VERWERKERSOVEREENKOMST

Wat is dit en wanneer af te sluiten volgens artikel 28 AVG?

Cuccibu, auteur Raneen Stanley
Cuccibook Verwerkersovereenkomsten

Uitgegeven door Cuccibu, Nederland

INHOUD

INTRODUCTIE

In deze digitale wereld ontkomen wij niet aan het verwerken van persoonsgegevens. In sommige gevallen wordt de verwerking van persoonsgegevens uitbesteed, uitgewisseld of overgedragen aan een andere partij. Wanneer bij de verwerking van persoonsgegevens meerdere, externe, partijen betrokken zijn, is het maken van (aanvullende) afspraken over de gegevensverwerking soms onvermijdelijk.

Als de verwerking van persoonsgegevens wordt overgedragen aan een externe partij, kan het in sommige gevallen nodig zijn om op grond van artikel 28 Algemene Verordening Gegevensbescherming (AVG), bepaalde afspraken schriftelijk vast te leggen.

Afhankelijk van de situatie kan een verwerkersovereenkomst worden gesloten tussen de partijen of de afspraken kunnen in een andere vorm overeenkomst worden gegoten. De meest voorkomende vorm in de praktijk om de eisen op grond van artikel 28 AVG vast te leggen, is het sluiten van een verwerkersovereenkomst.

Dit informatieboekje verschaft toelichting over het onderwerp verwerkersovereenkomsten. Er wordt een blik geworpen op de verschillende verhoudingen tussen partijen en de vorm waarin de afspraken gemaakt moeten worden. Ook kan aan de hand van een beslisboom in dit boekje nagegaan worden of het sluiten van een verwerkersovereenkomst al dan niet nodig is. Tot slot is er aandacht voor de borging en monitoring van verwerkersovereenkomsten.

Reduce Risk, Create Value!

VERWERKERSOVEREENKOMST

Wat is het?

In een verwerkersovereenkomst worden afspraken omtrent de omgang met en beveiliging van persoonsgegevens vastgelegd bij verwerking door een externe partij. Allereerst worden de rollen van de partijen weergegeven, zodat het duidelijk is wie de verwerkingsverantwoordelijke is en wie de verwerker is ten aanzien van de gegevensverwerking. Verder wordt onder andere aangegeven welke persoonsgegevens er zullen worden uitgewisseld, op welke concrete wijze de gegevens worden beveiligd, wat er dient te gebeuren in het geval van een datalek en wat er met de persoonsgegevens gebeurt aan het einde van de samenwerking.

Wanneer nodig?

De samenwerkende partijen dienen een verwerkersovereenkomst te sluiten in het geval een externe partij (verwerker) voor de andere partij (verwerkings-verantwoordelijke) persoonsgegevens gaat verwerken. Op grond van de AVG is de term ''verwerken'' een veelomvattend begrip. Dit kan namelijk het verzamelen, vastleggen, ordenen, bijwerken of wijzigen, raadplegen, verzenden of vernietigen, etc. van persoonsgegevens betreffen.[1]

Wanneer een verwerkings-verantwoordelijke een nieuw product aanschaft of een nieuwe dienst of applicatie wil inzetten, is het van belang om af te vragen of het nodig is om een verwerkersovereenkomst te sluiten. Bij bestaande samenwerkingen kan het ook nodig zijn dat er (alsnog) een verwerkersovereenkomst moet worden gesloten.

Hieronder volgt een aantal voorbeelden waarbij tussen de verwerkingsverantwoordelijke en verwerker een verwerkersovereenkomst nodig is:

- Uitbesteding van de salarisadministratie aan een externe partij;
- Aanschaf van een applicatie waarbij de leverancier via remote-access toegang kan verkrijgen tot de persoonsgegevens bij een eventueel incident of storing;
- Inschakelen van een extern bureau om een medewerkers enquête af te nemen;
- Aanschaf van een SaaS-oplossing bij een extern bedrijf, waarbij de software op eigen locatie is en beheer bij de verwerker plaatsvindt.

[1] Art. 4 lid 2 AVG.

