



## Algemene Verordening Gegevensbescherming (AVG)



**Vanaf 25 mei 2018 geldt de Algemene Verordening Gegevensbescherming (AVG). Dat betekent dat vanaf deze datum dezelfde privacyregels gelden in alle landen van de Europese Unie.**

### Waarom nieuwe privacyregels?

De huidige regels zijn opgesteld in een tijdperk waarin het internet nog in de kinderschoenen stond. De nieuwe wet is aangepast aan het digitale tijdperk. We delen onze persoonsgegevens steeds vaker. Soms bewust, vaak onbewust. Deze gegevens worden ergens opgeslagen. En vervolgens gebruikt en soms gedeeld en verkocht. De nieuwe privacywet zorgt ervoor dat onze gegevens beter worden beschermd. Organisaties krijgen meer verplichtingen en moeten in heldere taal uitleggen welke gegevens ze gebruiken.

### Wat voegt de AVG toe?

De Algemene Verordening Gegevensbescherming (AVG) sluit beter aan op het digitale tijdperk waarin we leven en heeft als doel om je meer controle te geven over jouw persoonsgegevens. We informeren je graag over hoe wij hiermee omgaan en wat dit voor jou betekent.

### Wat betekent de AVG voor jou?

Post Risicobeheer werkt met persoonsgegevens en verwerkt ook persoonsgegevens van jou. Deze gegevens zijn noodzakelijk voor de uitvoering van onze dienstverlening. Wij zijn de afgelopen maanden druk bezig geweest om ons voor te bereiden op de AVG. Op onze website vind je onze aangepaste [Dienstenwijzer](#) en [Privacyverklaring](#). Hierin lees je alles over wat we doen om jouw gegevens te beschermen en wat de AVG voor jou betekent.

### Wat kun je van ons verwachten?

In onze [privacyverklaring](#) kun je lezen dat wij zorgvuldig omgaan met jouw gegevens. Hierin staat welke gegevens we verzamelen, waarom we dat doen en hoe lang we deze gegevens bewaren. Mocht je hier toch nog vragen over hebben, neem dan gerust contact met ons op.

[Privacyverklaring >](#)

## Verwerkersovereenkomst niet nodig bij advies werknemersvoorzieningen en -regelingen



**Als werkgever hoef je geen verwerkersovereenkomst met ons te sluiten voor het treffen van regelingen ten aanzien van werknemers (bijv. voor verzuim- en inkomensverzekeringen). Weliswaar verstrek je hiervoor persoonsgegevens van medewerkers aan ons, maar daarmee worden wij nog niet gezien als 'Verwerker' in de zin van de wet.**

Dit blijkt uit de AVG en de uitleg die het ministerie van Justitie en Veiligheid hier aan geeft. Het enkele feit dat een derde partij in opdracht van een werkgever werknemersgegevens verwerkt, maakt hem nog niet tot een 'Verwerker'. Een derde partij kan op grond van de privacyregelgeving namelijk ook de positie van een 'Verwerkingsverantwoordelijke' hebben. Dit is het geval als het verwerken van de gegevens van de werknemers *geen primaire opdracht* is ten behoeve van de werkgever, maar logischerwijs voortvloeit uit een vorm van dienstverlening die de derde partij aanbiedt. Deze situatie doet zich voor bij de dienstverlening van een financieel adviseur aan de werkgever bij het adviseren en bemiddelen bij regelingen voor werknemers.

Uiteraard zijn wij (als verwerkingsverantwoordelijke) onverminderd verplicht zeer zorgvuldig met de verkregen werknemersgegevens om te gaan in overeenstemming met de privacyregels uit de AVG.

