AUTORITEIT
PERSOONSGEGEVENS

<Onderzoeksrapport>

Werkende verwerkersovereenkomsten

Onderzoek naar de toepassing in de private sector

September 2019

Over de Autoriteit Persoonsgegevens
Iedereen heeft recht op een zorgvuldige omgang met zijn persoonsgegevens. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving.

AUTORITEIT
PERSOONSGEGEVENS

Inhoudsopgave

1 Inleiding en achtergronden

1.1 Inleiding

De Autoriteit Persoonsgegevens (AP)heeft een verkennend onderzoek uitgevoerd naar verwerkersovereenkomsten (art. 28 lid 3 AVG). Dit rapport is daarvan het verslag.
In een verwerkersovereenkomst worden door de verwerkingsverantwoordelijke en verwerker afspraken gemaakt over wat de verwerker wel en niet mag/moet doen met de persoonsgegevens die de verwerkingsverantwoordelijke aanlevert. Denk aan afspraken over o.a. het beveiligingsbeleid en het doel van de verwerking. Het opstellen van een verwerkersovereenkomst is geen optionele activiteit. Het is een 'accountability' verplichting die in de Algemene Verordening Gegevensbescherming (AVG) terug te vinden is in art. 28. Een verwerkersovereenkomst regelt op een transparante wijze de verhouding tussen een verwerkingsverantwoordelijke en verwerker. Denk aan een adviesbureau (verwerkingsverantwoordelijke) dat een online-marketing bedrijf inschakelt (verwerker 1), een callcenter terug laat bellen (verwerker 2) of bij een hostingprovider zijn website laat hosten (verwerker 3). Daarbij stelt een verwerkersovereenkomst de kaders waarbinnen de verwerker verwerkingen mag uitvoeren.

Degelijke, periodiek bijgewerkte verwerkersovereenkomsten vormen onderdeel van een goede bedrijfsvoering. Organisaties die in toenemende mate door data gedreven worden, doen er goed aan om te investeren in werkende verwerkersovereenkomsten als onderdeel van hun datahuishouding.

1.2 Wat is een verwerkersovereenkomst?

Een organisatie die verwerkingsverantwoordelijke is kan een andere organisatie inschakelen om persoonsgegevens voor hem te verwerken. Bijvoorbeeld voor het uitbesteden van de boekhouding. Of door gebruik te maken van een clouddienst die persoonsgegevens opslaat. Deze andere organisatie wordt een verwerker genoemd. In dat geval is het verplicht een verwerkersovereenkomst op te stellen. Een verwerkersovereenkomst bevat de afspraken die de verwerkingsverantwoordelijke en de verwerker hebben gemaakt over de verwerkingen die de verwerker mag uitvoeren van en voor de verwerkingsverantwoordelijke. Niet alleen moet daarin zijn opgenomen welke verwerkingen en persoonsgegevens er worden verwerkt, er moeten ook afspraken zijn gemaakt over tal van andere zaken. Te denken valt aan afspraken over de beveiliging, het al dan niet mogen inschakelen van subverwerkers en afspraken over de omgang met verzoeken van betrokkenen. Omdat de risico's rondom verwerkingen niet statisch zijn is het nodig een verwerkersovereenkomst periodiek te herzien en bij te stellen. Een volledig overzicht van de eisen die in een verwerkersovereenkomst moeten worden geadresseerd, is opgenomen in art. 28 AVG.

1.3 Verkennend onderzoek

In het eerste half jaar van 2019 heeft de Autoriteit Persoonsgegevens (AP) bij 31 organisaties uit de private sector, variërend van de sectoren handel, gezondheidszorg, media, vrije tijd en energie onderzoek gedaan naar verwerkersovereenkomsten. Het doel was om een beter beeld te krijgen over de wijze waarop invulling wordt gegeven aan de verplichting van het opstellen van een verwerkersovereenkomst bij het inschakelen van een verwerker door de verwerkingsverantwoordelijke. Het doel was niet om de rechtmatigheid van de in verwerkersovereenkomst beschreven verwerkingen te beoordelen, of een oordeel te geven over de rechtmatigheid of volledigheid van de verwerkersovereenkomsten in hun specifieke context. Dit rapport moet dan ook niet worden gezien als een oordeel over de rechtmatigheid van de verwerkingsovereenkomsten.

De onderzochte organisaties hebben een vragenlijst van de AP gekregen en bij elke organisatie zijn 3 verwerkersovereenkomsten opgevraagd waarbij persoonsgegevens van klanten van deze organisaties worden verwerkt door een verwerker. De gestelde vragen zijn opgenomen in bijlage 2.

De AP heeft een groot aantal verwerkersovereenkomsten ingezien. De door de organisaties gegeven antwoorden en overhandigde verwerkersovereenkomsten zijn door de AP geanalyseerd. In dit rapport worden de conclusies van het onderzoek en aanbevelingen voor de praktijk beschreven. Vanwege de uitgebreide eisen in art. 28 AVG (zie bijlage 1 voor het juridisch kader) en de verscheidenheid aan bevraagde organisaties, zowel vanuit de aard van hun werkzaamheden als vanuit hun omvang, zijn er uiteenlopende beelden ontstaan. Daarom gelden de bevindingen die hier worden genoemd ook niet onverkort voor alle organisaties. Zelfs binnen organisaties bleken er soms verschillen in verwerkersovereenkomsten te zijn. De bevindingen en aanbevelingen in dit rapport achten wij nuttig voor een ieder die te maken heeft met verwerkersovereenkomsten.

In dit rapport heeft de AP enkele geanonimiseerde voorbeelden opgenomen van passages uit verwerkersovereenkomsten. Deze voorbeelden zijn puur illustratief en bieden verwerkingsverantwoordelijke handvatten bij het concretiseren en nader uitwerken van art. 28 AVG. De AP heeft niet vastgesteld of verwerkersovereenkomsten inhoudelijk volledig en juist zijn in de specifieke context, ook niet voor wat betreft de specifiek overgenomen voorbeelden. De voorbeelden dienen dan ook niet rechtstreeks overgenomen te worden daar er altijd, door de verwerkingsverantwoordelijke, rekening moet worden gehouden met de specifieke context.

Het verkennende onderzoek heeft geleid tot het algemene beeld dat er zeer diverse verwerkersovereenkomsten in gebruik zijn bij organisaties. Dit past bij het beeld dat de AVG door de open normen mogelijkheden biedt voor maatwerk. Niet elke organisatie of verwerking is immers hetzelfde. Dit brengt met zich mee dat er verwerkersovereenkomsten zijn die ruimte bieden voor nadere uitwerking. Een aantal organisaties heeft dit verkennend onderzoek aangegrepen om de procedures rondom verwerkersovereenkomsten aan te scherpen door bijvoorbeeld extra reviews te houden op de verwerkersovereenkomsten of verwerkersovereenkomsten te herzien. In zoverre heeft de aankondiging van dit onderzoek en het bevragen van organisaties geleid tot acties bij verwerkingsverantwoordelijken.

2 Conclusies en aanbevelingen

De conclusies van het verkennend onderzoek zijn als volgt:

1. Krap een jaar na inwerkingtreding van de AVG[1] zijn er nog verwerkersovereenkomsten die niet volledig voldoen aan de eisen uit de AVG. Dit varieert van kleine en eenvoudig aan te passen zaken tot het niet volledig opnemen van specifieke verplichtingen uit art. 28 lid 3 AVG (zie bijlage 1). Ook is het niet altijd eenvoudig waar te nemen waar in de verwerkersovereenkomst een bepaald AVG vereiste is uitgewerkt. Het niet volledig voldoen aan de eisen vanuit de AVG vormt een risico voor de verwerkingsverantwoordelijke, de verwerker maar zeker ook voor de betrokkenen. Het is primair aan de verwerkingsverantwoordelijke om vast te stellen of er in de door hem afgesloten verwerkersovereenkomsten risico's aanwezig zijn.

Aanbeveling 1: Houd overzicht en wees volledig.
Maak een overzicht van de eisen in art. 28 lid 3 AVG en leg dit naast alle reeds bestaande verwerkersovereenkomsten. Pas verwerkersovereenkomsten aan op punten waar er discrepanties bestaan tussen de reeds bestaande verwerkersovereenkomst en de vereisten die gelden krachtens de AVG. Neem in het overzicht op in welke contract clausule welke wettelijke eis wordt beschreven.

2. De AP heeft enkele verwerkersovereenkomsten ontvangen met een dagtekening die lag na het bezorgen van de door de AP uitgestuurde brief met vragen. Dit kan meerdere oorzaken hebben. Mogelijk was er ten tijde van het bezorgen van de brief van de AP een onder de Wbp opgestelde bewerkersovereenkomst en werd er gewerkt aan een nieuwe vorm geënt op de normen uit de AVG. Een andere reden kan zijn dat de brief van de AP ervoor heeft gezorgd dat er, in een situatie waarin nog geen afspraken waren gemaakt tussen verwerkingsverantwoordelijke en verwerker, er alsnog een verwerkersovereenkomst is opgesteld. Mogelijk is de afweging of er ergens een verwerkersovereenkomst diende te zijn eerder in onvoldoende mate gemaakt en heeft de brief van de AP de verwerkingsverantwoordelijke tot een heroverweging bewogen. De AP heeft de achterliggende reden nu niet onderzocht.

