Rijksinkoopsamenwerking
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Handreiking: *Wat doe je als inkoper of contractmanager bij verwerking van persoonsgegevens?*

Binnen de Europese Unie geldt sinds 25 mei 2018 de Algemene Verordening Gegevensbescherming (AVG). Aanvullend hierop valt binnen Nederland de Uitvoeringswet Algemene Verordening Gegevensbescherming (uAVG). Deze factsheet benoemt een aantal belangrijke zaken waar een inkoper of contractmanager rekening mee dient te houden voor het verwerken van persoonsgegevens bij de uitvoering van een overeenkomst.

Wat is de AVG en wat is de Uitvoeringswet AVG?

De AVG is een verordening vanuit de Europese Unie die rechtstreeks van toepassing is op Nederland en andere landen binnen de Europese Unie. In de AVG staat regelgeving over privacybescherming. De AVG is van toepassing zodra je persoonsgegevens van EU-burgers verwerkt. Maar ook als in de Europese Unie gevestigde organisaties of personen persoonsgegevens verwerken. De AVG stelt dat een verantwoordelijke voor een verwerking passende maatregelen neemt voor de privacyrisico's die met de verwerking van persoonsgegevens samenhangen.

Een aantal aspecten op het gebied van privacybescherming mogen EU-landen op nationaal niveau regelen. Nederland legde dit vast in de Uitvoeringswet Algemene Verordening Gegevensbescherming. Hiermee heeft ook de verordening een wettelijke basis in Nederland.

Wat zijn "persoonsgegevens"?

De AVG legt persoonsgegevens als volgt uit: *"alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon"*. (artikel 1, lid 1 AVG). Voorbeelden van persoonsgegevens zijn NAW-gegevens, telefoonnummer, e-mailadres etc.

Wat is "verwerken"?

De AVG legt "een verwerking" *als volgt uit: bewerking of een geheel van bewerkingen 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, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.* (artikel 1, lid 2 AVG)

Wat zijn de relevante rollen bij het verwerken van persoonsgegevens?

Verwerkingsverantwoordelijke
Een verwerkingsverantwoordelijke is de natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die, alleen of samen met anderen, het doel van- en de middelen voor de verwerking van persoonsgegevens vaststelt. De verwerkingsverantwoordelijke bepaalt welke persoonsgegevens worden verwerkt en welke technische- en organisatorische maatregelen worden genomen ter bescherming van deze gegevens.

Verwerker
Een verwerker is een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die voor een verwerkingsverantwoordelijke persoonsgegevens verwerkt. Wanneer bij de uitvoering van de overeenkomst de leverancier persoonsgegevens voor / namens de verwerkingsverantwoordelijke verwerkt, is dit de "verwerker".

Privacy officer /privacy jurist/CISO
Een privacy officer of een CISO adviseert de verwerkingsverantwoordelijke over te nemen technische- en organisatorische maatregelen ter bescherming van de persoonsgegevens. Een privacy jurist helpt bepalen in welke mate de AVG van toepassing is.

Inkoper of contractmanager
De inkoper en/of contractmanager stelt samen met een opdrachtgever vast of de opdrachtgever, als verwerkingsverantwoordelijke, persoonsgegevens door de leverancier laat verwerken bij de uitvoering van de overeenkomst. Is dit het geval? Dan stellen de inkoper of contractmanager samen met de opdrachtgever een verwerkersovereenkomst op.

Betrokkene
Een persoon van wie persoonsgegevens worden verwerkt.

Ontvangers
Personen, organisaties, instanties etc. welke persoonsgegevens van anderen ontvangen.

Wat doe je als inkoper of contractmanager als de leverancier namens de opdrachtgever bij de uitvoering van een overeenkomst persoonsgegevens verwerkt?

Dan stel je een verwerkersovereenkomst op.

Een inkoper of contractmanager stelt samen met de opdrachtgever een verwerkersovereenkomst op. Het vooraf uitvoeren van een Gegevensbeschermingseffectbeoordeling (GEB) helpt bij het opstellen van een verwerkersovereenkomst. Een GEB staat ook bekend als een Data Protection Impact Assessment (DPIA) of Privacy Impact Assessment (PIA). Voor sommige verwerkingen (bijvoorbeeld met een hoog privacyrisico) is het uitvoeren van een GEB verplicht. Het uitvoeren van een DPIA bestaat uit vier stappen:
1. Beschrijving kenmerken gegevensverwerkingen;
2. Beoordeling rechtmatigheid gegevensverwerkingen;
3. Beschrijving en beoordeling risico's voor de betrokkenen;
4. Beschrijving voorgenomen maatregelen.

