Gemeente Utrecht

Interne Bedrijven
Informatievoorzieningen &
Juridische Zaken en Inkoop
Postbus 16200, 3500 CE Utrecht
www.utrecht.nl

Leidraad AVG Verwerkersovereenkomst

De gemeente schakelt regelmatig externe partijen in bij het uitoefenen van een taak. Als deze partij in opdracht van de gemeente werkt met persoonsgegevens, kan deze 'verwerker' zijn in de zin van de Algemene Verordening Gegevensbescherming (AVG). Als dat zo is, moeten beide partijen - vóórdat de verwerker met de persoonsgegevens aan de slag gaat - specifieke afspraken maken. In deze leidraad staat welke stappen je moet nemen om tot passende afspraken te komen.

Is er sprake van een verwerker?

Persoonsgegevens zijn alle gegevens die direct óf indirect tot een persoon herleidbaar zijn. Bijna alles wat je doet met persoonsgegevens wordt gezien als 'verwerking' in de zin van de wet, behalve *denken* aan persoonsgegevens.

De (verwerkings)*verantwoordelijke* (hierna: verantwoordelijke) is degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. De *verwerker* is vervolgens de partij die voor de verantwoordelijke persoonsgegevens verwerkt, zonder onder zijn rechtstreekse gezag te vallen. Om te bepalen wat de precieze rol is van de betrokken partijen en daarmee of het dan ook nodig is om een verwerkersovereenkomst af te sluiten, verwijzen wij naar de **Factsheet Verwerkingsverantwoordelijke of verwerker** .

Voorbeelden van organisaties die vaak een verwerkersrol vervullen, zijn softwareleveranciers, website hosts en administratiekantoren.

Verplichtingen voor verwerkersovereenkomsten

Als er sprake is van een verhouding tussen de gemeente als verantwoordelijke en een externe 'verwerker', moeten deze partijen afspraken maken over hoe de verwerker omgaat met de persoonsgegevens en wie welke verantwoordelijkheden heeft.

Vanuit de gemeente gebruiken we een standaard modelovereenkomst. Deze standaard is in VNG-verband afgestemd met de belangrijkste leveranciers en voor alle gemeenten bindend verklaard (pas toe of leg uit). Deze leidraad gaat uit van deze gemeentelijke standaard.

Waar het niet mogelijk is om de gemeentelijke standaard te gebruiken (=onwenselijk) is het belangrijk om aandacht te hebben voor de volgende zaken: Vanuit de AVG is het niet verplicht een aparte verwerkers-overeenkomst af te sluiten, de afspraken mogen ook worden opgenomen in een andere overeenkomst (contract, SLA, etc..). Art 28 van de AVG beschrijft wat er verplicht opgenomen moet worden. Ook is het mogelijk een verwerkersovereenkomst van de leverancier te gebruiken. Let dan wel altijd extra goed op de afspraken die worden gemaakt, deze zijn immers vanuit het belang van de leverancier opgeschreven.

Vooraf: Opstellen conceptovereenkomst

Moet je een verwerkersovereenkomst afsluiten dan maak je een conceptovereenkomst op die je meestuurt met je offerteverzoek of meeneemt in de aanbesteding (net als de algemene voorwaarden). Dit is van belang omdat de verwerkersovereenkomst bepalingen bevat die randvoorwaardelijk zijn voor de overeenkomst. Niet meesturen kan achteraf tot vervelende consequenties leiden zoals dat het contract wel betaald, maar niet uitgevoerd mag worden.

Beschrijf de verwerking

Een verwerkersovereenkomst moet helder weerspiegelen waar het betrekking op heeft. Waar heeft de overeenkomst betrekking op. Dit wordt ingevuld in *Bijlage 1: Overzicht van te verwerken persoonsgegevens* van de standaard verwerkersovereenkomst.

Deel 1 'Neem verwerking, doeleinden, categorieën betrokkenen, soorten gegevens en doorgifte' wordt ingevuld voordat de verwerkersovereenkomst wordt meegestuurd in een aanbesteding / offerte-uitvraag. Waar de exacte invulling niet bekend is wordt volstaan met algemene informatie. Het doel is echter overal zo duidelijk mogelijk op te nemen wat de partij in kwestie gaat doen met welke gegevens van welke personen. Wijzigt dit gedurende de overeenkomst dan moet deze verwerkersovereenkomst worden geactualiseerd.