Aanbeveling 2: Duid risico's en stel zo nodig verwerkersovereenkomsten op.
Maak op basis van het, vaak verplichte, register van verwerkingen dat verwerkersverantwoordelijken dienen te hebben duidelijk welke organisaties er worden ingeschakeld en voor welke verwerking zij persoonsgegevens verwerken, welke rol zij daarin hebben, wat de risico's zijn en welke verwerkersovereenkomsten daarbij reeds gelden of benodigd zijn. Indien blijkt dat er voor een verwerker geen verwerkersovereenkomst is opgesteld waar dit wel vereist is, stel dan een verwerkersovereenkomst op.

3. Organisaties pakken het opstellen van een verwerkersovereenkomst soms zeer systematisch aan. Zij maken het onderdeel van hun inkoopproces, waarbij alleen met partijen wordt onderhandeld die voldoende maatregelen kunnen bieden om aan de AVG te voldoen, en zij maken duidelijke afspraken over rollen, taken en activiteiten, en richten een systeem in voor het monitoren en aanpassen van de verwerkersovereenkomst.

Aanbeveling 3: Veranker het opstellen, beoordelen en aanpassen van verwerkersovereenkomsten in bestaande processen.

[1] De vragen in het kader van dit onderzoek zijn door de AP in januari 2019 gesteld.

Veranker het opstellen, beoordelen en aanpassen van verwerkersovereenkomsten in bestaande processen voor contractmanagement. Zo kan worden voorkomen dat een verwerkersovereenkomst in onvoldoende mate onderwerp is van rapportage en overleg, als losstaand instrument wordt gezien en een eigen leven leidt los van hoofdovereenkomsten. Ook kan een verwerkersovereenkomst door gewijzigde omstandigheden of verwerkingen aanpassing behoeven. Herzie periodiek, bijvoorbeeld als onderdeel van een jaarlijkse beoordeling, of de verwerkersovereenkomst nog voldoet aan de eisen.

4. Uit de opgeleverde informatie blijkt dat het opstellen van de verwerkersovereenkomsten voor sommige verwerkingsverantwoordelijken, door de grote hoeveelheid verwerkers, een behoorlijke inspanning is. Enkelen zijn dan ook nu nog bezig met het aanpassen van reeds voor de AVG bestaande bewerkersovereenkomsten naar onder de AVG vallende verwerkersovereenkomsten. Tevens heeft de AP een aantal overeenkomsten ontvangen die nog verwijzen naar artikelen uit de niet meer van kracht zijnde Wbp.

Aanbeveling 4: Toets bestaande overeenkomsten aan de verscherpte eisen uit de AVG.
Verwerkersovereenkomsten zijn geen volledig nieuw middel bij de bescherming van persoonsgegevens, onder de Wbp bestonden namelijk bewerkersovereenkomsten. Daaruit kan de indruk ontstaan dat er dan ook geen nieuwe eisen zijn aan deze overeenkomsten. In de AVG zijn echter een aantal elementen verder uitgewerkt. Te denken valt bijvoorbeeld aan de nadere uitwerking van de informatieplicht die rust op verwerkingsverantwoordelijken. Deze ziet, volgens art. 13 lid 2 onder a AVG, ook op de periode gedurende welke de persoonsgegevens worden opgeslagen. Dit is gerelateerd aan eventuele overeengekomen bewaartermijnen tussen verwerkingsverantwoordelijke en een verwerker. Het is daarom noodzakelijk om de bewerkersovereenkomsten aan te passen aan de aangescherpte eisen uit de AVG.

5. Uit de beoordeelde verwerkersovereenkomsten komt een wisselend beeld naar voren ten aanzien van de wijze waarop de afspraken in de verwerkersovereenkomst worden geconcretiseerd. In sommige gevallen bevatten de verwerkersovereenkomsten slechts artikelen die letterlijk zijn overgenomen uit de AVG. Dit is onvoldoende: in het kader van de verantwoordingsplicht is het noodzakelijk dat bijvoorbeeld duidelijk wordt beschreven welke persoonsgegevens er worden verwerkt, voor welke doeleinden en hoe bijvoorbeeld het beveiligingsbeleid en maatregelen in elkaar zitten, niet slechts dat er een beveiligingsbeleid of certificaat is.

Aanbeveling 5: Maak afspraken en maatregelen concreet.
De AVG bevat veelal open normen die invulling behoeven naar de specifieke situatie waarin verwerkingsverantwoordelijke en verwerkers zich bevinden. Een verwerkersovereenkomst dient ter nadere invulling van die norm zodat beide partijen weten hoe zij de open norm in de specifieke situatie samen invullen. Leg bijvoorbeeld vast hoe persoonsgegevens geleverd aan de verwerker door de verwerkingsverantwoordelijke bij het beëindigen van de verwerkersovereenkomst worden vernietigd of weer worden teruggegeven aan de verwerkingsverantwoordelijke. Te denken valt bijvoorbeeld aan de termijn waarbinnen dit gebeurt, in welk bestandsformaat de persoonsgegevens worden aangeleverd en hoe deze persoonsgegevens beveiligd zijn. Slechts stellen dat de data worden teruggegeven is niet erg concreet.

Tevens moeten er afspraken worden gemaakt over onder andere welke persoonsgegevens worden verwerkt, wie doel en middelen bepaalt (wie de verwerkingsverantwoordelijke is), hoe de gegevens worden beveiligd en welke verwerkingen er door de verwerker zullen worden uitgevoerd.

3 Onderzoeksmethode en aanpak

In dit hoofdstuk legt de AP uit hoe zij het onderzoek heeft uitgevoerd.

De AP heeft voor dit onderzoek sectoren in de private sector gekozen die niet eerder in verkennende onderzoeken van de AP aan de orde zijn geweest. Het gaat dan om de sectoren handel, gezondheidszorg, media, vrije tijd en energie.

De AP heeft een willekeurige selectie gemaakt van organisaties binnen deze sectoren die naar verwachting persoonsgegevens van klanten verwerken en daarbij waarschijnlijk verwerkers inschakelen.

Bij de selectie van organisaties heeft de AP zowel grote als middelgrote organisaties geselecteerd.

De AP heeft vervolgens 31 geselecteerde organisaties aangeschreven en hen vragen gesteld. Deze vragen behelsden zowel het proces rondom het opstellen en waarborgen van verwerkersovereenkomsten als wel de inhoud van de verwerkersovereenkomsten. De AP heeft zich daarbij specifiek gericht op het verwerken van persoonsgegevens van klanten, niet op het verwerken van bijvoorbeeld persoonsgegevens van personeel. De gestelde vragen zijn opgenomen in de bijlagen bij dit rapport.

Daarnaast heeft de AP bij deze organisaties de verwerkersovereenkomsten van de drie verwerkers opgevraagd die de grootste hoeveelheid persoonsgegevens van klanten voor de organisatie verwerken.

Van de 31 bevraagde organisaties bleken drie organisaties uiteindelijk één en dezelfde verwerkingsverantwoordelijke zodat er 29 verwerkingsverantwoordelijken resteerden. Alle bevraagde organisaties hebben de vragenlijst beantwoord en de verwerkersovereenkomsten aan de AP gestuurd.

De AP heeft geen contact opgenomen met door verwerkingsverantwoordelijken genoemde verwerkers.

4 Bevindingen

4.1 Soorten verwerkers

De AP heeft de door een groot aantal verwerkingsverantwoordelijken opgeleverde verwerkersovereenkomsten ingezien. De verwerkingsverantwoordelijken zijn actief in diverse branches. Dat heeft er mede voor gezorgd dat de ingeschakelde verwerkers ook divers zijn. Vaker genoemde soorten verwerkers zijn:

- Diensten op het gebied van (direct) marketing.
  Het gaat daarbij om het benaderen van bestaande klanten en potentiële klanten waarvan persoonsgegevens worden verwerkt. Bij het gebruik van deze diensten is het noodzakelijk om te letten op de benodigde grondslag voor de verwerking.[2]
- Logistieke dienstverleners en uitbesteding voorraadbeheer.
  Deze organisaties leveren een aantal diensten. Ten eerste worden hierbij zowel pakketten als poststukken opgehaald en bezorgd. Hiervoor worden evident persoonsgegevens verwerkt. Het valt de AP op dat niet alle partijen op de hoogte zijn van het feit dat de AP logistieke dienstverleners in dit geval in de regel als verwerkingsverantwoordelijke ziet.[3] Ten tweede bestaan er situaties waarbij een organisatie het volledige logistieke proces inclusief voorraadbeheer overneemt van een andere organisatie. In die gevallen zal inhoudelijk moeten worden onderzocht wat de rolverdeling is tussen organisaties.
- Financiële dienstverlening, incasso en accountancy.
  In deze situaties worden bijvoorbeeld financiële controles uitgevoerd op de juistheid van persoonsgegevens en betalingen of worden vorderingen overgedragen ter incasso. Hierbij is het verstandig om goed te overleggen welke werkzaamheden er worden uitgevoerd. Indien er voor deze werkzaamheden ook een wettelijke basis bestaat, kunnen deze organisaties zelfstandig verwerkingsverantwoordelijke zijn. In die gevallen is een verwerkersovereenkomst niet noodzakelijk.
- Software as a Service (SaaS), webhosting en cloudopslag.
  Hierbij worden persoonsgegevens verwerkt in online omgevingen. Dat kan gaan om het online gebruik van een applicatie, website waarop persoonsgegevens kunnen worden ingevoerd of het enkel bieden van opslagruimte of serverruimte.

