtredingen van de AVG die in de keten gemaakt worden. Dit maakt het maken van afspraken moeilijk. Om wel tot afspraken te komen is in hoofdstuk 3 een stappenplan beschreven.

2.3.3 Keten met een verwerker die autonomie claimt

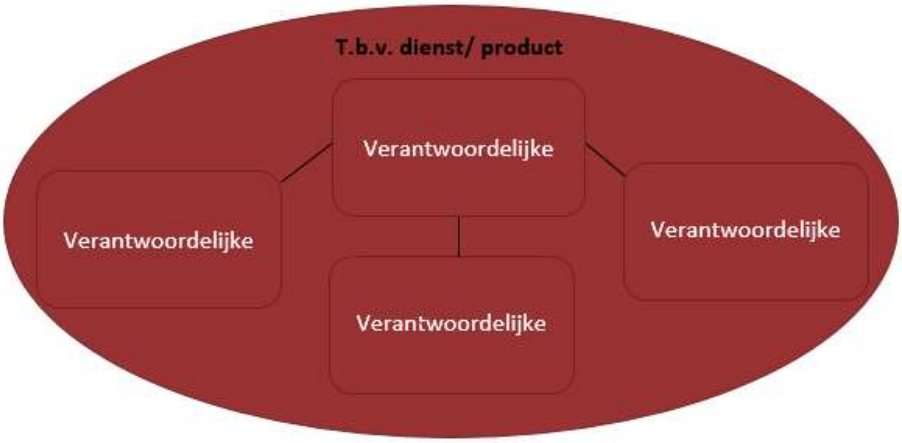
Extra complexiteit ontstaat wanneer een verwerker ten behoeve van meerdere verantwoordelijken werkzaamheden uitvoert, daarbij autonomie claimt en zich niet als verwerker ziet die zich moet committeren aan de eisen van de verwerkingsverantwoordelijken. In die situatie wordt het borgen van een door de verwerkingsverantwoordelijke vereist niveau van gegevensbescherming afhankelijk van de gehanteerde maatstaven van de verwerker. De keten kan als volgt worden weergegeven:



Een praktijkvoorbeeld: verschillende zelfstandige ziekenhuizen hebben voor het beheer en onderhoud van hun informatiesystemen dezelfde aanbieder gecontracteerd, waarbij de beheerder (in de rol van verwerker) een monopoliepositie inneemt en vervolgens weigert om in te stemmen met een door de ziekenhuizen (de verwerkingsverantwoordelijken!) voorgestelde verwerkersovereenkomst.

[3] AVG art. 6 lid 3 en Privacy Baseline criterium U.01

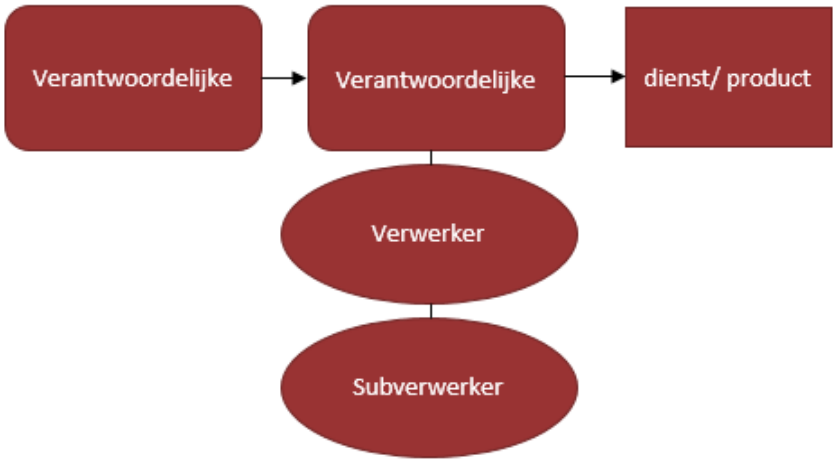
Een keten, waarin de verhoudingen liggen zoals hierboven geschetst, levert een onwenselijke situatie op, omdat de verwerkingsverantwoordelijke de verwerking die onder zijn verantwoordelijkheid plaatsvindt, niet meer kan verantwoorden. En dat is niet het enige gevolg.
Wanneer geen goede afspraken gemaakt kunnen worden met de partij die verwerker zou moeten zijn, dan kan deze partij niet als verwerker worden gezien, maar is hij door zijn opstelling een verwerkingsverantwoordelijke geworden die zelf beslist over de in te zetten middelen. Een weergave die aansluit op deze ketenverhoudingen is de volgende:



In deze situatie neemt het aantal wettelijke verplichtingen, dat op de partij rust die autonomie claimt, toe doordat hij niet gezien kan worden als verwerker. Op basis van de AVG sluit deze partij zich als ketenpartij buiten: hij heeft immers voor de verwerking geen wettelijke verwerkingsgrondslag.

2.3.4 Keten met meerdere verwerkingsverantwoordelijken, verwerkers en subverwerkers

In de praktijk komt het geregeld voor dat een keten niet beperkt blijft tot slechts enkele schakels, tot een enkele verwerkingsverantwoordelijke of een enkele verwerker. Een voorbeeld van zo'n keten is:



Deze keten bestaat uit meerdere verantwoordelijken die gegevens met elkaar uitwisselen, waarbij één of meer verwerkers en subverwerkers zijn ingeschakeld door een verwerkingsverantwoordelijke. Deze situatie kan bijvoorbeeld voorkomen bij een uitvoeringsorganisatie die onder bepaalde voorwaarden gegevens verstrekt aan gemeenten ten behoeve van het behandelen van een aanvraag in het kader van Wmo of Participatiewet. De gemeente maakt gebruik van een ICT-leverancier die vervolgens weer gegevens opslaat op een externe server van een cloudprovider. Hoe meer verantwoordelijken,

verwerkers en subverwerkers er op deze wijze aan elkaar verbonden zijn, hoe onoverzichtelijker het wordt voor - in dit geval - de uitvoeringsorganisatie. De ketenproblematiek komt hierbij vooral tot uiting in het feit dat een juiste omgang met de gegevens moeilijk te monitoren en te handhaven wordt voor de uitvoeringsorganisatie, die daardoor minder garanties kan afgeven aan betrokkenen over wie de gegevens verwerkt worden.

Een schematische weergave van de verhoudingen van de relaties in de keten (d.m.v. rollen en schakels), zoals bij de voorbeelden van ketens in dit hoofdstuk, kan helpen tot het komen tot ketenafspraken. Toetsing of een schematische weergave daadwerkelijk aansluit op de praktijk kan worden bepaald aan de hand van in het volgende hoofdstuk beschreven stappen.

Praktijkvoorbeeld: Een publiek-private samenwerking waarbij meerdere partijen betrokken zijn

JOGG

De afdeling Maatschappelijke ontwikkeling van een gemeente initieert het JOGG-programma (Jongeren Op Gezond Gewicht). Een gemeente heeft op grond van artikel 2 van de Wet publieke gezondheid een verplichting om een preventieprogramma's uit te voeren voor de het bevorderen van de gezondheid. Deze lokale verantwoordelijkheid om de gezondheid van jongeren te stimuleren wordt tezamen met onderwijsinstellingen uitgevoerd. In het JOGG-programma worden de motorische vaardigheden en gezondheid van jongeren gemonitord.

De gemeente stelt het budget voor onderwijs-instellingen ter beschikking om het JOGG-programma uit te voeren en ontvangt geanonimiseerde data van fittesten en interventies op school- of wijkniveau retour. Jongeren die deelnemen aan het programma worden gedurende een periode van 3 jaar gemonitord.

De deelname aan het JOGG-programma is niet verplicht, derhalve vragen de onderwijsinstelling toestemming aan ouders voor deelname van hun kind aan dit programma. De onderwijsinstelling levert de toestemmingverklaring van de ouders en de persoonsgegevens van deze kinderen aan een sportorganisatie die als verwerker de testen uitvoert. Deze sportorganisatie geeft een terugkoppeling aan de onderwijsinstelling over de testresultaten en adviseert een vervolgtraject om de gezondheid te verbeteren indien dit nodig is. Omdat de Sportorganisatie gebruik maakt van een leerlingvolgsysteem van een externe partij, zal de leverancier van het leerlingvolgsysteem als subverwerker onderdeel uitmaken van de verwerkersovereenkomst tussen gemeente en onderwijsinstelling als gezamenlijke verantwoordelijke en de sportorganisatie als verwerker.

3. De totstandkoming van ketenafspraken

Nu helder is wat voor soorten relaties in een ketens kunnen bestaan (hoofdstuk 2), is het belangrijk binnen een keten inzichtelijk te krijgen wat de rol van de partijen is en welke schakels zij vormen. Om hierover het gesprek te kunnen voeren moet duidelijk zijn wie van de eigen organisatie verantwoordelijk is en dus aanspreekpunt voor het aandeel binnen de keten, en wie dat zijn bij de andere ketenpartijen. Duidelijkheid over de betrokken rollen en de aanspreekpunten vormt het uitgangspunt om te komen tot ketenafspraken. Om ketenafspraken tot stand te brengen beschrijven we 6 stappen.

3.1 Een multidisciplinaire aanpak

In een keten kunnen zich veel privacyvraagstukken voordoen. Uit de voorbeelden in hoofdstuk 2 bleek al dat er verschillende (juridische) verhoudingen tussen ketenpartners mogelijk zijn. Hierdoor is het vaak onduidelijk hoe de privacy wet- en regelgeving toegepast moet worden. Doordat een keten vaak complex in elkaar zit, zijn er mensen nodig die de nodige inhoudelijke kennis hebben van de aard van de betreffende gegevensverwerking, van privacybescherming en van informatiebeveiliging. Tevens moeten zij kunnen laten zien hoe een situatie of product in elkaar zit en hoe het principe Privacy by Design wordt of kan worden toegepast. Kortom, het is wenselijk dat hiervoor een multidisciplinair team wordt ingezet. Er zijn veel verschillende rollen betrokken bij het tot stand komen van de afspraken, waardoor het belangrijk is dat de deelnemers kennis hebben van elkaars rollen en mogelijkheden, elkaar weten te vinden en de privacyvraagstukken begrijpen. Bij het samenstellen van het team kan gedacht worden aan de lijnverantwoordelijke disciplines (bij voorkeur mensen die eenzelfde traject eerder hebben doorlopen), (business-) architecten en houders van een projectportfolio (projectmanagement). Als er niemand in de organisatie is met dergelijke kennis dan kan ervoor worden gekozen om deze kennis op te doen of in te huren. Daarnaast moeten de Functionaris voor de Gegevensbescherming en de Information Security Officer, indien aanwezig, worden betrokken.

Als hulpmiddel om een afweging te kunnen maken over het juiste gebruik van gegevens is de WMK-toets ontwikkeld. Deze toets is in een factsheet "Willen-Mogen-Kunnen Toets" van de Rijksoverheid beschreven[4]. De toets helpt organisaties om in een korte tijd 'het goede gesprek' te voeren over een voorliggende gegevensvraag én tot een betere onderbouwing en vastlegging van de gemaakte afweging en een (voorgesteld) besluit te komen.

Stap 1:	*Kies een multidisciplinaire aanpak, zodat de verantwoordelijkheden en te bespreken aandachtspunten belegd kunnen worden en de kennis en kunde beschikbaar is.*

Nadat de juiste disciplines bij elkaar zijn gebracht is het van belang dat dat ieders verantwoordelijkheid en bevoegdheid helder is. Wij adviseren om dit in twee stappen te doen, te weten: het bepalen van de doeleinden en de rechtvaardigingsgronden en Het beleggen van de verantwoordelijkheden. De stappen 2 en 3 hierna gaan hierover.

3.2 Het bepalen van doeleinden en rechtvaardigingsgronden

Een verwerking van persoonsgegevens is alleen toegestaan wanneer bijbehorende doeleinden 'welbepaald, uitdrukkelijk omschreven en gerechtvaardigd' zijn (U.01 van de Privacy Baseline). Daarnaast moet het doeleinde ook rechtmatig zijn, oftewel het moet voldoen aan één van de 6 voorwaarden die de AVG daarvoor stelt.