Een DPIA is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. Je kunt daarna maatregelen nemen om de risico's te verkleinen. Het is aan de opdrachtgever om een DPIA uit te voeren. De rol van een contractmanager of inkoper is hierbij beperkt. Een DPIA bestrijkt in de regel het hele werkproces bij de opdrachtgever. De door de inkoper of contractmanager op te stellen overeenkomst, omvat bijvoorbeeld uitsluitend een applicatie of in te kopen dienstverlening voor dat werkproces.

Hoe stel je een verwerkersovereenkomst op[1]?
Een verwerkersovereenkomst verdeel je in twee onderdelen:
1. De artikelen (semi-generiek);
2. De bijlagen (specifiek).

[1] Uitgangspunt zijn de model verwerkersovereenkomsten en toelichtingen van de Rijksoverheid.

Hieronder een toelichting bij deze twee onderdelen.

De artikelen van een verwerkersovereenkomst
De artikelen leggen een aantal verplichtingen vast op basis van de AVG. Veel artikelen zijn generiek en hoef je als inkoper of contractmanager niet aan te passen. Wil je meer weten over de achtergrond van deze artikelen of het toepassingsbereik van de verwerkersovereenkomst? Lees dan de toelichting bij de verwerkersovereenkomst. Naast een aantal administratieve invul zaken maak je in artikelen 10 en 11 een aantal keuzes.

In artikel 10 leg je vast wat de leverancier moet doen met de verwerkte persoonsgegevens bij het einde van de overeenkomst. Denk aan het retourneren van de persoonsgegevens aan de opdrachtgever of het wissen van persoonsgegevens. Het is belangrijk om je bewust te zijn van deze keuze. Weeg dus zorgvuldig af of je al voor het einde van de overeenkomst over de persoonsgegevens wilt beschikken of dat de leverancier de persoonsgegevens al voor het einde verwijdert. In de artikelleden 2 en 3 geef je bij het retourneren van de persoonsgegevens aan binnen welke termijn en in welk bestandsformaat je de persoonsgegevens wilt ontvangen.

Artikel 11 gaat over het recht om audits (te laten) uitvoeren. Een verwerkingsverantwoordelijke heeft volgens de AVG een verantwoordingsplicht over de verwerking van persoonsgegevens. Dit artikel helpt je invulling te geven aan deze verantwoordingsplicht. Je kunt een leverancier namelijk verzoeken (afhankelijk van de gekozen optie) om aan te tonen dat hij voldoet aan de afspraken uit de verwerkersovereenkomst. Een opdrachtgever maakt zelf de keuze of hij een audit periodiek laat uitvoeren of dat hij juist op een zeker moment een bepaalde (onafhankelijke) verklaring wil over de naleving.

De bijlagen van de verwerkersovereenkomst:
De verwerkersovereenkomst heeft drie bijlagen. De eerste twee bijlagen zijn specifiek voor de verwerking. De derde bijlage is vaak specifiek per organisatie. De drie bijlagen zijn:
1. De Verwerking van Persoonsgegevens;
2. Passende technische en organisatorische maatregelen;
3. Afspraken betreffende Inbreuken in verband met Persoonsgegevens.

In de eerste bijlage geef je het onderwerp/aard en doel van de verwerking, het soort persoonsgegevens, beschrijving categorieën persoonsgegevens, beschrijving categorieën betrokkenen, beschrijving categorieën ontvangers van persoonsgegevens aan. Na een uitgevoerde DPIA, vul je de resultaten uit stap 1 van de DPIA in deze bijlage eenvoudig in.

In de tweede bijlage specificeer je de technische- en organisatorische maatregelen die een leverancier moet nemen in het kader van de bescherming van de te verwerken persoonsgegevens. Deze bijlage vul je eenvoudig met de resultaten uit stap 4 van de uitgevoerde DPIA.