4.2 Het opstellen en de vorm van een verwerkersovereenkomst

In dit onderdeel geeft de AP een beeld van de bevindingen betreffende het proces rondom het opstellen van verwerkersovereenkomsten.

4.2.1 Persoonsgegevens bij een verwerker

De vraag of artikel 28 AVG inzake de verwerker van toepassing is in de relatie tussen twee organisaties begint met de vraag of de in het bezit van de verwerker zijnde gegevens wel persoonsgegevens zijn. Daarbij dient te worden aangesloten bij de definitie van 'persoonsgegeven' uit art. 4 lid 1 AVG. Om deze afweging goed te kunnen maken is het verstandig om te kijken naar de overwegingen die hiervoor zijn gemaakt in de AVG. Te denken valt bijvoorbeeld aan overweging 26. Veranderende activiteiten in een organisatie kunnen er bijvoorbeeld voor zorgen dat een organisatie die eerst geen persoonsgegevens doorgaf dat later wel lijkt te doen. Ook kan het zo zijn dat de verwerker persoonsgegevens niet direct van de

[2] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/direct-marketing
[3] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/verwerkers#moet-ik-als-logistieke-dienstverlener-verwerkersovereenkomsten-afsluiten-met-mijn-opdrachtgevers-7105.

verwerkingsverantwoordelijke verkrijgt maar bijvoorbeeld van de betrokkene zelf. Het is daarom goed om periodiek na te gaan welke gegevens er worden gebruikt door de andere organisatie en of deze daarmee persoonsgegevens verwerkt. Eventuele wijzigingen kunnen dan worden doorgevoerd in het register van verwerkingen dat de verwerkingsverantwoordelijke vaak dient bij te houden.

Bijna zonder uitzondering schakelen de ondervraagde organisaties anderen in om persoonsgegevens te verwerken. Slechts een enkeling gaf aan dat niet te doen. De organisaties die verwerkers inschakelen schakelen ook zonder uitzondering meer dan één verwerker in. Logischerwijs schakelen grote organisaties meer verwerkers in, tot soms meer dan honderd verwerkers.

Enkele, vooral grote, organisaties die gebruik maken van grote hoeveelheden verwerkers hebben deze verwerkers, al dan niet op basis van een risicoschatting, gegroepeerd. Dit kan de overzichtelijkheid ten goede komen, zeker indien het soort informatie en de soort verwerking daarbij wordt onderkend en wordt gekoppeld aan risico's zoals het risico op een inbreuk. Een dergelijke indeling kan ook helpen bij het bepalen van de zwaarte van in te zetten controlemiddelen.

Do

"Als er een behoefte en / of noodzaak ontstaat tot de inzet van een externe partij voor het leveren van specifieke diensten, dan vindt er eerst een verkennend onderzoek plaats vanuit de betreffende business verantwoordelijke al dan niet samen met de afdeling inkoop. Dit om te bekijken welke externe organisatie deze behoefte aan dienstverlening kan invullen én om te bekijken in welke mate deze dienstverlening compliant is ingericht, In de verkennende fase vindt, indien benodigd, overleg plaats met de Juridische afdeling binnen X om de compliance aspecten, waar privacy naleving onderdeel van uitmaakt, te onderzoeken"

"Ten aanzien van X op de lijst bij ... geldt dat er geen verwerkersovereenkomst is getekend omdat de door X voorgestelde overeenkomst niet aan de vereisten van artikel 28 lid 3 AVG voldoet en X niet akkoord wenst te gaan met de door de Y voorgestelde overeenkomst in overeenstemming met artikel 28 lid 3 AVG. Y zal het gebruik van de diensten van X mede hierom op korte termijn staken"

4.2.2 Het gebruik van (sub) verwerkers buiten de Europese Economische Ruimte

Buiten de scope van het onderzoek viel een integrale beoordeling van de verwerkingsovereenkomsten in de concrete situatie. Desondanks valt het op dat er organisaties zijn die gebruik maken van (sub)verwerkers, of dit gebruik toestaan, waarbij er medewerkers van de (sub)verwerker buiten de Europese Economische Ruimte (EER) inzage in persoonsgegevens kunnen krijgen. De AP heeft niet onderzocht of inzage daadwerkelijk plaatsvindt. Dit punt verdient bijzondere aandacht bij verwerkersverantwoordelijken. De AVG kent strikte regels over het buiten de EER verwerken van persoonsgegevens. Het opvragen en raadplegen persoonsgegevens is krachtens art. 4 AVG namelijk ook een verwerking. Daarvoor geldt een "nee tenzij". Dit geldt ook bij toegang tot persoonsgegevens in de EER door verwerkers die zich fysiek niet binnen de EER bevinden en bij verschaffen van persoonsgegevens buiten de EER. Hiervoor gelden speciale eisen die zijn opgenomen in hoofdstuk V van de AVG, bijvoorbeeld het afsluiten van zgn. Standard Contractual Clauses.

4.2.3 Rolverdeling tussen verwerkingsverantwoordelijke, verwerker en de gedeelde verwerkingsverantwoordelijkheid

In het onderzoek zijn de organisaties bevraagd over de wijze waarop zij vaststellen of ze verwerkingsverantwoordelijke zijn, verwerker of gezamenlijk verwerkingsverantwoordelijk. Deze

afweging wordt onder andere beheerst door de definities in art. 4 AVG. De meeste organisaties gaven aan dit te doen door middel van het vaststellen wie doel en middelen voor de verwerking bepaalt, zoals de AVG voorschrijft. Soms is deze afweging lastig. Daarom kan hierbij worden aangesloten bij eerdere door de EDPB gegeven voorbeelden.[4] Tevens is het goed om op de website van de AP te kijken waar een aantal oordelen staan over de vraag wanneer een organisatie verwerker is, bijvoorbeeld in het geval van logistieke dienstverlening.[5,6]

Aan te bevelen is om uit te gaan van het vaak verplicht opgestelde verwerkingsregister, daarin concreet te benoemen welke verwerkingen er plaatsvinden, wie daarvoor doel en middelen bepaalt en deze concrete verwerkingen ook op te nemen in de verwerkersovereenkomsten.

Do's en don'ts

Do
"In deze gevallen bepaalt X het doel en de middelen voor de verwerking van de persoonsgegevens en voert de andere partij verwerkingen voor X uit."

Don't
"In alle gevallen geldt dat wij verwerkingsverantwoordelijke zijn en de andere partij de verwerker."

Een klein aantal organisaties ziet zich samen met een andere organisatie als gezamenlijk verwerkingsverantwoordelijke. Wellicht is deze mogelijkheid niet bekend bij alle verwerkersverantwoordelijken. Echter, dit kan onder omstandigheden een meer passende invulling van de relatie zijn. Het is daarom ook aan te bevelen in die situaties waarbij de afweging tussen verwerkingsverantwoordelijke en verwerker lastig is nogmaals goed te kijken naar de regeling in art. 26 AVG. Mogelijk sluit deze beter aan bij de concrete situatie. Bij de beoordeling of een organisatie verwerker is geeft een eventuele verwerkersovereenkomst wel een beeld, maar de feitelijke situatie is leidend bij de beoordeling.[7]

Het is aan te raden, en enkele vooral grote organisaties geven ook aan dit al te doen, om deze afwegingen en vaststellingen vroegtijdig in het inkoopproces te maken, zodat criteria die gesteld worden aan verwerkers bijvoorbeeld meegenomen kunnen worden in het aanbestedingsproces. Zo wordt voorkomen dat er eerst een verwerker wordt gekozen en er daarna nog over privacywaarborgen dient te worden onderhandeld.

Het was voor de AP in een aantal gevallen niet direct duidelijk welke verwerking er exact plaatsvond bij de verwerker. Het is wenselijk dat dit onomstotelijk uit de verwerkersovereenkomst blijkt. Ook voor de verwerker is dit wenselijk. Bij een onduidelijke omschrijving kan het ook zomaar zijn dat er door perceptieverschillen verwerkingen bij de verwerker plaatsvinden die niet zijn voorzien door de

[4] Opinion 1/2010 on the concepts of "controller" and "processor" WP 169 (16.02.2010).
[5] Zie de vraag en antwoorden op https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/verantwoordingsplicht.
[6] Zie de campagne met praktische informatie over verwerkers van persoonsgegevens op https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-vervolgt-campagne-met-praktische-informatie-over-verwerkers-van-persoonsgegevens.
[7] Zie stroomschema over verwerker of verwerkingsverantwoordelijke op https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stroomschema_verwerker.pdf.

verwerkingsverantwoordelijke. Daarmee kan een verwerker ook ineens (gezamenlijk) verwerkingsverantwoordelijke blijken te zijn. Bovendien is het in het kader van het toezicht en de controle op de naleving van de AVG, goed om de FG mee te laten lezen of te laten adviseren over (het opstellen van) verwerkersovereenkomsten.

