AVG-seminar
voor marketeers

iConneqt
Online Marketing Automation

Privacy Advocaat

Stationsplein 28 | 1382 AD Weesp | +31 (0) 20 308 0645

AVG-seminar
voor marketeers

7 september 2017,

De nieuwe AVG gaat gelden vanaf 25 mei 2018. Een groot verschil is dat bedrijven en instellingen die persoonsgegevens beheren vanaf die datum meer verantwoordelijkheden hebben om persoonsgegeven adequaat te beheren. En pas op. Naast de nieuwe AVG zijn ook met de regels van de Telecommunicatiewet en waarschijnlijk zal de vijf jaar oude Code e-mail van het DDMA, EMMA-nl en Thuiswinkel.org ook na vijf jaar worden aangepast.

En daar zit direct een probleem. Want niet alles is al duidelijk of is duidelijk beschreven. Bijvoorbeeld het nemen van passende technische en organisatorische maatregelen binnen de AVG is natuurlijk arbitrair. Wat is passend?

En waarom stelt de ene organisatie, anders dan de wetgever, dat ook in de webshop of bij de boekingsengine, na aankoop de klant, bewust nog een keuze moet worden gemaakt (vinkje) wanneer men ook de nieuwsbrief wil ontvangen. Doet de nieuwe klant dat niet, dan ontvangt hij/zij geen nieuwsbrief. Dat is niet fijn. Kost conversie, zo leert de praktijk. In de praktijk moet nog helder worden, hij de wetgever en de branche hierna kijkt.

Toezegging

Wij zullen - als verwerker van klantgegevens namens jouw organisatie - zorgen dat de technische en organisatorische aspecten in relatie met de wet- en regelgeving zo optimaal mogelijk zijn geregeld. Sterker, op dit moment zijn zaken binnen iConneqt reeds beter geregeld dan in de toekomst waarschijnlijk zal worden vereist. Je kunt stellen; we lopen met iConneqt voor op de wetgever.

Internationaal

Het goede nieuws is dat de nieuwe AVG geldt voor alle landen van Europa. Dat maakt het leven van de internationale marketeer een stuk gemakkelijker.

Boetes

Er wordt verwacht dat de handhaving stenger is, de boetes op overtredingen zijn aanzienlijk. Tot 20 miljoen euro of 4% van de wereldwijde jaaromzet.

Seminar

Daarom een seminar over de AVG en de andere wetten, die mogelijk van belang zijn in je marketing - en sales operatie vanaf 28 mei volgend jaar. Het seminar wordt gegeven door privacyrecht specialist Mr. Kirsten van der Zwan. In haar praktijk wordt nauw samengewerkt met andere privacy advocaten, IT-auditors en ICT'ers. Zij ondersteunt organisaties met audits, certificering en bij het technisch inregelen van de privacy verplichtingen. Op haar website: Privacy-advocaat.nl, kun je meer informatie vinden en veel documenten kosteloos downloaden.

Ruud Lampers

CEO iConneqt

iConneqt
Online Marketing Automation

Privacy Advocaat

PRIVACY WAARBORG

Wat we doen, hoe we het doen en of en we dat volgend jaar wel kunnen blijven doen

Hieronder de belangrijkste functionaliteiten/mogelijkheden van iConneqt in relatie met de opslag en/of bewerking van klantgegevens. We hebben het opgezet vanuit de mogelijke vragen van de marketeer/e-commerce manager.

Service

Aan het onderstaande kunnen geen rechten worden ontleend. Dit document dient uitsluitend om de beheerders van klantgegevens (persoonsgegevens) binnen de marketing- en sales afdelingen in hoofdlijnen te informeren over vooral de wet- en regelgeving vanaf 1 mei 2018 in algemene zin.

Dit document moet dan ook worden gezien als een richtinggevend servicedocument. De implementatie en de te nemen organisationele maatregelen m.b.t. de nieuwe wet- en regelgeving en de branchecode ligt volledig bij de eigen organisatie. Wij adviseren tenminste een privacy quickscan te laten uitvoeren, immers ieder bedrijf/instelling is anders en de wetgeving is nog steeds aan verandering onderhevig.