## Cyberrisicoverzekering



AUTORITEIT  
PERSOONSGEGEVENS

**Sinds de invoering van de Wet bescherming persoonsgegevens op 1 januari 2016 is het verplicht om binnen 72 uur een datalek te melden.**

**Doe je dat niet, dan loop je het risico op een hoge boete, die kan oplopen tot € 820.000,-. Vanaf de invoering van de AVG worden de regels alleen maar strenger en kan de boete voor het niet juist omgaan met persoonsgegevens oplopen tot 4% van de wereldwijde omzet of € 20.000.000,-.**

**Een cyberrisicoverzekering kan je helpen om dit risico te beperken! Maar wat voor dekking biedt nu zo'n verzekering?**

### Controle basis veiligheid

Op grond van de AVG dient elk bedrijf een minimale basis van cyberveiligheid te hebben. In het aanvraagproces voor een cyberrisicoverzekering wordt deze basis via de acceptatievragen doorgenomen.

### Onderzoek wel of geen toegang door onbevoegden

Bij een beveiligingsincident volgt een meldplicht indien niet uitgesloten is dat persoonsgegevens door onbevoegden zijn ingezien. Denk aan een situatie van tijdelijk verlies van een laptop. Via een cyberrisicoverzekering krijg je direct toegang tot deskundigen die vaak kunnen vaststellen of er wel of geen onbevoegden kennis hebben genomen van je data. Het niet hoeven melden is uiteraard een te verkiezen situatie. Door gegevens versleuteld op te slaan, kan ook een situatie worden voorkomen dat bij verlies een meldingsplicht ontstaat.

### Ondersteuning bij melding aan AP

Indien een datalek wel aan de Autoriteit Persoonsgegevens moet worden gemeld, leidt dit tot de nodige correspondentie. Via een cyberrisicoverzekering krijg je hierbij in veel gevallen ondersteuning door een gespecialiseerd advocatenkantoor.

### Ondersteuning bij melding aan klanten

Bij een datalek waarbij persoonsgegevens verloren zijn gegaan die een grote impact kunnen hebben op de privacy van betrokkenen, dienen deze betrokkenen individueel te worden gewaarschuwd. Zijn er heel veel betrokkenen dan dient dit te worden vervangen door het plaatselijke pers. Beiden leveren veel werk en kosten op. Ook hierin voorziet de cyberrisicoverzekering. De dekking kan zelfs voorzien in adequate begeleiding door een (crisis) communicatiebureau.

### Herstel beschadigde data

Hebben onbevoegden zich toegang tot de data verschaft dan zal gecontroleerd moeten worden of zij data hebben aangepast. De gemanipuleerde data zal moeten worden hersteld. Controle en herstel brengen kosten met zich mee. De praktijk rondom ransomware laat zien dat het hier om aanzienlijke kosten kan gaan.

### Verweer claims

De AVG geeft eenieder (dus niet alleen klanten!) het recht om in verband met materiele en immateriële schade als gevolg van het niet voldoen aan de eisen van de AVG deze op de aansprakelijke partij te verhalen. Naast de vergoeding van deze schade kan de verzekering ook belangrijk zijn in verband met het weerstaan van (soms volstrekt) onterechte claims.

### Boetes Autoriteit Persoonsgegevens

Een boete van de AP valt niet onder de dekking van een beroeps- en/of bedrijfsaansprakelijkheidsverzekering. In de reguliere cyberrisicoverzekeringen zijn boetes gedekt. Wel staat hierbij dat de boetes conform wet- en regelgeving verzekeraar moeten zijn.

Hiermee is de organisatie en/of de bestuurder echter niet gevrijwaard voor alle mogelijke boetes en aansprakelijkheden op grond of als gevolg van de AVG. Naast een datalek kan op basis van de AVG ook op andere gronden een boete worden opgelegd; bijvoorbeeld rondom dataportabiliteit, weigering tot inzage geven in het dossier, het verzamelen van gevoelige informatie zonder noodzaak etc. Deze boetes zijn over het algemeen niet verzekerd.

**Wil je meer weten over de mogelijkheden van een cyberrisicoverzekering?**

**Neem dan gerust contact met ons op!**