4.2.4 Vorm van een verwerkersovereenkomst

Alle bevraagde organisaties hebben aangegeven verwerkersovereenkomsten te hebben opgesteld. De AP heeft hier enkele opmerkingen over. In paragraaf 4.3 geeft de AP meer informatie over de eisen die ex art. 28 lid 3 AVG worden gesteld aan overeenkomsten.

Een enkele verwerkingsverantwoordelijke heeft documentatie opgeleverd welke gebaseerd is op een door de verwerker opgestelde privacy policy. Dit is een voor de verwerker aantrekkelijke wijze, mede vanuit oogpunt van uniformering. Het is wel de vraag in hoeverre deze verwerkingsverantwoordelijken de eisen die normaalgesproken worden gesteld door een verwerkingsverantwoordelijke aan een verwerker over laten. Als dit het geval is, mag van de verwerkingsverantwoordelijke worden verwacht dat hij nauwkeurig is nagegaan of die privacy policy een juiste en volledige invulling van de eisen uit art. 28 AVG omvat. De verwerkingsverantwoordelijke blijft verantwoordelijk voor het opstellen van de verwerkersovereenkomst.

Het merendeel van de verwerkersovereenkomsten is helder en beschrijft wat de verhouding is tussen de partijen en waar de verwerker aan is gehouden. Een aantal overeenkomsten bevat echter een summiere tekstuele uitwerking van de AVG, bijvoorbeeld als het gaat om art. 32 AVG (beveiliging van de verwerking). In enkele gevallen omvat deze eigenlijk niet meer dan een louter tekstuele herhaling van de AVG. Dat is onduidelijk en onwenselijk. Er dient meer duidelijkheid te zijn over de vraag wat de exacte invulling is van, in dit geval, art. 32 AVG.

Grotere organisaties maken daarnaast vaak gebruik van een standaard vorm voor een verwerkersovereenkomst. Dat kan goed werken omdat daarmee voor de verwerkingsverantwoordelijke een uniform beeld bestaat en afspraken eenduidig en gemakkelijk te vinden zijn.

Do
"X standaard verwerkersovereenkomst binnen European Economic Area (EEA)
X standaard verwerkersovereenkomst buiten EEA (Standard Contractual Clauses)
X standaard verwerkersovereenkomst binnen/buiten EEA"

Niet uit alle verwerkersovereenkomsten blijkt heel duidelijk in welk hoofdstuk of paragraaf een specifieke wettelijke eis uit de AVG is opgenomen. Verwijzingen aan het begin van een hoofdstuk kunnen daarbij helpen maar ook een referentietabel kan heel nuttig zijn. Zo kan men, bij gewijzigde wetgeving, of de wens om een clausule in het contract aan te passen, eenvoudiger de verbinding leggen tussen die clausule en relevante wetgeving.

4.3 De inhoud van de verwerkersovereenkomsten

In dit onderdeel geeft de AP een beeld van de bevindingen betreffende de inhoud van de verwerkersovereenkomsten en de daarin opvallende zaken, uitgaande van de specifieke eisen die in art. 28 lid 3 AVG aan een verwerkersovereenkomst worden gesteld.

4.3.1 De te verwerken persoonsgegevens en de verwerking

Een verwerker mag persoonsgegevens uitsluitend verwerken op basis van schriftelijke instructies van de verwerkingsverantwoordelijke (art. 28 lid 3 sub a AVG). De AP heeft dat in vrijwel alle verwerkersovereenkomsten ook gezien.

Ook dienen er afspraken te zijn gemaakt over de doorgifte van persoonsgegevens aan landen die niet onder het regime van de AVG vallen (zgn. derde landen) en waarvoor de Europese Commissie (EC) niet heeft besloten dat ze een passend beschermingsniveau bieden (art. 28 lid 3 sub a AVG).[8] De meeste verwerkersovereenkomsten bevatten een algemene regel over het niet buiten de EER mogen brengen van persoonsgegevens zonder toestemming van de verwerkingsverantwoordelijke.
De AP merkt op dat wanneer organisaties gebruik maken van verwerkers in derde landen er niet altijd een bepaling is opgenomen over het beschermingsniveau van het desbetreffende derde land. Hierboven is aangegeven dat de AVG vereist dat verwerkingsverantwoordelijken alleen een beroep doen op verwerkers die afdoende garanties kunnen bieden onder de AVG (art. 28 lid 1 AVG). Daarnaast gelden de AVG eisen aan doorgifte van persoonsgegevens (art. 28 lid 3 sub a AVG).

Do's en don'ts

Do

"Opdrachtnemer zal, tenzij zij hiervoor uitdrukkelijke voorafgaande schriftelijke toestemming heeft verkregen van Opdrachtgever, geen persoonsgegevens verwerken of laten verwerken door haarzelf of door derden in landen buiten de Europese Economische Ruimte ("EER"). Opdrachtnemer stelt de contactpersoon van Opdrachtgever onmiddellijk schriftelijk op de hoogte van alle (geplande) permanente of tijdelijke doorgiftes van persoonsgegevens naar een land buiten de EER en zal pas uitvoering geven aan dergelijke geplande doorgiftes na schriftelijke toestemming van Opdrachtgever. Opdrachtgever heeft te allen tijde het recht om aanvullende voorwaarden te verbinden aan haar toestemming voor een dergelijke verwerking."

".... De toestemming van Opdrachtgever voor het uitbesteden van werkzaamheden aan een sub-verwerker laat onverlet dat voor de inzet van sub verwerkers in een land buiten de EER toestemming vereist is in overeenstemming met artikel X van deze Verwerkersovereenkomst."

Don't

"X agrees that Y may, subject to Section Z, store and process Customer Personal Data in U and any other country in which Y or any of its Subprocessors maintains facilities."

De AP heeft ook waargenomen dat er in veel verwerkersovereenkomsten is stilgestaan bij welke persoonsgegevens er worden verstrekt aan de verwerker (art. 28 lid 3 AVG). Dat is verstandig, zeker ook als het gaat om het verwerken van bijzondere persoonsgegevens waar een verbod op geldt. Immers, bijzondere persoonsgegevens mogen slechts worden verwerkt als er een uitzondering is op het algemene verwerkingsverbod (art. 9 AVG) en er een geldige grondslag is (art. 6 AVG). Bijvoorbeeld in het geval van zorgaanbieders kan het zijn dat er bijzondere persoonsgegevens worden verstrekt aan een verwerker. Daarbij kan dan tevens worden opgenomen waarom de verwerker deze verwerking wel mag uitvoeren. Hierbij verdient het extra de aandacht om, gezien een eventueel verbod, goede afspraken te maken over de (on)mogelijkheid een subverwerker in te schakelen, zie daarvoor verder ook paragraaf 4.3.3. Een ander

[8] Landen die een passend beschermingsniveau bieden zie https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal-gegevensverkeer/doorgifte-binnen-en-buiten-de-eu.

aspect is dat het verwerken van bijzondere persoonsgegevens grotere risico's voor de rechten en vrijheden van natuurlijke personen met zich meebrengt.[9] Dit kan van invloed zijn op de keuze voor passende technische en organisatorische maatregelen om de verwerking te beschermen.

Opgemerkt dient te worden dat in verwerkersovereenkomsten in het kader van het leveren van opslag door een verwerker aan een verwerkingsverantwoordelijke het onder omstandigheden zo kan zijn dat de verwerkingsverantwoordelijke nog niet weet welke persoonsgegevens hij exact gaat opslaan bij de verwerker. In die gevallen is het niet altijd mogelijk dit nader uit te werken. Het verdient wel aanbeveling om in die gevallen dat wat wel bekend is vast te leggen en bij periodieke herzieningen aandacht te besteden aan een verdere uitwerking.

Do
"Records met naam, adres, woonplaats, telefoonnummer, geboortedatum , geslacht, emailadres en bankrekeningnummer van consumenten met als doel ...."

Niet altijd is het uit de verwerkersovereenkomst helder op te maken wat de exacte verwerking inhoudt (art. 28 lid 3 AVG). Soms is dit wel af te leiden uit de overwegingen bij de verwerkersovereenkomst. Het is de bedoeling dat een verwerker voldoende nauwkeurig kan bepalen wat hij wel en niet mag in het kader van de verwerkersovereenkomst. De AP heeft meerdere malen gezien dat er wordt aangegeven dat verwerkingen "in het kader van de hoofdovereenkomst" zijn toegestaan. Daarbij hangt het dus af van de wijze waarop de hoofdovereenkomst de werkzaamheden beschrijft. Een ruime definitie in die hoofovereenkomst brengt dan het risico met zich mee dat de verwerker te veel verwerkingen gaat uitvoeren waarbij er discussie kan ontstaan of deze nog wel passen binnen die hoofdovereenkomst. Daarbij kan de verwerker onder omstandigheden voor een bepaalde verwerking toch verwerkingsverantwoordelijke blijken te zijn (art. 28 lid 10 AVG). Het is de vraag of organisaties zich hiervan voldoende bewust zijn.

Do's en don'ts

Do
"Opdrachtnemer zal de persoonsgegevens voor (uitsluitend) de volgende doeleinden verwerken:
• het verzorgen van de salarisadministratie;
• het verwerken van loonbelasting en overige financiële dienstverlening;
• het uitvoeren van declaraties voor uitgevoerde handelingen en het in behandeling nemen van de vergoeding die een patiënt voor een bepaalde behandeling kan krijgen van een zorgverzekeraar;
• ..."

