Whitepaper Privacy wetgeving (AVG)

De nieuwe privacy wetgeving raakt álle ondernemers.

Ben jij al voorbereid?

Willeke van den Heuvel
Mijn Gereedschapskist
Juli 2017

De nieuwe privacy wetgeving raakt álle ondernemers. Ben jij al voorbereid?

Per 28 mei 2018 gaat de nieuwe Europese privacywetgeving in en maar liefst 60% van de bedrijven is niet op de hoogte hiervan. Zij lopen daarmee een risico op boetes die op kunnen lopen tot 20 miljoen euro, 4% van hun (wereldwijde) jaaromzet of een behoorlijke reputatie/imago schade.

In dit artikel probeer ik zoveel mogelijk in te gaan op de consequenties voor bedrijven als gevolg van deze nieuwe wetgeving. Nog niet alle informatie is op dit moment 'eenduidig' uit te leggen, al in zijn geheel uitgewerkt of het ontbreekt gewoonweg nog aan jurisprudentie. Nieuwe informatie zal worden aangevuld zodra deze beschikbaar is.

Waarom privacy wetgeving?

Het vertrouwen van consumenten in de mate waarin zij zich veilig voelen op internet, is de afgelopen jaren fors afgenomen. 80% van de consumenten geeft aan zich zorgen te maken over de hoeveelheid (persoonlijke) gegevens die online bekend zijn en bijna 70% voelt zich niet beschermt door wetgeving.

Nieuwe wetten en regels moeten ervoor zorgen dat dat vertrouwen weer toeneemt. Door de invoering hiervan wil de Europese Unie ervoor zorgen dat bedrijven "adequate maatregelen" treffen om de data die zij verwerken, voldoende te beschermen.

Welke nieuwe wetgeving?

Wet bescherming persoonsgegevens

De Wet bescherming persoonsgegevens (Wbp) bepaalt op dit moment binnen Nederland aan welke eisen een bedrijf moet voldoen als het gaat om het in bezit hebben, verwerken en gebruiken van persoonlijke data (http://wetten.overheid.nl/BWBR0011468/2017-07-01).

Deze wetgeving is in het jaar 2000 in gegaan. In de afgelopen 17 jaar zijn de technische ontwikkelingen echter in een gigantische stroomversnelling geraakt met als gevolg dat er veel meer persoonlijke gegevens van consumenten beschikbaar zijn.

Voorbeeld: wanneer iemand een e-boek download dan is vaak naast het e-mail adres ook de voornaam bekend maar ook het IP adres. Deze gegevens zijn weer te koppelen aan social media profielen waardoor nog meer informatie beschikbaar is (geslacht, foto, woonplaats, huwelijkse staat, etc). Al die gegevens van verschillende bronnen zijn makkelijker aan elkaar te koppelen waardoor een bedrijf een heel profiel van jou als burger kan samenstellen. Deze informatie is heel relevant om je directe, op maat gemaakte, aanbiedingen te doen, maar levert ook een risico op. Wat als een hacker er met deze data vandoor gaat, wat als een bedrijf deze data verkoopt?

Algemene Verordening Gegevensbescherming

Sinds 2012 werkt de Europese Commissie aan vernieuwde wetgeving: de **Algemene Verordening Gegevensbescherming** (AVG). In Europa beter bekend als de Global Data Protection Regulation (GDPR). Deze nieuwe wet is al op 28 mei 2016 ingegaan, maar Europa heeft bepaald dat bedrijven 2 jaar de tijd krijgen om alle aanpassingen door te voeren. Uiterlijk 28 mei 2018 moeten bedrijven dus voldoen aan deze nieuwe wetgeving! Tot die tijd geldt de Wet bescherming persoonsgegevens nog.

Naleving van nieuwe wetgeving

De controle op de naleving en het opleggen van boetes wordt uitgevoerd door de Europese privacy toezichthouders. In Nederland is dit de Autoriteit Persoonsgegevens (AP).

Een bedrijf dat zich niet houdt aan de privacywetgeving loopt het risico een boete te krijgen die kan oplopen tot 4% van de jaarlijkse omzet die het bedrijf wereldwijd realiseert of maximaal 20 miljoen euro.