[4] https://www.digitaleoverheid.nl/document/wmk-toets

Een verwerkingsketen heeft dus alleen bestaansrecht wanneer het doel is gebaseerd op de toestemming van de betrokkene, op een overeenkomst, op een wettelijke taak, op een vitaal belang (weinig voorkomend), een taak van algemeen belang of een gerechtvaardigd belang (alleen voor niet-overheidstaken), toegewezen aan de verwerkingsverantwoordelijken in de keten. Dit betekent dat het aangaan van een ketensamenwerking alleen mogelijk is als iedere partij hiervoor rechtvaardigingsgronden heeft conform U.01.

NB: in veel ketens wordt vaak gewerkt op basis van een grondslag of een uitzonderingsbepaling die beperkt is tot het primaire doel van één van de verwerkingsverantwoordelijken, terwijl er een gezamenlijk doel van de gegevensuitwisseling verondersteld wordt. Er is dan bijvoorbeeld geen wettelijke taak voor een van de organisaties om verwerkingsactiviteiten uit te voeren, terwijl die organisatie in praktijk wel een rol speelt in de samenwerking.

Stap 2: *Bepaal de legitimiteit van de keten door de juistheid te controleren van de doeleinden en de rechtvaardigingsgronden voor iedere partij binnen de keten.*

3.3 Het beleggen van de verantwoordelijkheden binnen de eigen organisaties

Per ketenpartij moet de eindverantwoordelijkheid worden vastgesteld en bij voorkeur ook worden vastgelegd. Dit kan bijvoorbeeld het hoogste 'dagelijkse bestuur' zijn van een organisatie, de hoogste functionaris van een gemeente of een gemandateerde.
Per (deel van de) verwerking moet duidelijk zijn wie aanspreekbaar is op die verwerking. Aangezien het hierbij om een interne rol gaat noemen we deze aansprakelijke een proceseigenaar, die werkt onder verantwoordelijkheid van de werkgever (dit zal meestal een verwerkingsverantwoordelijke zijn, hoewel een verwerker in theorie ook interne processen kan mandateren aan proceseigenaren). Een proces-eigenaar is degene die het proces binnen de eigen organisatie vormgeeft, beheert en de middelen beschikbaar stelt. Bedenk dat wanneer persoonsgegevens voor één of meer proceseigenaren worden beheerd door een externe partij zoals een cloudprovider, deze partij optreedt als verwerker. Doordat deze verwerker ook onderdeel gaat uitmaken van de keten wordt de keten groter.

Stap 3: *Beleg de verantwoordelijkheden binnen de eigen organisaties op basis van kennis en kunde (stap 2) en bevoegdheden, zodat de juiste kennis, kunde en bevoegdheden aanwezig is om afspraken te kunnen maken binnen de keten.*

3.4 Verwerkingsverantwoordelijken binnen de keten

De doorgifte van persoonsgegevens aan een andere verwerkingsverantwoordelijke in een keten is alleen toegestaan als de onderlinge verantwoordelijkheden duidelijk zijn (U.07 van de Privacy Baseline). Hiervoor is het van belang dat iedere verwerkingsverantwoordelijke zijn verantwoordelijkheid invult en vastlegt hoe die invulling plaatsvindt. De vastlegging is, hoewel een vereiste vanuit de AVG, daarbij geen doel op zich, maar vormt de basis voor een gezamenlijke aanpak van het *privacymanagement in de keten*.
Naast ieders verantwoordelijkheid als verwerkingsverantwoordelijke is er dus de verantwoordelijkheid van de keten. Bij de invulling daarvan moeten dus steeds alle partijen betrokken worden, om eenduidig als keten te kunnen functioneren.

Dit geldt ook voor ketens waarbij verwerkers een belangrijke rol spelen. Zij moeten niet slechts verantwoordelijkheden opgelegd krijgen, er moet ook een dialoog zijn waarin van beide kanten zaken kunnen worden geadresseerd en aandachtspunten voor een goede omgang met gegevens in het proces

kunnen worden aangedragen. De keten zal daardoor een meer horizontale verhouding krijgen, waarin gelijkwaardigheid het uitgangspunt is. Het is raadzaam om de keten uit te tekenen, zodat voor elk van de ketenpartners inzichtelijk wordt wat de samenstelling is van de keten, hoe de flow, overdracht en verwerking van gegevens precies verloopt, welke rollen en verantwoordelijkheden daarbij bestaan, en wat het belang van de betrokkenen is bij de inrichting van het ketenproces; het gaat immers om hun persoonsgegevens.
In de praktijk liggen de belangen van de partijen in een keten niet altijd op één lijn. Een nuttige maatregel is dan de aanstelling van een onafhankelijke 'ketenregisseur' die als spin in het web functioneert bij het maken van en wijzigen van afspraken in de keten.

Stap 4: *Leg de onderlinge verantwoordelijkheden van de verwerkingsverantwoordelijken binnen de keten vast (U.07 van de Privacy Baseline) en waarborg de alignment, zodat privacymanagement plaatsvindt, bijvoorbeeld door de inzet van een ketenregisseur.*

3.5 In dialoog samenwerken in een keten voor transparantie

Om op gestructureerde wijze te kunnen komen tot een gezamenlijke aanpak met inachtname van elkaars begrenzingen en belangen, is het belangrijk om een goede dialoog te houden in de keten, waarbij per organisatie een centraal privacy-aanspreekpunt bestaat. Dit bevordert de communicatie in de keten, zodat onduidelijkheden vermeden en opgelost kunnen worden. Daarbij moet ook stil worden gestaan bij de rolverdeling in de keten. Dit is niet alleen van belang voor de onderlinge verantwoordelijkheidsverdeling en aansprakelijkheden, maar ook voor de omgang met betrokkenen. Zij moeten eenvoudig te weten kunnen komen welke partij ze moeten benaderen voor hun vragen over de verwerking van hun gegevens en het uitoefenen van hun rechten[5]. Om de benodigde transparantie te bereiken moet de verantwoordelijkheidsverdeling openbaar zijn[6]. Daardoor kunnen de rechten van betrokkenen gewaarborgd worden en is het bovendien duidelijk voor de ketenpartners welke informatieplicht zij hebben.

Stap 5: *Waarborg de transparantie voor de betrokkenen door het neerzetten van een structuur, waarbij de betrokkenen altijd weten bij welke partij ze moeten zijn voor hun vragen en het uitoefenen van hun rechten. Doe dit door in de keten in dialoog hierover proactief het gesprek te voeren.*

3.6 Verwerkers binnen de keten

De doorgifte van persoonsgegevens aan een verwerker is alleen toegestaan als er afdoende garanties zijn (U.07 van de Privacy Baseline). Een nuttig hulpmiddel hierbij is een verwerkersovereenkomst (het vastleggen van verwerkersafspraken is overigens verplicht, dit mag echter ook onderdeel uitmaken van een andere overeenkomst[7]).

Om te komen tot een verwerkersovereenkomst geldt een aantal aandachtspunten. Als eerste is het van belang voor alle partijen duidelijk te krijgen wie precies een verwerkersovereenkomst mag aangaan:

[5] In U.07/01.01 van de Privacy Baseline staat dat hier vanuit de AVG (art. 26, lid 1) eisen aan worden gesteld.
[6] In U.07/01.01 van de Privacy Baseline staat dat hier vanuit de AVG (art. 26, lid 3) eisen aan worden gesteld.
[7] Overheidspartijen onderling sluiten juridisch gezien geen overeenkomsten; zij maken afspraken. Het hiervoor te hanteren protocol is echter bij het maken van dit document nog niet gepubliceerd.

- **Aan de kant van de verwerkingsverantwoordelijke**:
  De verwerkingsverantwoordelijke binnen een organisatie kan de afspraken zelf aangaan of kan deze bevoegdheid mandateren aan een lijnverantwoordelijke.

- **Aan de kant van de verwerker**:
  Bij inschakeling van een verwerker (dit is altijd een externe partij) worden afspraken gemaakt tussen de eindverantwoordelijken van de verwerkingsverantwoordelijke partij en van bedoelde externe partij. Voor niet-overheden kan in het KvK-register gecheckt worden wie eindverantwoordelijk is namens de organisaties.
  De aangewezen persoon die namens de eindverantwoordelijken van deze organisaties de afspraken voorbereidt, moet een zekere link te hebben met de keten en moet ook blijvend als aanspreekpunt kunnen fungeren, zodat er een doorlopende dialoog kan zijn.

Het maken van afspraken om te komen tot garanties is een wettelijk vereiste vanuit de AVG. Om de samenwerking in de schakel tussen verwerkingsverantwoordelijke en verwerker effectief en efficiënt te laten werken zijn meer additionele afspraken nodig. Zie hiervoor het volgende hoofdstuk.

Stap 6: *Maak afspraken over de verwerking van persoonsgegevens door een verwerker en leg de garanties vast (U.07 van de Privacy Baseline), bijvoorbeeld in de vorm van een verwerkersovereenkomst.*

Waarborg daarbij de samenwerking door te kijken of additionele afspraken nodig zijn (zie hoofdstuk 4).

- Zie voor een algemeen toepasbaar model: Bijlage 1
- Zie voor een model voor de rijksoverheid bij de aanbesteding van diensten (ARVODI): Bijlage 2
- Zie voor een model voor de rijksoverheid bij de aanbesteding van IT (ARBIT): Bijlage 3

4. Aandachtspunten bij een verwerkersovereenkomst

Wanneer een verwerker namens een verwerkingsverantwoordelijke persoonsgegevens verwerkt dan kunnen de in de AVG vereiste garanties[8] in een verwerkingsovereenkomst worden vastgelegd. Om de garanties in de praktijk te laten werken is het van belang antwoord te krijgen op een aantal vragen. Deze vragen worden in dit hoofdstuk gesteld en kunnen zo helpen om in control te komen. Hoewel een deel van deze vragen ook dienen om de onderlinge verantwoordelijkheden[9] bij doorgifte van persoonsgegevens aan een andere verwerkingsverantwoordelijke duidelijk te krijgen, zijn deze vragen gericht op de garanties die nodig zijn tussen een verwerkingsverantwoordelijke en een verwerker.

4.1 Wat zijn de duur, aard en het doel van de overeenkomst?

Bij de duur, de aard en het doel van de overeenkomst is het van belang om stil te staan bij wat precies de relatie is tussen de partijen en of er sprake is van een eenzijdige verantwoordelijkheid of een gezamenlijke verantwoordelijkheid. Hierbij geldt wel dat alleen de verwerkingsverantwoordelijke verantwoordelijk is voor het bepalen van het verwerkingsdoeleinde[10]. Wanneer deze zaken niet helder zijn voor de verwerkingsverantwoordelijke, is het nuttig te overleggen met de verwerker.
Om te komen tot een overeenkomst heeft de verwerkingsverantwoordelijke de lead: hij moet komen met uitgangspunten. Omdat uitgangspunten contextafhankelijk kunnen zijn, kan een overeenkomst verschillen van de in Bijlage 1 gegeven Model Bewerkersovereenkomst. De dialoog staat hier centraal om te komen tot de duur, aard en het doel van de overeenkomst.

4.2 Welke definities worden gehanteerd?

Gehanteerde definities moeten eenduidig zijn, zodat iedere partij in de keten dezelfde taal spreekt. De eenduidigheid kan verkregen worden door middel van dialoog. Daarbij kun je de wettelijke definities in artikel 4 van de AVG gebruiken, zoals hierboven beschreven in paragraaf 2.1. De in de Model Verwerkersovereenkomst gebruikte definities staan in artikel 1 van de Model Verwerkersovereenkomst.

4.3 Welke persoonsgegevens worden doorgegeven?

In een verwerkersovereenkomst is het verplicht om de verwerking van gegevens nader te duiden. Slechts verwijzen naar het feit dat er persoonsgegevens worden verwerkt of uitgewisseld geeft onvoldoende houvast om te kunnen sturen op de te nemen maatregelen ter bescherming van de persoonsgegevens. Daarom onderscheidt de AVG 'gewone persoonsgegevens'[11], zoals NAW-gegevens, mailadres en IBAN-nummer, en 'bijzondere categorieën van persoonsgegevens'[12], zoals gezondheidsgegevens en gegevens over etniciteit.
In een verwerkersovereenkomst is een opdracht van een verantwoordelijke aan een verwerker aan de orde. In de overeenkomst staat welke verwerkingen het betreft. Er moet afstemming zijn tussen de verwerkingsverantwoordelijke en de verwerker over de voorwaarden en afspraken in de verwerkersovereenkomst, maar over de gegevens of de verwerking zelf hoeft geen 'onderhandeling' te zijn, omdat de verantwoordelijke daarover zelfstandig een keuze moet kunnen maken en kunnen beslissen. Het vastleggen van een eventuele verdeling van taken/werkzaamheden is vooral aan de orde als er een *gezamenlijke* verwerkingsverantwoordelijkheid is.