Don't
"Verwerker verwerkt de persoonsgegevens in het kader van de hoofdovereenkomst"

4.3.2 Vertrouwelijkheid

De meeste verwerkersovereenkomsten bevatten een clausule over vertrouwelijkheid of geheimhouding. In die gevallen waarin zo'n clausule is opgenomen verschilt de omvang en reikwijdte van deze clausules. Zo is niet altijd beschreven of en hoe deze geheimhouding geldt voor werknemers van de verwerker en of er een wettelijke geheimhoudingsplicht bestaat voor bepaalde personen. Het is aan te raden hier nauwkeurig bij

[9] Zie overweging 75 AVG.

stil te staan nu, uitgaande van een specifieke verwerking, dient te worden vastgesteld of deze onder de AVG/UAVG valt, bijvoorbeeld wanneer het gaat om verwerkingen in een derde land (art. 44 e.v. AVG).

Do

"Verwerker draagt ervoor zorg dat personen, niet beperkt tot werknemers, die bij Verwerker deelnemen aan de Verwerkingen zijn gebonden aan een geheimhoudingsverplichting ter zake het geheimhouden van de Persoonsgegevens."

4.3.3 Mogelijke inzet van subverwerkers

De AVG kent twee regimes voor het inschakelen van subverwerkers en de toestemming van de verwerkingsverantwoordelijke die daarvoor vereist is (art. 28 lid 3 sub d AVG). Dit zijn de specifieke voorafgaande toestemming en generieke voorafgaande toestemming met recht van bezwaar. Beide regimes zijn aangetroffen in de verwerkersovereenkomsten waarbij vaak gebruik wordt gemaakt van de laatste vorm. Daarbij zijn soms passages opgenomen waarbij de verwerkingsverantwoordelijke alleen op redelijke gronden bezwaar mag hebben. Ook is waargenomen dat bij inschakeling van een subverwerker de verwerkingsverantwoordelijke het recht heeft de overeenkomst te ontbinden.

Ook zijn er verwerkersovereenkomsten aangeleverd waarin geen clausule is opgenomen inzake het inschakelen van subverwerkers. Daarmee is het inschakelen van subverwerkers dan ook kennelijk niet beoogd door de verwerkingsverantwoordelijke en derhalve niet toegestaan.

Do

"Zonder voorafgaande schriftelijke toestemming van Opdrachtgever zal Opdrachtnemer haar activiteiten die (deels) bestaan uit het verwerken van persoonsgegevens of vereisen dat persoonsgegevens verwerkt worden, niet uitbesteden aan een derde partij ("sub-verwerker"). Opdrachtnemer zal aan de door haar ingeschakelde sub-verwerkers dezelfde verplichtingen opleggen als voor haarzelf uit deze Verwerkersovereenkomst en de wet voortvloeien en ziet toe op de naleving daarvan door de sub-verwerker. De betreffende afspraken met de sub-verwerker zullen schriftelijk worden vastgelegd. Opdrachtnemer zal Opdrachtgever op verzoek afschrift verstrekken van deze overeenkomst(en) voor zover relevant voor naleving van deze Verwerkersovereenkomst.
Niettegenstaande de toestemming van Opdrachtgever voor het inschakelen van een sub-verwerker, blijft Opdrachtnemer volledig aansprakelijk jegens Opdrachtgever voor de gevolgen van het uitbesteden van werkzaamheden aan een sub-verwerker. De toestemming van Opdrachtgever voor het uitbesteden van werkzaamheden aan een sub-verwerker laat onverlet dat voor de inzet van sub verwerkers in een land buiten de EER toestemming vereist is in overeenstemming met artikel X van deze Verwerkersovereenkomst.
Opdrachtgever geeft hierbij toestemming voor het inschakelen van de in Bijlage 3 opgenomen sub verwerker(s) door Opdrachtnemer. Partijen zorgen ervoor dat deze bijlage up to date blijft.
Opdrachtnemer zal Opdrachtgever direct informeren wanneer een overeenkomst met een sub-verwerker is beëindigd."

"Controller provides Processor hereby with a general authorisation to engage Sub-Processors. Processor will impose the same material data protection obligations on the Sub-Processors as set out in this DPA, in particular in relation to the implementation of appropriate technical and organisational measures.
Processor shall notify Controller of any intended changes concerning the engagement or replacement of a Sub-Processor and Controller shall be given thirty (30) days to object, duly motivated and in writing, after

receiving such notification. If Processor fails to address such objection, Controller's sole and exclusive remedy is to terminate the Merchant Agreement and this DPA immediately by providing written notice to Processor. For the avoidance of doubt, in the event Processor uses Sub-Processors, Processor shall remain fully liable to the Controller for the fulfilment of its obligations under this DPA."

De AP beveelt verwerkingsverantwoordelijken en verwerkers aan afspraken te maken over de wijze van het maken van bezwaar tegen het inschakelen van een subverwerker. Zo kan het zinvol zijn een termijn overeen te komen waarbinnen een verwerkingsverantwoordelijke bezwaar mag maken tegen inschakeling en welke criteria er kunnen zijn om een subverwerker af te wijzen.

Art. 28 lid 4 AVG legt verwerkers nog de eis op om de eisen uit art 28 lid 3 AVG die de verwerkingsverantwoordelijke aan de verwerker stelt, ook van toepassing te laten zijn in de verhouding verwerker-subverwerker. Dit is niet altijd te zien in de verwerkersovereenkomst tussen de verwerkingsverantwoordelijke en verwerker. Het is echter goed dit expliciet te maken mede gezien de aansprakelijkheid van een verwerker bij niet functioneren van een door hem ingeschakelde subverwerker.

4.3.4 Rechten van betrokkenen

Op een enkele verwerkersovereenkomst na zijn er clausules opgenomen ten aanzien van de rechten van betrokkenen en de bijstand die verwerkers dienen te verlenen bij de uitoefening van die rechten (art. 28 lid 3 sub e AVG). Dit kunnen meer algemene clausules zijn of specifieke waarin de rechten van betrokkenen ook daadwerkelijk zijn genoemd. Dat laatste is helder voor de verwerker en eventuele subverwerkers, zeker omdat onder de AVG in ieder geval het recht op dataportabiliteit nieuw is. Ook zijn er in de AVG rechten van betrokken verder uitgewerkt dan in de Wbp. Mogelijk dienden verwerkers daarvoor extra maatregelen te nemen bij de inwerkingtreding van de AVG. De AP heeft ook waargenomen dat er verwerkersovereenkomsten zijn waarin is opgenomen dat verzoeken van betrokkenen worden doorgeleid naar de verwerkingsverantwoordelijke. Dat laatste is begrijpelijk gezien het feit dat de rechten van betrokkenen bedoeld zijn om primair tegen de verwerkingsverantwoordelijke te worden ingeroepen en deze een juiste uitvoering van de rechten van betrokkenen, die zich mogelijk uitstrekken over meerdere verwerkers, gecoördineerd kan faciliteren.

Do

" - Indien Verwerkingsverantwoordelijke zelf toegang heeft tot de Persoonsgegevens voldoet hij zelf aan alle verzoeken van de betrokkenen met betrekking tot de Persoonsgegevens. Verwerker zal eventueel door Verwerker ontvangen verzoeken onverwijld aan Verwerkingsverantwoordelijke doorgeven.

- Alleen voor zover het in het voorgaande lid bedoelde niet mogelijk is, zal Verwerker zijn volledige en tijdige medewerking verlenen aan Verwerkingsverantwoordelijke om:
(i) na goedkeuring van en in opdracht van Verwerkingsverantwoordelijke betrokkenen toegang te laten krijgen tot de hun betreffende Persoonsgegevens,
(ii) Persoonsgegevens te verwijderen of te corrigeren,
(iii) aan te tonen dat Persoonsgegevens verwijderd of gecorrigeerd zijn indien zij incorrect zijn (of, ingeval Verwerkingsverantwoordelijke het er niet mee eens is dat de Persoonsgegevens incorrect zijn, het feit vast te leggen dat de betrokkene zijn Persoonsgegevens als incorrect beschouwt)
(iv) de betreffende Persoonsgegevens aan Verwerkingsverantwoordelijke dan wel aan een door de Verwerkingsverantwoordelijke aangewezen derde te verstrekken in een gestructureerde, gangbare en machineleesbare vorm en
(v) Verwerkingsverantwoordelijke anderszins in de gelegenheid te stellen om aan zijn verplichtingen onder de AVG of aan andere toepasselijke wetgeving op het gebied van verwerking van de Persoonsgegevens te voldoen."

Zoals hierboven aangegeven zijn niet in alle verwerkersovereenkomsten clausules opgenomen over de rechten van betrokkenen. Het opnemen van een regeling omtrent de rechten van betrokkenen is echter wel een verplicht onderdeel. Het is van belang om deze clausules op te nemen zodat verwerkingsverantwoordelijke en verwerker weten waar zij aan toe zijn en verzoeken van betrokkenen zo efficiënt mogelijk kunnen worden behandeld. De AP beveelt aan om te onderzoeken of de huidige overeengekomen afspraken voldoende helder zijn.