Mocht er sprake zijn van verwerking buiten de Europese Economische Ruimte (= Europese Unie + Noorwegen, IJsland en Liechtenstein) dan is er sprake van 'doorgifte naar derde landen'. Dit moet dan ook worden opgenomen in het gemeentelijke privacyregister. Daarbij moet worden vermeld op basis van welke uitzondering[1] dit toegestaan is, zoals uitgewerkt in hoofdstuk 5 van de AVG. Neem hiervoor contact op met je DISO.

Bepaal een passend niveau van beveiliging

In bijlage 2 van de standaard verwerkersovereenkomst neem je de gemeentelijke eisen op ten aanzien van de beveiliging. Deze stem je af op het risico dat gepaard gaat met wat de partij gaat doen. Dit is altijd een afweging die gemaakt moet worden. Doe dit samen met je inkoopadviseur en DISO.

Neem in de overweging de volgende zaken mee:

Om wat voor persoonsgegevens gaat het?

- Gaat het om gewone of bijzondere persoonsgegevens?
- Gaat het om veel gegevens (de absolute omvang), dus gegevens van veel personen?
- Gaat het om veel gegevens per persoon? Veel gegevens per persoon is risicovol omdat er dan qua misbruik meer mogelijk is (bijvoorbeeld door identiteitsdiefstal).
- Is de context van de gegevens gevoelig? (bijvoorbeeld een kwetsbare groep, of 'zandpad-klanten')

Wat gaat de verwerker met de persoonsgegevens doen?

- Gaat de verwerker de gegevens alleen opslaan, of gaat de verwerker meer 'verwerking' doen?
- Gaat de verwerker geautomatiseerd persoonsgegevens bijeen brengen of gegevens uit verschillende bronnen combineren? (dit wordt als bijzonder risicovol gezien);
- Wordt er gewerkt met (of via) veel subverwerkers en/of subsubverwerkers? Dus is er een ketenrisico?

Op basis van het risico denk je na over wat een passend niveau van bescherming is. Bescherming verankeren we op twee manieren in de verwerkersovereenkomst:

1. Een norm waar de beveiliging aan moet voldoen
2. Afspraken over de wijze van verantwoording óver de norm.

Hoe hoger het risico is dat gepaard gaat met de verwerking hoe hoger de norm is die je wil afspreken (strengere eisen en meer beveiligingsmaatregelen) en hoe meer zekerheid we als gemeente willen hebben over de naleving van de norm door de verwerker.

Tabel: denkkader voor norm en verantwoording

Risico inschatting	Norm	Verantwoording / assurance (zie ook bijlage 1)	Risico inschatting
Laag	Baseline Informatiebeveiliging Overheid [BBN1], ISO 27001 of gelijkwaardig.	Jaarlijkse zelfevaluatie met bespreking in contractoverleg (of met mededeling uitkomsten aan gemeente)	Laag

1 De volgende uitzonderingsgronden zijn er:

- Er is een adequaatheidsbesluit van de Europese Commissie.
- Er is sprake van bindende bedrijfsvoorschriften (binding corporate rules)
- Er is een contract met afdwingbare modelclausules.

	+Baseline Informatiebeveiliging Overheid [BBN2]	+ Een ISO 27001 certificering	
Hoog	+Baseline Informatiebeveiliging Overheid [BBN 3]	+ Een jaarlijkse assuranceverklaring (zie bijlage 1) van een onafhankelijke RE Auditor over het van toepassing verklaarde normenkader.	Hoog

De norm en de verantwoording dekken samen het risico af.

Afweging in relatie met andere factoren
Als je hebt bedacht wat wenselijk is qua bescherming is het zinvol om nog te kijken naar enkele andere zaken die daar mogelijk van invloed op zijn. Deze factoren kunnen ertoe leiden dat je andere normen of wijze van verantwoording opneemt dan ‘objectief gezien’ het meest optimaal is.