Klanten mailen

Volgens de huidige wetgeving is het simpel. Iemand is een klant wanneer je hem of haar een product of dienst hebt verkocht. Wil je de klant een commerciële of charitatieve email zenden, dan hoef je niet vooraf toestemming te vragen. Maar je moet klanten wel de optie geven om zich eenvoudig af te melden.

Binnen iConneqt is simpel afmelden een standaard functionaliteit. Niet alleen in elke nieuwsbrief/aanbiedingsmail, maar ook via de website, de webshop of de boekingsengine wordt die optie reeds (24/7) aan de klant aangeboden.

Mogen we na 25 mei volgend jaar klanten nog steeds zonder specifieke toestemming blijven mailen?

Mr. Kirsten van der Zwan: Naar verwachting niet, maar de wetgeving die dit onderwerp specifiek regelt (E-Privacyrichtlijn) wordt vervangen door de E-Privacyverordening. De bedoeling is dat ook deze verordening per 25 mei 2018 van toepassing wordt. De tekst van deze verordening staat, anders dan de tekst van de AVG, nog niet vast.

Aanmelden Nieuwsbrief

Opt-in en Double opt-in

Wanneer via een webformulier (en pop-up) een emailadres wordt opgeslagen dan worden automatisch de volgende gegevens ook in de iConneqt database vastgelegd:

- Datum
- Tijd
- IP-adres
- Welk webformulier is gebruikt
- Het verzendmoment van de bevestigingsmail (mist geactiveerd)
- De GEO-locatie (zichtbaar op Google maps)

Deze informatie moet vijf jaar worden bewaard om eventueel te bewijzen dat de ontvangers vooraf toestemming hebben gegeven. We kiezen vaak voor van single opt-in omdat dit de hoogste conversie geeft. Maar...we weten dus niet of het emailadres ook daadwerkelijk van de de eigenaar is die het emailadres heeft opgegeven.

WelkomMail

Een goede methode om je database 'schoon' te houden is het automatisch sturen van een bevestiging in de vorm van een WelkomMail. (Ook goed in het kader van de opbouw van de relatie). De ontvanger kan, wanneer iemand anders zijn/haar emailadres heeft gebruikt, zich eenvoudig met een muisklik afmelden.

Double opt-in

Wanneer je aangeeft bij het ontwikkelen van een webformulier dat je double opt-in wilt gebruiken, dan ontvangt de (potentiële) klant automatisch na het invullen een email waarbij op een button moet worden geklikt als bevestiging dat hij/zij ook echt eigenaar is van het emailadres.

De eigenaar van een emailadres geeft bij double opt-in dus expliciet toestemming voor het gebruik van zijn adres om dus via email communicatie te ontvangen.

Is double opt-in een verplichting vanaf 25 mei 2018? In Nederland is double opt-in op dit moment nog geen verplichting, in Duitsland wel. Gaat dit ook veranderen na 25 mei 2018?

Mr. Kirsten van der Zwan: Naar verwachting niet, maar de wetgeving die dit onderwerp specifiek regelt (E-Privacyrichtlijn) wordt vervangen door de E-Privacyverordening. De bedoeling is dat ook deze verordening per 25 mei 2018 van toepassing wordt. De tekst van deze verordening staat, anders dan de tekst van de AVG, nog niet vast.

Database verrijking

In de WelkomMail kan een button worden geplaatst die de de klant leidt naar de eigen Customer Page.
Daar kan men dan zelf de gegevens aanvullen. Je wilt om te personaliseren minimaal de naam weten. Je kunt die verrijking ook in stappen doen (vanuit conversie oogpunt).

Customer Page via de website toegankelijk (24/7)

Via het geverifieerde emailadres komt de klant veilig op de eigen pagina.

1. De klant heeft direct inzicht in welke gegevens het bedrijf/de instelling vastlegt.
2. De klant kan zijn/haar gegevens zelf eenvoudig muteren en aanvullen.
3. De klant kan de frequentie van het aantal nieuwsbrieven aanpassen.
4. De klant kan voorkeurs-onderwerpen aangeven.
5. En...de klant kan zich simpel afmelden voor bijvoorbeeld het ontvangen van de nieuwsbrief.