4.3.5 Bijstand bij beveiliging, datalekmeldingen en DPIA's

De verwerkingsverantwoordelijke en de verwerker dienen overeen te komen dat de verwerker de verwerkingsverantwoordelijke ondersteunt bij zijn verplichtingen uit de artikelen 32-36 AVG. Deze artikelen regelen de persoonsgegevensbeveiliging (art. 32 AVG), datalekmeldingen (art. 33 en 34 AVG) en de gegevensbeschermingseffectbeoordeling (vaak aangeduid met de Engelse benaming Data Protection Impact Assesment, afgekort tot DPIA) en voorafgaande raadpleging (art. 35 t/m 36 AVG).

4.3.5.1 Art. 32 AVG; Beveiliging van de verwerking

Waar het gaat om de beveiliging ex art. 32 AVG verwijst de AP naar paragraaf 4.3.8.

4.3.5.2 Art 33 en 34 AVG; Melden van inbreuken

De artikelen 33 en 34 AVG bevatten de regeling omtrent inbreuken in verband met persoonsgegevens (ook wel datalekken genoemd). Het eerste artikel behandelt de meldplicht richting de toezichthouder en het tweede richting betrokkenen. Zoals reeds aangegeven is het verlenen van bijstand van de verwerker aan de verwerkingsverantwoordelijke bij het nakomen van de verplichtingen uit hoofde van artikel 32 tot en met 36 AVG niet facultatief. Toch bevatten enkele verwerkersovereenkomsten geen uitgewerkte regeling hiervoor. Een verwerkingsverantwoordelijke dient bijvoorbeeld een inbreuk te melden conform de in art. 33 lid 1 AVG genoemde termijnen en condities. Zo is er een termijn opgenomen van 72 uur waarbinnen inbreuken, "*nadat hij er kennis van heeft genomen*", door de verwerkingsverantwoordelijke dienen te worden

gemeld bij de toezichthouder. De AP signaleert in verwerkersovereenkomsten meerdere termijnen waarbinnen verwerkers meldingen moeten doen aan de verwerkingsverantwoordelijke. Van “onverwijld”, via “binnen vier uur” tot binnen “48 uur”, zelfs “72 uur” is voorgekomen. Mogelijk is deze laatste termijn voor verwerkingsverantwoordelijke overgenomen uit de AVG en als maatstaf gekozen voor de termijn die de verwerker richting de verwerkingsverantwoordelijke heeft. Het is verstandig om te overleggen wat een passende termijn zou zijn waarbinnen een melding door de verwerker aan de verwerkingsverantwoordelijke is voorzien en als doelstelling te nemen dat deze termijn zo kort mogelijk is.

Do

"Om Verwerkingsverantwoordelijke in staat te stellen aan de op haar rustende kennisgevingsverplichting te kunnen voldoen stelt Verwerker Verwerkingsverantwoordelijke onmiddellijk na het ontdekken van een beveiligingsincident (maar uiterlijk binnen .. uur na het ontdekken van het beveiligingsincident) in kennis van het beveiligingsincident.."

"In respect of assisting the Controller in fulfilling the obligation to notify a Personal Data Breach to the supervisory authority and to communicate a Personal Data Breach to data subjects, as referred to in Article 28(3)(f) of the GDPR, taking into account the nature of the Processing and the information available to it, X shall:
...
5.6.2. provide the Customer, where feasible, with additional information about any Personal Data Breach of which the Customer has become aware or which has been notified by X, in the scope required by the Customer to determine the likelihood of risk to the rights and freedoms of persons whose Personal Data are covered by the breach and in the scope required by the Customer to notify the Personal Data Breach to the supervisory authority in accordance with Article 33 and Article 34 of the GDPR or to communicate the Personal Data Breach to the data subjects — in response to the Customer's request submitted under .... hereof;
5.6.3. Promptly investigate the Personal Data Breach and take reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from such Personal Data Breach.
5.7. If a Personal Data Breach is established that was caused by fault of X or X's subcontractor, X shall review the applied technical and organisational measures and, if needed and where feasible, shall make appropriate changes to prevent such Personal Data Breach from reoccurring."

4.3.5.3 Art 35 en 36; Gegevensbeschermingseffectbeoordeling en Voorafgaande Raadpleging

De artikelen 35 en 36 AVG beschrijven de procedure van de gegevensbeschermingseffectbeoordeling, ook bekend als de DPIA en de mogelijk daarop volgende Voorafgaande Raadpleging. Ook hiervoor geldt dat het goed is om een instructie tot bijstand overeen te komen. Een DPIA of voorafgaande raadpleging kan een lastige afweging bevatten waarvoor veel kennis nodig is. Het is dan nuttig deze vanuit een verwerker te kunnen inzetten. Dit kan bijvoorbeeld wenselijk zijn om te bepalen welke maatregelen er dienen te worden overeengekomen voor het sluiten van een verwerkersovereenkomst of uit hoofde van art. 35 lid 11 AVG, wat bepaalt: “*Indien nodig verricht de verwerkingsverantwoordelijke een toetsing om te beoordelen of de verwerking overeenkomstig de gegevensbeschermingseffectbeoordeling wordt uitgevoerd, zulks ten minste wanneer sprake is van een verandering van het risico dat de verwerkingen inhouden.*”. Het is zeer wel mogelijk dat die toetsing bij de verwerker plaatsvindt, in dat geval is het verlenen van bijstand door de verwerker in het algemeen wenselijk.

Ten aanzien van de voorafgaande raadpleging ex art. 36 AVG is de rol van de verwerker wat explicieter beschreven, daarin is opgenomen dat in voorkomende gevallen de toezichthouder ook richting de

verwerker communiceert. Niet altijd wordt, als er wel een verplichting is opgenomen om te assisteren bij het uitvoeren van een DPIA, eenzelfde verplichting opgenomen voor de Voorafgaande Raadpleging.

Do

"Verwerker verleent Verantwoordelijke op eerste verzoek van Verantwoordelijke en binnen de door Verantwoordelijke gestelde termijn of — indien geen termijn wordt gesteld — binnen .. werkdagen volledige medewerking aan Verantwoordelijke in het kader van i) een verzoek van een betrokkene, ii) het verrichten van een Privacy Impact Assessment door Verantwoordelijke, iii) een verzoek, onderzoek of voorafgaande raadpleging door een toezichthouder, of iv) enige andere wettelijke verplichting van Verantwoordelijke."

Uit de beoordeelde verwerkersovereenkomsten is naar voren gekomen dat de bepalingen uit art. 35 en 36 AVG niet altijd specifiek zijn opgenomen of uitgewerkt. Bij het uitvoeren door de verwerkingsverantwoordelijke van een DPIA en het aanvragen van een voorafgaande raadpleging bij de AP kan het echter noodzakelijk zijn de verwerker te betrekken.

4.3.6 Persoonsgegevens na afloop van de verwerkingsdiensten

In de AVG is opgenomen dat na afloop van de verwerkingsdiensten de verwerkingsverantwoordelijke de keuze heeft of de verwerker alle persoonsgegevens wist of deze aan de verwerkingsverantwoordelijke terugbezorgt en alle bestaande kopieën verwijdert. Uitgezonderd een wettelijke verplichting om deze persoonsgegevens te bewaren (art. 28 lid 3 sub g AVG). Het is overigens niet per definitie zo dat persoonsgegevens dienen te worden bewaard tot het einde van de looptijd van de verwerkersovereenkomst, ex art. 4 lid e AVG geldt er immers een opslagbeperking.

Vrijwel alle verwerkersovereenkomsten bevatten een regeling over de omgang met persoonsgegevens bij het einde van de verwerkersovereenkomst. De AP heeft daar meerdere soorten afspraken aangetroffen. Zo zijn er verwerkersovereenkomsten waarbij het uitgangspunt is dat de persoonsgegevens worden verwijderd, al dan niet binnen een bepaalde termijn. Dit kan een risico opleveren indien de relatie met de verwerker eindigt maar die met betrokkenen doorloopt en de verwerkingsverantwoordelijke zelf niet beschikt over een kopie van de gegevens. Bijvoorbeeld wanneer de verwerkingsverantwoordelijke gebruik gaat maken van een andere verwerker en de persoonsgegevens moeten worden overgezet naar de nieuwe verwerker. Hier kan ook een risico op inbreuken ontstaan nu ook tijdelijke niet beschikbaarheid van persoonsgegevens een inbreuk kán vormen.[10] Een voorbeeld kan zijn het tijdelijk niet beschikbaar zijn van persoonsgegevens die essentieel zijn, bijvoorbeeld in geval van spoedeisende medische behandelingen in ziekenhuizen. Hierbij speelt ook mee dat sommige rechten van betrokkenen niet effectief kunnen worden uitgevoerd indien zijn persoonsgegevens langduriger of niet langer voorhanden zijn via de verwerkingsverantwoordelijke. Te denken valt aan het recht op dataportabiliteit ex art. 20 AVG.

Aan het andere uiterste staat de standaard verplichting, die ook is aangetroffen door de AP, om de persoonsgegevens weer aan de verwerkingsverantwoordelijke te verschaffen na afloop van de verwerkingsovereenkomst. Een veelvoorkomende tussenvorm is het laten kiezen uit overdragen, gevolgd door een plicht tot verwijdering van de persoonsgegevens door de verwerker, of verwijderen van de persoonsgegevens zonder verstrekking aan de verwerkingsverantwoordelijke.

