



TOOLKIT



Checklist register van verwerkingen

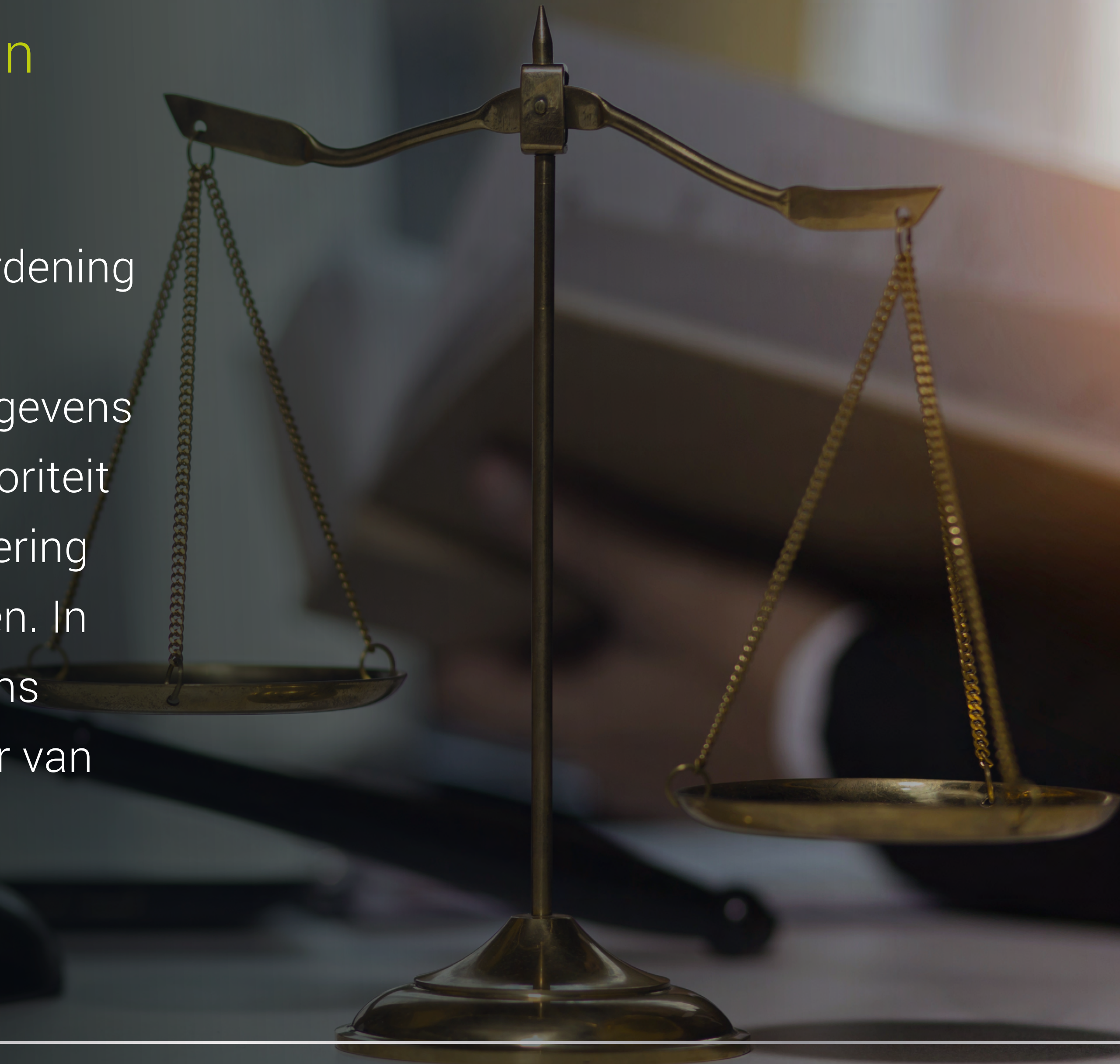


DPO Consultancy
Experts in Data Privacy

Jeremy Bode

Waarom heb je een register van verwerkingen nodig?

Voor de komst van de Algemene Verordening Gegevensbescherming (AVG) waren organisaties verplicht om persoonsgegevens die ze verwerkten te melden bij de Autoriteit Persoonsgegevens (AP). Door de invoering van de AVG is deze meldplicht vervallen. In plaats daarvan zijn organisaties volgens de wetgeving verplicht om een register van verwerkingen bij te houden.



