Privacy Management

Hoe zet je de verplichting om naar meerwaarde?

Met de snelle ontwikkelingen op het gebied van digitalisering was de Wet Bescherming Persoonsgegevens niet meer toereikend om onze privacy te beschermen. Met de komst van de Algemene Verordening Gegevensbescherming zijn de rechten van individuen op het gebied van privacy versterkt en uitgebreid. Na het lezen van deze whitepaper weet u wat uw organisatie aan privacy management kan doen om te voldoen aan uw verantwoordingsplicht, wat de bijkomende voordelen zijn en hoe de Functionaris Gegevensbescherming hieraan bijdraagt.

CONSIGNIUM
we create impact

Inhoud

Samenvatting

Onder de Algemene Verordening Gegevensbescherming (hierna: AVG) hebben organisaties meer verplichtingen bij het verwerken van persoonsgegevens. De verantwoordingsplicht houdt in dat u als verwerkingsverantwoordelijke moet kunnen aantonen dat uw privacy management voldoet aan de AVG. Bent u in overtreding dan kan de Autoriteit Persoonsgegevens (hierna: AP) u een boete opleggen, oplopend tot maximaal 20 miljoen euro of een boete van 4% van de wereldwijde jaaromzet, mocht dat bedrag hoger uitkomen.

Bij het opzetten van een privacy managementsysteem bepaalt u welke technische en organisatorische beveiligingsmaatregelen genomen moeten worden. De al dan niet verplicht aan te stellen Functionaris Gegevensbescherming (hierna: FG) kan hierin adviseren en houdt toezicht. Het is toegestaan om een FG extern aan te stellen of in te huren.

Met een goed privacy management optimaliseert u uw gegevensverwerkende processen, bent u als organisatie meer toegespitst op de gedigitaliseerde samenleving en wint u klantvertrouwen. Daarnaast kan het van positieve invloed zijn op uw administratie qua kosten en werklast.

Algemene Verordening Gegevensbescherming

- De AVG legt rechtstreeks verplichtingen op aan de lidstaten van de Europese Unie. Er is dus sprake van één uniforme wetgeving die in het Engels de General Data Protection Regulation (GDPR) wordt genoemd.
- Van kracht sinds 25 mei 2018. Van elke organisatie die persoonsgegevens verwerkt, moet de bedrijfsvoering in overeenstemming zijn met de AVG.
- De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de privacywetgeving.

Type persoonsgegevens en verwerking hiervan

Privacy gaat over persoonsgegevens. De definitie van een persoonsgegeven in de AVG omvat alle informatie die (in)direct te herleiden is naar een geïdentificeerd of identificeerbaar natuurlijk persoon. De AVG hanteert de categorieën 'gewone', bijzondere en strafrechtelijke persoonsgegevens.

Een aantal voorbeelden van bijzondere persoonsgegevens zijn politieke opvattingen, religieuze overtuigingen, genetische en biometrische gegevens. Van bijzondere en strafrechtelijke persoonsgegevens is in de AVG vastgesteld dat zij gezien hun gevoeligheid een speciale regeling behoeven.

Persoonsgegevens mogen alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verwerkt. Een verwerkingsdoel is gerechtvaardigd wanneer u deze kunt baseren op één van de zes rechtsgrondslagen.

De rechtsgrondslagen

- Toestemming
- Uitvoering van een overeenkomst
- Wettelijke verplichting
- Vitaal belang
- Algemeen belang of uitoefening van openbaar gezag
- Gerechtvaardigd belang

Verantwoordingsplicht

De verwerkingsverantwoordelijke is de partij die het doel van en de middelen voor het gebruik van persoonsgegevens bepaalt. Wanneer uw organisatie verwerkingsverantwoordelijke is, bent u verplicht om uw privacy management dusdanig in te richten dat u aantoonbaar compliant bent aan de AVG. Hierbij wordt uitgegaan van een 'risicogebaseerde benadering' oftewel: de maatregelen die u moet nemen, zijn afhankelijk van de hoogte van uw privacyrisico's. Het is dan ook aan te raden om te beginnen met een analyse van deze risico's en vervolgens uw privacy management hierop af te stemmen.

