

Bent u klaar voor de Europese Privacy Verordening?

Wat de verzwaring van de privacywetgeving betekent voor uw organisatie en welke acties u moet ondernemen

Data
protection



Privacybescherming niet langer vrijblijvend voor organisaties

Elke organisatie verwerkt privacygevoelige informatie. Het wordt bewaard, gedeeld en bewerkt. Naast personeelsgegevens betreft het gegevens van klanten en/of consumenten. In veel gevallen gaat het om bijzondere persoonsgegevens. Bijvoorbeeld om gegevens die extra gevoelig zijn vanwege hun medische karakter of omdat deze van financiële aard zijn.

Organisaties moeten in kunnen staan voor de adequate bescherming van aan hen toevertrouwde gegevens. De wetgever maakt in toenemende mate organisaties expliciet verantwoordelijk voor de bescherming van persoonsgegevens. Deze trend is per 2016 ingezet met de aanscherping van de Wet Bescherming Persoonsgegevens (Wbp), met name door de meldplicht datalekken en de hieraan gekoppelde boetebevoegdheid. Deze trend zet zich tot en met medio 2018 voort, wanneer de Europese privacyverordening, General Data Protection Regulation (GDPR) van kracht zal zijn. Deze nieuwe verordening stelt aanvullende eisen aan gegevensbescherming door organisaties.

Veel organisaties kennen de nieuwe eisen onvoldoende en worstelen met de praktische vertaling van de nieuwe verplichtingen.

De nieuwe verordening stelt aanvullende eisen voor gegevensbescherming. Veel organisaties kennen de nieuwe eisen onvoldoende en worstelen met de praktische vertaling van de nieuwe verplichtingen.



De belangrijkste veranderingen

Vanaf 25 mei 2018 is de General Data Protection Regulation (GDPR) van toepassing. In het Nederlands heet deze regelgeving de Algemene Verordening Gegevensbescherming (AVG).

Organisaties moeten aantonen dat ze voldoen aan de nieuwe verordening die op 25 mei 2018 ingaat. Dat vergt inspanningen en investeringen. Zo dient u een verwerkingsregister op te stellen, waarmee u onder

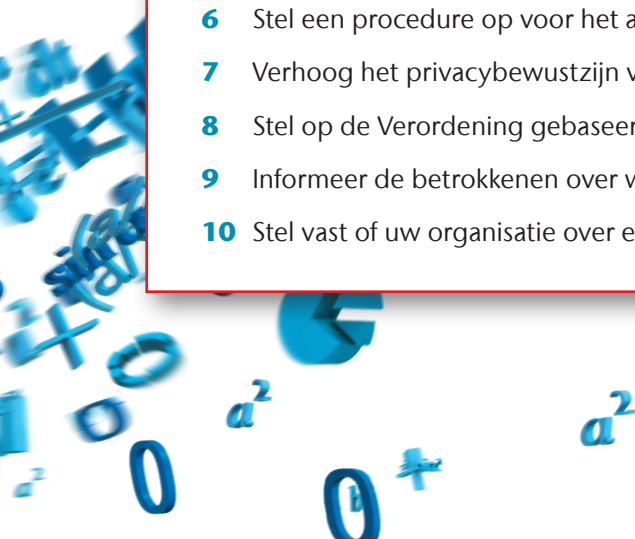
andere moet bijhouden welke persoonsgegevens uw organisatie verwerkt, wat de verwerkingsdoeleinden zijn, hoe lang de gegevens worden bewaard en welke maatregelen zijn getroffen om privacyrisico's te beperken.

U dient alles volgens de nieuwe verordening te doen, te documenteren, te evalueren, te wijzigen en te verbeteren. De boetes voor het niet voldoen aan de wettelijke vereisten kunnen oplopen tot EUR 20 mln of 4% van de omzet van uw organisatie.

Dit staat u te doen

Om te voldoen aan de nieuwe verordening staat u het volgende te doen.

- 1** Veranker privacy- en gegevensbescherming op het hoogste niveau binnen uw organisatie
- 2** Voer een analyse uit om uw privacyrisico's te identificeren en middels passende technische en organisatorische maatregelen te beheersen (DPIA)
- 3** Maak een verwerkingsregister met daarin de vastlegging hoe privacygevoelige gegevens worden verwerkt.
- 4** Classificeer uw persoonsgegevens zodanig dat u voldoet aan wettelijke bewaartermijnen én zodat u gegevens tijdig kunt verwijderen
- 5** Evalueer bestaande contracten met partijen waarmee u gegevens deelt.
U bent verplicht verwerkersovereenkomsten te sluiten
- 6** Stel een procedure op voor het adequaat anticiperen en afhandelen van een datalek
- 7** Verhoog het privacybewustzijn van uw medewerkers door gerichte activiteiten
- 8** Stel op de Verordening gebaseerd privacybeleid op of pas het bestaande beleid hierop aan.
- 9** Informeer de betrokkenen over wat er met hun persoonsgegevens gebeurt
- 10** Stel vast of uw organisatie over een functionaris gegevensbescherming moet beschikken