PARTIJEN

Betrokken partijen
Eerder zijn de termen ''verwerkings-verantwoordelijke'' en ''verwerker'' genoemd. Om te bepalen wanneer er sprake is van een verwerkingsverantwoordelijke/verwerkers-relatie, worden de definities van beide rollen toegelicht. Op die wijze kan worden nagegaan of er sprake is van gegevensverwerking door een externe partij en dus of er een verwerkersovereenkomst nodig is.

De verwerkingsverantwoordelijke[2] is de partij die het doel en de middelen voor de gegevensverwerking vaststelt. Met andere woorden: het is de partij die beslist waarom de persoonsgegevens worden verwerkt en hoe dat gebeurt. De verwerkings-verantwoordelijke heeft de zeggenschap over hetgeen wordt verwerkt, kan instructies geven en heeft hier invloed op.

De verwerker[3] is de partij die persoonsgegevens verwerkt ten behoeve van de verwerkingsverantwoordelijke. Een verwerker gebruikt de ontvangen persoonsgegevens alleen voor de doelen die de verwerkingsverantwoordelijke heeft bepaald. Een verwerker kan soms de middelen (tool, systeem, etc.) kiezen die worden ingezet om de doelen te bereiken.

Gezamenlijke verwerkingsverantwoordelijkheid
Bij sommige samenwerkingen is er niet één specifieke partij als verwerkings-verantwoordelijke of verwerker aan te wijzen, maar hebben beide partijen een gelijksoortige rol. In een dergelijk geval wordt van gezamenlijke verwerkings-verantwoordelijken[4] gesproken.

Deze horizontale samenwerking vindt plaats op basis van gedeelde verantwoordelijkheid, waarbij een bedrijf of rechtspersoon samen met een andere partij, het doel en de middelen voor de verwerking van persoonsgegevens bepalen. In zulke gevallen hoeft geen verwerkersovereenomst te worden gesloten, maar kan volstaan worden met een samenwerkingsconvenant dan wel een privacyovereenkomst.

Denk in zulke gevallen aan de uitvoering van wetenschappelijke onderzoeken of de samenwerking tussen een aantal gemeenten op een bepaald gebied of aan een belastingsamenwerking.

Twee zelfstandige verwerkingsverantwoordelijken
Als een bedrijf persoonsgegevens verwerkt voor haar eigen doeleinden en deze gegevens deelt met een ander bedrijf die de persoonsgegevens ook voor eigen doelen verwerkt, dan spreken we van twee zelfstandige verwerkings-verantwoordelijken. Ieder bedrijf legt de doelen en middelen vast voor het eigen proces. In deze is de aanbeveling om een gegevensuitwisselingsovereenkomst te sluiten.

[2] Art. 4 lid 7 AVG.
[3] Art. 4 lid 8 AVG.
[4] Art. 26 AVG.