- Gelden er al normen voor deze sector of vanuit andere hoeken? Denk aan NEN7510 voor zorggegevens, DigiD normen bij een DigiD aansluiting of ISAE 3402 waar er een link is met de financiële verantwoording van de gemeente?
- Hoe ziet de markt eruit? Bestaan de mogelijke partijen allemaal uit multinationals of zijn het vaker eenmanszaken of het MKB die hierin acteert? En wat is hier ‘standaard’ qua beveiliging?
- Wat is de marktvolwassenheid qua gegevensbescherming? Zijn bedrijven in deze sector vaak al gecertificeerd voor gegevensbescherming of gelden er goedgekeurde privacy-gedragscodes?
- Staat de norm in verhouding met de verwerking? Als een leverancier een heel beperkte verwerking uitvoert, dragen dan alle onderdelen van het normenkader bij aan een passend beveiligingsniveau?
- Is er voor de verwerking al een DPIA gedaan waar bepaalde maatregelen uitkomen? En komen die terug in de norm?

Voor de afspraken rondom beveiliging is het handig om – indien mogelijk - aan te sluiten bij bestaande werkwijzen van de verwerker. Heeft deze een bepaalde certificering of systematiek dan is het wenselijk om daarbij aan te sluiten. De kans op naleving is dan het grootst en de impact voor de verwerker het kleinst. Bedenk hierbij dat we ook moeten *sturen* op datgene dat we afspreken. Hoe meer maatwerk we afspreken, hoe meer werk de jaarlijkse controle/sturing zal zijn.

Contractvorming: aanvullen en ondertekenen

Over de te sluiten verwerkersovereenkomst vindt vaak nog overleg of discussie plaats met de verwerker. Een deel van de afspraken is onderhandelbaar en een deel niet, in verband met wettelijke bepalingen. Degene die het contract sluit (de contractverantwoordelijke) voert het overleg en bepaalt uiteindelijk wat er wordt opgenomen in de overeenkomst. Deze kan de DISO en/of de jurist van het betreffende organisatieonderdeel vragen om advies. Komen zij er niet uit, dan kan CIPM of het privacy spreekuur benaderd worden voor een tweedelijns advies.

Ingeschakelde derden ('subverwerkers')

In Bijlage 1 van de standaard verwerkersovereenkomst wordt tevens opgenomen welke subverwerkers de verwerker mag inschakelen voor de uitvoering (realisatie) van de verwerking. Deze velden worden pas ingevuld als een partij is geselecteerd voor een opdracht.

> De verwerker mag een andere verwerker inschakelen: een subverwerker. Een subverwerker is een andere zelfstandige partij die in opdracht van de 1e verwerker (een deel) van de persoonsgegevens verwerkt. Deze subverwerker opereert zelfstandig, maar moet de persoonsgegevens wel verwerken volgens de schriftelijke instructies van de verwerkingsverantwoordelijke, net als de 1e verwerker. Als de verwerker een persoon inhuurt voor bepaalde werkzaamheden, hoeft dat niet automatisch te betekenen dat er sprake is van een subverwerker *(je DISO kan helpen bij de interpretatie hiervan).* De subverwerker heeft t.a.v. de gegevensbescherming dezelfde verplichtingen die de 1e verwerker heeft. Als de subverwerker zijn verplichtingen niet nakomt, blijft de 1e verwerker t.a.v. de gegevensbescherming volledig aansprakelijk voor het niet nakomen van de verplichtingen door de subverwerker. In het geval het niet (direct) mogelijk is om dezelfde afspraken te maken met een subverwerker (bv. In geval van multinationals als Microsoft/Google), dan moet de subverwerker in ieder geval voldoen aan de verplichtingen van de AVG. Ook na de ingangsdatum van de verwerkersovereenkomst moet de verwerker de verantwoordelijke informeren over de inschakeling van nieuwe subverwerkers. Verantwoordelijke heeft overeenkomstig artikel 28.2 AVG het recht om bezwaar te maken tegen een subverwerker. Als een verantwoordelijke daadwerkelijk bezwaar heeft tegen een subverwerker, gaan partijen hierover in overleg.