Recht op verwijderen

Nieuw wordt dat de AVG aangeeft dat de klant het recht geeft om de gegevens volledig te laten verwijderen. Is pseudonimiseren* voldoende ?

Mr. Kirsten van der Zwan: Dit is relevant in verband met het belang van historische data. Dit is niet nieuw. Staat al in de Wet bescherming persoonsgegevens (Wbp). Pseudonimiseren is een vorm van beveiliging. Heeft niets van doen met verwijderen.

Rechten van de betrokkene (klanten)

Klanten hebben diverse wettelijke rechten die ze mogen uitoefenen. Het recht van verwijdering, het recht van inzage, het recht om toestemming net zo makkelijk in te trekken als dat het wordt gegeven. Als databasebeheerder moet je aan deze verzoeken mee werken. Zelfs binnen hele korte termijnen. Welke rol speelt een Customer Page hierbij?

Mr. Kirsten van der Zwan: Naar verwachting niet, maar de wetgeving die dit onderwerp specifiek regelt (E-Privacyrichtlijn) wordt vervangen door de E-Privacyverordening. De bedoeling is dat ook deze verordening per 25 mei 2018 van toepassing wordt. De tekst van deze verordening staat, anders dan de tekst van de AVG, nog niet vast.

* Pseudonimiseren is een procedure waarmee identificerende gegevens met een bepaald algoritme worden vervangen door versleutelde gegevens (het pseudoniem). Het algoritme kan voor een persoon altijd hetzelfde pseudoniem berekenen, waardoor informatie over de persoon, ook uit verschillende bronnen, kan worden gecombineerd. Daarin onderscheidt pseudonimiseren zich van anonimiseren, waarbij het koppelen op persoon van informatie uit verschillende bronnen niet mogelijk is.

Bouwen klantprofiel in de CRM-database

In principe geeft de klant zelf aan welke gegevens men mag opslaan. Maar we houden ook gegevens bij die de klant niet heeft opgegeven, we leggen meer vast zonder dat de klant zich dat realiseert. We bouwen aan een zo compleet mogelijk klantprofiel.

1. **Email Engagement -** We genereren data vanuit het klikgedrag in de emailcampagnes. We kennen dus de belangstelling van de klant en leggen die vast. We anticiperen automatisch op de deze data met mailflows.
2. **Aankoopgedrag -** We leggen alle details vast van het aankoop en/of boekingsgedrag van de klant. (connectoren met webshop en boekingsengines) Ook op deze data genereren we (automatisch) mailflows.
3. **Voorkeuren -** Klanten geven zelf hun belangstelling en voorkeuren aan ook deze data in onderdeel van het klantprofiel.
4. **Geografische informatie -** We leggen IP-adressen vast en koppelen daar een locatie aan op deze aardbol. Wanneer we postcode/huisnummer vastleggen hebben we een exacte woonlocatie van de klant en projecteren we dit op Google maps binnen het klantprofiel. We koppelen automatisch klanten vanuit hun geo-locatie aan de winkel bij hen in de buurt. Deze data integreren we in de digitale marketing communicatie met de klant.
5. **Social Share -** We leggen data vast m.b.t. het delen van berichten en aanbiedingen door klanten via hun social media kanalen. Op de data kan worden geanticipeerd.
6. **Web Klikgedrag -** Ook verzamelen we steeds meer data m.b.t. het klikgedrag op websites en binnen webshops. Ook die data kan onderdeel uitmaken van het klantprofiel en ook die data wordt gebruikt binnen de marketing en verkoop.
7. **Mailen vanuit geboortedatum datum informatie -** We leggen geboorte data vast. Op die gegevens creëren we mailflows.

Kunnen we al deze data blijven vastleggen?

Mr. Kirsten van der Zwan: In principe kan alles, zolang de gegevens maar op basis van de juiste grondslag worden verwerkt. Bij marketing is de grondslag toestemming de meest voor de hand liggende grondslag. Dat betekent dat de klant duidelijk, tijdig en specifiek geïnformeerd moet worden. In een privacy statement. Afhankelijk van het soort gegevens moet dit privacy statement als geheel of in onderdelen (granulair) worden geaccepteerd.