In de derde bijlage beschrijf je de procedure - in het geval van een inbreuk in verband met persoonsgegevens (voormalige datalek-procedure). Je legt in deze bijlage vast op welke wijze de leverancier de opdrachtgever informeert over een (mogelijke) inbreuk op persoonsgegevens (ook wel datalek genoemd). Deze bijlage is vaak specifiek voor een organisatie, ongeacht het type opdracht.

Een inkoper of contractmanager stelt samen met de opdrachtgever de verwerkersovereenkomst op. De inkoper of contractmanager helpt de klant bij het opstellen van de artikelen in de verwerkersovereenkomst. De bijlagen vult de opdrachtgever zelf in. Natuurlijk kun je als contactmanager of inkoper de opdrachtgever helpen. Kom je er niet uit? Neem contact op met een specialist. Denk aan een privacy officer, privacy jurist, een CISO of een functionaris gegevensbescherming. Dit kan verschillen per organisatie.

Aansprakelijkheid
Leveranciers stellen regelmatig vragen over de aansprakelijkheid in relatie tot de risico's met de verwerking van persoonsgegevens. Aansprakelijkheid is een belangrijk thema. De toezichthouder op de AVG (=in Nederland de Autoriteit Persoonsgegevens) kan aan overheidsorganisaties boetes opleggen tot wel 20 miljoen euro. Daarnaast kunnen betrokkenen schaden verhalen, wanneer er fouten zijn gemaakt bij de verwerking van hun persoonsgegevens. Hier vind je het boetebeleid van de Autoriteit Persoonsgegevens.

Wanneer sluit je een verwerkersovereenkomst af?
Als een verwerkingsverantwoordelijke persoonsgegevens (al dan niet geautomatiseerd) laat verwerken door een derde, waarbij de verwerking onder het toepassingsbereik van de AVG valt. Bijvoorbeeld wanneer een ministerie een meldingenregistratiesysteem gebruikt om klachten van burgers te registreren en dit systeem als dienst afneemt van een derde partij.

Let op: Toets vooraf altijd goed of de opdrachtgever de verwerkingsverantwoordelijke is. Oftewel, of hij of zij het doel- & de middelen van de verwerking bepaalt. Bij een inspanningsverplichting is bijvoorbeeld geen sprake van een verwerking door een derde en daarom is het niet nodig een verwerkersovereenkomst af te sluiten.

Twijfel je?
Neem dan contact op met de privacyspecialist in jouw organisatie.

Hoe manage je een verwerkersovereenkomst?
Ook na het afsluiten van een verwerkersovereenkomst heeft deze overeenkomst aandacht nodig. Een goede verwerkersovereenkomst biedt opdrachtgevers de mogelijkheid om aan hun verantwoordingsplicht te voldoen. Bijvoorbeeld via audits. Een contractmanager kan toezien op naleving van het auditartikel en/of andere specifieke afspraken in een verwerkersovereenkomst. Daarnaast kunnen verwerkingen of daarmee samenhangende risico's tussentijds veranderen. Als contractmanager kun je hierop toezien en leg je waar nodig nadere afspraken vast.

Mag je persoonsgegevens buiten de Europese Unie verwerken?
Ja, indien aan een aantal voorwaarden is voldaan. Verwerkingen van persoonsgegevens die onder de reikwijdte van de AVG vallen, mogen alleen buiten de EU worden verwerkt op basis van één van de volgende voorwaarden:

- Doorgifte op basis van een adequaatheidsbesluit (artikel 45 AVG);
- Doorgifte op basis van passende waarborgen artikel 46 AVG);
- Doorgifte op basis van bindende bedrijfsvoorschriften (BCR) (artikel 47);
- Doorgifte op basis van specifieke uitzonderingen. (artikel 48 AVG).

Meer informatie over doorgifte van persoonsgegevens naar derde landen vind je ook op de website van de Autoriteit Persoonsgegevens.

Meer informatie over de AVG vind je hier:
- Algemene Verordening gegevensbescherming;
- Autoriteit Persoonsgegevens;
- Handleiding AVG en uitvoeringswet Algemene verordening gegevensbescherming.

Vragen?
Neem contact op met Daan Moerman.

Deze factsheet is geschreven vanuit het oogpunt van de Rijksoverheid.

Dit is een uitgave van

Rijsinkoopsamenwerking
Postbus 20011 | 2500 EA Den Haag
T 070 758 56 78
November 2022 | Publicatie-nr. 22408095

Partner in inkoop