Beoordeel welke subverwerkers er worden ingeschakeld. Wij als gemeente stemmen in met deze subverwerkers en als wij zorgen hebben over de partij of de noodzaak van een subverwerker dan is het zinvol dat in deze fase te bespreken. Een subverwerker voert een deel van de verwerking uit zoals beschreven in bijlage 1 van de standaard verwerkersovereenkomst, check of dit klopt.

Let op: Verwerkt een subverwerker de persoonsgegevens buiten de Europese Economische Ruimte, denk dan aan het punt dat hierover is beschreven op pagina 2. Let op, wij moeten als verantwoordelijke altijd uitdrukkelijke toestemming geven voor de verwerking buiten de E.E.R. op grond van artikel 45 en 46 van de AVG. Dit staat ook expliciet in artikel 4.3 van de verwerkersovereenkomst.

De verwerker mag pas beginnen met zijn/haar werkzaamheden wanner alle afspraken zijn gemaakt; bevoegd ondertekend door beide partijen èn de afgesproken maatregelen daadwerkelijk zijn getroffen. Het is dus zaak de voorgaande stappen op tijd te starten. Begin niet pas vlak voordat de verwerker aan de slag moet!

Contractuele fase: Sturen en toezicht houden

Met het vastleggen van afspraken hebben we alleen nog maar aan onze ‘papieren plichten’ als verantwoordelijke voldaan. Vervolgens is de gemeente ook verplicht om erop toe te zien dat de afspraken nagekomen worden en hierop eventueel actie te ondernemen. Richt dus een proces in waarbij jaarlijks de beveiliging van de verwerker wordt gecontroleerd. Is een leverancier bijvoorbeeld gecertificeerd, controleer dan jaarlijks of hij dat nog steeds is. Twijfel je of de leverancier nog voldoet aan de afspraken, informeer dan je DISO.

Door periodiek te sturen zorg je ervoor dat het voor de partij in kwestie ook niet alleen een papieren werkelijkheid is, maar dat ze hier doorlopend aandacht voor moet hebben. Dit voorkomt dat dit thema van de radar verdwijnt, wat belangrijk is, want dat voorkomt datalekken.

Let er op dat wij als verantwoordelijke partij moeten kunnen laten zien dat we zorgen voor de bescherming van persoonsgegevens. Het contract zelf is daar één deel van, de sturing op het contract hoort daar onlosmakelijk bij. Leg dus bij het contract vast wat je aan controles hierop hebt gedaan zodat je – mocht het een keer mis gaan bij deze partij- altijd kunt laten zien dat wij onze verantwoordelijkheid hebben genomen.

Overweeg om voor je organisatieonderdeel of afdeling een register van verwerkers bij te houden om eventuele risico’s blijvend te kunnen beheersen.

Bijlage 1: Assuranceverklaring en certificering

Wat is ‘assurance’ en ‘certificering’?
Een assuranceverklaring of certificaat kan het toezien vergemakkelijken op afspraken met derden over onderwerpen zoals informatiebeveiliging of privacy. Afhankelijk van de afstand en de invloed die de gemeente heeft op een derde partij en de afgenomen dienstverlening kan een gemeente kiezen welke soort zekerheid gewenst is om sluitend te kunnen verantwoorden. Met een assuranceverklaring of certificaat wordt op een eenduidige manier verantwoording afgelegd. Als een assuranceverklaring of certificaat goed aansluit op de behoeften van de afnemer scheelt dit zowel de afnemer als de leverancier tijd en kosten.