In de AVG staan een aantal verplichte maatregelen genoemd waarmee u aan de verantwoordingsplicht voldoet, zijnde:

- het bijhouden van een verwerkingsregister waarin u informatie vastlegt óver de persoonsgegevens die u verwerkt (niet de persoonsgegevens zelf);
- het uitvoeren van een 'data protection impact assessment' voor gegevensverwerkingen met een hoog privacyrisico;
- het bijhouden van een datalekregister;
- het kunnen aantonen dat toestemming is gegeven voor een gegevensverwerking wanneer de rechtsgrondslag 'toestemming' is;
- onderbouwing van het besluit om al dan niet een FG aan te stellen.

Boetes onder de AVG

- Maximaal 10 miljoen euro of een boete van 2% van de wereldwijde jaaromzet wanneer een verwerkingsverantwoordelijke zijn verplichtingen niet nakomt.
- Maximaal 20 miljoen euro of een boete van 4% van de wereldwijde jaaromzet wanneer een verwerkingsverantwoordelijke de beginselen of grondslagen van de AVG, of de privacyrechten overtreedt.

Privacy Management

Bij het opzetten van een privacy managementsysteem bepaalt u welke technische en organisatorische beveiligingsmaatregelen genomen moeten worden, hoe deze maatregelen er in de praktijk uitzien en wie daarin welke rol speelt. Het beveiligen van de persoonsgegevens die u verwerkt, is een continu proces. U zult periodiek moeten toetsen of de genomen beveiligingsmaatregelen nog voldoen.

Beveiligingsmaatregelen op organisatorisch vlak kunnen o.a. zijn:

- verhoging van het bewustzijn van uw personeel;
- het opstellen van een protocol voor het geval zich een data-incident voordoet;
- het sluiten van verwerkersovereenkomsten.

Beveiligingsmaatregelen op technisch vlak kunnen o.a. zijn:

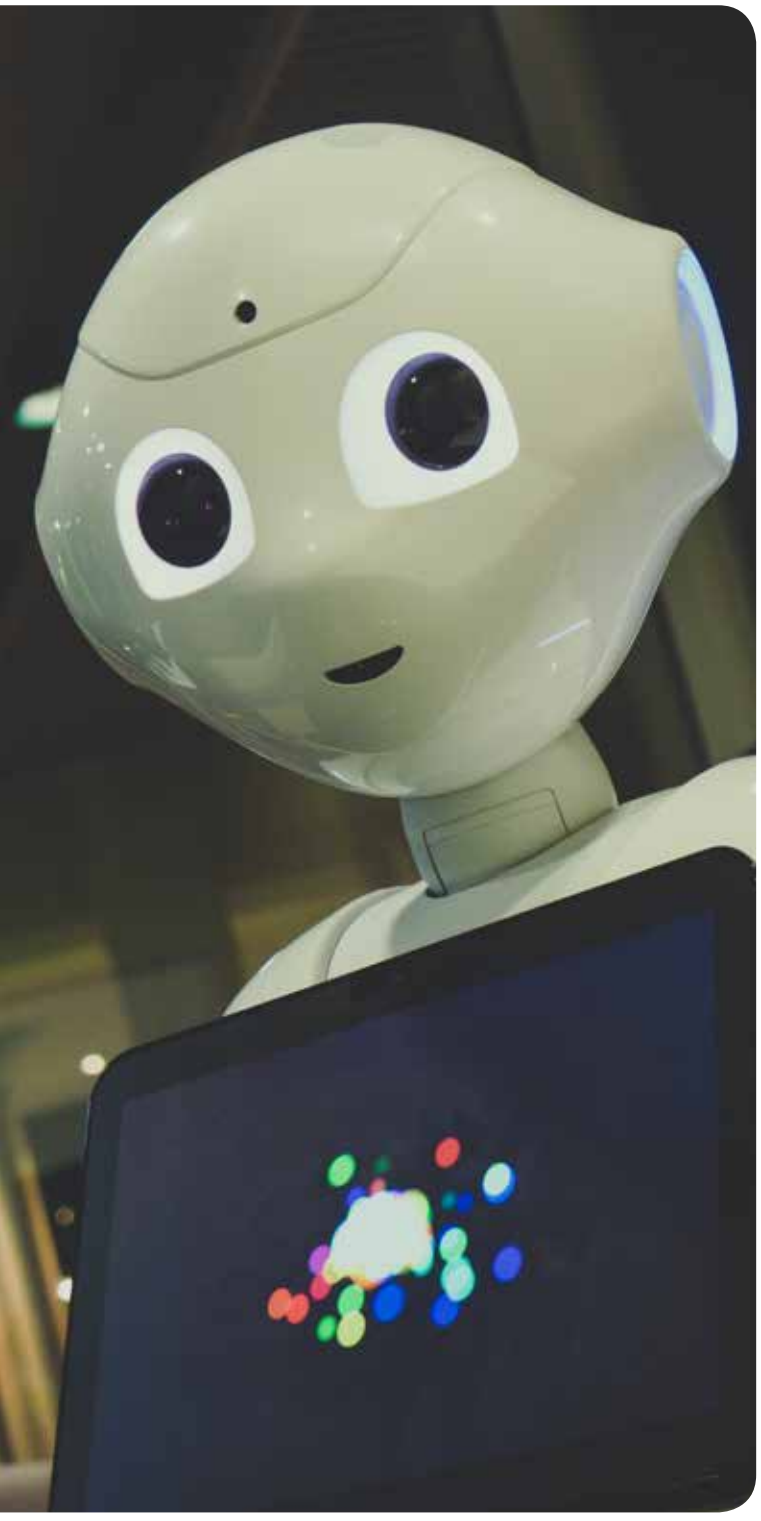
- het toepassen van multi-factor authenticatie;
- het up-to-date houden van software;
- het verwijderen van gegevens waarvan de bewaartermijn is verstreken.