[8] Zie U.07/02 van de Privacy Baseline
[9] Zie U.07/01 van de Privacy Baseline
[10] Zie U.01/02 van de Privacy Baseline
[11] Art. 5 t/m 8 van de AVG
[12] Art. 9 van de AVG

4.4 De verantwoordelijkheden van de verwerkingsverantwoordelijke en de verwerker

De verwerkingsverantwoordelijke staat ervoor in dat de verwerking van de persoonsgegevens in overeenstemming is met de AVG. De Privacy Baseline geeft in de vorm van 13 criteria duidelijkheid wat hiervoor gedaan moet worden. Geredeneerd vanuit de AVG verwerkt een - eventuele - verwerker persoonsgegevens slechts in opdracht van verwerkingsverantwoordelijke. De verwerker verwerkt gegevens dan ook overeenkomstig de instructies van verwerkingsverantwoordelijke en onder diens verantwoordelijkheid. Een verwerkersovereenkomst legt de afspraken daarover vast. Eventuele prestatienormen kunnen zijn vastgelegd in een onderliggende Service Level overeenkomst (SLA). Zoals in eerder is beschreven, geldt daarbij het uitgangspunt dat de verwerker geen zeggenschap heeft over het doel en de middelen voor de verwerking van persoonsgegevens en geen beslissingen neemt over het gebruik van de persoonsgegevens en de verstrekking aan derden. Tevens zal de verwerker persoonsgegevens die hem in het kader van een verwerkersovereenkomst ter beschikking zijn gesteld niet langer bewaren dan noodzakelijk is:

i. voor de uitvoering van de Overeenkomst, of:
ii. om een op hem rustende wettelijke verplichting na te komen.

In een bijlage van de Verwerkersovereenkomst kan gespecificeerd worden hoe lang Persoonsgegevens worden bewaard. De verwerker dient in lijn met de AVG zorg te dragen voor de naleving van de overeenkomst.
Wanneer de verwerker een organisatie(onderdeel) is, verschaft hij alleen toegang tot de persoonsgegevens aan zijn werknemers voor zover die nodig is voor het verrichten van de diensten op grond van de verwerkingsovereenkomst. De verwerker moet een logging bijhouden van de verwerking (bijv. raadplegen van) van bijzondere categorieën van persoonsgegevens, zodat gecontroleerd kan worden wie op welk moment inzage had. Op die manier kan snel gefilterd worden wie in systemen te ruim gebruik heeft gemaakt van toegangsrechten. De logging bevat gegevens over de werknemer en het tijdstip van inzage.

4.5 Hoe vindt beëindiging van de verwerkersovereenkomst plaats?

De persoonsgegevens die worden verwerkt moeten vernietigd/geretourneerd worden aan het einde van de overeenkomst. Er moet daarom een verantwoorde beëindigingsstrategie zijn die duidelijk maakt wanneer is beëindiging/ontbinding mogelijk is en op welke wijze dat gebeurt. Hierbij moet rekening gehouden worden met de wettelijke verplichtingen vanuit de Archiefwet, het kunnen nakomen van de verplichtingen van de verwerkingsverantwoordelijke, bijvoorbeeld m.b.t. de beschikbaarheid van de gegevens) en het vernietigen van (fysieke) backups.
Het kan soms moeilijk zijn om het vernietigen gegevens te garanderen. Denk bijvoorbeeld aan e-mails, die na het 'vernietigen' ervan in beginsel nog op een mailserver staan opgeslagen. Hiervoor moet een oplossing worden gevonden, waarbij overigens ook naar kosten/baten en dus naar het passend zijn van de maatregel kan (mag) worden gekeken[13], zie hiervoor ook de volgende paragraaf. Van belang is dat de wijze van vernietiging duidelijk is voor de verwerkingsverantwoordelijke. Het is een goed idee om een terugkoppeling te bedingen bij de verwerker over de wijze waarop hij de gegevens vernietigt. Het is belangrijk dat in de scope van een dergelijke audit ook de fysieke gegevensdragers worden meegenomen. Let erop dat dit een additionele afspraak is naast de wettelijke verplichting om de mogelijkheid tot het uitvoeren van audits

> Advies: als een audit het gevraagde inzicht moet bieden, dan is het raadzaam tevens vooraf overeen te komen wie de kosten van de audit draagt.

[13] U.04/02 van de Privacy Baseline of art. 32 van de AVG.

op beveiligingsmaatregelen op te nemen in een verwerkersovereenkomst. Verder kan aansluiting gezocht worden bij reguliere exitstrategieën voor overeenkomsten met een leverancier[14].

4.6 Welke beveiligingsmaatregelen moeten genomen worden?

De verwerker zal passende maatregelen moeten nemen om de te verwerken persoonsgegevens te beveiligen en beveiligd te houden tegen indringers en tegen van buiten komend onheil, alsmede onzorgvuldig, ondeskundig of ongeoorloofd gebruik. Afhankelijk van de aard van de verwerking zou onder meer kunnen worden gedacht aan maatregelen omtrent het beheer van bevoegdheden en autorisaties van de medewerkers ter voorkoming van onbevoegde kennisname, maatregelen ter voorkoming van virussen, bedreigingen c.q. technische kwetsbaarheden en logging. Partijen zullen elkaar op verzoek van de andere Partij periodiek (nader in te vullen op welke termijn) informeren in hoeverre de tussen Partijen overeengekomen beveiligings- en continuïteitsplannen worden uitgevoerd. Indien nodig worden deze plannen geactualiseerd.
De door of vanwege verwerker aan verwerkingsverantwoordelijke verstrekte toegangs- of identificatiecodes en certificaten zijn vertrouwelijk en zullen door verwerkingsverantwoordelijke als zodanig worden behandeld en slechts aan geautoriseerde medewerkers uit de eigen organisatie van verwerkingsverantwoordelijke kenbaar worden gemaakt. Verwerker is gerechtigd toegewezen toegangs- of identificatiecodes en certificaten te wijzigen. De verwerker rapporteert regelmatig aan de verwerkingsverantwoordelijke over de maatregelen die zijn genomen ter beveiliging van de persoonsgegevens. Een verwerker moet meewerken aan een audit van de verwerkingsverantwoordelijke[15].

Het borgen van de beveiligingsmaatregelen door het summier verwijzen naar artikel 33 AVG, waarin staat dat technische en organisatorische maatregelen genomen moeten worden, is onvoldoende. Je moet aangeven tegen welke risico's beschermd moet worden en welke aanvullende (wettelijke) eisen gelden voor de verwerkingsverantwoordelijke en daarmee voor de verwerker. Pas dan kan bepaald worden of een maatregel passend is[16]. Een keuze van een framework, zoals BIR, BIG, BIC, ISO27001 en NEN7510 om het passend zijn van de maatregelen te bepalen is hiervoor nuttig. Welk framework of welke frameworks daarbij door de partijen mogen of moeten worden gehanteerd, is onderdeel van de tussen de partijen te maken afspraken. Uiteindelijk moeten deze gespecificeerd op papier komen, zodat beide partijen weten waar ze aan toe zijn. Bij de vastlegging zou als uitgangspunt gehanteerd moeten worden: "dit en dat zijn de beveiligingsmaatregelen, en deze zijn passend bij de verwerking van deze persoonsgegevens, omdat…''. Deze vastlegging moet als onderdeel in de verwerkersovereenkomst worden opgenomen.

Bedenk steeds wat er fout kan gaan als er geen afspraken zijn gemaakt over een passende mate van beveiliging, bijvoorbeeld:

- Onrechtmatige toegang tot gegevens; verlies van vertrouwelijkheid;
- Verlies van bedrijfsdata en data van betrokkenen door datalekken of diefstal van data of programma's;
- Negatieve publiciteit in de media (imagoschade);
- Klachten van betrokkenen;
- Aansprakelijkheid voor schade en schadeloosstelling van betrokkenen in verband met lekken, verlies gegevens;

[14] Als het een SAAS-provider betreft dan wil je bijvoorbeeld niet dat alle data ineens weg is bij beëindiging van een overeenkomst. Denk aan een afspraak die garandeert dat bestanden in een open format (ook elders) worden veiliggesteld.
[15] U.08/02/02 van de Privacy Baseline of art. 28 lid 3 AVG
[16] U.04/02 van de Privacy Baseline of art. 32 van de AVG.

- Verwerkingsverantwoordelijke kan de schuld van een wanprestatie van een verwerker (mogelijk) niet verhalen op die verwerker;
- Niet bereikbaar zijn van het systeem c.q. dienstverlening (discontinuïteit/onbeschikbaarheid);
- Reconstructiekosten voor herstel bestanden, programma's en systemen;
- Onderzoek van de AP; boetes.

4.7 Wat moet er geregeld worden omtrent de Meldplicht Datalekken?

De Meldplicht Datalekken wordt beschreven in criterium C.03 van de Privacy Baseline[17]. Aanvullend daarop hebben het CIP en de Autoriteit Persoonsgegevens goede handleidingen opgesteld hoe een organisatie zich moet voorbereiden op datalekken. Daarin staat in principe alles wat nodig is om een goede procedure in te richten voor het afhandelen van datalekken.
Aandachtspunten om te komen tot een goede afhandeling van datalekken zijn:

- Leg vast wie meldt en wanneer. In de wet staat dat een 'redelijke' termijn moet worden gehandhaafd; in artikel 33 lid 1 AVG staat dat uiterlijk 72 uur na het ontdekken van het datalek moet worden gemeld door de verwerkingsverantwoordelijke in de keten.
- Spreek af wie in de organisatie een melding doet. Veelal zal dit de Functionaris voor de Gegevensbescherming (FG) zijn. Als deze niet is aangesteld binnen de organisatie, dan moet er een ander centraal aanspreekpunt te zijn. Denk aan de Corporate Information Security Officer (CISO), Privacy Officier (PO) of Compliance Officer (CO). Contactgegevens van de personen, belast met het doen van de datalekmeldingen aan de Autoriteit Persoonsgegevens, moeten voor de partijen (in de keten) duidelijk te zijn. Bij plaatsvervanging moet daarover helder gecommuniceerd te worden.
- Consequenties voor het niet nakomen van de afspraken omtrent meldplicht datalekken moeten helder zijn voor de partijen (in de keten). Een voorbeeld is het aansprakelijk stellen van de verwerker voor het overschrijden van de termijn of het niet melden van een datalek. (Sub)verwerker moet zich zo snel mogelijk bij het centrale aanspreekpunt melden van de verwerkingsverantwoordelijke, zodat deze tijdig aan zijn meldingsplicht aan de Autoriteit Persoonsgegevens kan voldoen. Boetes van de toezichthouder die het gevolg zijn van het feit dat verwerker de verwerkingsverantwoordelijke niet tijdig op de hoogte heeft gesteld van het datalek, zouden hierdoor op de verwerker verhaald kunnen worden.
- Ook als het nog niet duidelijk is of er daadwerkelijk sprake is van een datalek, is het verstandig om de Autoriteit Persoonsgegevens op de hoogte te stellen. Dit kan door het doen van een voorlopige melding, die later eventueel ook weer ingetrokken kan worden.

4.8 Hoe moeten de rechten van de betrokkenen gewaarborgd worden?

De AVG bepaalt in artikel 28, lid 1 dat uitsluitend verwerkers mogen worden ingeschakeld die "afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden, opdat de verwerking aan de vereisten van deze verordening voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd". Welke deze garanties dit zijn staan beschreven in U.07/02 van de Privacy Baseline.
Over de afhandeling van verzoeken van betrokkenen moeten daarom dus afspraken gemaakt worden: hoe wordt hiermee omgegaan? binnen welke termijn? wat te doen met herhaaldelijke verzoeken? Over deze laatste onderwerpen komt in de Uitvoeringswet van de AVG nog het een en ander te staan. Onder de AVG is de antwoordtermijn in beginsel één maand. Bij complexe verwerkingen mogen hier (indien nodig) twee maanden extra voor worden genomen. Het is verstandig om bij herhaaldelijke verzoeken een termijn van zes maanden aan te houden. Ook geeft artikel 12 hier duidelijk aan wat wel en niet mag. Het recht om vergeten te worden gaat niet op als er een wettelijke bewaringsverplichting bestaat of als de verwerking van persoonsgegevens noodzakelijk is voor de uitvoering van een overeenkomst.