Verder kan de Meldplicht Datalekken (die nu al in Nederland van kracht is) tot behoorlijke reputatie/imagoschade leiden. Bedrijven die gehackt zijn moeten dit doorgeven, niet alleen aan het Meldpunt maar ook soms aan de personen van wie de gegevens zijn gestolen. Een dergelijke publicatie kan al snel leiden tot merkschade, verlies van klanten en eventueel juridische kosten als klanten hun schade gaan verhalen. Het kan zelfs voorkomen dat de toezichthouder het gebruiken van data stop zet (tijdelijk of definitief) als herstel van het lek niet adequaat wordt uitgevoerd. Je kunt dan als bedrijf vaak niet veel meer.

Voor wie geldt de Algemene Verordening Gegevensbescherming?

De wetgeving geldt voor alle organisaties die persoonlijke data van Europese burgers verwerken. In eerste instantie geldt de wet alleen voor organisatie met meer dan 250 werknemers die meer dan 5.000 records per jaar verwerken. Later (wanneer is niet bekend*[1]) gaat de wet ook in voor zelfstandig ondernemers (ZZP'ers) en het MKB, ongeacht hun grootte en het aantal records dat ze verwerken.

Heb je als bedrijf, ongeacht de grootte, te maken met het vastleggen en gebruiken van persoonsgegevens, dan heb je te maken met de Algemene Verordening Gegevensbescherming per 28 mei 2018. **Dus als je e-mail adressen vastlegt en mails verstuurd dan ben je al verplicht te voldoen aan deze wetgeving.**

[1] Er zijn verschillende berichten over de ingangsdatum voor de overige bedrijven. Dit varieert van 'gewoon ook per 28 mei 2018' tot een jaar na invoeringsdatum.

Wat houdt de AVG in?

De nieuwe wetgeving houdt in dat overal waar **gegevens worden opgeslagen, geanalyseerd, bewerkt en gebruikt** maatregelen genomen moeten worden.

Onder de wetgeving vallen zowel **persoonlijke** data (bijvoorbeeld naam, e-mail adres, foto) als **vertrouwelijke** data (bijvoorbeeld medische bestanden of financiële gegevens) van zowel klanten als van werknemers.

In het kort komt de AVG op het volgende neer:

1. Je moet exact weten welke bestanden met persoonsgegevens je beheert en in je bezit hebt.
2. Je moet weten welke rechten de personen je hebben gegeven van wie je de gegevens hebt.
3. Data die een hoog risico lopen moeten een privacy risico krijgen, de Privacy Impact Analyse (PIA).
4. Je mag persoonsgegevens alleen maar gebruiken voor het doel waar de informatie oorspronkelijk voor verzameld is.
5. Je mag alleen die persoonsgegevens vastleggen die je ook daadwerkelijk nodig hebt.

De te nemen maatregelen voor bedrijven

In deze paragraaf probeer ik een zo praktisch mogelijke vertaling te maken van wetgeving naar maatregelen die bedrijven moeten nemen om te voldoen aan de AVG.

Melden van beveiligingsproblemen

Als er met opzet of per ongeluk data verloren gaat of geopenbaard wordt , dan moet dit binnen 72 uur aan de toezichthouder worden gemeld.
Houdt het lek een hoog risico in voor de personen waar de gegevens betrekking op hebben, dan moeten zij ook op de hoogte worden gesteld.

Dit is bijvoorbeeld het geval bij bankgegevens of inloggegevens van webwinkels. Als iemand ingehuurd wordt voor het technisch onderhoud van een webwinkel, dan is deze persoon ervoor verantwoordelijk bij een inbraak de eigenaar van de webwinkel hierover te informeren zodat deze dit probleem kan melden.

Verwerkersovereenkomst

Werk je als bedrijf met andere bedrijven die jouw data (voor jou) gebruiken? Dan ben je verplicht een verwerkersovereenkomst op te stellen.

Voorbeeld: een bedrijf laat de salarisadministratie door een extern bedrijf uitvoeren. Om de salarisstroken te maken heeft dit bedrijf de personeelsgegevens nodig. Hier is een verwerkersovereenkomst nodig. Maar ook bij het inschakelen van een **online marketing bureau** voor het versturen van mailings of het aanmaken van Facebook advertenties op basis van een e-maillijst, is een dergelijke overeenkomst nodig. Of de Virtueel Assistente die jouw klantregistratie systeem en mails beheert.

