DATA DRIVEN MARKETING ASSOCIATION

DE AVG IN 10 STAPPEN

CHECKLIST VOOR ORGANISATIES

DE AVG IN 10 STAPPEN – CHECKLIST VOOR ORGANISATIES

Staat privacy al op de agenda van jouw organisatie? Gebruik deze checklist en maak je collega's bewust van de impact van de AVG!

Vanaf 25 mei 2018 moeten bedrijven, overheidsorganisaties, non-profits en verenigingen die persoonsgegevens verwerken zich houden aan de nieuwe privacywetgeving: de Algemene Verordening Gegevensbescherming (AVG). Deze wet vervangt de huidige Wet bescherming persoonsgegevens en stelt strengere eisen aan de manier waarop persoonsgegevens worden verwerkt.

Uit de AVG Status Check van DDMA, waarin wordt gevraagd naar de stand van zaken op verschillende onderdelen van de AVG, blijkt dat organisaties 2,1 op een schaal van 4 scoren. De meeste organisaties voldoen dus nog niet aan alle nieuwe verplichtingen. Daarom heeft DDMA een checklist opgesteld ter ondersteuning bij de invoering van de AVG.

Over DDMA

DDMA is de brancheverenigingvoor data driven marketing. De AVG is daarom voor de leden van DDMA van groot belang. Wil je meer weten van de AVG? Schrijf je dan hier in voor de DDMA nieuwsbrief. Als je naar aanleiding van deze checklist vragen hebt, neem dan contact op via **legal@ddma.nl**, of bel naar 020 - 45 28 413.

STAP 1.
MAAK BELANGRIJKE PERSONEN BINNEN JOUW ORGANISATIE BEKEND MET DE AVG.

Implementatie van de AVG kan, afhankelijk van de manier waarop persoonsgegevens binnen jouw organisatie worden verwerkt, veel tijd en budget in beslag nemen. Een goed plan van aanpak is daarom onmisbaar. Breng verantwoordelijken en uitvoerders op het gebied van IT, marketing, data, beveiliging en juridische zaken bij elkaar en zorg voor een plan van aanpak, afgestemd op de dataverwerkingen binnen jouw organisatie en de bijkomende risico's.

Het succes van dit plan van aanpak hangt voor een groot deel af van interne communicatie. Privacy wordt pas goed beschermd als het onderwerp binnen de hele organisatie bekend is. Een datalek kan immers ook binnen de hele organisatie optreden. Juist ook op de marketingafdeling, waar dagelijks gewerkt wordt met data, is bewustzijn voor een mogelijk datalek of een schending van de privacywet cruciaal.

Het intern bekendmaken van de AVG-aanpak is geen eenmalige exercitie. Training vormt een belangrijk onderdeel van bewustwording binnen de organisatie. Denk aan webinars, kennissessies of verplichte workshops voor huidige en nieuwe werknemers. Ook is het belangrijk om, zeker in de eerste periode na de invoering van de wet, de AVG continue top-of-mind te houden van medewerkers.

STAP 2.
BRENG IN KAART WELK(E) (TYPE) PERSOONSGEGEVENS JOUW ORGANISATIE VERWERKT, VOOR WELKE

DOELEINDEN JE DE GEGEVENS GEBRUIKT EN MET WELKE ORGANISATIES JE ZE HEBT GEDEELD. EN, LEG (INDIEN NODIG) EEN VERWERKINGSREGISTER AAN.

Onder de AVG moeten organisaties kunnen laten zien dat zij zich houden aan de privacywetgeving. Daarvoor kun je een 'verwerkingenregister' bijhouden. In veel gevallen is dit zelfs verplicht. Uit dit register moet bijvoorbeeld duidelijk worden welk(e) (categorieën) persoonsgegevens je verwerkt, wat de verwerkingsdoeleinden zijn, wat de bron van die gegevens is, met welke partijen de gegevens worden gedeeld, of de gegevens worden doorgegeven naar buiten de EU en wat de bewaartermijn van de gegevens is.