[17] Leidend voor C.03 van de Privacy Baseline zijn art 33 en art 44 van de AVG

In principe moet de verwerkingsverantwoordelijke precies weten welke verwerkingen onder zijn verantwoordelijkheid plaatsvinden. Als er sprake is van een verwerker dan moet deze de verwerkings-verantwoordelijke assisteren bij het vervullen van de plicht van de verantwoordelijke om verzoeken van betrokkenen te behandelen.

4.9 Wat moet opgenomen worden over aansprakelijkheid en geheimhouding?

Het uitgangspunt van de AVG is dat zowel de verwerkingsverantwoordelijke als de verwerker aansprakelijk kunnen zijn voor de onzorgvuldige verwerking van de persoonsgegevens; zo ook voor eventuele boetes van de Autoriteit Persoonsgegevens dientengevolge. In artikel 83 lid 4 AVG en artikel 82 AVG staat een zelfstandige aansprakelijkheid voor de verwerker opgenomen. Wellicht kan in de keten afgesproken worden hoe de aansprakelijkheid van de verantwoordelijke verdeeld of afgewenteld kan worden in bepaalde gevallen, bijvoorbeeld bij datalekken of liegen over beveiligingsmaatregelen. In een keten is het belangrijk dat er een zogenaamde 'hoofdelijke aansprakelijkheid' bestaat. Hierdoor kunnen organisaties en/of betrokkenen zich wenden tot iedere organisatie in de keten. Via een zogenaamde "regres-constructie" kan de schade dan verdeeld worden in de keten.
Geheimhouding staat als vereiste in de AVG opgenomen. Het overtreden daarvan is ook strafbaar. Hier is van belang dat de duur van de geheimhouding duidelijk wordt bedongen. Het is in eerste instantie een voor de hand liggende keuze om dit tot de duur van de overeenkomst te beperken. Ook is het mogelijk om deze geheimhouding nog enkele jaren door te laten lopen, of zelfs tot in de eeuwigheid. De gedachte hierachter is dat in een keten gevoelige informatie kan uitlekken, bijvoorbeeld over beveiligingsmaatregelen of over de omgang met persoonsgegevens. Dit zou tot onderzoeken van de Autoriteit Persoonsgegevens kunnen leiden of tot imagoschade. Op grond van bovenstaande zou een boetebeding opgenomen kunnen worden. De constructie daarvan zou gelijk kunnen zijn wat gebruikelijk is in het civiele recht, een vaste som geld, of een bepaald bedrag per dag dat de overtreding voortduurt.

4.10 Waar bevinden de gegevens zich?

Het uitgangspunt van de wet is dat de verwerking van persoonsgegevens in beginsel binnen de EER moet blijven (de Europese Economische Ruimte = EU + Noorwegen, Liechtenstein en Zwitserland). Toch zijn er bepalingen opgenomen die het mogelijk maken om van dit uitgangspunt af te wijken. Vanwege verschillen tussen wettelijke regimes is het van het grootste belang dat inzichtelijk is waar c.q. onder welk regime de persoonsgegevens worden verwerkt. De uitzondering op die regel is als er een adequaatheidsbesluit van de Europese Commissie is[18] of wanneer er passende waarborgen worden geboden. Welke waarborgen afdoende zijn wordt bepaald door de Europese Commissie, de Nationale (de Nederlandse) AP en certificering[19]. Welke landen dit betreft staat opgenomen in een lijst die op de website van de Autoriteit Persoonsgegevens valt te raadplegen. Voor meer informatie kan ook worden gekeken naar de besluiten van de Europese Commissie[20]. De modelovereenkomst van de EU zou gebruikt kunnen worden voor verwerkingen buiten de EER zonder passende waarborgen.[21]

4.11 Hoe weet ik of de afspraken in de keten worden nageleefd?

In de wet staat opgenomen dat moet worden voorzien in de mogelijkheid om audits uit te laten voeren. Wie hiervan de kosten draagt kan onderling geregeld worden. In de praktijk blijkt dat vaak het recht wordt voorgehouden om dit maximaal eenmaal per jaar uit te laten voeren, of vaker indien daar goede

[18] U.07/05 van de privacy Baseline of art. 45 van de AVG
[19] U.07/06 van de privacy Baseline of art. 46 van de AVG
[20] http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm
[21] Het Europees Hof van Justitie heeft in juli 2020 het Privacy Shield verdrag uit 2016 nietig verklaard (https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091nl.pdf); handelsorganisaties moeten vooralsnog vervangende overeenkomsten sluiten.

redenen voor zijn. Wat onder deze goede redenen valt moet overeengekomen worden in de keten. In de wet staat verder dat in bepaalde situaties een Gegevensbeschermingseffectbeoordeling (GEB, ook wel: DPIA) moet worden uitgevoerd. Het is goed om in de keten hierover afspraken te maken. Te denken valt aan inzichtelijk maken wat de resultaten van een GEB zijn. Er moeten in ieder geval concrete afspraken zijn over de wijze van de samenwerking in de keten en periodieke rapportage over naleving van de ketenafspraken.

Bijlage 1: Model verwerkersovereenkomst

Deze verwerkersovereenkomst is van algemene aard en kan in diverse ketens worden ingezet. De inhoud moet 'organisatie-eigen' gemaakt worden, bekijk goed wat voor uw organisatie wel/niet van toepassing is.

VERWERKERSOVEREENKOMST behorende bij <<overeenkomst/order inzake …>>

Partijen

<<Bedrijfsnaam>>, <<Adres>> <<Postcode, Vestigingsplaats>>, ingeschreven bij de Kamer van Koophandel onder nummer <<…>>, te dezen vertegenwoordigd door <<…>>, in de hoedanigheid van <<functie>>, hierna te noemen: "Verwerkingsverwerkingsverantwoordelijke";

en

<<Bedrijfsnaam>> <<Adres>> <<Postcode, Vestigingsplaats>> ingeschreven bij de Kamer van Koophandel onder nummer <<nummer KvK>>, hierbij vertegenwoordigd door <<naam tekenbevoegde>>, in de hoedanigheid van <<functie>>, hierna te noemen: "Verwerker";

Verwerkingsverantwoordelijke en Verwerker hierna gezamenlijk ook aan te duiden als "**Partijen";**

IN AANMERKING NEMENDE:

- dat Verwerkingsverantwoordelijke beschikt over persoonsgegevens van diverse Betrokkenen;
- dat Verwerkingsverantwoordelijke bepaalde vormen van Verwerking wil laten verrichten door Verwerker;
- dat Verwerker hiertoe bereid is en tevens bereid is verplichtingen omtrent beveiliging en andere aspecten van de Wetgeving op zich te nemen;
- Partijen, mede gelet op de vereisten uit artikel 28 van de Algemene Verordening Gegevensbescherming, hun rechten en plichten schriftelijk in deze Verwerkersovereenkomst wensen vast te leggen.

KOMEN HET VOLGENDE OVEREEN:

Artikel 1 Definitiebepalingen
De in deze Verwerkersovereenkomst gebruikte en met een hoofdletter geschreven woorden of formuleringen hebben de volgende betekenis:

- **Betrokkene**: een geïdentificeerde of identificeerbare natuurlijke persoon;
- **Onderliggende Overeenkomst**: de overeenkomst d.d. [DATUM] waarbij Verwerkingsverantwoordelijke aan Verwerker opdracht heeft gegeven om Verwerkingen te verrichten;
- Verwerkersovereenkomst: deze overeenkomst;
- **FG**: Functionaris Gegevensbescherming als bedoeld in de artikelen 37-39 van de Algemene Verordening Gegevensbescherming;
- **Persoonsgegevens**: elk gegeven betreffende een of meerdere Betrokkenen die Verwerker op grond van de Onderliggende Overeenkomst verwerkt of dient te verwerken;
- **Bijzondere categorieën van persoonsgegevens**: Persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, het lidmaatschap van een vakvereniging, alsmede strafrechtelijke gegevens en

persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag;
- **Subverwerker**: een natuurlijke of rechtspersoon die de Verwerking van Persoonsgegevens ten behoeve van de Onderliggende Overeenkomst in opdracht van Verwerker uitvoert;
- **Verwerken/Verwerking**: de verwerking als bedoeld in artikel 4, aanhef en onder 2 van de AVG;
- **Wetgeving**: de Algemene Verordening Gegevensbescherming (AVG) en de daarop gebaseerde Nederlandse Uitvoeringswet Algemene Verordening Gegevensbescherming;

Artikel 2 Onderwerp van de overeenkomst
2.1 Deze Verwerkersovereenkomst wordt door Partijen aangegaan in verband met de uitvoering van de Onderliggende Overeenkomst. De algemene voorwaarden die in de Onderliggende Overeenkomst van toepassing zijn verklaard, zijn evenzeer van toepassing op deze Verwerkersovereenkomst. Door ondertekening van deze Verwerkersovereenkomst bevestigt Verwerker reeds een exemplaar van de algemene voorwaarden te hebben ontvangen. De bepalingen van deze Verwerkersovereenkomst zijn van toepassing op iedere Verwerking door Verwerker op grond van de Onderliggende Overeenkomst.
2.2 Verwerker verbindt zich door ondertekening van deze Verwerkersovereenkomst om in opdracht van Verwerkingsverantwoordelijke Persoonsgegevens te verwerken in overeenstemming met de in deze Verwerkersovereenkomst gestelde voorwaarden. Het doel van de Verwerking is om <<invullen doel van de verwerking en beschrijven soort gegevens en doelgroep; wat wil de Verwerkingsverantwoordelijke bereiken met de verwerking van wat voor soort persoonsgegevens voor welke doelgroep?>>. De verwerking die Verwerker in opdracht van Verwerkingsverantwoordelijke gaat uitvoeren is de volgende: [Omschrijving verwerking]. Daarbij worden de volgende Persoonsgegevens verwerkt: [opsomming betrokken Persoonsgegevens]. De Persoonsgegevens hebben betrekking op de volgende categorieën van Betrokkenen: [opsomming categorieën Betrokkenen].
2.3 Verwerker zal de Persoonsgegevens alleen Verwerken voor de in artikel 2.2 van deze Verwerkersovereenkomst genoemde doeleinden. Verwerker zal de Persoonsgegevens niet voor enig ander doel Verwerken.
2.4 De Persoonsgegevens blijven eigendom van Verwerkingsverantwoordelijke. Zij behoudt daarover steeds de volledige zeggenschap.