Aon helpt u te voldoen aan de verordening

Aon kan u op vier manieren ondersteunen om aan de nieuwe eisen te voldoen:

1. Voldoet u aan de nieuwe privacy-eisen? - [GDPR volwassenheidstoets](#)
2. Welke privacyrisico's loopt u en hoe beheerst u deze momenteel? - [Privacy-risicobeoordeling](#)
3. Voldoen aan de nieuwe verordening voor 25 mei 2018 - [Privacy-actieplan](#)
4. Samen zorgen wij voor de implementatie van privacy-vereisten! - [Implementeren maatregelen](#).

1 GDPR volwassenheidstoets

Doel

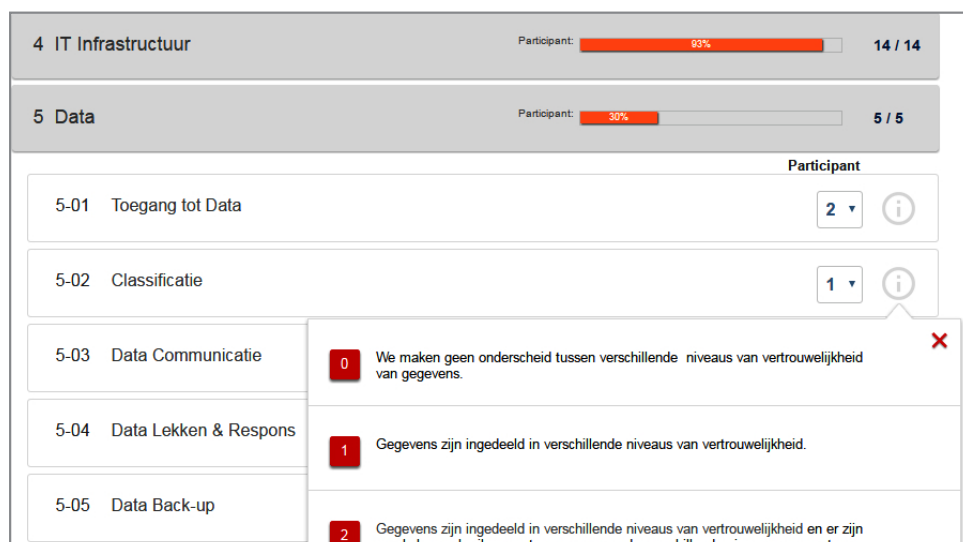
Middels een nulmeting toetsen wij in hoeverre u momenteel voldoet aan de nieuwe privacy-vereisten en welke aanvullende maatregelen noodzakelijk zijn.

Werkwijze

Aon's GDPR volwassenheidstoets wordt ondersteund door een webgebaseerde Self Assessment Tool. Deze biedt makkelijke en veilige toegang via ons webportaal AonLine. Op basis van Aon's advies en de resultaten uit de tool toetsen we in hoeverre u voldoet aan de wetgeving.

Resultaat

- Inzicht in uw huidige volwassenheid inzake de privacy-vereisten.



