



## Factsheet

### Privacy Nulmeting



## Privacy nulmeting uitvoeren?

De Europese Algemene verordening gegevensbescherming (AVG) heeft gevolgen voor de governance en compliance van de organisatie. Ook de hoogte van de sancties is aanleiding om gegevensbescherming hoog op de agenda van bestuurders te plaatsen.

Om aan de eisen van deze wet- en regelgeving te voldoen, zal de organisatie inzicht moeten hebben in de eigen 'organisatiestructuur', inclusief de verbonden partijen waarmee contractuele relaties bestaan.

*Centrale vraag is: 'heb ik een helder overzicht en inzicht van de risico's en aansprakelijkheden die voortkomen uit de wetgeving voor bescherming van persoonsgegevens en de mate van beheersing van deze risico's?'*

Om dit inzicht te verkrijgen bieden wij het uitvoeren van de privacy nulmeting aan. De gegevensbescherming nulmeting is een verkennend onderzoek gericht op het verkrijgen van inzicht in de naleving van wet- en regelgeving op het vlak van gegevensbescherming. Het onderzoek geeft de verantwoordelijke, raad van bestuur en raad van commissarissen, inzicht in de mate waarin de risico's zijn afgedekt door maatregelen en de effectieve werking van deze maatregelen.

### **Wat is de toegevoegde waarden?**

Een organisatie moet zich vergewissen dat technische en organisatorische maatregelen getroffen zijn om de risico's af te dekken en dat deze maatregelen effectief werken. Immers, als een maatregel ontbreekt dan wel niet effectief is gebleken en dit geleid heeft tot een datalek, dan moet de organisatie dit datalek meestal melden aan de Autoriteit Persoonsgegevens (AP) en in een aantal gevallen ook aan de betrokkene. Als de organisatie niet in staat is om een datalek zelf te signaleren – en melding achterwege blijft – kan het hierop aangesproken worden door de AP of één of meer betrokkene(n). Dit kan leiden tot boetes en claims.

Ook uw partners in de keten willen weten in hoeverre uw organisatie voldoet aan de wetgeving. Als uw organisatie een verwerker is, dan is de verwerkingsverantwoordelijke verplicht na te gaan of uw organisatie voldoet aan de AVG.

De gegevensbescherming nulmeting levert tevens een document op dat u kan overhandigen aan uw accountant. Deze accountant kan gebruik maken van dit document ter ondersteuning van diens eigen controlewerkzaamheden. Hierdoor kunt u de accountantskosten verlagen.

## De verantwoordingsplicht

De AVG kent een verantwoordingsplicht voor bedrijven en instellingen. Deze plicht houdt in dat organisaties op elk moment moet kunnen aantonen dat de maatregelen ter bescherming van de persoonsgegevens ook echt werken en dat de bepalingen van de AVG worden nageleefd.

De verantwoordingsplicht brengt onder meer met zich mee dat er overzicht en inzicht moet zijn in de verwerkingen, dat het gegevensbeschermingsbeleid moet zijn verankerd in de organisatie en wordt nageleefd en dat de effectieve werking van de informatiebeveiliging moet kunnen worden aangetoond. Daarbij komt dat de verantwoordingsplicht ook betrekking heeft op het verwerken van persoonsgegevens waarvoor de organisatie externe partijen (verwerkers en subverwerkers) heeft ingeschakeld.

De samenvatting uit de rapportage van de gegevensbescherming nulmeting kan worden opgenomen in het Bestuurdersverslag waardoor de organisatie hiermee voldoet aan een governance verplichting.

## Wat is onze aanpak?

Het onderzoek kent een praktische aanpak: samen met u wordt een eerste stap gezet op weg naar een gezonde huishouding voor het beschermen van persoonsgegevens. Tijdens het onderzoek worden beschikbare beleidsdocumenten beoordeeld en worden interviews gehouden met medewerkers en/of stakeholders. De daarbij verkregen inzichten worden afgezet tegen de eisen die worden gesteld aan het verwerken van persoonsgegevens, de beoordeling van de mate waaraan uw organisatie voldoet aan de eisen met betrekking tot gegevensbescherming. Dit gebeurt aan de hand van een normenkader, dat gebaseerd is op de relevante wet- en regelgeving voor de organisatie.

Het onderzoek resulteert in een verslag van bevindingen en bijbehorend advies. Dit advies voorziet onder andere in een globale aanpak voor uw organisatie hoe vervolgstappen te zetten om de gegevensbescherming en het borgen van de privacy naar een hoger niveau te brengen en compliant te worden. Hierbij maken we gebruik van een volwassenheidsmodel met 5 niveaus.

Activiteiten tijdens het onderzoek:

- Normenkader gericht op de organisatie vaststellen;
- Inventarisatie van de belangrijkste verwerkingen;
- Toetsen aan het normenkader: interviews, documentatie en eigen onderzoek;
- Opstellen rapport van bevindingen, actieplan en presentatie; *en*
- Afstemming en onvoorziene werkzaamheden.

De diepgang van de gegevensbescherming nulmeting en gedetailleerdheid van de rapportage worden bepaald door de scope van het onderzoek en de beschikbare tijd.

## Heeft u vragen of behoefte aan een afspraak?

Wij voeren al meer dan 20 jaar privacy nulmetingen bij veel verschillende opdrachtgevers uit. Wij hebben ervaring in verschillende sectoren en beschikken over kennis en kunde. Wij werken efficiënt en effectief om de opdrachtgever zo goed mogelijk te bedienen.

Ingeval van vragen of u wilt een vrijblijvende offerte ontvangen, aarzelt u niet contact met ons op te nemen. Dit kan via +31 (0)70 – 392 22 09 of [info@duthler.nl](mailto:info@duthler.nl).





Afspraak maken en contact

Wilt u meer weten? Neem dan contact op met ons op via de onderstaande gegevens. Of bezoek onze website: [www.duthler.nl](http://www.duthler.nl)

**Kantoor:**

Frankenslag 137

2582 HH Den Haag

+31 (0) 70 392 22 09

[info@duthler.nl](mailto:info@duthler.nl)