Een register moet worden bijgehouden wanneer je als organisatie meer dan 250 personen in dienst hebt. Een organisatie met minder dan 250 personen moet een register bijhouden als een of meer van de volgende situaties van toepassing is:

- Je verwerkt structureel persoonsgegevens. In de praktijk zijn veel verwerkingen van persoonsgegevens structureel. Denk bijvoorbeeld aan een nieuwsbrief aan klanten die je ieder kwartaal verstuurd of salarisbetalingen die je elke maand doet.
- Je verwerkt persoonsgegevens die een hoog risico hebben voor de rechten en vrijheden van de personen van wie je de persoonsgegevens verwerkt. Denk aan het opstellen van klantprofielen of het verwerken van grote hoeveelheden gegevens (gegevens van grote groepen personen óf heel veel gegevens van een paar personen).
- Je verwerkt gevoelige gegevens die vallen onder de categorie 'bijzondere persoonsgegevens', zoals gegevens over gezondheid, strafrechtelijke gegevens, ras of etnische afkomst, politieke opvattingen en geloofsovertuigingen.

Wat is een verwerking van persoonsgegevens?

Het begrip 'verwerking' heeft betrekking op allerlei verschillende verwerkingen van persoonsgegevens, zowel handmatig of geautomatiseerd uitgevoerd. Eigenlijk wordt bijna alles wat je met persoonsgegevens doet gezien als een verwerking. Enkele voorbeelden:

- De personeels- en salarisadministratie
- Het raadplegen van een bestand met contactgegevens van personen
- Het verzenden van een nieuwsbrief of andere marketing-gerelateerde e-mails
- Het versnipperen van documenten met persoonsgegevens
- Het plaatsen van foto's van personen op een website
- Het opslaan van IP-adressen

“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 is een register van verwerkingen?

Een register van verwerkingen is een document waarin alle verwerkingen die een organisatie doet bijgehouden worden. Daarmee krijgt je inzicht in de verwerkingen binnen je organisatie en kun je voldoen aan de verantwoordingsplicht van de AVG. Als de Autoriteit Persoonsgegevens je organisatie vraagt om een register van verwerkingen, moet je kunnen aantonen welke persoonsgegevens je verwerkt en waarom.

Hoe stel je een register van verwerkingen op?

Het register van verwerkingen is een levend document dat je als organisatie voortdurend aanvult met nieuwe verwerkingen en update als er zaken bij een verwerking veranderen. In het document worden herhaalde en eenmalige verwerkingen opgenomen. Voor een nieuwsbrief die je per kwartaal verstuurd of de salarisadministratie maak je dus één keer een verwerking aan. Je hoeft dus niet voor iedere nieuwsbrief opnieuw een verwerking te registreren. Bij activiteiten die slechts eenmalig plaatsvinden moet je wel iedere keer een nieuwe verwerking aanmaken.

Als organisatie mag je zelf bepalen hoe je het register opstelt. Veel organisaties kiezen ervoor om het register bij te houden in Excel. Bij een klein aantal verwerkingen is dit een prima optie, maar het is behoorlijk foutgevoelig en bewerkelijk als je tientallen of honderden verwerkingen registreert. Daarom zijn er verschillende (online) tools beschikbaar die de mogelijkheid bieden om het register op een veilige, gebruiksvriendelijke en snelle manier samen te stellen en aan te vullen.



Checklist register van verwerkingen

Met deze checklist leggen we je uit welke zaken je volgens de AVG in een register van verwerkingen moet opnemen. Daarnaast geven we ook een toelichting bij ieder punt en leggen we uit waar je rekening mee moet houden.