In de AVG wordt "profilering" specifiek benoemd. Meer vastleggen dan de klant zich realiseert, is nu al niet toegestaan. Gegevens moeten namelijk op transparante wijze worden verwerkt. De informatieverstrekking, vooraf, over profilering zal onder de AVG nog duidelijker moeten zijn. Geolocatiegegevens die als metadata worden meegezonden worden specifiek behandeld in het voorstel voor de e-Privacyverordening. Deze komen waarschijnlijk onder regime van uitdrukkelijke toestemming, dat is dus zwaarder dan ondubbelzinnige toestemming.

Verplaatsen klanten/prospects naar een andere database binnen het systeem

Er is een eenvoudige optie om klanten/prospects te verplaatsen naar een andere database. Bijvoorbeeld naar een ander label of ander merk.

Kunnen we dit blijven doen in het kader van de AVG?

Mr. Kirsten van der Zwan: Nee, dit mag onder de Wbp ook al niet. Dit komt in principe neer op het wijzigen van het doel waarvoor de gegevens zijn verkregen in een nieuw gebruiksdoel (ander merk). Dit kan - mits heel duidelijk - worden ondervangen door dit vooraf bij het vragen van toestemming duidelijk te maken.

Importeren, exporteren, verzenden en bewaren van persoonsgegevens via en op kantoor

Je kunt als gebruiker van iConneqt niet zomaar gegevens vanuit iConneqt exporteren.

- Het systeem wil weten dat jij gerechtigd bent om die gegevens te exporteren
- Dat gebeurt via het geverifieerd emailadres
- Pas na het klikken op de Security Button in de ontvangen email kan data worden geëxporteerd

Het probleem is dat je vervolgens die persoonsgegevens hebt opgeslagen in een niet beveiligde kantooromgeving. Dat is natuurlijk risicovol. Hetzelfde geldt voor het veel voorkomende verzenden van persoonsgegevens via de mail als bestandsbijlage.

De vraag is hoe gaan we hier volgend, of eigenlijk vandaag al, mee om?

Mr. Kirsten van der Zwan: Dit zijn typische onderwerpen die in een privacybeleid moeten worden afgesproken. Dit gaat over het gedrag van de mensen die met de gegevens werken. Deze mensen vormen een belangrijke schakel in de beveiliging van persoonsgegevens. Beveiliging betekent naast het treffen van technische ook het treffen van organisatorische maatregelen. Privacybeleid (interne gedragsregels), training van medewerkers (awareness) en het aanstellen van een privacy officer horen daarbij. Vergeet ook het draaiboek datalekken niet. Zodra gegevens buiten de organisatie worden gedeeld, dan moeten er ook bewerkersovereenkomsten worden gesloten.

Telefonisch bij klantenservice persoonsgegevens aanpassen, aanmelden/afmelden

In de praktijk zien we dat klanten de klantenservice bellen om te vragen persoonsgegevens te registreren, aan te passen of klanten geven bijvoorbeeld aan dat ze zich willen afmelden van een nieuwsbrief.

We kunnen moeilijk vaststellen dat de persoon aan de telefoon ook de persoon is die in de database is vastgelegd.

Hoe gaan we hier mee om?

Mr. Kirsten van der Zwan: Leuke vraag. Als je het boek van Maria Genova, "Komt een vrouw bij de hacker" leest of een van haar lezingen bijwoont, dan weet je dat de klantenservice van veel bedrijven de zwakke schakel in de beveiliging zijn. Ook hier geldt weer: maak een privacybeleid. Maak afspraken over het aanpassen, verstrekken en verwerken van persoonsgegevens door een klantenservice. En beter nog: verwijs mensen naar Customer Page en laat ze zelf de aanpassingen doen.

Aankoop van bestanden van listbrokers

In bepaalde branches en door gebruikers van iConneqt wordt regelmatig gebruik gemaakt van externe bestanden. Dat zijn dan persoonsgegevens die verzameld zijn door externe partijen.
Deze - bijvoorbeeld nieuwsbriefabonnees- worden dan geïmporteerd of vaak automatisch via een connector/API, ingevoerd als nieuwe potentiële klant.

