De nieuwe Europese wet databescherming (GDPR): tien veranderingen

Op 25 mei 2018 treedt de General Data Protection Regulation (GDPR), de nieuwe Europese wet voor databescherming, in werking. Dit heeft gevolgen voor Europese marketeers en marketeers die gegevens verwerken van Europese consumenten. De nieuwe wet verscherpt regels uit de huidige Wet Bescherming Persoonsgegevens, maar voegt ook een aantal nieuwe verplichtingen toe. Wat verandert er dan concreet?

1. Toepassing

De GDPR is niet alleen van toepassing op Europese organisaties die persoonsgegevens (laten) verwerken. De wet geldt ook voor organisaties die niet in de EU zijn gevestigd, maar wel persoonsgegevens (laten) verwerken van EU inwoners. Ook is het begrip 'persoonsgegevens' ge-update naar: 'alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon'. Dit wil zeggen: wanneer een persoon met behulp van een (online) identificator geïdentificeerd kan worden, of geïsoleerd kan worden uit een groep ('single-out'). Een identificator is bijvoorbeeld een naam of kenteken, maar ook een online nickname of een IP-adres.

Actie: Beoordeel of de GDPR op jouw organisatie en eventueel zuster-, of dochterorganisaties van toepassing is en breng de datastromen binnen jouw organisatie in kaart.

2. Toestemming

Naast vrij, specifiek en op informatie berust, moet toestemming onder de GDPR ook een 'ondubbelzinnige' wilsuiting zijn. Dit houdt onder andere in dat toestemming uit een actieve handeling moet bestaan; geen vooraf aangevinkte hokjes meer. De vraag om toestemming te geven moet duidelijk en begrijpelijk zijn en in eenvoudige taal worden gepresenteerd. Als er toestemming voor meerdere doeleinden wordt gevraagd, dan moet daarvoor apart toestemming worden gevraagd. Als organisatie moet je uiteindelijk kunnen bewijzen dat de betrokkene toestemming heeft gegeven. De betrokkene heeft ten alle tijde het recht de toestemming in te trekken, en moet daar ook op worden gewezen.

Actie: Waar vraagt jouw organisatie toestemming aan betrokkenen voor een verwerking? En, waar zou jouw organisatie wellicht nog meer toestemming moeten vragen? Is deze toestemming 'ondubbelzinnig'? Ga ook na hoe de gegeven toestemming wordt vastgelegd: kun jij bewijzen dat rechtmatig toestemming is verkregen?

3. **Verwerkingsbeginselen**

De GDPR introduceert kernbeginselen waaraan alle verwerkingen van persoonsgegevens moeten voldoen:

- persoonsgegevens moeten op behoorlijke, rechtmatige en transparante manier worden verwerkt;
- persoonsgegevens mogen alleen voor een bepaald, uitdrukkelijk omschreven doel worden verwerkt;
- alleen persoonsgegevens die noodzakelijk zijn voor het doel mogen worden verwekt;
- gegevens moeten correct en actueel zijn;
- als identificatie niet meer noodzakelijk is voor het doel, dan moeten de persoonsgegevens worden verwijderd of geanonimiseerd, en;
- de persoonsgegevens moeten worden beveiligd door middel van technische en organisatorische maatregelen.

Actie: De verantwoordelijke, bijvoorbeeld de opdrachtgever, moet kunnen bewijzen dat wordt voldaan aan deze verwerkingsbeginselen. De verantwoordelijke kan hier natuurlijk afspraken over maken met de

De nieuwe Europese wet databescherming (GDPR): tien veranderingen

bewerker, bijvoorbeeld een dienstverlener (zie ook punt 7). Beoordeel of het privacy en datasecurity beleid van jouw organisatie in lijn is met de GDPR.

4. Rechten van betrokkene

Transparantie staat voorop: de betrokkene moet geïnformeerd worden over wat er met zijn persoonsgegevens gebeurt. Alles moet in eenvoudige en duidelijke taal worden gecommuniceerd. Naast het bekende recht op verzet, inzage en rectificatie, heeft de betrokkene onder de GDPR ook het recht om vergeten te worden, het recht op overdraagbaarheid van zijn data (ook wel: dataportabiliteit), het recht de verwerking te beperken en het recht bezwaar te maken tegen bepaalde verwerkingen. De betrokkene heeft ten alle tijde het recht om bezwaar te maken tegen de verwerking van zijn gegevens voor direct marketing doeleinden. Als de betrokkene een dergelijk bezwaar indient, dan mogen zijn gegevens niet meer voor marketing doeleinden worden verwerkt.

Actie: Pas het privacy statement van jouw organisatie aan en bedenk welke processen binnen jouw organisatie moeten worden aangepast om de rechten van betrokkenen te waarborgen.