2 Privacy-risicobeoordeling

Doel

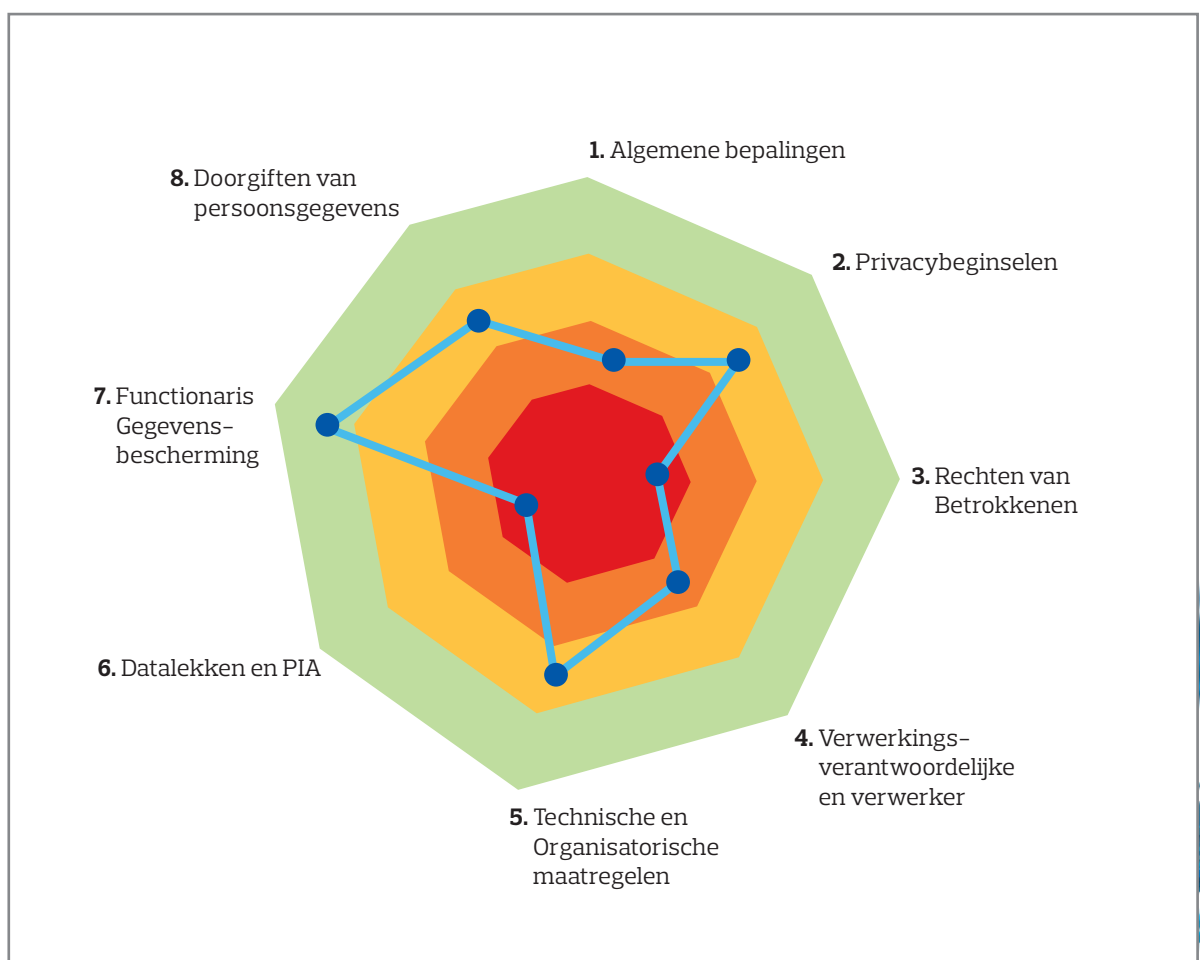
Vaststellen welke privacyrisico's écht relevant zijn voor uw organisatie, inschatten en prioriteren van deze risico's en het achterhalen van de huidige beheersmaatregelen.

Werkwijze

Na het uitvoeren van Aon's risicoanalyse zijn uw privacyrisico's geïdentificeerd en wordt duidelijk welke passende technische en organisatorische maatregelen u moet treffen.

Resultaat

- Een uitgebreid risicoprofiel;
- Een duidelijk geprioriteerde basis voor een actieplan.



3

GDPR actieplan

Doel

Een compacte actiegericht rapportage die inzicht geeft in de inspanningen en investeringen die noodzakelijk zijn om te kunnen voldoen aan de GDPR.

Werkwijze

In de rapportage leggen wij de verbeteracties vast die uw organisatie kan uitvoeren om te voldoen aan de nieuwe verordening. Er wordt rekening gehouden met de belangrijkste privacyrisico's die uw organisatie loopt. Samen bepalen we welke acties prioriteit hebben en wie de actie-eigenaar wordt.

Resultaat

Het actieplan geeft inzicht in de vereisten en aanvullende beheersmaatregelen vanuit verordening. We maken een planning (inclusief deadlines) met daarin de taken die moeten worden uitgevoerd. Het actieplan wordt gebaseerd op de resultaten vanuit de GDPR volwassenheidstoets en de Privacy-risicobeoordeling. Hiermee kunnen de belangrijkste privacyrisico's tijdig worden beheerst.

4

Implementatie privacymaatregelen

Doel

Het implementeren van de privacyvereisten waaraan uw organisatie nog moet voldoen.