[10] Zie de voorbeelden in Richtsnoeren voor de melding van inbreuken in verband met Persoonsgegevens krachtens Verordening 2016/679 WP250rev.01.

Do

"- Verwerker is verplicht de Persoonsgegevens na beëindiging van deze overeenkomst, als ook op elk eerste verzoek van Verantwoordelijke, onverwijld aan Verantwoordelijke te verstrekken.
- Verwerker is verplicht alle bij hem aanwezige Persoonsgegevens na beëindiging van deze overeenkomst, als ook op elk eerste verzoek van Verantwoordelijke, onverwijld te vernietigen. Op eerste verzoek van Verantwoordelijke toont Verwerker aan dat dit daadwerkelijk is gebeurd.
- Verwerker zal alle op grond van artikel .. ingeschakelde derden in kennis stellen van een beëindiging van deze overeenkomst dan wel een daartoe strekkend verzoek van Verantwoordelijke en zal waarborgen dat zij de bij hen aanwezige Persoonsgegevens (laten) vernietigen."

Deze keuze lijkt vaak aan het einde van de looptijd van de verwerkersovereenkomst te worden gemaakt. Het is de vraag of deze keuze niet eerder kan worden gemaakt bij goed gedocumenteerde en overeengekomen verwerkingen. Dat kan ook problemen voorkomen ten aanzien van de vorm waarin de persoonsgegevens worden verstrekt, een gangbaar bestandsformaat ligt bijvoorbeeld voor de hand, en onder welke condities deze verstrekking zal plaatsvinden.

4.3.7 Controle op naleving en audits

De AP heeft een breed scala aan instrumenten waargenomen om te ondersteunen bij het aantonen van de naleving van de AVG. Daarbij gaat het bijvoorbeeld om rapportages, certificeringen en audits. Enkele verwerkersovereenkomsten bevatten in het geheel geen afspraken over periodieke controle van de gehele set aan maatregelen die art. 28 lid 3 AVG noemt terwijl de AVG dit wel eist (art. 28 lid 3 sub h AVG).

De AP ziet in de overeenkomsten soms nog terugkomen dat de naleving vooral is geënt op die maatregelen die zijn overeengekomen in het kader van de invulling van de beveiligingseisen uit art. 32 AVG. De AVG vereist in art. 28 lid 3 sub h dat in een verwerkersovereenkomst een regeling is opgenomen die toeziet op de naleving van de gehele verwerkersovereenkomst. Aan te raden is om na te gaan of verwerkersovereenkomsten in ieder geval zo'n afspraak bevatten.

Bij verwerkers die een generieke verwerking voor meerdere verwerkersverantwoordelijken uitvoeren wordt soms gebruik gemaakt van certificaten of generieke verklaringen. Zie hiervoor het gestelde in paragraaf 4.3.8 . Soms gaat dit vergezeld van de afspraak dat, indien deze certificaten onvoldoende zekerheid bieden een audit alsnog is toegestaan. Dat is een voor beide partijen werkbare oplossing.

Ook komt het voor dat verwerkingsverantwoordelijken, zeker indien zij grote aantallen verwerkers inschakelen, op basis van een risicoschatting bepalen welk middel er wordt ingezet om aan te kunnen tonen dat aan de verplichtingen uit art. 28 AVG wordt voldaan. Daarbij wordt dan meestal ook gekeken naar de frequentie waarmee een middel wordt ingezet. Elementen die zouden kunnen worden meegenomen in het maken van zo'n afweging zijn bijvoorbeeld, maar niet beperkt tot; het soort en de hoeveelheid persoonsgegevens die worden verwerkt, de risico's rondom de verwerking, de mate waarin de verwerker kan worden vervangen, eventuele incidenten enz.

Don't

"X behoudt zich bovendien het recht voor, zoals in de verwerkersovereenkomst is vervat, om toe te zien op naleving. Indien hier aanleiding toe is wordt gecontroleerd of de technische en organisatorische beveiligingsmaatregelen afdoende zijn voor de bescherming van de verwerkte persoonsgegevens."

Hoewel eventuele incidenten zwaar kunnen meewegen bij het bepalen van de wijze waarop controles plaatsvinden, heeft de AP ook waargenomen dat het recht op controle vooral lijkt te zijn gekoppeld aan een vermoeden van niet nakoming of het bestaan van tekortkomingen. Het is de vraag of dat een verstandige keuze is. In de praktijk kan dat er namelijk toe leiden dat er pas na incidenten wordt gecontroleerd terwijl juist de preventieve functie van controles zekerheid geeft over de juiste uitvoering van de verwerkersovereenkomst. Een dergelijke afspraak kan wel goed werken als er ter compensatie afspraken zijn gemaakt over het periodiek aanleveren van generieke rapporten en rapportages die toezien op de naleving van de verwerkersovereenkomst.

4.3.8 Beveiliging van de verwerking

Artikel 32 AVG stelt eisen aan passende technische en organisatorische maatregelen die de verwerkingsverantwoordelijke en de verwerker moeten treffen voor de beveiliging van de persoonsgegevens. De AP neemt waar dat verwerkingsverantwoordelijken hier verschillende invullingen kiezen. Een aantal verwerkersovereenkomsten bevat een algemene opmerking vergezeld van een bijlage met meer specifieke technische en organisatorische maatregelen die dienen te worden genomen door de verwerker. Dat is aan te raden nu art. 32 AVG stelt: "*treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen*". Uiteraard kan het zo zijn dat een verwerker deskundig is en soms zelfs deskundiger dan de verwerkingsverantwoordelijke. Dit doet echter niets af aan de mate van vastlegging van de maatregelen. Het is in ieder geval verstandig om na overleg vast te leggen welke risico's er door de verwerker dienen te worden gemitigeerd en/of op te nemen met welke maatregelen men dat doet.

Ook zijn er veel verwerkersovereenkomsten die verwijzen naar de contractuele plicht van de verwerker tot het hebben van een certificaat. Voor de duidelijkheid, het gaat hier niet om certificaten die ex. art. 42 AVG zijn uitgegeven maar om andere standaarden. Certificaten kunnen een goede basis zijn om de beveiliging van verwerkingen te waarborgen. Daarbij moet de vraag worden beantwoord in hoeverre het certificaat voldoende is in het kader van de AVG. Een veel aangevoerde eis is het hebben van een ISO-27001 certificaat (informatiebeveiliging) waar het gaat om de levering van ICT. Er zal in zo'n geval moeten worden nagegaan wat de exacte bijbehorende scope is van zo'n certificaat om zeker te stellen dat alle elementen van de verwerking onder de scope van dat certificaat vallen. Deze afweging zal vaak voor het sluiten van de verwerkersovereenkomst zijn gemaakt. Daarbij wil de AP opmerken dat de risicoanalyse die wordt vereist in art. 32 lid 1 AVG expliciet uitgaat van de: "*qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen*", waar een risicoanalyse via ISO-27001 soms betrekking heeft op de risico's voor een bedrijfsproces, systeem of onderneming, en deze afweging vaak ook alleen door de verwerker is gemaakt.

Do

Passages die zijn opgenomen in de verwerkersovereenkomst in dit kader kunnen zeer uitgebreid zijn, derhalve staan hier slechts enkele clausules als voorbeeld.

"Access to internal systems and environments and the Customer data is only possible for authorised employees or co-workers after logging into the specific account and with the use of the specific password compliant with the password policy."

"Verwerker neemt in ieder geval de technische en organisatorische beveiligingsmaatregelen die op grond van de AVG en in het bijzonder op grond van artikel 32 AVG van haar worden geëist. Een en ander zoals nader uitgewerkt in Bijlage 2...

Bijlage 2: Beveiligingsmaatregelen
Verwerker heeft in ieder geval de volgende beveiligingsmaatregelen met betrekking tot persoonsgegevens genomen: Binnen het netwerk van de verwerker wordt gebruik gemaakt van sterke wachtwoorden, welke buiten het netwerk worden aangevuld met 2-factor authenticatie. Wachtwoorden worden versleuteld opgeslagen in de database, waarbij het originele wachtwoord niet is terug te halen."

"Risico: Weglekken van data door onvoldoende vernietiging van datadragers
Maatregel: Standaardprocedure is dat schijven worden vernietigd door gecertificeerde instantie X met daarbij bewijs van vernietiging."

"Verwerkingsverantwoordelijke heeft zich goed geïnformeerd over de beveiligingsmaatregelen die Verwerker heeft genomen en is van mening dat deze maatregelen een beveiligingsniveau hebben dat past bij de aard van de Persoonsgegevens en de omvang, context, doeleinden en risico's van de Verwerking.
Partijen erkennen dat het waarborgen van een passend beveiligingsniveau voortdurend kan dwingen tot het treffen van aanvullende beveiligingsmaatregelen. Verwerker waarborgt een op het actuele risico afgestemd beveiligingsniveau. Verwerker zal Vetwerkingsverantwoordelijke informeren als een van de beveiligingsmaatregelen substantieel wijzigt."

De AP beveelt verwerkingsverantwoordelijken dan ook aan om periodiek de risico's voor de rechten en vrijheden van personen in kaart te brengen, te herzien, en in overleg te treden met de verwerker over passende maatregelen en mogelijke aanpassingen daarop. Certificaten kunnen hierbij helpen indien is vastgesteld dat zij daadwerkelijk de geïdentificeerde risico's mitigeren.