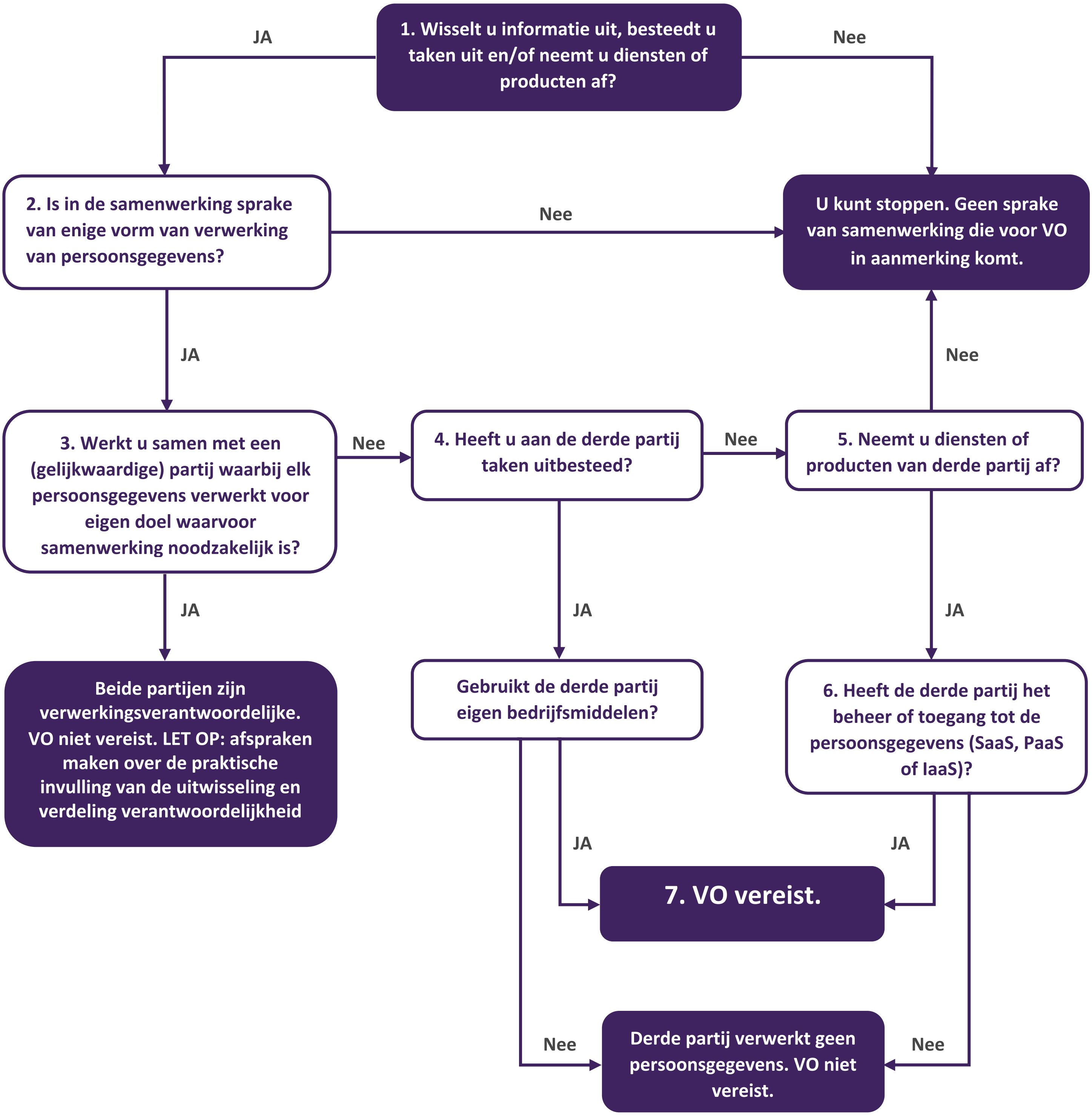
VERWERKERSOVEREENKOMST NODIG?

Om na te gaan of een verwerkersovereenkomst nodig is, is het van belang dat de verwerkingsverantwoordelijke stil staat bij de onderstaande vragen (geen cumulatieve vragen). De vragen zijn opgesteld aan de hand van praktijksituaties en iedere situatie is anders en moet apart worden beoordeeld.

1. Worden de persoonsgegevens uitbesteed, uitgewisseld of worden producten of diensten afgenomen?
2. Worden de persoonsgegevens in opdracht van de verwerkingsverantwoordelijke verwerkt?
3. In hoeverre heeft de verwerker invloed op de verwerking?
4. Worden persoonsgegevens aan een externe partij verstrekt, waarbij de instructies en doeleinden voor de verwerking van de persoonsgegevens door de verwerkingsverantwoordelijke worden bepaald?
5. Worden persoonsgegevens verstrekt aan een externe partij in het kader van kwaliteitsregistraties of (wetenschappelijk) onderzoek of andersoortige samenwerkingen, waarbij het om identificeerbare personen gaat?
6. Kan de externe partij inzage (eventueel van een afstand) verkrijgen in de persoonsgegevens?

BESLISBOOM

Om te bepalen of de verwerkingsverantwoordelijke een verwerkersovereenkomst (VO) dient te sluiten, kan onderstaande beslisboom worden doorlopen.