De voordelen

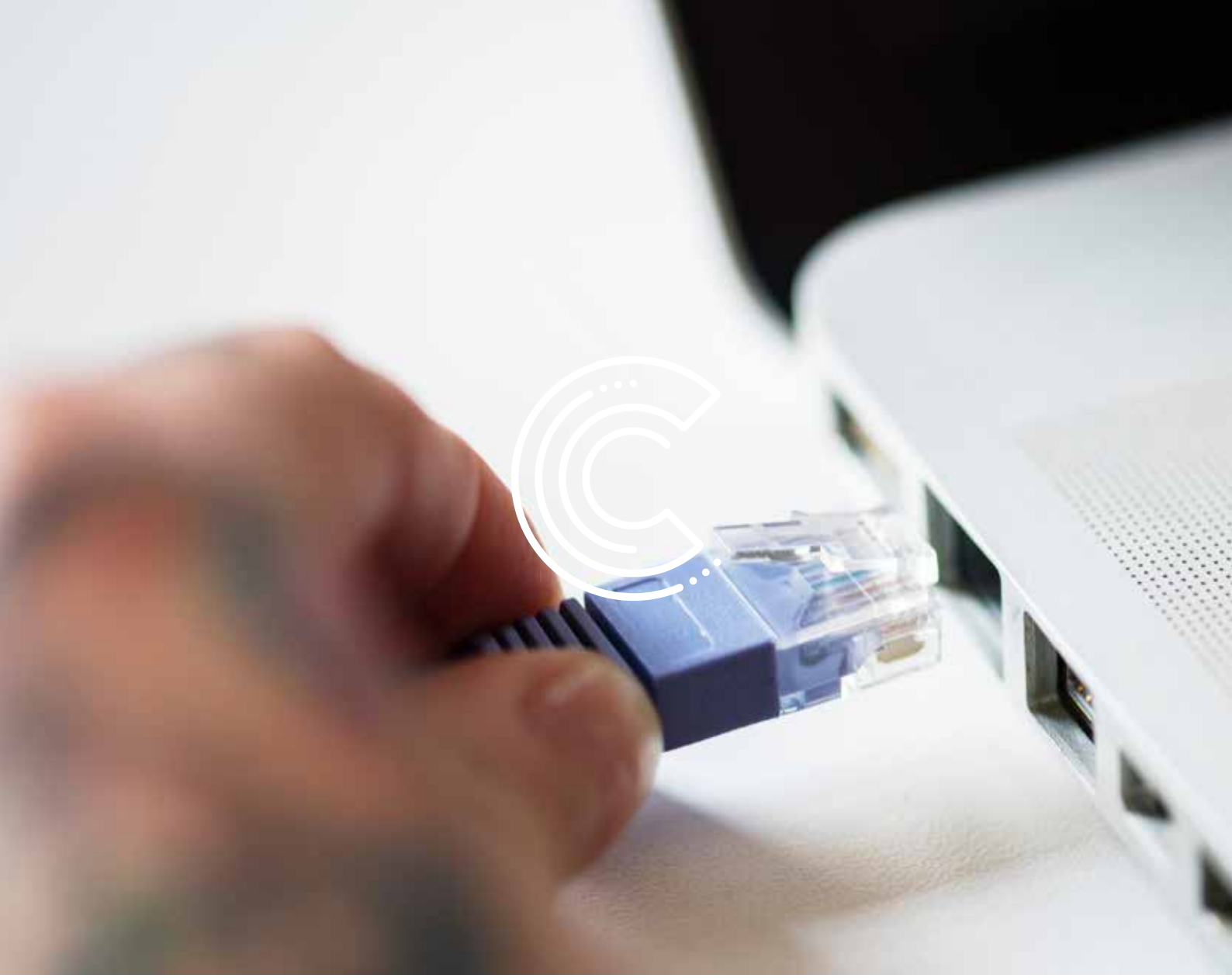
- De AVG dwingt u tot het krijgen van inzicht in uw gegevensverwerkende processen. Dit biedt overzicht en kansen op verbetering van deze processen.
- Als organisatie bent u meer toegespitst op de gedigitaliseerde samenleving.
- Goede bescherming van persoonsgegevens wint klantvertrouwen en verbetert het imago van uw organisatie.
- Dataminimalisatie heeft een positieve invloed op de administratieve werklast.
- Wanneer u in meerdere EU-lidstaten actief bent, hoeft u nog maar met één toezichthouder zaken te doen met als gevolg minder administratie- en nalevingskosten.

Functionaris Gegevensbescherming

De FG (Data Protection Officer in het Engels) ziet toe op uw privacy management en adviseert over de toepassing en naleving van de AVG door uw organisatie. In een aantal gevallen is het aanstellen van een FG verplicht. Ook wanneer uw organisatie niet de verplichting heeft, kunt u vrijwillig de functie van FG inrichten. In beide gevallen moet diegene worden aangemeld bij de AP. Privacy Officers of medewerkers gegevensbescherming hoeven niet te worden aangemeld.



De rol van FG kunt u intern beleggen, maar mag ook worden ingevuld door een externe. Vaak hebben organisaties niet alle middelen beschikbaar om iemand op te leiden tot FG. Met het uitbesteden van de werkzaamheden ter bescherming van persoonsgegevens kan de organisatie aantonen dat zij een FG heeft die over professionele kwaliteiten en deskundigheid beschikt en diepgaande kennis heeft van de nationale en Europese privacywetgeving. Het outsourcen van een FG biedt verder een betere waarborg voor de onafhankelijkheid van de FG. Bijkomend voordeel is dat een externe FG toegang heeft tot een netwerk van functionarissen en advocaten waarbij kennis en ervaringen gedeeld kunnen worden. Dit komt de organisatie ten goede.



Conclusie

Met een goed privacy managementsysteem kan uw organisatie beantwoorden aan de verantwoordingsplicht en bent u compliant aan de AVG. De voordelen zijn optimalisatie van uw gegevensverwerkende processen, toegespitst zijn op de gedigitaliseerde samenleving en meer klantvertrouwen.

Het bepalen en implementeren van de juiste organisatorische en technische beveiligingsmaatregelen is een niet te onderschatten proces op maat, waarbij de FG als adviesorgaan van grote waarde is. Voor organisaties met een hoog privacyrisico kan het zelfs verplicht zijn om een FG aan te stellen.

Gesteld kan worden dat het bedrijfseconomisch gezien in veel gevallen niet haalbaar is om voldoende deskundigheid op te bouwen en te onderhouden op het gebied van informatiebeveiliging en privacy. Organisaties mogen een externe FG aanstellen met als bijkomend voordeel dat hij/zij naast het benodigde niveau van kennis, expertise en onafhankelijkheid ook beschikt over een breed juridisch netwerk.

Over Consignium

Het realiseren van optimaal risicomanagement, verbeteren van prestaties, optimaliseren van uw organisatie en het efficiënt inrichten van wet- en regelgeving. Dat is waar de consultants van Consignium goed in zijn. Elke organisatie is anders en Consignium kan met haar verschillende producten en diensten aansluiten bij uw specifieke situatie. Wij zorgen voor impact. We create impact.

Neem vrijblijvend contact met ons op voor een kennismaking en het bespreken van de mogelijkheden voor een optimale oplossing.

Meer informatie

Consignium B.V.
Koningsweg 2-30
3762 EC Soest
035-879 56 48

Op de hoogte blijven?

www.consignium.nl
info@consignium.nl

Via de website kunt u zich inschrijven voor onze nieuwsbrief.

CONSIGNIUM
we create impact