Bijlage 1 Juridisch kader

Relevante bepalingen uit de AVG

Artikel 4 Definities

7. „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 Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen;
8. „verwerker": een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;

Artikel 28 - Verwerker

1. Wanneer een verwerking namens een verwerkingsverantwoordelijke wordt verricht, doet de verwerkingsverantwoordelijke uitsluitend een beroep op verwerkers 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.
2. De verwerker neemt geen andere verwerker in dienst zonder voorafgaande specifieke of algemene schriftelijke toestemming van de verwerkingsverantwoordelijke. In het geval van algemene schriftelijke toestemming licht de verwerker de verwerkingsverantwoordelijke in over beoogde veranderingen inzake de toevoeging of vervanging van andere verwerkers, waarbij de verwerkingsverantwoordelijke de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken.
3. De verwerking door een verwerker wordt geregeld in een overeenkomst of andere rechtshandeling krachtens het Unierecht of het lidstatelijke recht die de verwerker ten aanzien van de verwerkingsverantwoordelijke bindt, en waarin het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen, en de rechten en verplichtingen van de verwerkingsverantwoordelijke worden omschreven. Die overeenkomst of andere rechtshandeling bepaalt met name dat de verwerker:
    a. de persoonsgegevens uitsluitend verwerkt op basis van schriftelijke instructies van de verwerkingsverantwoordelijke, onder meer met betrekking tot doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, tenzij een op de verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling hem tot verwerking verplicht; in dat geval stelt de verwerker de verwerkingsverantwoordelijke, voorafgaand aan de verwerking, in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt;
    b. waarborgt dat de tot het verwerken van de persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden;
    c. alle overeenkomstig artikel 32 vereiste maatregelen neemt;
    d. aan de in de leden 2 en 4 bedoelde voorwaarden voor het in dienst nemen van een andere verwerker voldoet;
    e. rekening houdend met de aard van de verwerking, de verwerkingsverantwoordelijke door middel van passende technische en organisatorische maatregelen, voor zover mogelijk,

bijstand verleent bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III vastgestelde rechten van de betrokkene te beantwoorden;

f. rekening houdend met de aard van de verwerking en de hem ter beschikking staande informatie de verwerkingsverantwoordelijke bijstand verleent bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36;
g. na afloop van de verwerkingsdiensten, naargelang de keuze van de verwerkingsverantwoordelijke, alle persoonsgegevens wist of deze aan hem terugbezorgt, en bestaande kopieën verwijdert, tenzij opslag van de persoonsgegevens Unierechtelijk of lidstaatrechtelijk is verplicht;
h. de verwerkingsverantwoordelijke alle informatie ter beschikking stelt die nodig is om de nakoming van de in dit artikel neergelegde verplichtingen aan te tonen en audits, waaronder inspecties, door de verwerkingsverantwoordelijke of een door de verwerkingsverantwoordelijke gemachtigde controleur mogelijk maakt en eraan bijdraagt.

Waar het gaat om de eerste alinea, punt h), stelt de verwerker de verwerkingsverantwoordelijke onmiddellijk in kennis indien naar zijn mening een instructie inbreuk oplevert op deze verordening of op andere Unierechtelijke of lidstaatrechtelijke bepalingen inzake gegevensbescherming.

4. Wanneer een verwerker een andere verwerker in dienst neemt om voor rekening van de verwerkingsverantwoordelijke specifieke verwerkingsactiviteiten te verrichten, worden aan deze andere verwerker bij een overeenkomst of een andere rechtshandeling krachtens Unierecht of lidstatelijk recht dezelfde verplichtingen inzake gegevensbescherming opgelegd als die welke in de in lid 3 bedoelde overeenkomst of andere rechtshandeling tussen de verwerkingsverantwoordelijke en de verwerker zijn opgenomen, met name de verplichting afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen te bieden opdat de verwerking aan het bepaalde in deze verordening voldoet. Wanneer de andere verwerker zijn verplichtingen inzake gegevensbescherming niet nakomt, blijft de eerste verwerker ten aanzien van de verwerkingsverantwoordelijke volledig aansprakelijk voor het nakomen van de verplichtingen van die andere verwerker.
5. Het aansluiten bij een goedgekeurde gedragscode als bedoeld in artikel 40 of een goedgekeurd certificeringsmechanisme als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat voldoende garanties als bedoeld in de leden 1 en 4 van dit artikel worden geboden.
6. Onverminderd een individuele overeenkomst tussen de verwerkingsverantwoordelijke en de verwerker kan de in de leden 3 en 4 van dit artikel bedoelde overeenkomst of andere rechtshandeling geheel of ten dele gebaseerd zijn op de in de leden 7 en 8 van dit artikel bedoelde standaardcontractbepalingen, ook indien zij deel uitmaken van de certificering die door een verwerkingsverantwoordelijke of verwerker uit hoofde van de artikelen 42 en 43 is verleend.
7. De Commissie kan voor de in de leden 3 en 4 van dit artikel genoemde aangelegenheden en volgens de in artikel 93, lid 2, bedoelde onderzoeksprocedure standaardcontractbepalingen vaststellen.
8. Een toezichthoudende autoriteit kan voor de in de leden 3 en 4 van dit artikel genoemde aangelegenheden en volgens het in artikel 63 bedoelde coherentiemechanisme standaardcontractbepalingen opstellen.
9. De in de leden 3 en 4 bedoelde overeenkomst of andere rechtshandeling wordt in schriftelijke vorm, waaronder elektronische vorm, opgesteld.
10. Indien een verwerker in strijd met deze verordening de doeleinden en middelen van een verwerking bepaalt, wordt die verwerker onverminderd de artikelen 82, 83 en 84 met betrekking tot die verwerking als de verwerkingsverantwoordelijke beschouwd.

Bijlage 2 Gestelde vragen

1) Maakt u als verwerkingsverantwoordelijke gebruik van diensten of producten van één of meerdere andere organisatie(s) waarbij u persoonsgegevens van klanten of potentiële klanten doorgeeft? Kunt u dit kort toelichten? Voorbeelden hiervan zijn advertentieorganisaties en -platformen, dienstverleners voor facturering en leveranciers van online opslagdiensten.
2) Welke organisaties (naam) zijn dit?
3) Indien het antwoord op de eerste vraag "ja" is, dan vragen wij u voor elk van de organisaties benoemd in de tweede vraag, de volgende vragen te beantwoorden. Indien voor meerdere organisaties exact dezelfde afwegingen en overwegingen gelden en u exact dezelfde afspraken en nalevingsmaatregelen bent overeengekomen en heeft geïmplementeerd, kunt u aangeven voor welke organisaties uw antwoord geldt.
   3a) Ziet u uzelf als verwerkingsverantwoordelijke en de andere organisatie als verwerker of is er bij sommige relaties wellicht sprake van een gezamenlijke verwerkingsverantwoordelijkheid? Kunt u dit kort toelichten?
   3b) Indien alleen u verwerkingsverantwoordelijke bent, en de andere organisatie is verwerker: Zijn er door u als verwerkingsverantwoordelijke en deze andere organisatie(s) schriftelijke afspraken gemaakt over het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen, de rechten en de verplichtingen van u als verwerkingsverantwoordelijke resp. de rechten en verplichtingen van de verwerker (zie voor de volledige wettelijke vereisten art. 28 lid 3 AVG)? Kunt u dit kort toelichten?
   3c) Indien er sprake is van een gezamenlijke verwerkingsverantwoordelijkheid: Zijn er afspraken gemaakt en vastgelegd om te voldoen aan de eisen zoals opgenomen in art. 26 AVG? Kunt u dit kort toelichten?
   3d) Indien het antwoord op vraag 3b) "ja" is:
      - Hoe stelt u vast dat deze overeenkomst daadwerkelijk wordt nageleefd? Kunt u dit kort toelichten?
      - Hoe geeft u opvolging aan eventueel geconstateerde tekortkomingen in de naleving van de overeenkomst? Kunt u dit kort toelichten?
   3e) Indien u bij één of meerdere van bovenstaande vragen "nee" hebt geantwoord verzoeken wij u gemotiveerd aan te geven waarom u deze vra(a)g(en) met nee heeft beantwoord.
4) Ten slotte vragen wij u voor de drie verwerkingen waarbij de grootste hoeveelheid persoonsgegevens van uw (potentiële) klanten worden verwerkt, de (verwerkers)overeenkomsten aan ons toe te sturen indien u daarvoor gebruikt maakt van een organisatie die als verwerker door u wordt aangezien, of de regeling tussen u en een organisatie waarbij u gezamenlijk verwerkingsverantwoordelijke bent. Kunt u kort toelichten waar de relevante passages in deze overeenkomsten of regelingen kunnen worden gevonden indien het geen separate overeenkomsten betreft?

Vragen over de Algemene verordening gegevensbescherming

Op onze website autoriteitpersoonsgegevens.nl vindt u informatie en antwoorden op vragen over de Algemene verordening gegevensbescherming (AVG). Heeft u op deze website geen antwoord op uw vraag gevonden? Dan kunt u contact opnemen met het Informatie- en Meldpunt Privacy van de Autoriteit Persoonsgegevens op 088-1805 250.