Artikel 3 Verplichtingen Verwerker
3.1 Verwerker verwerkt de Persoonsgegevens slechts op basis van de schriftelijke instructies van de Verwerkingsverantwoordelijke. Verwerker verplicht zich om die instructies steeds omgaand en nauwgezet op te volgen. Verwerker zal zich bij gebrek aan instructies daartoe van Verwerkingsverantwoordelijke onthouden van het doorgeven van Persoonsgegevens aan derde landen of internationale organisaties, tenzij een op de Verwerker van toepassing zijnde Unierechtelijke of Nederlandse wettelijke bepaling hem tot verwerking verplicht. In laatstbedoeld geval stelt de Verwerker de Verwerkingsverantwoordelijke, voorafgaand aan de verwerking, in kennis van die wettelijke bepaling, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.
3.2 Verwerker verplicht zich om de Persoonsgegevens ontoegankelijk te maken voor die personen binnen haar organisatie die voor de uitvoering van hun werkzaamheden niet noodzakelijkerwijs toegang tot de Persoonsgegevens behoeven te hebben. Verwerker waarborgt dat de wel tot het verwerken van Persoonsgegevens gemachtigde personen zich ertoe hebben verbonden om vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden.
3.3 Verwerker waarborgt dat passende technische en organisatorische maatregelen worden getroffen om een passend beveiligingsniveau te waarborgen die – onder meer – het volgende bevatten:
(a) de pseudonimisering en versleuteling van de Persoonsgegevens;
(b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
(c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de Persoonsgegevens tijdig te herstellen;

(d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de Verwerking. De exacte maatregelen die Verwerkingsverantwoordelijke tenminste van Verwerker verwacht en waartoe Verwerker zich door ondertekening van deze Overeenkomst verplicht zijn beschreven in bijlage x.
3.4 Verwerker verplicht zich om steeds op het eerste verzoek van Verwerkingsverantwoordelijke bijstand te verlenen aan Verwerkingsverantwoordelijke bij het vervullen van diens plicht om verzoeken tot uitoefening van rechten van betrokkenen te beantwoorden en om verplichtingen uit hoofde van artikel 32 tot en met 36 van de AVG na te komen.
3.5 Tevens zal Verwerker Persoonsgegevens die haar in het kader van deze Verwerkingsovereenkomst ter beschikking zijn gesteld niet langer bewaren dan noodzakelijk is (i) voor de uitvoering van deze Overeenkomst; of (ii) om een op hem rustende wettelijke verplichting na te komen. In Bijlage A staat per (onderdeel van de) Dienst gespecificeerd hoe lang Persoonsgegevens worden bewaard. Verwerker verplicht zich om de Persoonsgegevens na het verstrijken van de in Bijlage A genoemde termijnen te verwijderen c.q. te vernietigen, althans om deze onder verwijdering van kopieën voor het overige op een door Verwerkingsverantwoordelijke aangewezen gegevensdrager aan Verwerkingsverantwoordelijke te overhandigen.
3.6 De Verwerker heeft [wel / geen] Functionaris Gegevensbescherming. De Verwerker wordt door Verwerkingsverantwoordelijke geacht [wel / geen] Functionaris Gegevensbescherming aan te stellen.
3.7 Verwerker houdt een logboek bij van de inzage van Bijzondere categorieën van persoonsgegevens. In dit logboek registreert Verwerker welke persoon of personen (van welke instantie(s)) toegang hebben gehad tot de Persoonsgegevens, op welke (wettelijke) grond toegang is verschaft, op welke momenten er toegang is geweest, tot welke gegevens men toegang heeft gehad, welke gegevens zijn bekeken en of er van die gegevens ook kopieën zijn gemaakt. Verwerker draagt er zorg voor dat dit logboek op elk moment en zoveel als Verwerkingsverantwoordelijke er om vraagt aan laatstgenoemde inzichtelijk kan worden gemaakt.
3.8 De Verwerker stelt aan de Verwerkingsverantwoordelijke alle informatie ter beschikking die nodig is om de nakoming van de in deze Verwerkersovereenkomst opgenomen verplichtingen aan te tonen en zal audits, waaronder inspecties, door de Verwerkingsverantwoordelijke of een door de Verwerkingsverantwoordelijke gemachtigde controleur mogelijk maken en daaraan bijdragen.

Artikel 4 Inzet Subverwerkers
4.1 Verwerker is zonder uitdrukkelijke, voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke niet gerechtigd de uitvoering van de Verwerkersovereenkomst geheel of ten dele uit te besteden aan Subverwerkers. Verwerker blijft, ook indien de uitvoering van de Verwerkersovereenkomst wel geheel of ten dele wordt uitbesteed aan Subverwerkers, voor Verwerkingsverantwoordelijke te allen tijde eerste en enig aanspreekpunt en verantwoordelijk voor de naleving van de bepalingen uit deze Verwerkersovereenkomst.
4.2 Verwerker zal hoe dan ook aan Subverwerkers dezelfde of soortgelijke verplichtingen opleggen als voor zichzelf uit deze Verwerkersovereenkomst voortvloeien en toezien op de naleving daarvan door Subverwerker.

Artikel 5 Doorgifte van Persoonsgegevens

5.1 Verwerker zal de Persoonsgegevens niet buiten Nederland verwerken of doen verwerken zonder voorafgaande schriftelijke toestemming van de Verwerkingsverantwoordelijke. Ook indien Verwerkingsverantwoordelijke Verwerking van Persoonsgegevens buiten Nederland toestaat, zullen Verwerkingsverantwoordelijke en Verwerker handelen in overeenstemming met hoofdstuk V van de AVG inzake doorgiften van persoonsgegevens. Dat betekent dat Persoonsgegevens alleen zullen worden doorgegeven aan derde landen of internationale organisaties indien de Europese 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 waarborgt. Is een dergelijk besluit niet van toepassing is voor de voorgenomen doorgifte, mag de doorgifte van de Persoonsgegevens indien sprake is van passende waarborgen in de zin van artikel 46 AVG of sprake is van toepasselijke en geldige bindende bedrijfsvoorschriften in de zin van artikel 47 AVG.
5.2 Verwerker zal geen Persoonsgegevens aan derden verstrekken of ter beschikking stellen, tenzij op grond van een uitdrukkelijke schriftelijk verzoek van Verwerkingsverantwoordelijke of op een bevoegd gegeven bevel van een gerechtelijke of bestuurlijke instantie, op voorwaarde dat Verwerker in dat geval Verwerkingsverantwoordelijke binnen 24 uur na ontvangst van een dergelijk bevel daarvan in kennis stelt om Verwerkingsverantwoordelijke zodoende in staat te stellen daartegen een haar ter beschikking staand rechtsmiddel in te stellen.
5.3 Indien Verwerker van oordeel is dat zij op grond van een wettelijke verplichting Persoonsgegevens ter beschikking dient te stellen aan een daartoe bevoegde instantie zal zij daar niet toe overgaan, dan na overleg met en instemming van Verwerkingsverantwoordelijke. Zij zal Verwerkingsverantwoordelijke zo spoedig mogelijk schriftelijk in kennis stellen van de wettelijke verplichting en daarbij alle relevante informatie verstrekken die Verwerkingsverantwoordelijke redelijkerwijs nodig heeft om de benodigde maatregelen te treffen om te bepalen of verstrekking kan plaatsvinden en, zo ja, onder welke voorwaarden. Daarnaast zal Verwerker: a) alles in het werk stellen om de verstrekking te beperken tot hetgeen wettelijk verplicht is; b) Verwerkingsverantwoordelijke in staat stellen om de rechten van Verwerkingsverantwoordelijke en Betrokkenen uit te oefenen en de belangen van Verwerkings-verantwoordelijke en Betrokkenen te verdedigen.

Artikel 6 Datalek

6.1 Verwerker dient Verwerkingsverantwoordelijke onverwijld en niet later dan 24 uur nadat Verwerker er kennis van heeft gekregen, in kennis te stellen van iedere inbreuk op de beveiliging van Persoonsgegevens met de mogelijke vernietiging, verlies, wijziging of ongeoorloofde verstrekking van of ongeoorloofde toegang tot Persoonsgegevens tot gevolg en Verwerkingsverantwoordelijke alle noodzakelijke informatie en medewerking te verlenen om de Verwerkingsverantwoordelijke in staat te stellen zo spoedig mogelijk de oorzaak en de omvang hiervan vast te stellen. Verwerker meldt dit aan een door Verwerkingsverantwoordelijke aan te wijzen persoon of personen. Hiervan wordt een afschrift verzonden naar de FG van Verwerkingsverantwoordelijke.
6.2 Deze meldplicht houdt in het melden door Verwerker bij Verwerkingsverantwoordelijke van het feit dat er een inbreuk is geweest, alsmede (i) wat de (vermeende) oorzaak is van de inbreuk, (ii) wat het (vooralsnog bekende en/of te verwachten) gevolg is van de inbreuk en (iii) wat de voorgestelde oplossing is. Melding dient plaats te vinden ook als nog geen antwoord gegeven kan worden op de vragen onder i, ii en/of iii.
6.3 Wanneer zich een inbreuk voordoet bij Verwerkingsverantwoordelijke, meldt Verwerkingsverantwoordelijke de inbreuk onverwijld aan een door Verwerker aan te wijzen persoon of personen onder opgave van de aard van de inbreuk, de geconstateerde en vermoedelijke gevolgen van de inbreuk voor de Verwerking van Persoonsgegevens zoals bedoeld in deze Verwerkersovereenkomst en de maatregelen die zijn getroffen om de gevolgen te verhelpen of te beperken. Tevens stelt Verwerkingsverantwoordelijke aan Verwerker maatregelen voor die Verwerker kan treffen om deze gevolgen te verhelpen of te matigen.
6.4 Tevens maken Partijen afspraken over de nadere invulling van de naleving van de Wetgeving meer in het bijzonder van de naleving van de Meldplicht Datalekken-. Deze betreffen in ieder geval de nadere

invulling van de meldplicht zelf, afspraken en afstemming over de uitvoering van onderzoeken naar oorzaken van incidenten, alsook afspraken over de wijze van detecteren van beveiligingsincidenten.

Artikel 7 Verzoeken van Betrokkenen

7.1 Verwerker dient Verwerkingsverantwoordelijke in kennis te stellen van alle verzoeken met betrekking tot inzage in de Persoonsgegevens die rechtstreeks van een Betrokkene zijn ontvangen. Verwerker geeft aan een dergelijk verzoek uitsluitend gevolg indien Verwerkingsverantwoordelijke Verwerker daartoe schriftelijk toestemming heeft gegeven. Deze inzage wordt alleen via Verwerkingsverantwoordelijke verschaft.
7.2 Verwerker handelt alle verzoeken om inlichtingen van Verwerkingsverantwoordelijke met betrekking tot de verwerking van de Persoonsgegevens onverwijld af.

Artikel 8 Opsporingsverzoek

8.1 Indien Verwerker een verzoek of een bevel van een Nederlandse of buitenlandse toezichthouder, overheidsinstantie of een opsporings-, strafvorderings- of nationale veiligheidsinstantie ontvangt om (inzage in) Persoonsgegevens te verschaffen, dan zal Verwerker de Verwerkingsverantwoordelijke onverwijld informeren. Bij de behandeling van het verzoek of bevel zal Verwerker alle instructies van Verwerkingsverantwoordelijke in acht nemen (waaronder de instructie om de behandeling van het verzoek of bevel geheel of gedeeltelijk aan Verwerkingsverantwoordelijke over te laten) en alle redelijkerwijs benodigde medewerking verlenen.
8.2 Indien het Verwerker op grond van het verzoek of bevel is verboden om te voldoen aan zijn verplichtingen op grond van het bovenstaande, dan zal Verwerker de redelijke belangen van Verwerkingsverantwoordelijke behartigen. Verwerker zal daartoe in ieder geval:

a. Juridisch laten toetsen in hoeverre (i) Verwerker wettelijk verplicht is om aan het verzoek of bevel te voldoen; en (ii) het Verwerker daadwerkelijk is verboden om aan haar verplichtingen jegens Verwerkingsverantwoordelijke op grond van het bovenstaande te voldoen;
b. Alleen aan het verzoek of bevel meewerken indien zij hiertoe wettelijk verplicht is en waar mogelijk (in rechte) bezwaar maken tegen het verzoek of bevel of het verbod om Verantwoordelijk hierover te informeren of haar instructies op te volgen;
c. Niet meer of andere Persoonsgegevens verstrekken dan strikt noodzakelijk om aan het verzoek of bevel te voldoen;
d. Indien sprake is van doorgifte naar een land buiten de EER zal Verwerker steeds zoveel mogelijk de voorschriften van artikel 44 tot en met 50 AVG opvolgen;
e. Verwerkingsverantwoordelijke onverwijld informeren zodra dit is toegestaan.