Onder de AVG moet je ook kunnen aantonen dat je persoonsgegevens verwerkt met een rechtmatige grondslag. Neem deze grondslagen daarom ook op in het register. Is het noodzakelijk om de gegevens te verwerken voor het uitvoeren van een overeenkomst? Bijvoorbeeld bij het toesturen van tickets of het factureren van een abonnement. Past het binnen het gerechtvaardigd belang van jouw organisatie, en zo ja waarom? Of heb je toestemming gevraagd voor de verwerking? Bijvoorbeeld bij het gebruik van social media. Als er geen rechtmatige grondslag is voor de gegevens die jouw organisatie verwerkt, dan loop je een risico. Verwijder daarom die gegevens.

Deze exercitie wordt ook wel 'data mapping' genoemd en kan soms behoorlijk wat tijd in beslag nemen. Een voordeel van data mapping is dat veel duidelijk wordt over de datastromen binnen jouw organisatie, dat het je helpt processen efficiënter in te richten en nieuwe verplichtingen onder de AVG helder te krijgen.

STAP 3.
CONTROLEER OF HET VERPLICHT IS OM EEN FUNCTIONARIS GEGEVENSBESCHERMING (FG) AAN TE STELLEN. EN ZO JA, SCHRIJF HEM/HAAR IN BIJ DE AP.

Een FG controleert de organisatie met betrekking tot privacy

en databescherming. Een FG ziet erop toe dat je organisatie de AVG naleeft, heeft eventueel contact met de AP en adviseert de organisatie over de inzet van persoonsgegevens. Je kan een FG in dienst nemen, maar je kan een FG ook extern aanstellen. Een FG opereert met een bepaalde onafhankelijkheid ten opzichte van de organisatie en kan bijvoorbeeld niet ontslagen worden omdat het advies tot gevolg heeft dat persoonsgegevens niet langer kunnen worden verwerkt.
De AVG stelt geen specifieke opleiding voor de FG verplicht, maar de FG moet wel de nodige kennis hebben van de privacy- en databeschermingsverplichtingen van de organisatie.

Voor sommige organisaties is een FG verplicht. Namelijk als je bijzondere persoonsgegevens verwerkt (zoals gegevens over gezondheid, ras of politieke voorkeur), als je bij een overheidsorganisatie werkt, of (kort gezegd) als de verwerking van persoonsgegevens vanwege andere redenen een hoog risico met zich meebrengt. Deze laatste grond is ruim geformuleerd, maar niet voor iedereen van belang. Bouw jij grote profielen op? Zijn persoonsgegevens verbonden met de kerntaak van je organisatie?

En verwerk je op grote schaal persoonsgegevens? Dan kan dat betekenen dat je een FG moet aanstellen.

STAP 4.
STEL EEN PRIVACY IMPACT ASSESSMENT (PIA) VAST EN BRENG IN KAART WANNEER JE DEZE UIT MOET VOEREN.

Met een PIA beoordeel je het effect van een specifieke verwerking van persoonsgegevens. Dit doe je onder andere door in kaart te brengen welk type gegevens wordt verwerkt, voor welke doeleinden, of er met derde partijen wordt samengewerkt, of de gegevens naar buiten de EU worden gebracht, of er

profielen worden opgebouwd en welke beslissingen er op basis van een profiel worden genomen. Afhankelijk van de uitkomst kan worden besloten de verwerking te stoppen, aan te passen of door te laten gaan.

In de PIA moet in ieder geval worden meegenomen welke gegevens worden verwerkt voor welke doeleinden, wat het gerechtvaardigde belang is om de verwerking uit te voeren, een beoordeling van de noodzaak en de evenredigheid van de verwerking, een beoordeling van de risico's voor de individuen en eventuele waarborgen of maatregelen om de impact te beperken.

Onder de AVG is een PIA in sommige gevallen verplicht, met name wanneer het waarschijnlijk is dat de verwerking, of een reeks verwerkingen, een hoog risico met zich meebrengt voor de privacy van individuen. Bijvoorbeeld bij uitgebreide profilering, automatische besluitvorming op basis van analyses, de verwerking van bijzondere persoonsgegevens (ras, gezondheid etc.) of gevoelige persoonsgegevens, de verwerking van persoonsgegevens van kwetsbare personen (bijvoorbeeld kinderen), bij nieuwe technologieën, of bij een verwerking op grote schaal.
Omdat bij veel innovaties data worden ingezet, is het aan te raden om bij het ontwikkelen van elke nieuwe dienst, veelomvattende campagne of applicatie een PIA te doen. Hiermee voeg je als het ware een extra controlesysteem aan je werkwijze toe. Bij een vaak terugkerende actie, zoals het sturen van een nieuwsbrief naar een vaste groep, hoef je niet steeds opnieuw een PIA te doen.

STAP 5.
IMPLEMENTEER PRIVACY BY DESIGN EN PRIVACY BY DEFAULT.

'Dataminimalisatie' is een belangrijk begrip onder de AVG. Dit houdt in dat je bij het verzamelen en verwerken van persoonsgegevens niet meer gegevens

verwerkt dan nodig is om het doel te bereiken waarvoor de gegevens gebruikt worden. Bijvoorbeeld door gegevens niet langer te bewaren dan nodig is. De verantwoordelijke moet daarom bewaartermijnen vaststellen van de persoonsgegevens die de organisatie verwerkt. Daarnaast realiseer je dataminimalisatie door het toepassen van privacy by design en privacy by default.

Privacy by design betekent dat je bij het ontwerp van producten al rekening houdt met gegevensminimalisatie. Bijvoorbeeld door gegevens zo veel mogelijk te pseudonimiseren en anonimiseren. En door overbodige gegevens direct te verwijderen. Privacy by default betekent dat de standaardinstellingen zo privacyvriendelijk mogelijk zijn. Bijvoorbeeld door de optie ‘gegevens delen met derden’ standaard uit te zetten, totdat een individu dat wijzigt.

STAP 6.
SLUIT (AANVULLENDE) VERWERKERSOVEREENKOMSTEN AF.

Bij de verwerking van persoonsgegevens zijn vaak meerdere partijen betrokken. Een organisatie werkt bijvoorbeeld samen met een marketingbureau om de websiteconversie te verhogen. Bepaal allereerst wat de rol van jouw organisatie is: ben je de primair verantwoordelijke of ben je verwerker? En sluit zo nodig een (aanvullende) verwerkersovereenkomst af.

Een verantwoordelijke is de partij die het ‘doel en de middelen’ van de verwerking bepaalt. Dit zijn vaak de kernvragen over de persoonsgegevens, zoals: welke persoonsgegevens worden gebruikt, hoe lang worden de gegevens opgeslagen en voor welk doeleinde worden de gegevens verwerkt? Een verwerker werkt vaak in opdracht van een verantwoordelijke om een deel van de verwerking uit te voeren. Denk aan een Email Service Provider, een telemarketingbedrijf of een search optimalisatie bureau. Het kan ook zijn dat twee partijen verantwoordelijke zijn. Dat hangt af van de manier waarop gegevens worden verwerkt. Ook indien er twee verantwoordelijken zijn,

moeten er duidelijke afspraken worden gemaakt over de beveiliging van de gegevens en de rechten van individuen.

Onder de AVG is het verplicht (net als onder de huidige wet) om een verwerkersovereenkomst te sluiten. In die verwerkersovereenkomst moet onder andere staan dat de verwerker de gegevens voldoende zal beveiligen, dat er toestemming wordt gevraagd voor het inschakelen van een sub-verwerker en dat de verwerker alleen handelt conform de instructies van de verantwoordelijke.
Modelverwerkersovereenkomst kan hier aangevraagd worden.

STAP 7.
STEL PROCEDURES OP OM DE RECHTEN VAN BETROKKENEN UIT TE KUNNEN VOEREN.

De AVG heeft onder andere als doel om individuen meer controle uit te laten oefenen over hun gegevens. Iedereen heeft al een aantal rechten, zoals het recht van verzet, recht op inzage en recht op correctie. Het recht op verzet bij marketing houdt bijvoorbeeld in dat iedereen verzet moet kunnen aantekenen tegen de verwerking van persoonsgegevens voor marketingdoeleinden. Zo´n verzet moet direct worden gehonoreerd. Mensen mogen ook inzage vragen in welke gegevens er van hen worden verwerkt, en voor welke doeleinden. Onder de AVG komen er een aantal nieuwe rechten bij.

Het recht op dataportabiliteit houdt in dat individuen hun persoonsgegevens kunnen overdragen van de ene organisatie naar de andere. Bijvoorbeeld doordat een consument zijn transactiedata naar een andere bank wil meenemen. Het idee hierachter is dat de concurrentie wordt vergroot. Dataportabiliteit heeft alleen betrekking op gegevens die de consument zelf heeft aangeleverd (bijvoorbeeld inloggegevens zoals e-mail en wachtwoord) en gegevens die een consument met het gebruik van het product heeft gegenereerd (bijvoorbeeld zoekgeschiedenis of klikgedrag). Profielinformatie of

een analyse naar aanleiding van het gedrag van het individu valt hier niet onder.

Het recht om vergeten te worden – onder de AVG ‘recht op vergetelheid’ – houdt in dat individuen in een aantal gevallen hun gegevens kunnen laten wissen. Bijvoorbeeld als de gegevens niet langer nodig zijn voor het doel waarvoor ze zijn verkregen, als de gegevens onrechtmatig zijn verwerkt of als iemand niet wil dat zijn gegevens voor direct-marketingdoeleinden worden verwerkt. Als de gegevens openbaar zijn gemaakt, moeten er maatregelen worden genomen om ervoor te zorgen dat de openbaar gemaakte gegevens ook worden gewist.

STAP 8.
BRENG IN KAART WAAR BINNEN JOUW ORGANISATIE TOESTEMMING WORDT GEVRAAGD VOOR DE VERWERKING VAN PERSOONSGEGEVENS EN CONTROLEER OF DIT VOLDOET AAN DE EISEN VAN DE AVG.

De verwerking van persoonsgegevens kan gebaseerd zijn op toestemming. Toestemming moet worden gegeven door een actieve handeling, bijvoorbeeld het aantikken van een vakje of een andere actieve handeling in de customer journey. De AVG stelt strengere eisen aan toestemming die er in de praktijk met name op neerkomen dat je beter moet kunnen aantonen dat toestemming is verkregen. Toestemming moet duidelijk en eenvoudig zijn. Ook moet het intrekken van toestemming net zo eenvoudig zijn als het geven van de toestemming. Daarnaast mag toestemming niet een voorwaarde zijn voor het uitvoeren van een overeenkomst. De toestemming is in dat geval niet ‘vrij’ gegeven.

Stel dat iemand online een krantabonnement afsluit. Een aantal persoonsgegevens zullen noodzakelijk zijn voor het uitvoeren van de overeenkomst; bijvoorbeeld het (bezorg)adres en het bankrekeningnummer.

Daarnaast mag je een aantal gegevens verwerken om je gerechtvaardigde (marketing)belang uit te oefenen. Maar voor vergaande verwerkingen zal je toestemming moeten vragen. Bijvoorbeeld het opbouwen van profielen met daarin gevoelige informatie, zoals gegevens over kinderen of andere kwetsbare groepen. Dit kun je doen door bij het aangaan van het krantabonnement actief deze toestemming te vragen. Informeer duidelijk waar de toestemming betrekking op heeft, geef individuen de mogelijkheid om geen toestemming te geven en verwijs naar een helder en overzichtelijk privacy statement waarin individuen alle nodige informatie kunnen nalezen. De toestemming moet te allen tijde ingetrokken kunnen worden.

STAP 9.
STEL EEN DATABEVEILIGINGSBELEID OP EN BLIJF DIT BELEID TOETSEN EN VERBETEREN.

De beveiliging van persoonsgegevens moet zowel technisch als organisatorisch goed geborgd zijn. Denk bij het opstellen van een databeveiligingsbeleid in ieder geval aan de volgende onderdelen:

- Toegangscontrole, met gebruik van wachtwoorden. Heeft iedereen alleen toegang tot de gegevens die hij/zij over een persoon nodig heeft?
- Logging van handelingen rondom de persoonsgegevens
- Fysieke maatregelen voor toegangsbeveiliging, bijvoorbeeld van het pand
- Encryptie (versleuteling) van digitale bestanden met persoonsgegevens
- Steekproefsgewijze controle op naleving van het beleid
- Beheer van kopieën en back-ups
- Beveiliging van netwerkverbindingen, zowel intern als extern

STAP 10.
STEL EEN PROTOCOL MELDPLICHT DATALEKKEN OP.

De meldplicht datalekken blijf onder de AVG bestaan. Je moet een register bijhouden van alle datalekken die hebben plaatsgevonden. Maar je hoef niet ieder datalek te melden bij de toezichthouder. Als het onwaarschijnlijk is dat het datalek leidt tot een risico voor de individuen dan hoef je het datalek niet te melden. Aan de andere kant moet je een datalek ook bij het individu melden als het lek een hoog risico met zich meebrengt. Een gehackte website, een verloren USB-stick, laptops etc. maar ook een vernietigde host-omgeving zonder back-up kan een datalek opleveren.

Afhankelijk van het type gegevens, de hoeveelheid gegevens en de context van het lek moet je bepalen of een lek gemeld moet worden bij de toezichthouder. Vervolgens moet je nagaan of een datalek ook bij het individu moet worden gemeld. De melding moet worden gedaan door de verantwoordelijke, niet door de verwerker. De toezichthouder heeft standaard meldingsformulieren opgesteld. Een melding moet binnen 72 uur na de ontdekking van het lek worden gedaan. Omdat dit in de praktijk vaak kort is, is het raadzaam een protocol op te stellen zodat snel gehandeld kan worden. Houd hierbij ook rekening met vakanties, ziekte en dergelijke.

CHECKLIST

	Actie	Door wie?	Gereed?
1	Maak belangrijke personen binnen jouw organisatie bekend met de AVG.		
2	Breng in kaart welk(e) (type) persoonsgegevens jouw organisatie verwerkt, voor welke doeleinden je de gegevens gebruikt en met welke organisaties je ze hebt gedeeld. En, leg (indien nodig) een verwerkingenregister aan.		
3	Controleer of het verplicht is om een Functionaris Gegevensbescherming (FG) aan te stellen. En zo ja, schrijf hem/ haar in bij de AP.		
4	Stel een Privacy Impact Assessment (PIA) vast en breng in kaart wanneer je deze moet uitvoeren.		
5	Implementeer privacy by design en privacy by default.		
6	Sluit (aanvullende) verwerkersovereenkomsten af.		
7	Stel procedures op om de rechten van betrokkenen uit te kunnen voeren		
8	Breng in kaart waar binnen jouw organisatie toestemming wordt gevraagd voor de verwerking van persoonsgegevens en controleer of dit voldoet aan de eisen van de AVG		
9	Stel een databeveiligingsbeleid op én blijf dit beleid toetsen en verbeteren.		
10	Stel een protocol meldplicht datalekken op.		

VOORUITBLIK: DE EPRIVACY VERORDENING

Het is nog niet gedaan na de AVG-voorbereidingsdeadline van 25 mei 2018. Als eerste is het zaak dat je compliant blijft aan de wetgeving en dat vraagt om een doorlopend proces: denk aan het onderhouden van het verwerkingenregister, het regelmatig uitvoeren van een Privacy Impact Assessment en bewustzijn blijven creëren onder medewerkers. Als tweede is er nog een nieuwe Europese wetgeving op komst die grote impact gaat hebben op je bedrijfsvoering: de ePrivacy Verordening.

De ePrivacy Verordening vervangt de huidige Telecommunicatiewet en bevat regelgeving over de inzet van verschillende marketingkanalen. Onder meer e-mail en telemarketing worden gereguleerd onder deze nieuwe wet en ook de huidige cookieregels moeten er aan geloven. Net als de AVG brengt ook de ePrivacywet de nodige voorbereidingen met zich mee voor bedrijven. Op dit moment is nog niet precies bekend hoe de wet er precies uit gaat zien en wanneer de wet ingaat. Toch is DDMA alvast gestart met een voorlichtingstraject, zodat we bedrijven nu al op de hoogte kunnen houden van alle ontwikkelingen.