Belangrijkste verschillen tussen een assuranceverklaring en een certificering

- Scope en diepgang
  Bij een certificaat ligt de nadruk op het toetsen of het managementsysteem functioneert. Bij een assurancerapportage ligt de focus op de naleving/het toetsen van individuele normen/ maatregelen.
- Inhoud
  Een assuranceverklaring is een redelijk uitgebreid document met daarin o.a. uitleg over het normenkader, de manier waarop getoetst is en eventuele bevindingen die geconstateerd zijn. Een certificaat is een stuk beperkter qua inhoud (meestal 1 a 2 pagina’s) en vertelt globaal de scope van het certificaat en de norm waartegen getoetst is.
- Eisen voor afgifte
  Een assuranceverklaring wordt afgegeven ongeacht of er afwijkingen zijn geconstateerd.
  Een certificaat wordt alleen afgegeven als de organisatie aan de eisen voor certificaat voldoet.
- Doelgroep en verspreiding
  Certificaten en assuranceverklaringen verschillen qua doelgroep en verspreidingskring. Een certificaat bevat algemene informatie over de scope en de norm en is gericht op meerdere doelgroepen zoals (potentiële)klanten, ketenpartners en andere belanghebbenden. Daardoor zal een certificaat ruimer gedeeld worden dan van een assuranceverklaring. Een assuranceverklaring is vooral gericht op klanten en is gevoeliger qua inhoud. Dit betekent dat een assuranceverklaring in de regel alleen gedeeld wordt met klanten die hier specifieke afspraken over hebben.
- Geldigheid
  Een assuranceverklaring zegt alleen iets over een periode in het verleden en is alleen geldig over die periode. Het geeft dus geen zekerheid over de toekomst. Een certificaat is gericht op het in control zijn rond informatiebeveiliging en is 3 jaar geldig vanaf de periode van afgifte. Een certificaat geeft dus ook enige zekerheid richting de toekomst.
- Audit tijd en kosten
  Voor een initiële certificeringsaudit is significant minder tijd nodig (gemiddeld ongeveer 25%) dan voor een initiële assuranceverklaring. Voor tussentijdse certificeringsaudits is de benodigde tijd nog veel minder (gemiddeld ongeveer 10%) ten opzichte van een assuranceverklaring. Dit vertaalt zich ook terug in de kosten, waarbij een assurance verklaring meestal significant duurder is dan een certificering.

Algemene aandachtspunten
Er is een aantal aandachtspunten dat voor alle typen assuranceverklaringen en certificaten geldt:

- De scope van de verklaring. Sluit deze aan op de dienst die afgenomen wordt? Als men bijvoorbeeld een SAAS dienst afneemt is een assuranceverklaring die enkel over de hosting gaat niet voldoende.
- Welke norm wordt gehanteerd?
- Welke controls van welke norm zijn in scope van de verklaring? Zijn die door te vertalen naar de BIO? En worden alle BIO maatregelen geraakt die je op basis van het risico van de dienst zou verwachten?
- Bij een ISO 27001 certificering hoort een document waarin staat beschreven welke maatregelen de partij in kwestie ‘passend’ vindt om te nemen. Certificering accepteren zonder beoordeling hiervan is vrij zinloos. Dit document heet ‘Verklaring van toepasselijkheid’ of ‘Statement of Applicability’.
- De bevoegdheid en kwalificaties van de auditor die de audit uitvoert. Afhankelijk van benodigde expertise moet in Nederland een assuranceverklaring worden afgegeven door een Register EDP (RE) auditor of een Register Accountant (RA).
- De positie van de auditor. In veel gevallen wordt een assuranceverklaring afgegeven door een externe auditor, dit kan echter ook een interne auditor zijn. Alhoewel de assuranceverklaring aan dezelfde kwaliteitseisen moet voldoen, kiest men vaak voor een externe auditor omdat deze een schijnbaar grotere onafhankelijkheid heeft.

De manieren van toetsing bij een assuranceverklaring

- In alle gevallen zal de verklaring door een onafhankelijke auditor afgegeven worden. De manier van toetsen van controls kan echter verschillen. In de meeste gevallen wordt er getoetst op opzet en bestaan of op opzet, bestaan en werking.
- Opzet: Betekent dat de auditor kijkt of een control beschreven is en eventueel of deze het risico (op papier) goed afdekt.
- Bestaan: Dit houdt in dat een auditor gaat kijken of de controls daadwerkelijk uitgevoerd worden zoals beschreven. Belangrijk om te weten is dat het hierbij om een momentopname gaat. Bij het toetsen op bestaan wordt ook de opzet meegenomen.
- Werking: Als er getoetst wordt op werking wordt er ook gekeken of de control over een bepaalde periode gefunctioneerd heeft. Meestal gebeurt dit op basis van samples waarbij over bijvoorbeeld een heel jaar gekeken wordt of de control gefunctioneerd heeft. Bij het toetsen op werking worden de opzet en bestaan ook mee getest. Toetsen op de werking geeft de meeste zekerheid, maar kost ook het meeste tijd.