Artikel 9 Beveiliging

9.1 Verwerkingsverantwoordelijke en Verwerker zullen de Verwerking van Persoonsgegevens beveiligen overeenkomstig de voorschriften gesteld bij of krachtens de Wetgeving.
9.2 Verwerkingsverantwoordelijke en Verwerker zullen daarbij zorg dragen dat het beveiligingsbeleid en de uitvoering van het beveiligingsbeleid tenminste voldoen aan het criterium van een "passend beveiligingsniveau" als bepaald in artikel 32 van de AVG. Dit passend beveiligingsniveau is momenteel als volgt ingericht: <<invullen soort technische & organisatorische beveiligingsmaatregelen door Verwerkingsverantwoordelijke en Verwerker>>. / verwijzen naar een **bijlage** waarin dat is geregeld.
9.3 Verwerkingsverantwoordelijke en Verwerker zullen zich maximaal inspannen om de te verwerken Persoonsgegevens te beveiligen en beveiligd te houden tegen indringers en tegen van buiten komend onheil alsmede tegen onzorgvuldig, ondeskundig of ongeoorloofd gebruik.
9.4 Partijen zullen elkaar op verzoek van de andere Partij periodiek informeren op welke wijze de tussen Partijen overeengekomen beveiligings- en continuïteitsplannen worden uitgevoerd. Indien nodig worden deze plannen geactualiseerd.
9.5 De door of vanwege Verwerker aan Verwerkingsverantwoordelijke verstrekte toegangs- of identificatiecodes en certificaten zijn vertrouwelijk en zullen door Verwerkingsverantwoordelijke als zodanig worden behandeld en slechts aan geautoriseerde Medewerkers uit de eigen organisatie van

Verwerkingsverantwoordelijke kenbaar worden gemaakt. Verwerker is gerechtigd toegewezen toegangs- of identificatiecodes en certificaten te wijzigen.

Artikel 10 Geheimhouding en vertrouwelijkheid

10.1 Verwerker verplicht zich tot geheimhouding van alle Persoonsgegevens die Verwerker van Verwerkingsverantwoordelijke ontvangt en/of zelf verzamelt in het kader van deze Verwerkersovereenkomst. Verwerker zal deze Persoonsgegevens niet aan derden ter beschikking stellen, tenzij met uitdrukkelijke voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke, indien het verstrekken van de Persoonsgegevens noodzakelijk is ter uitvoering van deze overeenkomst of de Onderliggende Overeenkomst, of indien Verwerker op grond van de wet verplicht is om Persoonsgegevens aan derden te verstrekken. Deze geheimhoudingsverplichting is bestemd om voort te duren ook nadat deze Overeenkomst zal zijn geëindigd. Verwerker zal deze informatie niet voor een ander doel gebruiken dan waarvoor zij deze heeft verkregen, zelfs niet wanneer deze in een zodanige vorm is gebracht zodat deze niet tot betrokkenen herleidbaar is.

10.2 Onder derden in de zin van deze bepaling wordt ook begrepen de medewerkers en/of opdrachtnemers van Verwerker voor zover het niet noodzakelijk is dat zij bij de Opdracht en/of deze overeenkomst kennis hoeven te nemen van de Persoonsgegevens. Dit verbod geldt niet indien in deze overeenkomst anders is bepaald en/of voor zover een wettelijk voorschrift of een in kracht van gewijsde gegane gerechtelijke uitspraak Verwerker tot enige bekendmaking verplicht.

10.3 Verwerker zorgt dat zijn personeel en opdrachtnemers gebonden zijn aan de in dit artikel opgenomen geheimhoudingsplicht en dat Verwerker van die gebondenheid schriftelijk bewijs bezit. Op eerste verzoek van Verwerkingsverantwoordelijke verstrekt Verwerker Verwerkingsverantwoordelijke dat bewijs.

10.4 Bij schending door Verwerker van de in dit artikel beschreven geheimhoudingsverplichting verbeurt Verwerker aan Verwerkingsverantwoordelijke een direct, zonder ingebrekestelling opeisbare contractuele boete van € 5.000, te vermeerderen met € 1.000 per dag dat de overtreding voortduurt, onverminderd het recht van Verwerkingsverantwoordelijke op aanvullende schadevergoeding indien en voor zover de door Verwerkingsverantwoordelijke geleden schade het bedrag van de boete overschrijdt.

Artikel 11 Aansprakelijkheid

11.1 Verwerker is aansprakelijk voor alle schade die Verwerkingsverantwoordelijke lijdt die voortvloeit uit of verband houdt met tekortkomingen in de nakoming van de op Verwerker rustende verplichtingen uit hoofde van deze Verwerkersovereenkomst en/of de Wetgeving.

11.2 Verwerker vrijwaart Verwerkingsverantwoordelijke tegen aanspraken van derden, waaronder Betrokkenen en toezichthouders, in verband met het toerekenbaar tekortschieten van Verwerker in de nakoming van de Verwerkersovereenkomst of overtreding door Verwerker van de Wetgeving en zal alle daarmee verband houdende en daaruit voortvloeiende kosten (waaronder mede begrepen kosten van juridische bijstand) en zal schade op eerste verzoek aan Verwerkingsverantwoordelijke vergoeden.

Artikel 12 Duur en beëindiging

12.1 Deze Verwerkersovereenkomst wordt aangegaan voor onbepaalde tijd, althans voor de duur van de Onderliggende Overeenkomst.

12.2 Tenzij anders overeengekomen zal Verwerker in geval van beëindiging van de onderliggende Overeenkomst onverwijld alle aan haar ter beschikking gestelde en door haar bij uitvoering van deze overeenkomst verzamelde Persoonsgegevens aan Verwerkingsverantwoordelijke retourneren en alle digitale kopieën van Persoonsgegevens vernietigen en aan Verwerkingsverantwoordelijke bevestigen dat zij dit heeft uitgevoerd. Daarnaast zal de Verwerker het bijgehouden logboek aan Verwerkingsverantwoordelijke ter beschikking stellen.

12.3 Verwerker zal zich na het einde van de Verwerkersovereenkomst onthouden van elk verder gebruik van de Persoonsgegevens.

Artikel 13 Overdracht rechten en plichten
13.1 De rechten en verplichtingen uit deze Verwerkersovereenkomst kunnen door Verwerker niet aan een andere partij worden overgedragen zonder de voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke.

Artikel 14 Intellectuele eigendomsrechten
14.1 Alle (aanspraken op) intellectuele eigendomsrechten - waaronder auteursrechten, databankrechten en alle overige rechten van intellectuele - op de verzameling van Persoonsgegevens, kopieën of bewerkingen daarvan, berusten te allen tijde bij en/of komen toe aan Verwerkingsverantwoordelijke. Verwerker erkent de (aanspraken op) intellectuele eigendomsrechten van Verwerkingsverantwoordelijke en verbindt zich ertoe het bestaan daarvan niet te betwisten. Indien en voor zover overdracht van enig intellectueel eigendomsrecht ten aanzien van de Persoonsgegevens noodzakelijk is om deze rechten bij Verwerkingsverantwoordelijke te laten belanden, dan verplicht Verwerker zich door ondertekening van deze Verwerkingsovereenkomst tot medewerking aan elke noodzakelijke handeling om die overdracht te bewerkstelligen.
14.2 Alle intellectuele eigendomsrechten - waaronder auteursrechten, databankrechten en alle overige rechten van intellectuele eigendom - op de producten en dienstverlening van Verwerker, berusten te allen tijde bij Verwerker. Verwerkingsverantwoordelijke erkent de intellectuele eigendomsrechten van Verwerker en verbindt zich ertoe het bestaan daarvan niet te betwisten.

Artikel 15 Deelbaarheid
15.1 Indien één of meer bepalingen van deze Verwerkersovereenkomst niet rechtsgeldig blijken te zijn, zal de Verwerkersovereenkomst voor het overige van kracht blijven. Partijen zullen over de bepalingen die niet rechtsgeldig zijn overleg plegen, teneinde een vervangende regeling te treffen die wel rechtsgeldig is en zoveel mogelijk aansluit bij de strekking van de te vervangen regeling.

Artikel 16 Toepasselijk recht en geschillen
16.1 Uitsluitend Nederlands recht is van toepassing op deze Verwerkersovereenkomst.
16.2 Eventuele geschillen in verband met deze Verwerkersovereenkomst zullen uitsluitend worden behandeld door de bevoegde rechtbank in de plaats van vestiging van Verwerkingsverantwoordelijke.
16.3 Deze Verwerkersovereenkomst kan slechts worden gewijzigd door middel van een schriftelijk stuk waarin uitdrukkelijk staat vermeld dat het stuk bedoelt een dergelijke wijziging aan te brengen en dat door ter zake bevoegde vertegenwoordigers van Partijen is ondertekend.

In tweevoud getekend op…… te……

<<Bedrijfsnaam>> <invullen gegevens andere partij>

<<Invullen gegevens ondertekenaar>>
<<Functie>>

Bijlage A verwerkersovereenkomst BDO: Register van verwerkingsactiviteiten

Let op het verschil in verplichting tussen het register van een verwerker en die van een verantwoordelijke (zie ook art. 30 AVG). Een deel van de vereiste informatie in het register is gelijk, er is echter een minder gedetailleerde registerplicht:

Voor een verantwoordelijke geldt de verplichting om de volgende informatie vast te leggen:
- de verwerkingsdoeleinden;
- een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;

Voor dit onderdeel geldt voor de verwerker de plicht om slechts de volgende informatie vast te leggen:
- de categorieën van verwerkingen die voor rekening van iedere verwerkingsverantwoordelijke zijn uitgevoerd.

Hierna volgen twee voorbeelden opgenomen van een register van verwerkingsactiviteiten.

<u>Voorbeeld - Register van verwerkingsactiviteiten</u>

Verwerkingsverantwoordelijke:

Naam en contactgegevens FG:

Naam verwerking	Doel verwerking	Betrokkenen	Welke Persoons-gegevens	Ontvanger(s)	Bewaar-termijn	Beveilings-maatregelen	Doorgifte buiten EU ja/nee land/organisa-tie
Facturatie	Facturatie/ Administra-tie	Abonnees; Afnemers producten	NAW, e-mailadres, Bankrek.nr	Debiteuren-administratie (intern); Cloudhosting provider	Wettelijke verjarings-termijn (7 jaar)	NEN 7510/ ISO 27001; Beveiligings-beleid; verwerkers-ovk	nee
CRM	Service-verlening aan klanten	Klanten	NAW emailadres tel.nr.	Afdeling verkoop (intern)	2 jaar	Beveiligings-beleid	nee

Een variatie op het vorige register:

Naam verwerking	Facturatie			
Doel verwerking	Facturatie/Administratie			
Betrokkenen	Abonnees	Afnemers producten		
Persoonsgegevens	NAW, e-mailadres, bankrekeningnr.	NAW, bankrekeningnr.		
Ontvanger(s)	Debiteurenadministratie, Cloudhosting provider			
Bewaartermijn	5 jaar	3 jaar		
Beveiligingsmaatregelen	ISO 27001, Verwerkersovereenkomst, *Privacy Shield[22]			
Doorgifte buiten EU ja/nee	ja			
Welk land/organisatie	VS/Microsoft			
Naam verwerking	CRM			
Doel verwerking	Serviceverlening aan klanten			
Betrokkenen	Klanten			

[22] *Van de redactie*: Het Europees Hof van Justitie heeft in juli 2020 het Privacy Shield verdrag uit 2016 nietig verklaard (https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091nl.pdf); handelsorganisaties moeten vooralsnog vervangende overeenkomsten sluiten.

Bijlage 2: Model verwerkersovereenkomst ARVODI

Bron: https://www.pianoo.nl/document/9596/model-verwerkersovereenkomst-arvodi

De Algemene Rijksvoorwaarden voor het verstrekken van opdrachten tot het verrichten van diensten (ARVODI 2017/17) zijn vastgesteld voor eenduidigheid van voorwaarden voor het Rijk. Het model Verwerkersoveenkomst ARVODI (met addendum meldplicht datalekken) is bedoeld voor publieke organisaties die onder het Rijk vallen. Het model is ook beschikbaar in het Engels.

Instructie:

- **Voor zover teksten '<*OPTIONEEL*>' zijn is dat aangegeven in de tekst**.
- **Bij teksten waar 'OF' tussen de bepalingen in staat, dient een keuze tussen de verschillende opties gemaakt te worden. De overige optie(s) verwijderen uit de overeenkomst**.
- **Deze Verwerkersovereenkomst kan alleen in combinatie met een Dienstverleningsovereenkomst worden gesloten**.

N.B. Bij gebruik van de overeenkomst, deze instructie verwijderen.

Inhoud:

Verwerkersovereenkomst ARVODI-2016
Contractnummer: […].