Als je als verwerker ingehuurd wordt en je schakelt zelf een derde in, dan heb je toestemming nodig van de eigenaar van de data door middel van een subverwerkersovereenkomst of paragraaf in de oorspronkelijke overeenkomst.

In de Verwerkersovereenkomst wordt vastgelegd:

- Algemene beschrijving over het onderwerp, duur, aard en doel van de verwerking, soort persoonsgegevens, etc.
- Instructies voor verwerking
- Geheimhoudingsplicht
- Beveiliging (technisch en organisatorisch) om de verwerking te beveiligen (bijvoorbeeld door pseudonimisering en versleuteling van persoonsgegevens)
- Subverwerkers (ook hier is een subverwerkersovereenkomst nodig)
- Privacyrechten (recht op inzage, correctie, vergetelheid)
- Verwijderen van gegevens
- Uitvoering van audits

Privacy by design & Privacy by default

Privacy by design: bij het ontwerp van een **nieuw systeem** waarin data vastgelegd gaat worden, dient al direct rekening gehouden te worden met privacy (zowel technisch als organisatorisch). Voorbeeld: welke data zijn noodzakelijk om op te slaan en welke gegevens zijn echt nodig en welke niet, maar ook welke medewerkers hebben toegang nodig tot het systeem en welke niet. Dit geldt bijvoorbeeld wanneer een bedrijf een nieuw CRM systeem aan gaat schaffen of een website waarin klantgegevens in vast worden gelegd.

Privacy by default: het nemen van technische en organisatorische maatregelen waardoor je **standaard** uitsluitend de strikt noodzakelijke gegevens verzamelt voor het specifieke doel. Ook de beveiliging van je website valt hieronder, maar ook het verzamelen van e-mail adressen op een website. Pas als iemand zich ergens voor heeft aangemeld, dan ontvangt hij de informatie (opt-in). Wat ook niet mag:

- Standaard ‘delen’ op sociale netwerken.
- Vooraf ingevulde velden bij formulieren. Iemand moet dus echt de optie aanvinken (bijvoorbeeld “Ik wil op de hoogte gehouden worden”).
- Vragen om gegevens die niet relevant zijn (bijvoorbeeld geboortedatum en telefoonnummer bij het abonneren op een nieuwsbrief).
- In Algemene Voorwaarden opnemen dat je gegevens met derden worden gedeeld.
- App’s die bij het installeren adresboeken kopiëren (LinkedIn doet dit bijvoorbeeld).

Aanstellen van een Data Privacy Officer (DPO)

De VGA stelt een dergelijke functionaris verplicht bij de volgende organisaties:

- die vanwege aard of omvang op grote schaal persoonsgegevens verwerken
- overheidsdiensten, uitgezonder gerechten.

Bedrijven kunnen iemand hiervoor aanstellen of de werkzaamheden uitbesteden aan een gecertificeerde deskundige.

Verplicht uitvoeren van een Privacy Impact Assessment (PIA)

Het uitvoeren van een PIA is verplicht als het verwerken van persoonsgegevens risico’s voor betrokkenen inhoudt. In elk geval is het verplicht bij profiling: grootschalige verwerking van bijzondere persoonsgegevens.

In de PIA wordt vastgelegd waarom, op welke wijze en hoelang er persoons data verwerkt mag worden. De risico’s worden hierbij in kaart gebracht en soms zelfs besproken met de betrokken personen.

Documentatieplicht: bijhouden van een register

Een register bijhouden is niet verplicht voor organisaties met minder dan 250 medewerkers, tenzij er stelselmatig bijzondere persoonsgegevens worden verwerkt of de verwerking een risico voor betrokkenen heeft.

Op verzoek van de toezichthouder dient het register overhandigd te worden ter controle.

Informeren van betrokkene

Bij het opslaan, verwerken en gebruiken van gegevens moet de betrokkene altijd op de rechten worden gewezen die hij heeft voor inzage, intrekking toestemming, wijziging en verwijderen voor gegevens. Dit geldt ook voor klanten maar ook voor werknemers.

Expliciete toestemming van betrokkene

"Toestemming dient te worden gegeven door middel van een duidelijke actieve handeling, bijvoorbeeld een schriftelijke verklaring, ook met elektronische middelen, of een mondelinge verklaring, waaruit blijkt dat de betrokkene vrijelijk, specifiek, geïnformeerd en ondubbelzinnig met de verwerking van zijn persoonsgegevens instemt."

