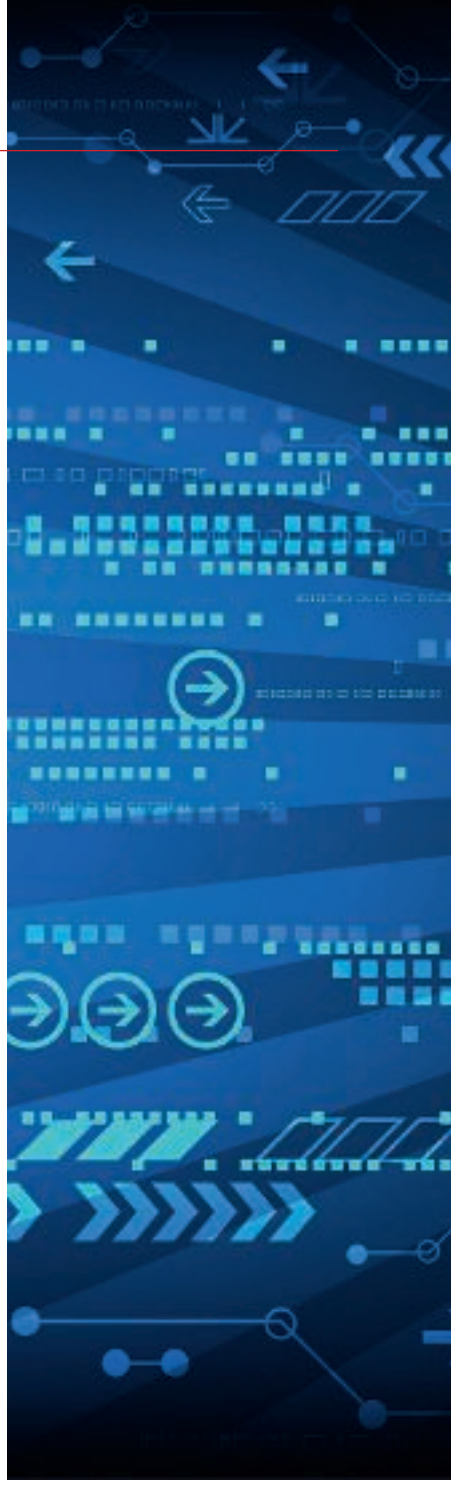
tekst **Peter Zwetsloot** foto **Jitty van Doodewaerd Giuseppe Toppers | Danto**



Nieuwe AVG heeft gevolgen voor grafische bedrijven

Verwerkers-overeenkomst *verplicht*

De Algemene Verordening Gegevensbescherming (AVG) wordt 25 mei 2018 ingevoerd. Dan is de nieuwe privacywetgeving voor alle organisaties binnen de EU van kracht. 'Grafische bedrijven die data van derden verwerken, moeten dan een verwerkersovereenkomst met hun opdrachtgever afsluiten', zegt Jitty van Doodewaerd, compliance officer bij DMCC.

Jitty van Doodewaerd: 'De nieuwe AVG heeft ingrijpende gevolgen voor elke organisatie – van groot tot klein – die data registreert en / of verwerkt. In feite wordt iedere organisatie verplicht om naast een financiële administratie ook een privacy-administratie in te richten. Hiermee moet ten alle tijden kunnen worden verantwoord hoe er met persoonsgegevens wordt omgegaan. Bovendien worden organisaties die het verwerken van persoonsgegevens uitbesteden verplicht om met deze partijen een zogeheten verwerkersovereenkomst af te sluiten. Verantwoordelijkheid vormt de basis van de nieuwe regels. Organisaties moeten kunnen aantonen dat zij begrijpen hoe de vereisten van de nieuwe wet ingrijpen op hun verwerkingen van persoonsgegevens. Ook moeten zij de juiste beheersmaatregelen hebben getroffen om *compliance* – in overeenstemming met de geldende wet- en regelgeving – te waarborgen. Voor organisaties die geen privacy-specialist in huis hebben, is het onderwerp *privacy compliance* en de nieuwe wetgeving hieromtrent vaak onduidelijk en ontbreekt het inzicht wat er exact moet gebeuren om in lijn met de nieuwe wetgeving te gaan werken. Zeker ook nu er forse boetes en imagorisico's aan het onderwerp kleven, neemt de belangstelling voor *privacy compliance* toe. Maar de vraag "Wat moeten we nu precies doen?", blijft leven.'

Vijf stappenplan

'Stilzitten en afwachten is geen optie', waarschuwt Van Doodewaerd. 'De AVG geldt voor iedereen. Het is zaak om stapsgewijs de implementatie voor te bereiden. Daar hebben wij een vijf stappenplan (zie kader onderaan pagina 21) voor ontwikkeld, met een overzicht van de belangrijkste *privacy compliance*-vereisten. Het plan vertelt hoe organisaties deze op een praktische manier kunnen implementeren. In

Verwerkersovereenkomst

Organisaties moeten verwerkersovereenkomsten afsluiten met hun leveranciers, met daarin:

- **Een duidelijke opdrachtomschrijving**
- **De doeleinden van de verwerking**
- **Een omschrijving van de (categorieën) data die verwerkt worden**
- **Geheimhouding**
- **Inschakelen van derden en onderaannemers**
- **Locatie van de data**
- **Afhandeling van verzoeken van de betrokkene (Recht op inzage, correctie en verzet en het recht om vergeten te worden)**
- **Instructie met betrekking tot datalekken**
- **Duur van de overeenkomst en wijze van beëindiging**
- **De termijnen waarbinnen de verwerker de data mag bewaren**
- **Dat persoonsgegevens moeten worden vernietigd**
- **Een omschrijving van de door de verwerker te hanteren beveiligingsmaatregelen**
- **Een mogelijkheid tot controle (audit) van naleving van de overeenkomst**
- **Aansprakelijkheid**
- **Recht op heronderhandeling van de overeenkomst**
- **Toepasselijk recht**

de nieuwe AVG mogen organisaties om (potentiële) klanten beter van dienst te zijn klant- en contacthistorie bijhouden. Dit is echter geen vrijbrief voor ongebreideld datagraaien. Organisaties mogen data verzamelen, maar alleen proportioneel voor het doel waarvoor ze die gegevens verzamelen. Voor Direct Mail blijft overigens gelden dat geen klantrelatie nodig is om iemand een geadresseerd poststuk te sturen. Het gebruik van adresdata voor direct mail blijft *opt-out*. Zo lang een adresbestand nog redelijk converteert, kunnen de gegevens voor direct mail gebruikt worden.'

Verwerkersovereenkomst

Jitty van Doodewaerd: 'De nieuwe wet verplicht organisaties die werkzaamheden uitbesteden waarbij data – denk bijvoorbeeld aan persoonsgegevens voor direct en of transactiemail – worden verwerkt, om met deze partijen een verwerkersovereenkomst af te sluiten. Dat is allang niet zomaar een paragraaf in de opdrachtovereenkomst, maar een volwaardig document met informatie over de

Jitty van Doodewaerd: 'In feite wordt iedere organisatie verplicht om naast een financiële administratie ook een privacy-administratie in te richten.'

In vijf stappen naar Privacy Compliance

- **Inventariseer welke gegevens u verzamelt (heeft u deze ook echt nodig?)**
- **Documenteer uw verwerkingen**
- **Beheer en controleer uw verwerkingen**
- **Delegeer niet ondoordacht aan verwerkers**
- **Informeer de personen in uw bestand**

opdracht, het type gegevens, bewaartermijnen, beveiligingsmaatregelen, enzovoort (zie kader op pagina 19). De verordening verplicht verwerkers om schriftelijk te administreren welke gegevens voor welke opdrachtgevers

'Stilzitten en afwachten is geen optie'

worden verwerkt. Opdrachtgevers zijn op hun beurt verplicht om die verwerking ook echt te controleren. Dat kan bijvoorbeeld door bij hen periodiek beveiligingsrapporten op te vragen of door een derde partij te vragen om de afspraken in de verwerkersovereenkomst op locatie te controleren.'

Zelfstandige verplichtingen

'Ook verwerkers (leveranciers) hebben een aantal zelfstandige verplichtingen op basis van de AVG', zegt Jitty van Doodewaerd. 'Zo moeten zij data adequaat beveiligen, mogen zij niet zonder meer sub-verwerkers inschakelen zonder toestemming van de verantwoordelijke en moeten zij een datalek zo snel mogelijk melden aan de verantwoordelijke. Daarnaast hebben zij ook de plicht om zelfstandig mee te werken aan verzoeken van de toezichthouder, de Autoriteit Persoonsgegevens. Kortom: de AVG betekent voor de meeste grafische bedrijven dat zij hun processen op orde moeten brengen. Mijn advies is simpel: "Doe dat ook", want de aangekondigde boetes op overtredingen zijn niet mals.'

Datalekken

Jitty van Doodewaerd: 'Naast alle eisen waaraan een verwerkersovereenkomst moet voldoen, kent Nederland sinds 1 januari 2016 een brede meldplicht datalekken. Als er bij een datalek kans is op privacy-schending van consumenten, moet dit gemeld worden bij de Autoriteit Persoonsgegevens. Een lek moet altijd gemeld worden door een opdrachtgever. Een grafisch bedrijf moet hierover als dienstverlener afspraken maken met zijn opdrachtgevers. Bovendien moet het, om de ernst van een datalek tijdig te kunnen beoordelen, een interne procedure opstellen aan de hand waarvan medewerkers vermoedelijke datalekken, of verlies of diefstal van bedrijfsapparatuur kunnen rapporteren. Naast de verwerkersovereenkomst heeft ook het protocol 'Datalekken' ingrijpende gevolgen voor alle verwerkers van persoonsgegevens. Kortom, er is nog veel te doen en 25 mei 2018 komt snel dichterbij. Mijn advies aan grafische bedrijven is dan ook: "Bespreek het met je opdrachtgevers", het is namelijk een gezamenlijke uitdaging om aan de nieuwe eisen van de AVG te voldoen.'

Compliance officer

Jitty van Doodewaerd is compliance officer bij DMCC Nederland. Daar is zij betrokken bij het uitgebreide dienstenportfolio op het gebied van *compliance* en ondersteunt zij energiemaatschappijen, telecombedrijven, uitgeverijen, loterijen, financiële instellingen en goede doelen op het gebied van *compliance* bij klantcontact.
Daarnaast is Jitty betrokken bij verschillende belangenbehartigingstrajecten, lid van het Legal Affairs Committee van de Federation for European Direct and Interactive Marketing (FEDMA) en de Privacy Commissie van VNO-NCW.
Het in dit artikel genoemde vijf stappenplan is aan te vragen bij DMCC: www.dmcc.nl.