De ondergetekenden:

1. De Staat der Nederlanden, waarvan de zetel is gevestigd te Den Haag,
te dezen vertegenwoordigd door de Minister/Staatssecretaris van/voor [naam portefeuille],
namens deze,
[functienaam en naam ondertekenaar]
hierna te noemen: Opdrachtgever,

en

2. [volledige naam en rechtsvorm contractant],
(statutair) gevestigd te [plaats],
te dezen vertegenwoordigd door
..... *(en .....)* [naam ondertekenaar]
hierna te noemen: Opdrachtnemer,

hierna gezamenlijk te noemen: Partijen;

OVERWEGENDE DAT:

- voor zover Opdrachtnemer Persoonsgegevens Verwerkt ten behoeve van Opdrachtgever in het kader van de Overeenkomst, Opdrachtgever krachtens artikel 4, onderdeel 7 en onderdeel 8, van de Verordening kwalificeert als verwerkingsverantwoordelijke voor de Verwerking van Persoonsgegevens en Opdrachtnemer als verwerker;
- Partijen in deze Verwerkersovereenkomst, zoals bedoeld in artikel 28, derde lid, van de Verordening, hun afspraken over de Verwerking van Persoonsgegevens door Opdrachtnemer wensen vast te leggen.

KOMEN OVEREEN:

Artikel 1. Begrippen
In deze Verwerkersovereenkomst wordt een aantal begrippen met een beginhoofdletter gebruikt. Aan deze begrippen komt de betekenis toe die hieraan wordt gegeven in artikel 1 van de Algemene Rijksvoorwaarden voor het verstrekken van opdrachten tot het verrichten van Diensten 2016 (ARVODI-2016). In afwijking daarvan of in aanvulling daarop wordt onder de volgende begrippen in deze Verwerkersovereenkomst verstaan:

1.1 Betrokkene: degene op wie een Persoonsgegeven betrekking heeft.

1.2 Inbreuk in verband met Persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

1.3 Overeenkomst: de overeenkomst tussen Opdrachtgever en Opdrachtnemer [titel] van [datum], met kenmerk [kenmerk].

1.4 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, die Opdrachtnemer in het kader van de Overeenkomst ten behoeve van Opdrachtgever verwerkt.

1.5 Verordening: 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 de Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

1.6 Verwerkersovereenkomst: deze overeenkomst inclusief overwegingen en bijbehorende bijlagen.

1.7 Verwerking: een bewerking of een geheel van bewerkingen in het kader van de Overeenkomst met betrekking tot Persoonsgegevens, of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen.

Artikel 2. Voorwerp van deze Verwerkersovereenkomst

2.1 Deze Verwerkersovereenkomst regelt de Verwerking van Persoonsgegevens door Opdrachtnemer in het kader van de Overeenkomst.

2.2 De aard en het doel van de Verwerking, het soort Persoonsgegevens en de categorieën van Persoonsgegevens, Betrokkenen en ontvangers zijn in Bijlage 1 omschreven.

2.3 Opdrachtnemer garandeert de toepassing van passende technische en organisatorische maatregelen, opdat de Verwerking aan de vereisten van de Verordening voldoet en de bescherming van de rechten van de Betrokkene is gewaarborgd.

2.4 Opdrachtnemer garandeert te voldoen aan de vereisten van de toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

Artikel 3. Inwerkingtreding en duur

3.1 Deze Verwerkersovereenkomst treedt in werking op het moment waarop deze door Partijen is ondertekend.

3.2 Deze Verwerkersovereenkomst eindigt nadat en voor zover Opdrachtnemer alle Persoonsgegevens overeenkomstig artikel 10 heeft gewist of terugbezorgd.

3.3 Geen van Partijen kan deze Verwerkersovereenkomst tussentijds opzeggen.

Artikel 4. Omvang verwerkingsbevoegdheid Opdrachtnemer

4.1 Opdrachtnemer Verwerkt de Persoonsgegevens uitsluitend in opdracht en op basis van schriftelijke instructies van Opdrachtgever behoudens afwijkende wettelijke voorschriften die op Opdrachtnemer van toepassing zijn.

4.2 Indien een instructie als bedoeld in het eerste lid naar het oordeel van Opdrachtnemer in strijd is met een wettelijk voorschrift inzake gegevensbescherming, stelt hij Opdrachtgever daarvan voorafgaand aan de Verwerking in kennis, tenzij een wettelijk voorschrift deze kennisgeving verbiedt.

4.3 Indien Opdrachtnemer op grond van een wettelijk voorschrift Persoonsgegevens dient te verstrekken, informeert hij Opdrachtgever onmiddellijk, en zo mogelijk voorafgaand aan de verstrekking.

4.4 Opdrachtnemer heeft geen zeggenschap over het doel van en de middelen voor de Verwerking van Persoonsgegevens.

Artikel 5. Beveiliging van de Verwerking

5.1 In aanvulling op artikel 15 van de ARVODI-2016 en onverminderd artikel 2.3 treft Opdrachtnemer de technische en organisatorische beveiligingsmaatregelen zoals beschreven in Bijlage 2.

5.2 Partijen erkennen dat het waarborgen van een passend beveiligingsniveau voortdurend kan dwingen tot het treffen van aanvullende beveiligingsmaatregelen. Opdrachtnemer waarborgt een op het risico afgestemd beveiligingsniveau.

5.3 Indien en voor zover Opdrachtgever daarom uitdrukkelijk schriftelijk verzoekt, zal Opdrachtnemer aanvullende maatregelen treffen met het oog op de beveiliging van de Persoonsgegevens.

5.4 Opdrachtnemer Verwerkt Persoonsgegevens niet buiten de Europese Unie, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming heeft verkregen van Opdrachtgever en behoudens afwijkende wettelijke verplichtingen.

5.5 Opdrachtnemer informeert Opdrachtgever zonder onredelijke vertraging zodra hij kennis heeft genomen van onrechtmatige Verwerkingen van Persoonsgegevens of inbreuken op beveiligingsmaatregelen zoals genoemd in het eerste en tweede lid.

5.6 Opdrachtnemer verleent Opdrachtgever bijstand bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36 van de Verordening.

Artikel 6. Geheimhouding door Personeel van Opdrachtnemer

6.1 De Persoonsgegevens hebben een vertrouwelijk karakter als bedoeld in artikel 13.1 van de ARVODI-2016.

6.2 Opdrachtnemer toont op verzoek van Opdrachtgever aan dat zijn Personeel zich ertoe heeft verbonden vertrouwelijkheid in acht te nemen als bedoeld in artikel 13.2 van de ARVODI-2016.

Artikel 7. Subverwerker

Wanneer Opdrachtnemer, met inachtneming van het bepaalde in artikel 8 van de ARVODI-2016, een andere verwerker inschakelt om ten behoeve van Opdrachtgever verwerkingsactiviteiten te verrichten, worden aan deze andere verwerker bij een overeenkomst dezelfde verplichtingen inzake gegevensbescherming opgelegd als die welke in deze Verwerkersovereenkomst zijn opgenomen.

Artikel 8. Bijstand vanwege rechten van Betrokkene

Opdrachtnemer verleent Opdrachtgever bijstand bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III van de Verordening vastgelegde rechten van de Betrokkene te beantwoorden.

Artikel 9. Inbreuk in verband met Persoonsgegevens

9.1 Opdrachtnemer informeert Opdrachtgever zonder onredelijke vertraging, zodra hij kennis heeft genomen van een Inbreuk in verband met Persoonsgegevens, overeenkomstig de afspraken zoals vastgelegd in Bijlage 3.

9.2 Opdrachtnemer informeert Opdrachtgever ook na een melding op grond van het eerste lid over ontwikkelingen betreffende de Inbreuk in verband met Persoonsgegevens.

9.3 Partijen dragen elk de door henzelf in verband met de melding aan de bevoegde toezichthoudende autoriteit en Betrokkene te maken kosten.

Artikel 10. Terugbezorgen of wissen Persoonsgegevens

10.1 Na afloop van de Overeenkomst draagt Opdrachtnemer, naar gelang de keuze van Opdrachtgever, zorg voor het terugbezorgen aan Opdrachtgever of het wissen van alle Persoonsgegevens. Opdrachtnemer verwijdert kopieën, behoudens afwijkende wettelijke voorschriften.

10.2 ***<OPTIONEEL>***Opdrachtnemer [wist of retourneert] de Persoonsgegevens binnen [aantal] [dagen/weken] na afloop van de Overeenkomst, bij gebreke waarvan Opdrachtnemer een boete verschuldigd is van €[bedrag] per dag, met een maximum van €[bedrag].

10.3 ***<OPTIONEEL>*** Persoonsgegevens worden in de door Opdrachtgever aangegeven vorm en op de door Opdrachtgever aangegeven wijze terugbezorgd.

OF

10.3 ***<OPTIONEEL>*** De Persoonsgegevens worden als volgt terugbezorgd: [bestandsformaat] [wijze] [adres].

Artikel 11. Informatieverplichting en audit

11.1 Opdrachtnemer stelt alle informatie ter beschikking die nodig is om aan te tonen dat de verplichtingen uit deze Verwerkersovereenkomst zijn en worden nagekomen.

11.2 Opdrachtnemer verleent alle benodigde medewerking aan audits.

11.3 ***<OPTIONEEL>*** Opdrachtgever laat eenmaal per […] een audit uitvoeren door een onafhankelijke partij.

OF

11.3 ***<OPTIONEEL>*** Opdrachtnemer verstrekt met een frequentie van eenmaal per […], uiterlijk op [datum] aan Opdrachtgever een verklaring van een onafhankelijke externe deskundige, waarin deze een oordeel geeft over de genoemde naleving.

Aldus op de laatste van de twee hierna genoemde data overeengekomen en in tweevoud ondertekend,

Den Haag, [datum] [Plaats], [datum]

DE MINISTER/STAATSSECRETARIS VAN/VOOR [naam Opdrachtnemer]
[naam portefeuille]

namens deze,
[functienaam ondertekenaar]

[naam ondertekenaar] [functie en naam ondertekenaar]

Bijlage 1 **Verwerkersovereenkomst ARVODI: De Verwerking van Persoonsgegevens**

In deze bijlage moet in ieder geval het volgende worden gespecificeerd:

Het onderwerp/aard en doel van de Verwerking	
Het soort Persoonsgegevens	
Beschrijving categorieën Persoonsgegevens	
Beschrijving categorieën Betrokkenen	
Beschrijving categorieën ontvangers van Persoonsgegevens	

Voor de inhoud van deze bijlage kan onder meer gebruik worden gemaakt van de registratie die de Verwerkingsverantwoordelijke op grond van artikel 30 van de Verordening dient aan te houden.

Bijlage 2 **Verwerkersovereenkomst ARVODI: Passende technische en organisatorische maatregelen**

In deze bijlage moeten de normen en maatregelen die Opdrachtnemer in het kader van de beveiliging van de Verwerking moet hanteren respectievelijk treffen worden gespecificeerd. Hiervoor kan worden verwezen naar documenten waarin normen en maatregelen zijn vastgelegd, zoals in voorkomend geval het programma van eisen of de offerteaanvraag.

Bijlage 3 **Verwerkersovereenkomst ARVODI: Afspraken betreffende Inbreuken in verband met Persoonsgegevens**

In deze bijlage moeten de afspraken over hoe Opdrachtnemer Opdrachtgever over Inbreuken in verband met Persoonsgegevens gaat informeren worden gespecificeerd.

Departementale procedure

Informatie die ten minste door Opdrachtnemer moet worden verstrekt

Aard van de Inbreuk in verband met Persoonsgegevens
De Persoonsgegevens en Betrokkene
Waarschijnlijke gevolgen van de Inbreuk in verband met Persoonsgegevens
Maatregelen die Opdrachtnemer heeft voorgesteld of genomen om de Inbreuk in verband met Persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan

Bijlage 3: Model verwerkersovereenkomst ARBIT
Bron: https://www.pianoo.nl/document/12027/model-verwerkersovereenkomst-arbit

De Algemene Rijksvoorwaarden bij IT-overeenkomsten (ARBIT 2016/17) zijn vooral bedoeld voor kleine en middelgrote IT-inkopen door de overheid en niet zozeer voor grote en bijzondere IT-projecten. Dat neemt niet weg dat ze ook dan als uitgangspunt voor het opzetten van een meer specifieke contractuele relatie met de IT markt kunnen dienen. Vanwege de flexibiliteit van de bijbehorende modelovereenkomst kan deze veelal ook gebruikt worden bij de inzet van specifieke IT-producten en diensten zoals bijvoorbeeld webhosting of SaaS (software as a service). Het model is ook beschikbaar in het Engels.