Hoe kan ik zorgen dat dit binnen de nieuwe wet- en regelgeving geen probleem gaat worden?

Mr. Kirsten van der Zwan: Dat wordt een uitdaging, en dat is het overigens nu al. Er zal in commerciële afspraken aandacht gegeven moeten worden aan aansprakelijkheid en vrijwaringen. Wie vraagt de toestemming? Op de juiste (duidelijk, specifiek) manier? Wie mag het woord voeren als de toezichthouder op bezoek komt. Wie betaalt de boete? Kortom, contractwerk.

Stuur door aan een vriend optie

Het is technisch mogelijk dat klanten, nieuwe klanten of nieuwe nieuwsbriefabonnees aanbrengen. Deze personenen hebben dus niet zelf een handeling uitgevoerd waarin ze aangeven dat ze informatie willen ontvangen.

Mag ik dan wel een mail sturen aan die mensen met de vraag of ze informatie willen ontvangen, met een referentie aan de klant die dit initiatief heeft genomen?

Mr. Kirsten van der Zwan: Tell-a-friend acties zijn nu onder voorwaarden toegestaan door de ACM. Dit staat ook vermeld op de website van de ACM. Ook dit onderwerp valt onder de wetgeving die gaat veranderen, maar waarvan we de tekst nu nog niet definitief weten.

Social Monitoring/Klantenservice

Er zijn connectoren gebouwd om gegevens vanuit uit iConneqt te integreren in Social Monitor systemen als Freshdesk. (.....wat schrijft men over mijn merk op social media...). Deze gegevens worden ook vastgelegd deels in de CRM-database van iConneqt en deels in de separate Social Monitor database.

De vraag is, mag ik de helpdesk/klantenservice incidenten vanuit het social media verkeer en vanuit telefoon- en emailverkeer vastleggen in de database?

Mr. Kirsten van der Zwan: Lastig. Wat is de grondslag van deze verwerking vanuit social media verkeer? In principe blijft alleen de “gerechtvaardigd belang” grondslag als mogelijkheid over. Om van die grondslag gebruik te maken moeten een behoorlijk zware belangenafweging worden uitgevoerd, moet ook sprake zijn van noodzakelijkheid om de gegevens te verwerken. Ik vermoed dat bij deze afweging de conclusie zal zijn dat deze vorm van monitoring net zo effectief op anonieme basis kan gebeuren. Wat is het belang van het vastleggen van een mening geuit op social media (en dus niet rechtstreeks aan de klantenservice) in het CRM systeem in iemands profiel?

Beveiliging gegevens

De gegevens van iConneqt worden opgeslagen in streng beveiligde datacenter binnen de Europese gemeenschap.

- Het inloggen wordt gecontroleerd op IP-niveau
- Wanneer een gebruiker op een andere locatie werkt. Bijvoorbeeld thuis, dan moet eerst via het geverifieerde emailadres de gebruiker aangeven dat hij of zij het daadwerkelijk is
- Dezelfde beveiliging geldt voor het verzenden van emailcampagnes en het exporteren van gegevens

Het bovenstaande betekent niet dat er binnen een woonomgeving geen ongeoorloofd gebruik van de persoonsgegevens kan worden gemaakt. Ook kan men online werken in openbare locaties als luchthavens, bibliotheken en coffeeshops. Dat zijn gevaarlijke locaties i.v.m. hacking. Is het niet wenselijk gezien de nieuwe zware verantwoordelijkheid rond het beheer van persoonsgegevens om de toegang tot die gegevens te beperken tot het vastgestelde kantooromgeving op basis van vastgelegde en geverifieerde IP-adressen?

Mr. Kirsten van der Zwan: De eisen rondom beveiliging van persoonsgegevens zijn niet nieuw. De aandacht ervoor wel. En terecht. Welke passende en organisatorische beveiligingsmaatregelen een onderneming neemt, is een eigen afweging. Uiteraard moet in die afweging gekeken worden naar de technische mogelijkheden, de aard van de gegevens (financiële gegevens? gezondheidsgegevens?) en de mogelijke risico's. Een BYOD protocol, privacybeleid waarin een verbod staat om via niet beveiligde wifi te werken en wachtwoordbeleid zijn allemaal zaken die goed vastgelegd moeten zijn. En geïmplementeerd door middel van training van medewerkers. Uiteraard moet er - voor het geval dat het fout gaat - ook een draaiboek datalekken klaar liggen. Een datalek moet binnen 72 uur worden gemeld. Als je dan eerst nog moet gaan nadenken over hoe je een lek achterhaald, waar je gegevens kan terugvinden, hoe je wilt communiceren naar klanten, dan heb je waarschijnlijk te weinig tijd. Een draaiboek datalekken geeft houvast op zo'n moment.

Personeelswisselingen

Om beveiligingsredenen hebben de gebruikers van iConneqt allen een persoonlijk gebruikerslicentie. Maar in de praktijk hebben we geleerd dat bij verloop van personeelsleden er niet altijd adequaat wordt gereageerd m.b.t. het afsluiten van de toegang tot de klantgegevens (persoonsgegevens).

Zegt de AVG hier iets van? Zouden bedrijven en hun leveranciers bijvoorbeeld niet technische maatregelen moeten nemen om de kans dat ongeoorloofde toegang tot de klantdata aan de orde is (niet meer werkzaam bij het bedrijf) te beperken?

Mr. Kirsten van der Zwan: Beveiliging van persoonsgegevens betekent maatregelen nemen tegen onrechtmatige verwerking. Dit is misbruik, ongeoorloofde toegang of ongewenste wijziging van gegevens. De maatregelen die genomen moeten worden zijn technische en organisatorische maatregelen. De omschreven situatie móet dus door organisatorische maatregelen worden voorkomen. Dit is simpelweg een verplichting voor iedereen die data beheert. In dit geval is een organisatorische maatregel: privacybeleid, wachtwoordbeleid, toegangsbeleid, diverse email/internet/BYOD protocollen en regelmatige van training medewerkers. Het bijhouden en up to date houden van wie welke toegangsrechten heeft, valt dus onder dit beleid. Als een controle op toegangsrechten technisch is in te regelen dan is dit absoluut aan te raden.

Wat levert het nemen van technische en organisatorische maatregelen op? Een risico verlaging op datalekken. In de praktijk kosten datalekken naast veel geld (forensische onderzoekskosten, tijd van medewerkers) ook de nodige reputatieschade op. De AP heeft naar aanleiding van de melding van datalekken (verplicht sinds 1 januari 2016) al een aantal onderzoeken gestart naar de gehele organisatie die het datalek melde. Reken maar dat daar een aantal overtreding van de wet uit blijken.

Bewaren persoonsgegevens

Organisaties mogen persoonsgegevens in een archief bewaren als dit bestemd is voor historische, statistische of wetenschappelijke doeleinden. De organisatie moet de gegevens vernietigen als ze niet meer nodig zijn voor het doel van het archief.

Klant en/of prospectgegevens wil je vanuit de marketing zelden vernietigen. Ze zijn om te beginnen noodzakelijk voor statistisch onderzoek. Daarnaast zou je afgemelde personen wellicht weer willen activeren. Legaal, dus bijvoorbeeld via de brievenbus. Mogen wij vanuit deze vaststelling ook onder het AVG-regime onbeperkt de klantgegevens bewaren?

Mr. Kirsten van der Zwan: De Wet bescherming persoonsgegevens (Wbp) bepaalt dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor de verwerkelijking van het doel waarvoor ze zijn verzameld. De AVG kent in artikel 5.1.e een soortgelijke bepaling. Dit is een algemene regel, waarvan de uitwerking per situatie kan verschillen. Is het doel waarvoor de persoonsgegevens zijn verwerkt niet meer aanwezig, dan moeten deze gegevens worden verwijderd. Aan de andere kant zijn er ook vanuit de overheid wetten die je verplichten bepaalde gegevens te bewaren. Kortom, dit vraagt om een individuele toetsing en een beleid dat per onderneming/instelling kan verschillen.

Data protection officer

We hebben begrepen dat er een DPO moet worden benoemd (Data Protection Officer). De DPO zou er vanuit het bedrijf op toe moeten zien dat de wet en regelgeving m.b.t.de privacy wordt nageleefd.

Moeten alle bedrijven een DPO aanstellen of is dit uitsluitend een verplichting van overheid- en overheidsorganisaties?

Mr. Kirsten van der Zwan: Er zijn verschillende gevallen waarin een organisatie verplicht is een DPO te hebben. Dit is een nieuwe verplichting in de AVG. Wanneer je organisatie een overheidsinstantie of overheidsorgaan is moet je een DPO hebben. Maar ook een bedrijf of instelling die marketing technologie hanteert en dus op grote schaal mensen regelmatig of stelselmatig monitort en deze data verwerkt zullen hier onder gaan vallen. Want alhoewel er geen definitie in AVG staat is monitoring in ieder geval elke vorm van tracking en profilering op binnen email campagnes en/of op internet. Dus ook behavioural advertising, marketing automation vallen hieronder.

Privacy beleid op papier

We begrepen dat er extra documentatieverplichtingen voor organisaties die persoonsgegevens verwerken bijkomen.

Moeten alle bedrijven en instellingen die klantgegevens (persoonsgegevens) verwerken hun activiteiten documenteren?

Mr. Kirsten van der Zwan: Ja en nee. De verplichting om een overzicht van verwerkingen bij te houden (art 30 AVG) geldt niet voor bedrijven met minder dan 250 werknemers. Tenzij de verwerking risicovol is, niet incidenteel is of tenzij er bijzondere persoonsgegevens worden verwerkt. Aan de andere kant brengt de beveiligingsverlichting automatisch met zich mee dat er een privacybeleid en diverse procedures moeten zijn. De informatieplicht brengt met zich mee dat er een privacy statement moet zijn. Als algemene verplichting geldt dat aantoonbaar in overeenstemming met de AVG wordt verwerkt. Dit kan eigenlijk ook alleen maar door een compliance programma te tonen. Het is op termijn ook mogelijk om dit door middel van certificering aan te tonen.

Handhaving en boetes

We begrepen dat de handhaving op de nieuwe regels strenger gaat worden en dat de boetes bij overtredingen hoog zijn.

Wanneer komen wij, die klantgegevens verwerken, in het risicogebied en wanneer lopen we kans op een boete?

Mr. Kirsten van der Zwan: EEen boete wordt alleen direct bij de constatering van een overtreding opgelegd als sprake is van opzettelijk handelen, voorwaardelijk opzet of ernstig verwijtbare nalatigheid. Dit zijn gevallen waarin bewust, opzettelijk of ernstig onzorgvuldig met gegevens wordt omgegaan. De Autoriteit Persoonsgegevens (afgekort AP) geeft zelf als voorbeeld de situatie waarin een tv-maker op de Eerste Hulp van een ziekenhuis filmde. In alle andere gevallen moet de AP eerst een bindende aanwijzing geven.

Een punt van aandacht is dat de AP, net als de ACM en AFM, een bestuursorgaan is. De boete is een administratieve boete in de zin van de Algemene Wet Bestuursrecht. Dit betekent dat de AP niet alleen de overtreder zélf een boete mag opleggen, maar ook de 'functionele dader', de 'feitelijk leidinggevende' en de 'medepleger'. In de praktijk kan dit betekenen dat een directeur of bestuurder naast de rechtspersoon een boete kan krijgen. Ook is het mogelijk dat de partij die in nauwe samenwerking ondersteuning biedt bij de dataverwerking, een boete krijgt. Dit speelt bijvoorbeeld bij het bouwen van een app of webshop of andere online marketing servers zoals CRM, en emailmarketing.

Hoogte boetes

De boetebedragen zijn ingedeeld in 3 bandbreedtes. De hoogste categorie bedraagt € 350.000 tot € 820.000 pér overtreding. Boetebedragen kunnen cumuleren. De AP kan ook besluiten om een boete gelijk aan 10% van de netto-omzet van de overtreder op te leggen. In 2018 wordt de maximale boete € 20 miljoen of 4% van de wereldwijde jaaromzet van de overtreder. De AP neemt alle omstandigheden van het geval mee in haar boeteoplegging.

www.iconneqt.nl