Naam Gert Walhof
Functie zelfstandig inkoopadviseur
Ook kennispartner E-proQure en lector aan de Hanzehogeschool Groningen

Naam Robert Grandia
Functie advocaat
Organisatie Legalz
Ook docent ICT-contractenrecht en bestuurslid van de NBCM

PRIVACY COMPLIANT CONTRACTEREN

Op 25 mei 2018 moet bij organisaties de ingrijpend gewijzigde privacywetgeving geïmplementeerd zijn. Veel contracten met leveranciers omvatten de verwerking van persoonsgegevens. Inkoopadviseur Gert Walhof en jurist Robert Grandia presenteren een stappenplan om op tijd klaar te zijn voor de nieuwe regels.

Onderzoek toont aan dat veel organisaties nog niet klaar zijn voor de komst van de AVG, de Algemene Verordening Gegevensbescherming (zie kader). Uit een rondvraag in juni 2017 van MKB Servicedesk onder ondernemers bleek dat ruim 60 procent van de ondervraagden niet bekend is met de AVG, laat staan dat zij bezig zijn met de implementatie. Voor inkopers begint de privacywetgeving primair bij alle goederen en diensten van leveranciers waarbij persoonsgegevens worden verwerkt. In het huidige tijdperk is informatietechnologie alom aanwezig en als ICT de motor is, dan is verwerking van data – waaronder persoonsgegevens – de brandstof. Enkele voorbeelden van contracten waarbij de uitwisseling van persoonsgegevens een rol speelt:

- de salarisadministratie die is uitbesteed aan een leverancier;
- het CRM-systeem in de cloud van een softwareleverancier;
- de vernietiging van dossiers uit het archief door een externe partij;
- de promotiecampagne waarbij klantgegevens worden gedeeld met het reclamebureau;
- het verzamelen en analyseren van big data door externe consultants.

CHECKLIST VERWERKINGSOVEREENKOMST

- Onderwerp, duur, aard en doel van de verwerking van persoonsgegevens
- Soort persoonsgegevens en categorieën van betrokkenen
- Uitsluitend verwerking op basis van schriftelijke instructies van de verwerkingsverantwoordelijke
- Gemachtigde personen gebonden vertrouwelijkheid (wettelijk of contractueel) in acht te nemen
- Verwerker neemt de vereiste technische en organisatorische maatregelen
- Geen andere (sub)verwerker in dienst zonder voorafgaande toestemming van de gegevensverantwoordelijke en als dat gebeurt dan tegen dezelfde verplichtingen als die in de overeenkomst tussen de verwerkingsverantwoordelijke en de verwerker zijn opgenomen (“doorzetverplichting”)
- Verwerker verleent bijstand bij verzoeken van betrokkenen om uitoefening van hun rechten
- Verwerker verleent bijstand bij nakoming verplichtingen ter zake onder andere inbreuk beveiliging/meldingen datalekken
- Na afloop van de verwerkingsdiensten wissen of vernietigen persoonsgegevens, tenzij opslag verplicht is
- Verwerker stelt alle informatie ter beschikking die nodig is om nakoming verplichtingen aan te tonen en audits mogelijk te maken.

Stappenplan

Een risicoanalyse leert dat afwachten geen optie is. Zeker niet gezien de forse boetes die op grond van de AVG kunnen worden opgelegd. Met het volgende stappenplan maak je een vliegende start.

1. Awareness en implementatie organisatiebreed

Begin binnen de organisatie met informeren naar de bekendheid van de AVG bekend en of al wordt gewerkt aan een plan van aanpak en de daarbij behorende implementatie. Je wil dan als inkoper natuurlijk vooral weten of in dit plan ook aandacht is voor de verwerking van persoonsgegevens door leveranciers in opdracht van je organisatie. Wordt nog niet aan een plan gewerkt, adviseer de directie dan om hier snel mee te beginnen. Zelf draag je bij door het uitvoeren van deze stappen.

2. Inventarisatie inkoopcontracten
De tweede stap is een inventarisatie. In welke contracten met leveranciers speelt de verwerking van persoonsgegevens? Denk daarbij ook aan de leveranciers van contracten waar jij of je inkoopcollega's niet bij betrokken waren toen ze werden afgesloten en die niet direct in de contractadministratie zichtbaar zijn. Realiseer je ook dat in contracten niet altijd het antwoord op deze vraag te vinden zal zijn. Tot de inventarisatie behoort ook de toets of deze contracten vóór 25 mei 2018 aflopen. In dat geval kun je de gevolgen van de AVG meenemen in de tender voor het nieuwe contract. Per contract inventariseer je om welke verwerking van welke persoonsgegevens het gaat en welke afspraken al gemaakt zijn over de bescherming van persoonsgegevens.