	Wettelijke verplichting	Toelichting
	De naam en contactgegevens van verantwoordelijke of diens vertegenwoordiger, wanneer de verantwoordelijke buiten de EU is gevestigd.	In de meeste gevallen ben je als organisatie zelf de verantwoordelijke. Als je organisatie van buiten de EU komt, maar gegevens verwerkt van mensen in de EU ben je verplicht om een Data Protection Representative (DPR) aan te stellen. Dat is je vertegenwoordiger binnen de EU en het aanspreekpunt voor de AP en betrokkenen als ze vragen hebben over verwerkingen van persoonsgegevens.
	Voor welke doeleinden worden de gegevens verwerkt?	Waar heb je deze gegevens voor nodig en hoe verwerk je ze? Bijvoorbeeld voor de werving en selectie van personeel, het bezorgen van producten of direct marketing. Je hebt altijd een duidelijk en weloverwogen doel nodig. Als je dat niet hebt, mag je geen persoonsgegevens verwerken. Daarnaast is het aan te raden om ook de grondslag te vermelden voor elk van uw verwerkingen. Je bent dit niet verplicht, maar het kan wel helpen om in een later stadium aan je verantwoordingsplicht te voldoen.
	Welke categorie persoonsgegevens verwerk je?	Je hoeft niet exact te beschrijven welke gegevens je gaat verwerken. De categorie is voldoende, als het maar duidelijk is waar het over gaat. Maak bijvoorbeeld onderscheid tussen NAW-gegevens, contactgegevens, betaalgegevens, medische gegevens, IP-adressen, creditcard-gegevens en inloggegevens.

	Wettelijke verplichting	Toelichting
	Van welke categorie betrokkenen verwerk je gegevens?	Hierbij beschrijf je de categorieën van personen van wie je gegevens verwerkt. Bijvoorbeeld klanten, websitebezoekers, werknemers, patiënten, cliënten etc. Houd er rekening mee dat je soms van meerdere categorieën tegelijkertijd gegevens verwerkt. Bijvoorbeeld bij een nieuwsbrief. Die stuur je mogelijk naar klanten en websitebezoekers.
	Aan welke categorie ontvanger worden de gegevens verstrekt?	Deze categorie is niet altijd van toepassing. Ontvangers zijn de partijen aan wie je de persoonsgegevens verstrekt. Bijvoorbeeld als gemeente bent je wettelijk verplicht om gegevens te verstrekken aan de belastingdienst. Voor een organisatie kan het bijvoorbeeld gaan om het verstrekken van persoonsgegevens aan een accountant, verzekeraar of de belastingdienst.
	Deel je gegevens met een land of internationale organisatie buiten de EU?	Dit is van toepassing als je gebruikmaakt van diensten die buiten de EU gevestigd zijn. Een goed voorbeeld hiervan is het opslaan van persoonsgegevens in de cloud bij een dienstverlener uit de Verenigde Staten. Als je dat doet, ben je verplicht om dat aan te geven in het register van verwerkingen. Meestal vul je hier de partij in waarvan je de dienst afneemt. Het is ook aan te raden om toe te lichten op grond van welk recht je gegevens deelt buiten de EU.
	Hoe lang bewaar je persoonsgegevens en wanneer worden deze gewist?	Het kan zijn dat je wettelijk verplicht bent om persoonsgegevens een aantal jaar te bewaren en/of dat je gegevens langer bewaart, omdat je klanten bijvoorbeeld tien jaar garantie geeft op bepaalde producten en daarom de noodzaak ziet om persoonsgegevens te bewaren. Dergelijke bewaartermijnen leg je hier vast.
	Hoe zijn de persoonsgegevens beveiligd?	Hier geef je een algemene beschrijving van de technische en organisatorische maatregelen die je hebt genomen om de persoonsgegevens die je verwerkt te beveiligen. Denk bij technische maatregelen aan encryptie, logische toegangscontrole en pseudonimisering. Bij de organisatorische maatregelen neem je onder andere een geheimhoudingsverklaring en de verwerkersovereenkomst op.



Aan de slag

Door een register van verwerkingen op te stellen, heb je altijd controle over welke persoonsgegevens je verwerkt binnen je organisatie, in welke systemen deze zich bevinden en voor welke doelen je deze verzameld. Zo is altijd inzichtelijk wat je met persoonsgegevens doet en waar je deze voor gebruikt. Bij een calamiteit is het dan ook eenvoudig terugzoeken welke gegevens er betrokken kunnen zijn bij deze calamiteit.

**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

Congresstraat 35
1000 Brussels
Belgium

19 The Square
RETFORD
Nottinghamshire
DN22 6DQ
England

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