5. Administratieplicht

Als organisatie moet je kunnen aantonen dat je voldoet aan alle verplichtingen uit de GDPR. Denk hierbij aan de toestemming, gegeven informatie, rechten van betrokkenen, beveiliging van gegevens, minimalisatie van de verwerkingen en afspraken met bewerkers. Dus: een gigantische compliance exercitie! Kernbegrippen hierbij zijn '*privacy by design*': een systeem is ontworpen om de privacy van betrokkenen zo goed mogelijk te beschermen. En '*privacy by default*': de standaardinstellingen van het systeem zijn zo privacyvriendelijk mogelijk en er worden niet meer persoonsgegevens verwerkt dan noodzakelijk.
Actie: Ga na welke rol jouw organisatie speelt en welke verantwoordelijkheden je hebt. Zet een documentatiesysteem op om aan te kunnen tonen dat jouw organisatie aan haar verplichtingen voldoet.

6. Profilering

Betrokkenen hebben het recht om niet te worden onderworpen aan profilering als daar rechtsgevolgen aan zijn verbonden of wanneer het besluit hem in 'aanmerkelijke mate treft'. Wat dit laatste betekent in de praktijk is nog onduidelijk. Het recht van bezwaar bij marketingdoeleinden -zoals onder [4] toegelicht- blijft ook bij profilering gelden.

Actie: Doet jouw organisatie aan profilering? Ga dan na wat de impact voor betrokkenen is, wees transparant over de doeleinden en wijs betrokkenen op hun rechten.

7. Inschakelen bewerker

Net als onder de Wbp is het onder de GDPR verplicht om een overeenkomst af te sluiten met bewerkers. Nieuw is echter dat de GDPR een aantal verplichte onderdelen van deze overeenkomst noemt, waaronder:

- het doel van de verwerking;
- het soort persoonsgegevens dat wordt verwerkt;
- de categorieën van betrokkenen;
- dat passende beveiligingsmaatregelen zullen worden genomen;
- dat de bewerker meewerkt aan audits om te controleren of de bewerker zich aan alle verplichtingen houdt, en;

- na afloop van de verwerking vernietiging of retourneren van de persoonsgegevens aan de verantwoordelijke.

Ook mag de bewerker niet meer een derde partij inschakelen zonder de voorafgaande schriftelijke toestemming van de verantwoordelijke.

Actie: Ga na welke bewerkers je organisatie inschakelt en welke afspraken er op dit moment vastliggen. Zijn de verplichtingen uit de GDPR voldoende gewaarborgd?

8. Privacy Impact Assessment (PIA)

In het Nederlands een 'gegevensbeschermingseffectbeoordeling' is een beoordeling om het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens in kaart te brengen. Deze beoordeling is met name verplicht wanneer er bij de verwerking nieuwe technologieën worden gebruikt en er, gelet op de aard, de omvang, de context en de doeleinden van de verwerking een hoog risico is. Een PIA is in ieder geval verplicht bij profilering indien die profilering een besluit met een rechtsgevolg tot gevolg heeft of de betrokkene 'wezenlijk treft'. Ook hier is nog onduidelijk wat dit laatste in de praktijk betekent.

Actie: Breng in kaart wat het privacyrisico is voor de betrokkenen van wie je organisatie persoonsgegevens verwerkt.

9. Meldplicht datalekken

Sinds 1 januari 2016 kennen we in Nederland de meldplicht datalekken. Deze meldplicht blijft onder de GDPR nagenoeg gelijk. Nieuw is dat de bewerker onder de GDPR verplicht is een datalek te melden aan de verantwoordelijke (bijvoorbeeld de opdrachtgever) en dat er pas een melding bij de toezichthouder hoeft te worden gedaan als er daadwerkelijk een lek heeft plaatsgevonden. Onder de Wbp moet er al een melding worden gedaan als niet kan worden uitgesloten dat er een onrechtmatige verwerking van persoonsgegevens kan plaatsvinden.

Actie: Stel een protocol datalekken op, passend bij jouw organisatie.

10. Overtredingen en sancties

De GDPR maakt het voor de Autoriteit Persoonsgegevens mogelijk hogere boetes op te leggen. De maximumboete (bijvoorbeeld voor het niet rechtmatig verkrijgen van toestemming of niet voldoen aan regels omtrent data-uitwisseling met niet EU-landen) is 20 miljoen euro of vier procent van de wereldwijde omzet.

Actie: Opzetten van compliance procedure en adequate processen, inclusief training van personeel, om zodoende te kunnen bewijzen dat jouw organisatie voldoet aan de GDPR.