TOELICHTING BESLISBOOM

1. Inventariseer of persoonsgegevens buiten het bedrijf om worden uitgewisseld dan wel overgedragen of uitbesteed. Ook al is de intentie niet het laten verwerken van persoonsgegevens door een externe partij, kan er toch sprake zijn van gegevensuitwisseling[1]. Bij twijfel vraag advies aan de juridische afdeling en/of privacy en IT. De proceseigenaar of afdelingshoofd/manager neemt de lead in het sluiten van de verwerkersovereenkomst en de leverancier levert aanvullende informatie aan.

2. Het begrip verwerken heeft een ruime definitie o.g.v. artikel 4 lid 2 AVG. Let wel op dat anonieme gegevens niet onder de AVG vallen (artikel 11 AVG) en gepseudonimiseerde gegevens wel. Bij anonieme gegevens is er geen enkele informatie voorhanden is waarbij de identiteit van de personen tot natuurlijke personen valt te herleiden. Bij gepseudonimiseerde gegevens worden de persoonsgegevens getransformeerd in een dataset die niet direct herleidbaar is tot de natuurlijke personen. Alleen met een ''toegangssleutel'' kan men toegang tot de overige gegevens verkrijgen en ze koppelen om volledige persoonsgegevens te verkrijgen.

3. Ga na of het aandeel in de samenwerking tussen de partijen van gelijkwaardige aard is. Zijn de partijen gezamenlijke verantwoordelijken of betreft het een horizontale samenwerking?

4. Ga na of het doel en eventueel de middelen door de verwerkingsverantwoordelijke worden vastgesteld. Is er sprake van gezagsverhouding tussen de samenwerkende partijen en geeft de verwerkingsverantwoordelijke instructies bij de uitvoering van de werkzaamheden?

5. In sommige gevallen is de gezagsverhouding niet gelijk duidelijk en is het niet duidelijk welke partij de instructies geeft. Bij het bepalen van een verwerkingsverantwoordelijke/verwerkersrelatie dient nagegaan te worden of een van de volgende situaties of een combinaties hiervan, zich voordoet:

- structurele verwerking; en/of
- uitbesteden aan een externe partij; en/of
- uitwisseling van persoonsgegevens; en/of
- externe partij heeft toegang tot de gegevens.

6. Ga na of de verwerker daadwerkelijk inzage heeft in de persoonsgegevens. In sommige gevallen kan de verwerker op afstand hulp aanbieden of de persoonsgegevens voor eigen doeleinden hergebruiken, bijvoorbeeld ter verbetering van de applicatie. In andere gevallen kan de applicatie ook als opslag voor de gegevens dienen en heeft de verwerker geen toegang of inzage in de gegevens.

7. In een verwerkersovereenkomst dient gespecificeerd te worden welke persoonsgegevens worden verwerkt, voor welke doeleinden en hoe lang de persoonsgegevens zullen worden bewaard. Daarnaast dient de verwerker aan te geven welke technische en organisatorische beveiligingsmaatregelen zijn getroffen om de persoonsgegevens te beveiligen en te beschermen.

Nadat de verwerkersovereenkomst is ingevuld met specificaties over persoonsgegevens en beveiligingsmaatregelen, moet het ter advies en beoordeling aan de Privacy Officer en de (Chief) Information Security Officer worden voorgelegd. De (Chief) Information Security Officer beoordeelt de beveiligingsmaatregelen.

BEVEILIGINGSMAATREGELEN

De AVG benoemt in art. 28 een aantal onderwerpen die in een verwerkersovereenkomst moeten worden geregeld. Een van de onderwerpen is het treffen van passende technische en organisatorische beveiligingsmaatregelen[5] op de verwerkte persoonsgegevens. Des te gevoeliger de persoonsgegevens, des te strenger de eisen rondom de beveiliging. Bijvoorbeeld: persoonsgegevens als naam en werk e-mailadres vallen in risicogroep laag en gezondheidsgegevens en etnische gegevens vallen in risicogroep hoog.

Onderstaande schema illustreert een voorbeeld van de minimale beveiligingsmaatregelen die kunnen worden gevraagd door de verwerkingsverantwoordelijke.

Minimum beveiligingseisen	Risicogroep		
	Laag	Midden	Hoog
Twee-factor-authenticatie			X
Beveiligd mailen		X	X
Logging op toegang en wijzigingen		X	X
Encryptie op transfer	X	X	X

[5] Art. 32 AVG.

BORGING EN MONITORING

Opstellen Verwerkersovereenkomst
Een verwerkersovereenkomst dient te worden opgesteld, nageleefd, gemonitord en gewijzigd indien relevante veranderingen optreden. Wat betreft het opstellen van verwerkersovereenkomsten; de meeste bedrijven zijn ondertussen in het bezit van een standaardmodel verwerkersovereenkomst. Bij het aangaan van een samenwerking wordt het standaardmodel aangeboden of wordt gebruik gemaakt van het standaardmodel van de wederpartij. Een aantal brancheorganisaties beschikt over een eigen standaardmodel verwerkersovereenkomst. Denk hierbij aan de zorg (BOZ/NVZ-model) en gemeenteland (VNG-model).

Naleving
De bepalingen in de verwerkersovereenkomsten dienen door zowel de verwerkingsverantwoordelijke als verwerker te worden nageleefd. Indien dit niet gebeurt, kan er sprake zijn van een tekortkoming in de nakoming, oftewel wanprestatie. De naleving van een verwerkersovereenkomst moet worden geïntegreerd in het contractmanagement (eventueel binnen de afdeling inkoop of juridische afdeling). Wanneer een samenwerking wordt aangegaan, beëindigd of processen/applicaties worden gewijzigd, dient naast de aanpassing van de hoofdovereenkomst ook de verwerkersovereenkomst te worden aangepast. Deze wijzigingen kunnen ook effect hebben op de gegevensverwerking. Om die reden dient nagegaan te worden of alle gemaakte afspraken omtrent de gegevensverwerking nog steeds van toepassing zijn.

Monitoring
Verder dient de naleving van de verwerkersovereenkomst jaarlijks te worden gemonitord. Op grond van de verwerkersovereenkomst heeft de verwerkingsverantwoordelijke het recht om een audit uit te laten voeren. Hierbij kan de naleving van de gegevensverwerking en beveiligingsmaatregelen worden gecontroleerd. De audit geschiedt door een externe onafhankelijke auditor of een interne auditor van de verwerkingsverantwoordelijke. Een interne medewerker dient aangewezen te worden om de opdracht tot het uitvoeren van een audit in gang te zetten. De afdeling inkoop of juridische afdeling kan de lead nemen in de monitoring van de verwerkersovereenkomst. Dit wordt gedaan in samenwerking met de Privacy Officer en de (Chief) Information Security Officer.

SLOTWOORD

De European Data Protection Board heeft relevante richtlijnen geschreven om de rol van de verwerkingsverantwoordelijke en verwerker vast te stellen.[6] Aan de hand hiervan kan door jouw organisatie nagegaan worden of het nodig is om een verwerkersovereenkomst te sluiten. Toch komen in de praktijk vele grijze gebieden voor omtrent het aangaan en de inhoud van een verwerkersovereenkomst.

Wil je meer informatie over het sluiten en naleven van verwerkersovereenkomsten of wil je dat wij deze taak voor jou op ons nemen?

Neem dan contact op via info@cuccibu.nl | +31 (0) 85 303 2984.

Reduce Risk, Create Value!

---

[6] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 2 September 2020.

In een wereld die in toenemende mate digitaliseert, zorgt Cuccibu ervoor dat de onbegrensde mogelijkheden van deze wereld worden benut op een verantwoorde en veilige manier. Cuccibu helpt organisaties met vraagstukken op het vlak van informatiebeveiliging, privacy, cyber security en audit/compliance. Onze professionals op deze gebieden hebben de achtergrond en ervaring om met creatieve en heldere oplossingen iedere organisatie, groot of klein, te helpen!

www.cuccibu.nl | Cuccibu B.V. | Boutenslaan 195 C | Eindhoven | KvK 61072923 | info@cuccibu.nl | +31 (0) 85 303 2984