3. Maatregelen per contract
Vervolgens bepaal je per contract welke afspraken in de verwerkingsovereenkomst op basis van de AVG gemaakt moeten worden met de leverancier. Ben je zelf geen specialist als het gaat om de AVG, zorg dan voor juridische ondersteuning bij het opstellen van deze afspraken. Een greep uit de vragen die voorliggen:

- Is een (verplichte) verwerkersovereenkomst gesloten en zo ja, voldoet deze aan de nieuwe eisen die worden gesteld door de AVG? (zie ook kader Checklist verwerkersovereenkomst)
- Heeft de gecontracteerde leverancier mogelijk delen van de verwerking van persoonsgegevens uitbesteed aan zijn leveranciers (subverwerkers)? En welke subverwerkers betreft het dan en wat heeft je leverancier daarmee afgesproken?
- Welke beveiligingsmaatregelen worden getroffen door de leverancier, de subverwerker(s) en door je eigen organisatie?
- Is sprake van gegevensverwerking in niet-EU-landen, bijvoorbeeld als data wordt opgeslagen op servers in de Verenigde Staten?

Dergelijke vragen kunnen worden beantwoord aan de hand van een zogenoemde Privacy Impact Assessment (PIA). De PIA is een middel om de effecten van de beoogde verwerking te beoordelen. Een handreiking en vragenlijst voor het uitvoeren van een PIA is bijvoorbeeld te vinden op de website van de beroepsorganisatie van IT-auditors: www.norea.nl/handreikingen.

Vandaag nog beginnen
Nadat de nodige maatregelen zijn vastgesteld, volgt uiteraard het bereiken van overeenstemming met de betreffende leverancier, het vastleggen van afspraken in de verwerkersovereenkomst, het actueel maken van het contract en het bijwerken van de contractadministratie. Daarnaast zul je mogelijk op basis van het plan implementatie AVG in je organisatie nog verdere acties moeten ondernemen.

Veel organisaties zijn nog niet voorbereid op de nieuwe wetgeving, ondanks de te verwachten impact die de AVG zal hebben. Daarbij is goed om je te realiseren dat de inventarisatie van de gevolgen, het ontwikkelen van een aanpak en implementatie hiervan deskundigheid, tijd en doorlooptijd vragen. Gelukkig is er nog tijd, ook als je nog moet beginnen. Maar wacht dan ook niet langer en doe het vandaag nog. ●

DE AVG IN EEN NOTENDOP

De Algemene Verordening Gegevensbescherming (AVG) vervangt per 25 mei 2018 de Wet bescherming persoonsgegevens. De Verordening geldt rechtstreeks in alle EU-lidstaten.

Persoonsgegevens van een betrokkene
Als persoonsgegeven geldt alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"). Denk aan naam, adres en BSN maar ook aan (zwaarder beschermde) bijzondere persoonsgegevens zoals ras, etnische afkomst, religie, of seksuele gerichtheid.

Verwerking
Centraal in de AVG staat het begrip "verwerking": het verzamelen, vastleggen, opslaan, raadplegen, wijzigen, gebruiken, verstrekken of vernietigen van persoonsgegevens.

Verwerkingsverantwoordelijke, verwerker en subverwerker
De "verwerkingsverantwoordelijke" is degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. De "verwerker" verwerkt persoonsgegevens ten behoeve van de verwerkingsverantwoordelijke. Indien deze werkzaamheden (deels) laat verrichten door een derde, dan spreken we over een subverwerker.

Verwerkersovereenkomst
Gegevensverantwoordelijke en verwerker moeten een verwerkersovereenkomst afsluiten waarin de afspraken over de omgang met persoonsgegevens schriftelijk vastliggen.

Beveiliging
De verwerkingsverantwoordelijke dient passende technische en organisatorische maatregelen te treffen om te waarborgen en aan te tonen dat de verwerking plaatsvindt in overeenstemming met de AVG.

Meldplicht datalekken
Onder de AVG geldt dat, in aanvulling op de bestaande meldingsplichten, alle datalekken intern gedocumenteerd moeten worden, ook wanneer geen meldingsplicht bestaat.

Boetes
De AVG introduceert een boetestelsel dat grote impact kan hebben. Boetes worden opgelegd door de Autoriteit Persoonsgegevens en kunnen oplopen tot 20 miljoen euro of 4 procent van de wereldwijde jaaromzet.