Instructie:

- **Voor zover teksten '<*OPTIONEEL*>' zijn is dat aangegeven in de tekst**.
- **Bij teksten waar 'OF' tussen de bepalingen in staat, dient een keuze tussen de verschillende opties gemaakt te worden. De overige optie(s) verwijderen uit de overeenkomst**.
- **Deze Verwerkersovereenkomst kan alleen in combinatie met een Dienstverleningsovereenkomst worden gesloten**.

N.B. Bij gebruik van de overeenkomst, deze instructie verwijderen.

Inhoud:

Verwerkersovereenkomst ARBIT-2016
Contractnummer: […].

De ondergetekenden:

1. De Staat der Nederlanden, waarvan de zetel is gevestigd te Den Haag,
te dezen vertegenwoordigd door de Minister/Staatssecretaris van/voor [naam portefeuille],
namens deze,
[functienaam en naam ondertekenaar]
hierna te noemen: Opdrachtgever,

en

2. [volledige naam en rechtsvorm contractant],
(statutair) gevestigd te [plaats],
te dezen vertegenwoordigd door
..... *(en .....)* [naam ondertekenaar]
hierna te noemen: Wederpartij,

hierna gezamenlijk te noemen: Partijen;

OVERWEGENDE DAT:

- voor zover Wederpartij Persoonsgegevens Verwerkt ten behoeve van Opdrachtgever in het kader van de Overeenkomst, Opdrachtgever krachtens artikel 4, onderdeel 7 en onderdeel 8, van de Verordening kwalificeert als verwerkingsverantwoordelijke voor de Verwerking van Persoonsgegevens en Wederpartij als verwerker;
- Partijen in deze Verwerkersovereenkomst, zoals bedoeld in artikel 28, derde lid, van de Verordening, hun afspraken over de Verwerking van Persoonsgegevens door Wederpartij wensen vast te leggen.

KOMEN OVEREEN:

Artikel 1. Begrippen
In deze Verwerkersovereenkomst wordt een aantal begrippen met een beginhoofdletter gebruikt. Aan deze begrippen komt de betekenis toe die hieraan wordt gegeven in artikel 1 van de Algemene Rijksvoorwaarden bij IT-overeenkomsten 2016 (ARBIT-2016). In afwijking daarvan of in aanvulling daarop wordt onder de volgende begrippen in deze Verwerkersovereenkomst verstaan:

1.1 Betrokkene: degene op wie een Persoonsgegeven betrekking heeft.

1.2 Inbreuk in verband met Persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

1.3 Overeenkomst: de overeenkomst tussen Opdrachtgever en Wederpartij [titel] van [datum], met kenmerk [kenmerk].

1.4 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, die Wederpartij in het kader van de Overeenkomst ten behoeve van Opdrachtgever verwerkt.

1.5 Verordening: 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 de Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

1.6 Verwerkersovereenkomst: deze overeenkomst inclusief overwegingen en bijbehorende bijlagen.

1.7 Verwerking: een bewerking of een geheel van bewerkingen in het kader van de Overeenkomst met betrekking tot Persoonsgegevens, of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen.

Artikel 2. Voorwerp van deze Verwerkersovereenkomst

2.1 Deze Verwerkersovereenkomst regelt de Verwerking van Persoonsgegevens door Wederpartij in het kader van de Overeenkomst.

2.2 De aard en het doel van de Verwerking, het soort Persoonsgegevens en de categorieën van Persoonsgegevens, Betrokkenen en ontvangers zijn in Bijlage 1 omschreven.

2.3 Wederpartij garandeert de toepassing van passende technische en organisatorische maatregelen, opdat de Verwerking aan de vereisten van de Verordening voldoet en de bescherming van de rechten van de Betrokkene is gewaarborgd.

2.4 Wederpartij garandeert te voldoen aan de vereisten van de toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

Artikel 3. Inwerkingtreding en duur

3.1 Deze Verwerkersovereenkomst treedt in werking op het moment waarop deze door Partijen is ondertekend.

3.2 Deze Verwerkersovereenkomst eindigt nadat en voor zover Wederpartij alle Persoonsgegevens overeenkomstig artikel 10 heeft gewist of terugbezorgd.

3.3 Geen van Partijen kan deze Verwerkersovereenkomst tussentijds opzeggen.

Artikel 4. Omvang verwerkingsbevoegdheid Wederpartij

4.1 Wederpartij Verwerkt de Persoonsgegevens uitsluitend in opdracht en op basis van schriftelijke instructies van Opdrachtgever behoudens afwijkende wettelijke voorschriften die op Wederpartij van toepassing zijn.

4.2 Indien een instructie als bedoeld in het eerste lid naar het oordeel van Wederpartij in strijd is met een wettelijk voorschrift inzake gegevensbescherming, stelt hij Opdrachtgever daarvan voorafgaand aan de Verwerking in kennis, tenzij een wettelijk voorschrift deze kennisgeving verbiedt.

4.3 Indien Wederpartij op grond van een wettelijk voorschrift Persoonsgegevens dient te verstrekken, informeert hij Opdrachtgever onmiddellijk, en zo mogelijk voorafgaand aan de verstrekking.

4.4 Wederpartij heeft geen zeggenschap over het doel van en de middelen voor de Verwerking van Persoonsgegevens.

Artikel 5. Beveiliging van de Verwerking
5.1 In aanvulling op artikel 19 van de ARBIT-2016 en onverminderd artikel 2.3 treft Wederpartij de technische en organisatorische beveiligingsmaatregelen zoals beschreven in Bijlage 2.

5.2 Partijen erkennen dat het waarborgen van een passend beveiligingsniveau voortdurend kan dwingen tot het treffen van aanvullende beveiligingsmaatregelen. Wederpartij waarborgt een op het risico afgestemd beveiligingsniveau.

5.3 Indien en voor zover Opdrachtgever daarom uitdrukkelijk schriftelijk verzoekt, zal Wederpartij aanvullende maatregelen treffen met het oog op de beveiliging van de Persoonsgegevens.

5.4 Wederpartij Verwerkt Persoonsgegevens niet buiten de Europese Unie, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming heeft verkregen van Opdrachtgever en behoudens afwijkende wettelijke verplichtingen.

5.5 Wederpartij informeert Opdrachtgever zonder onredelijke vertraging zodra hij kennis heeft genomen van onrechtmatige Verwerkingen van Persoonsgegevens of inbreuken op beveiligingsmaatregelen zoals genoemd in het eerste en tweede lid.

5.6 Wederpartij verleent Opdrachtgever bijstand bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36 van de Verordening.

Artikel 6. Geheimhouding door Personeel van Wederpartij
6.1 De Persoonsgegevens hebben een vertrouwelijk karakter als bedoeld in artikel 17.1 van de ARBIT-2016.

6.2 Wederpartij toont op verzoek van Opdrachtgever aan dat zijn Personeel zich ertoe heeft verbonden vertrouwelijkheid in acht te nemen als bedoeld in artikel 17.2 van de ARBIT-2016.

Artikel 7. Subverwerker
Wanneer Wederpartij, met inachtneming van het bepaalde in artikel 23 van de ARBIT-2016, een andere verwerker inschakelt om ten behoeve van Opdrachtgever verwerkingsactiviteiten te verrichten, worden aan deze andere verwerker bij een overeenkomst dezelfde verplichtingen inzake gegevensbescherming opgelegd als die welke in deze Verwerkersovereenkomst zijn opgenomen.

Artikel 8. Bijstand vanwege rechten van Betrokkene
Wederpartij verleent Opdrachtgever bijstand bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III van de Verordening vastgelegde rechten van de Betrokkene te beantwoorden.

Artikel 9. Inbreuk in verband met Persoonsgegevens
9.1 Wederpartij informeert Opdrachtgever zonder onredelijke vertraging, zodra hij kennis heeft genomen van een Inbreuk in verband met Persoonsgegevens, overeenkomstig de afspraken zoals vastgelegd in Bijlage 3.

9.2 Wederpartij informeert Opdrachtgever ook na een melding op grond van het eerste lid over ontwikkelingen betreffende de Inbreuk in verband met Persoonsgegevens.

9.3 Partijen dragen elk de door henzelf in verband met de melding aan de bevoegde toezichthoudende autoriteit en Betrokkene te maken kosten.

Artikel 10. Terugbezorgen of wissen Persoonsgegevens

10.1 Na afloop van de Overeenkomst draagt Wederpartij, naar gelang de keuze van Opdrachtgever, zorg voor het terugbezorgen aan Opdrachtgever of het wissen van alle Persoonsgegevens. Wederpartij verwijdert kopieën, behoudens afwijkende wettelijke voorschriften.

10.2 ***<OPTIONEEL>***Wederpartij [wist of retourneert] de Persoonsgegevens binnen [aantal] [dagen/weken] na afloop van de Overeenkomst, bij gebreke waarvan Wederpartij een boete verschuldigd is van €[bedrag] per dag, met een maximum van €[bedrag].

10.3 ***<OPTIONEEL>*** Persoonsgegevens worden in de door Opdrachtgever aangegeven vorm en op de door Opdrachtgever aangegeven wijze terugbezorgd.

OF

10.3 ***<OPTIONEEL>*** De Persoonsgegevens worden als volgt terugbezorgd: [bestandsformaat] [wijze] [adres].

Artikel 11. Informatieverplichting en audit

11.1 Wederpartij stelt alle informatie ter beschikking die nodig is om aan te tonen dat de verplichtingen uit deze Verwerkersovereenkomst zijn en worden nagekomen.

11.2 Wederpartij verleent alle benodigde medewerking aan audits.

11.3 ***<OPTIONEEL>*** Opdrachtgever laat eenmaal per […] een audit uitvoeren door een onafhankelijke partij.

OF

11.3 ***<OPTIONEEL>*** Wederpartij verstrekt met een frequentie van eenmaal per […], uiterlijk op [datum] aan Opdrachtgever een verklaring van een onafhankelijke externe deskundige, waarin deze een oordeel geeft over de genoemde naleving.

Aldus op de laatste van de twee hierna genoemde data overeengekomen en in tweevoud ondertekend,

Den Haag, [datum] [Plaats], [datum]

DE MINISTER/STAATSSECRETARIS VAN/VOOR [naam portefeuille]

[naam Wederpartij]

namens deze,
[functienaam ondertekenaar]

[naam ondertekenaar] [functie en naam ondertekenaar]

Bijlage 1 **Verwerkersovereenkomst ARBIT: De Verwerking van Persoonsgegevens**

In deze bijlage moet in ieder geval het volgende worden gespecificeerd:

Het onderwerp/aard en doel van de Verwerking	
Het soort Persoonsgegevens	
Beschrijving categorieën Persoonsgegevens	
Beschrijving categorieën Betrokkenen	
Beschrijving categorieën ontvangers van Persoonsgegevens	

Voor de inhoud van deze bijlage kan onder meer gebruik worden gemaakt van de registratie die de Verwerkingsverantwoordelijke op grond van artikel 30 van de Verordening dient aan te houden.

Bijlage 2 **Verwerkersovereenkomst ARBIT:. Passende technische en organisatorische maatregelen**

In deze bijlage moeten de normen en maatregelen die Wederpartij in het kader van de beveiliging van de Verwerking moet hanteren respectievelijk treffen worden gespecificeerd. Hiervoor kan worden verwezen naar documenten waarin normen en maatregelen zijn vastgelegd, zoals in voorkomend geval het programma van eisen of de offerteaanvraag.

Bijlage 3 **Verwerkersovereenkomst ARBIT: Afspraken betreffende Inbreuken in verband met Persoonsgegevens**

In deze bijlage moeten de afspraken over hoe Wederpartij Opdrachtgever over Inbreuken in verband met Persoonsgegevens gaat informeren worden gespecificeerd.

Departementale procedure

Informatie die ten minste door Wederpartij moet worden verstrekt

Aard van de Inbreuk in verband met Persoonsgegevens
De Persoonsgegevens en Betrokkene
Waarschijnlijke gevolgen van de Inbreuk in verband met Persoonsgegevens
Maatregelen die Wederpartij heeft voorgesteld of genomen om de Inbreuk in verband met Persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan