



TOOLKIT

Checklist verwerkersovereenkomst



DPO Consultancy
Experts in Data Privacy

Wanneer moet je een verwerkersovereenkomst hebben?

Als organisatie deel je persoonsgegevens met andere organisaties voor verschillende redenen. Bijvoorbeeld bij het uitbesteden van de boekhouding of het opslaan van persoonsgegevens in een clouddienst. In bijna alle gevallen waarbij je persoonsgegevens deelt, ben je verplicht een verwerkersovereenkomst af te sluiten en te zorgen dat je alle regels naleeft die daarin zijn opgenomen. Het afsluiten van deze overeenkomst is verplicht voor zowel de verwerkingsverantwoordelijke en de verwerker.

Wie zijn de verwerkings-verantwoordelijke & verwerker?

De verwerkingsverantwoordelijke is de organisatie die het doel en de middelen van het gebruik van de persoonsgegevens bepaalt. Een werkgever is bijvoorbeeld verantwoordelijk voor de persoonsgegevens van werknemers en een gemeente is verantwoordelijk voor persoonsgegevens van inwoners. De verwerker is de organisatie aan wie de personeelsadministratie wordt uitbesteedt of de clouddienstverlener waar persoonsgegevens worden opgeslagen.

Waar is de verwerkers-overeenkomst voor bedoeld?

Als verwerkingsverantwoordelijke blijf je altijd verantwoordelijk voor de persoonsgegevens die je verwerkt. Je werknemers, klanten, burgers of patiënten hebben hun gegevens immers met jouw organisatie gedeeld en niet met een verwerker. Daarom stel je samen een verwerkersovereenkomst op, waarin je juridisch de verantwoordelijkheden regelt en vastlegt wat er moet gebeuren met de gegevens en hoe dat gedaan moet worden. Zo voorkom je dat een andere partij persoonsgegevens voor eigen doelen verwerkt. Het is mogelijk om verschillende verwerkingen die één partij voor je uitvoert op te nemen in een verwerkersovereenkomst.

Hoe stel je een verwerkers-overeenkomst op?

Een verwerkersovereenkomst is een juridisch document. Je mag geen afspraken opnemen die in strijd zijn met de Algemene Verordening Gegevensbescherming (AVG). Daarmee loop je het risico dat je wet- en regelgeving overtreedt. Om dat te voorkomen is het goed om te weten welke zaken er wettelijk in een verwerkersovereenkomst moeten staan. Met deze checklist helpen we je organisatie om daar grip op te krijgen. Daarnaast geven we je ook enkele tips welke zaken je verder nog op kan nemen in een verwerkersovereenkomst, om onduidelijkheden te voorkomen. Zo houd je altijd controle over de situatie.

“It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you’ll do things differently.”

Warren Buffett

Wat staat er wettelijk in een verwerkersovereenkomst?

Bij het opstellen van een verwerkersovereenkomst ben je wettelijk verplicht om een aantal onderwerpen vast te leggen. We zetten ze kort op een rij:

	Wettelijke verplichting	Toelichting
	Is er een duidelijke omschrijving van de aard en het doel van de verwerking?	In de overeenkomst moet een omschrijving staan van het doel en de aard van de verwerking. Bijvoorbeeld dat je de personeelsadministratie uitbesteedt aan een boekhouder om de salarissen uit te betalen.
	Is er een duidelijke omschrijving van de duur van de verwerking?	Er moet omschreven zijn welke bewaartermijnen worden gehanteerd bij de verwerking en hoe gegevens worden verwijderd. Bijvoorbeeld dat gegevens maximaal een jaar mogen worden bewaard, nadat ze zijn verwerkt.
	Is er een duidelijke omschrijving van de (categorieën van) persoonsgegevens die worden verwerkt?	De categorieën van persoonsgegevens moeten duidelijk beschreven zijn. Maak bijvoorbeeld onderscheid tussen NAW-gegevens, contactgegevens, betaalgegevens, medische gegevens, IP-adressen, creditcardgegevens en inloggegevens.
	Is er een duidelijke omschrijving van de (categorieën van) betrokkenen van wie persoonsgegevens worden verwerkt?	Bijvoorbeeld klanten, websitebezoekers, werknemers, patiënten, cliënten etc. Houd er rekening mee dat je soms van meerdere categorieën tegelijkertijd gegevens verwerkt.
	Is het duidelijk dat de verwerker verplicht is om de instructies van de verwerkingsverantwoordelijke op te volgen?	Hier moet duidelijk omschreven zijn dat de verwerker zijn werkzaamheden uitsluitend verricht op basis van instructies van de verwerkingsverantwoordelijke.
	Wordt de verwerker verplicht om mee te werken aan het uitvoeren van een Data Protection Impact Assessment (DPIA) of andere risicobeoordelingen?	Wanneer er een DPIA of risicobeoordeling moet worden uitgevoerd bij een verwerking, wil je dat een verwerker daaraan meewerkt. Dat moet je ook wettelijk opnemen in de overeenkomst.

	Wettelijke verplichting	Toelichting
	Wordt de verwerker verplicht om mee te werken aan audits, waaronder inspecties die worden uitgevoerd door de verwerkingsverantwoordelijke of een onafhankelijke partij?	Als een verwerker is ingeschakeld, is het belangrijk dat die verwerker meewerkt aan mogelijke audits die gedaan kunnen worden bij het verwerken van persoonsgegevens. Zo kan (tussentijds) beoordeeld worden of een verwerker voldoet aan de eisen van de AVG.
	Is de verwerker verplicht om mee te werken of hulp te verlenen bij verzoeken van betrokkenen?	Betrokkenen hebben volgens de AVG het recht om hun gegevens in te zien, te laten verwijderen, bezwaar te maken etc. Wanneer ze een beroep doen op dit recht, moet de verwerker hieraan meewerken.
	Garandeert de verwerker de vertrouwelijkheid van gegevens, ook onder medewerkers?	Een verwerker heeft een vertrouwelijkheidsplicht bij het verwerken van persoonsgegevens en moet die verplichting ook vertalen naar de medewerkers die met de gegevens werken. Bijvoorbeeld door een geheimhoudingsclausule in het arbeidscontract op te nemen.
	Wordt er beschreven welke exacte technische en organisatorische beveiligingsmaatregelen een verwerker heeft genomen?	Een verwerker moet passende technische en organisatorische maatregelen treffen om de verwerking zo veilig mogelijk uit te voeren. In de verwerkersovereenkomst moet worden gespecificeerd welke maatregelen de verwerker heeft genomen.
	Voldoen de beveiligingsmaatregelen aan de wettelijke vereisten van de AVG?	Bij beveiligingsmaatregelen gaat het voornamelijk om de wettelijke vereisten volgens Artikel 32 van AVG, waar specifieke voorwaarden worden genoemd waar de beveiliging van de verwerking minimaal aan moet voldoen.
	Zijn er afspraken in de overeenkomst opgenomen over het melden van een datalek en binnen welke termijn dat moet gebeuren?	Wanneer een datalek plaatsvindt bij een verwerker moet de verantwoordelijke dit binnen 72 uur melden bij de Autoriteit Persoonsgegevens. Daarom is het van belang dat de verwerker het datalek zo snel mogelijk meldt bij de verwerkingsverantwoordelijke.

	Wettelijke verplichting	Toelichting
	Is het duidelijk of persoonsgegevens worden verwerkt buiten de Europese Economische Ruimte?	Als er persoonsgegevens buiten de EU worden verwerkt (bijvoorbeeld bij een cloudleverancier in de US) moeten er aanvullende maatregelen worden getroffen om de transfer buiten de EU mogelijk te maken.
	Wordt de verwerker verplicht om voorafgaand schriftelijk toestemming te vragen van de verwerkingsverantwoordelijke als de verwerker een sub-verwerker in wil zetten?	Voor het aanhaken van een sub-verwerker (een verwerker die wordt ingeschakeld door een verwerker) is toestemming nodig van de verwerkingsverantwoordelijke. Dit moet worden opgenomen in de overeenkomst.
	Is het duidelijk wat er met de persoonsgegevens gedaan moeten worden, bijvoorbeeld na het aflopen van het contract of bij een calamiteit?	In de verwerkersovereenkomst moet duidelijk beschreven staan wat er met de persoonsgegevens gebeurt bij teruggave of het einde van een opdracht, maar ook als de gegevens verloren zijn gegaan en/of om technische redenen niet kunnen worden geretourneerd.
	Is het duidelijk wat er is afgesproken over de aansprakelijkheid van de verwerker, ook als afspraken niet worden nagekomen?	Een belangrijk onderdeel van een verwerkersovereenkomst is aansprakelijkheid. Wie is waarvoor verantwoordelijk en tot welke hoogte in het geval van boetes/claims van betrokkenen? Daarover wil je vooraf goede afspraken hebben gemaakt.

Wat is slim om verder op te nemen in de verwerkersovereenkomst?

Naast de bovengenoemde verplichte onderdelen van een verwerkersovereenkomst, zijn er ook belangrijke zaken die niet genoemd worden in de wet. Hieronder zetten we de belangrijkste zaken op een rij die niet in de AVG staan, maar wel handig zijn om op te nemen in de verwerkersovereenkomst.

		Toelichting
	Bevat de overeenkomst de naam en adresgegevens van ondergetekende en de naam van een Data Protection Officer (indien van toepassing)?	Het is goed om te weten door wie de overeenkomst is ondertekend en of de organisatie een DPO heeft zodat deze ook benaderd kan worden als er vragen zijn.
	Is het duidelijk wanneer de overeenkomst in werking treedt?	Neem altijd de startdatum van de overeenkomst op, om onduidelijkheid daarover te voorkomen.
	Is het duidelijk wie de verwerker is en wie de verwerkings-verantwoordelijke is?	In de overeenkomst moet duidelijk beschreven zijn wie de verwerker en wie de verantwoordelijke is voor de verwerking is. Beide hebben namelijk ook andere verplichtingen in de AVG.
	Is er een duidelijke omschrijving van de opdracht en het soort verwerking dat een verwerker uitvoert.	Een verwerkersovereenkomst is altijd onderdeel van een algemene overeenkomst (zoals een SLA) waarin de diensten zijn beschreven die worden geleverd voor de verwerking. Deze beschrijving moet ook terug te vinden zijn in de verwerkersovereenkomst.
	Staat in de overeenkomst welke wetgeving van toepassing is en dat de verwerking plaatsvindt in overeenstemming met de regels van de AVG?	Bij iedere verwerking van persoonsgegevens heb je een rechtsgrond nodig. Dit is raadzaam om op te nemen in de overeenkomst, zodat er geen onduidelijkheid kan ontstaan over de reden waarom een verwerker persoonsgegevens ontvangt.
	Beschrijft de overeenkomst dat de toegang tot persoonsgegevens voor medewerkers van de verwerker beperkt is?	Een verwerker heeft vaak een aantal medewerkers die de daadwerkelijke verwerking verricht. Het is goed om op te nemen hoe zij toegang krijgen tot de persoonsgegevens en welke afspraken er zijn gemaakt over autorisatie binnen de organisatie van de verwerker.

		Toelichting
	Wordt er regelmatig gerapporteerd over de beveiligingsmaatregelen?	De maatregelen die een verwerker neemt moeten wettelijk worden vastgelegd in de overeenkomst. Daarnaast wil je dat er ook gerapporteerd wordt over deze maatregelen om te toetsen of de maatregelen ook effectief zijn in de praktijk. Denk aan een periodieke audit of andere manieren om vast te stellen of de afspraken nagekomen worden.
	Is duidelijk beschreven hoe een verwerker melding moet doen van een datalek?	Een verwerker is verplicht om de verantwoordelijke op de hoogte te brengen van een datalek. Daarom is wenselijk om afspraken te maken over welke informatie zij moeten aanleveren en hoe ze dat moeten doen. Zodat je als verantwoordelijke weet dat je de juiste informatie krijgt om een datalek binnen de kaders van de wetgeving te melden.
	Is duidelijk aangegeven wie er verantwoordelijk is voor de juistheid, kwaliteit en rechtmatigheid van de verwerking en op welke wijze de persoonsgegevens worden verzameld?	Als een verwerker wordt ingeschakeld om persoonsgegevens te verwerken, kan het zomaar zijn dat de gegevens veranderen in de loop van de tijd. Het is goed om in de overeenkomst op te nemen hoe deze veranderingen worden doorgegeven tussen beide partijen en wie ze verwerkt.
	Bevat de overeenkomst een medewerkingsplicht bij het off-boarden van persoonsgegevens?	Zodra het contract met een verwerker afloopt, moeten er afspraken zijn over wat er met de data moet gebeuren. Bijvoorbeeld dat de verwerker alle persoonsgegevens verwijderd zodra de samenwerking stopt.
	Is er duidelijk aangegeven dat de verwerker de persoonsgegevens niet mag gebruiken voor andere doeleinden dan die zijn overeengekomen in de verwerkersovereenkomst?	De AVG staat verwerkingen alleen toe als er een duidelijk doel is voor deze verwerking. Deze doelen moeten ook door de verwerker worden gehanteerd en daar mag niet van worden afgeweken. Dat staat meestal wel vermeld in een normale overeenkomst, maar niet altijd in verwerkersovereenkomst.
	Staat er in de overeenkomst dat de verwerker de verwerkingsverantwoordelijke direct informeert als de ingezette middelen in strijd zijn met de AVG?	Als de verwerker zelf een verandering doorvoert binnen zijn organisatie (technisch of organisatorisch) wat een conflict met de vereisten uit de AVG kan opleveren, is de verwerker verplicht om de verantwoordelijke hiervan op de hoogte te stellen.



Conclusie

Met een goede verwerkersovereenkomst zorg je ervoor dat de afspraken tussen verwerkingsverantwoordelijke en verwerker duidelijk op papier staan. Hiermee voorkom je dat er onduidelijkheid bestaat over afspraken tussen beide partijen wanneer het gaat over de verwerking van persoonsgegevens. Het voordeel van een gedegen verwerkersovereenkomst is dat bij een calamiteit of andere aangelegenheid met persoonsgegevens altijd kan worden teruggevallen op de afspraken die zijn opgenomen in deze overeenkomst en iedere partij weet van elkaar wat de verplichtingen over en weer zijn.

**Kom je er niet helemaal uit, of heb je
nog aanvullende vragen bij specifieke
onderwerpen? Neem dan contact met ons op
via info@dpoconsultancy.nl of **+31 85 0711080****

Australiëlaan 12a
5232 BB 's-Hertogenbosch
the Netherlands

Rue du Congres 35
1000 Brussel
Belgium

1 Lyric Square
London, W6 0NB
England

+31 850 711 080
info@dpoconsultancy.nl
www.dpoconsultancy.com