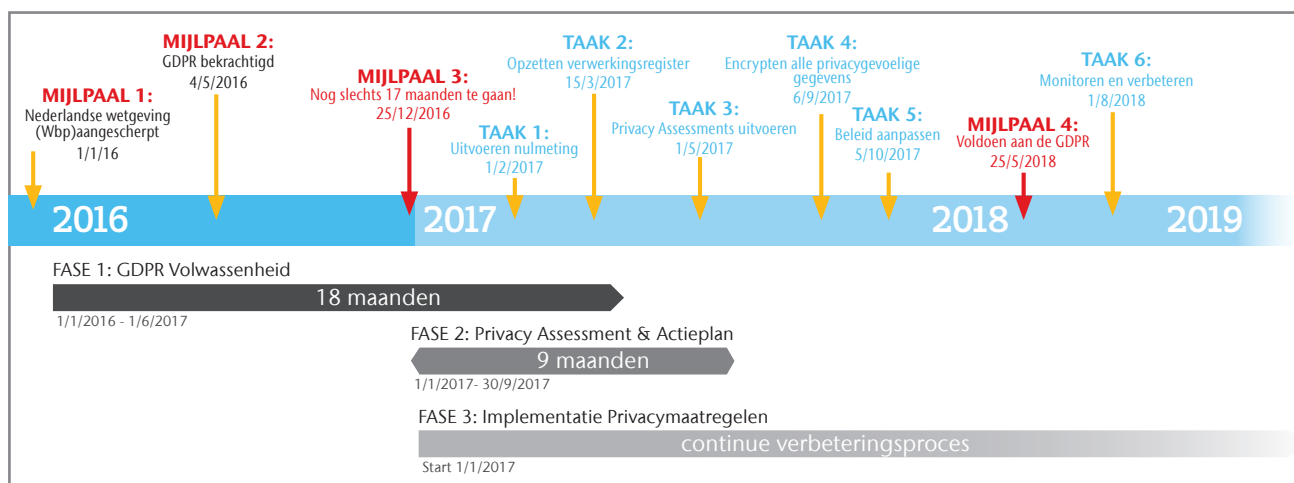
Werkwijze

Door middel van het actieplan kunnen wij u helpen bij het implementeren van privacyvereisten, eventueel samen met onze IT en juridische partners. Te denken valt daarbij aan de implementatie van:

- Data Privacy Impact Assessment
- Passende technische en organisatorische maatregelen
- Opstellen verwerkingsregister
- Dataclassificatie
- Protocol datalekken
- Bewustwordingscampagne
- Beoordelen contracten en verwerkersovereenkomsten
- Optimaliseren/opzetten privacy- en informatie-beveiligingsbeleid
- Opzetten documentatiesysteem GDPR

Resultaat

Implementatie van privacyvereisten zodat uw organisatie voldoet aan de verordening voor 25 mei 2018.



Contact

Leslie Clement | Consultant AGRC Cyber Practice

t (0)10 448 78 02 | **m** +31 (0)6 46 34 22 94

e leslie.clement@aon.nl

www.aon.nl/cyber

Aon's Cyber Risk Practice

Cyberisicomanagement is de managementdiscipline gericht op het terugdringen van cyberrisico's. De expertise van Aon inzake cyberisicomanagement is samengebracht in de Cyber Risk Practice. Vanuit deze adviesgroep werkt een aantal ervaren adviseurs samen met onze opdracht-gevers aan het inzichtelijk maken, beheersen als ook verzekeren van digitale en datarisico's. Onderscheidend aan onze Cyber Risk Practice is de geïntegreerde benadering van risicomanagement en organisatieadvies gericht op het beperken van privacy- en securityrisico's. Tevens onderscheiden onze adviseurs zich door hun nadruk op de impact van cyberrisico's – en dan met name ook de financiële impact. Met dit onderscheidend vermogen stellen wij onze opdrachtgevers in staat om hun risico's nuchter in te schatten en om meer te doen dan beveiligen: door inzicht en beheersing van financiële schade van cyberrisico's. Tevens helpen wij hen te voldoen aan (nieuwe) eisen die de wetgever stelt aan de bescherming van privacygevoelige gegevens.



Over Aon

Aon plc, genoteerd aan de effectenbeurs van New York (NYSE:AON), is een toonaangevende wereldwijde adviseur op het gebied van risicomanagement, makelaar van (her) verzekeringen en biedt HR-oplossingen en outsourcing services. Onze organisatie heeft wereldwijd meer dan 72.000 medewerkers in ruim 120 landen en heeft maar een doel: het innovatief ondersteunen van klanten op het gebied van risico's en mensen. We empower results: wij delen onze kennis en data, zodat klanten zich kunnen blijven bezighouden met succesvol ondernemen. In Nederland heeft Aon negen vestigingen met 1.650 medewerkers. Aon maakt deel uit van Aon plc in Londen, Verenigd Koninkrijk.

Ga naar www.aon.nl voor meer informatie over Aon en naar www.aon.com/manchesterunited om meer te lezen over het wereldwijde partnership met Manchester United.

© 2017 Aon Nederland

Alle rechten voorbehouden. Niets uit deze rapportage mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen, of op enige andere manier, zonder voorafgaande schriftelijke toestemming van Aon.