Impliciete toestemming (de kleine lettertjes) zijn verboden, vooraf aanvinken van een optie mag ook niet meer. Voor het verkrijgen van toestemming moet in duidelijke en begrijpelijke taal worden uitgelegd wat er met welke informatie gedaan gaat worden. Hetzelfde geldt voor het intrekken van toestemming.

Algemene voorwaarden en de privacy statement moeten zo opgesteld worden dat de betrokkene begrijpt wat er met zijn persoonsgegevens gebeurt.

Het recht om te vergeten en verwijderen

De eigenaar van de data heeft de plicht om data te verwijderen zodra de betrokken persoon daarom vraagt. Als de data uit handen is gegeven aan derden dan dient deze ook daar verwijderd te worden.

Voorbeeld: iemand maakt gebruik van zijn recht om vergeten te worden. Deze persoon moet dan verwijderd worden uit het CRM systeem maar ook uit de mailingslijst die wordt beheerd door het online marketing bureau.

Recht op toegang

Iedereen (burgers, patiënten, klanten) heeft het recht om inzage te ontvangen van de eigen digitale gegevens. Bedrijven moeten hier een mogelijkheid voor inbouwen zodat mensen online (via bijvoorbeeld een beveiligde website) bij hun gegevens kunnen.

ePrivacy Verordening

In januari 2017 is ter aanvulling op de AVG een ePrivacy Verordening toegevoegd. Deze set wetten regelen de vertrouwelijkheid van communicatie bij internet- en telecomdiensten en gaat ook 25 mei 2018 in.

Onder deze regels vallen ook diensten als Skype, WhatsApp, Facebook Messenger en e-mail, maar ook tracking cookies, direct marketing en machine-naar-machine communicatie (the internet of things). De regels gelden ook voor alle bedrijven die bijvoorbeeld online marketing diensten aanbieden of ervan gebruik maken.

Alle communicatie is geheim

Ook voor online geldt dat alleen die gegevens opgeslagen en gebruikt mogen worden die ook daadwerkelijk gebruikt gaat worden en waar expliciet door de betrokkene toestemming voor is gegeven. Gegevens dienen ook geanonimiseerd opgeslagen te worden.

Dit geldt ook voor gegevens (metadata) die door het gebruik van dergelijke diensten beschikbaar komen (IP-adres, tijdstip, duur van een gesprek, afzender, locatie, etc.).

Tracking en cookies

De Europese Unie heeft besloten dat het instellen, accepteren en weigeren van cookies van aanbieders voortaan via de browsers gaat verlopen. Op deze manier zou het mogelijk worden om in één keer je privacy voorkeuren voor alle websites door te geven.

Spam

Het spamverbod wordt verder uitgebreid dan dat wij in Nederland al gewend zijn. Een opt-in (toestemming vooraf) is vereist voor alle vormen van commerciële communicatie, ongeacht de techniek die gebruikt wordt. Voor een bestaande klantrelatie geldt dit niet (mits een opt-out wordt geboden). Er gaat waarschijnlijk naast het Bel-me-niet register ook een E-mail-me-niet registratie komen.

Retargeting

Retargeting (bezoekers die je website hebben gezocht opnieuw bereiken via beeld of tekstadvertenties op websites van derden of via social media) is zeer effectief en veelvuldig ingezet in bijvoorbeeld Facebook.

Als gevolg van de nieuwe wetgeving behoor je aan je bezoekers (vooraf!!) toestemming te vragen (via een opt-in) om retargeting in te mogen zetten. Omdat je ook werkt met een derde partij aan gegevenserwerkers (Facebook) zou je ook een verwerkersovereenkomst met Facebook moeten afsluiten.

Mocht je later besluiten om retargeting in te zetten voor je bestaande mailinglijst (die retargeting nog niet goed hebben gekeurd), dan moet je opnieuw toestemming vragen.

E-mail opt-in

De opt-in moet aan een aantal eisen voldoen met de nieuwe AVG wetgeving. Zo moet in de opt-in in duidelijke woorden beschreven staan waarvoor men toestemming geeft (en waarvoor niet), mag de checkbox niet automatisch aangevinkt staan, moet het voor je contactpersonen duidelijk zijn hoe ze zich kunnen uitschrijven en moet de opt-in gescheiden zijn van je Algemene voorwaarden.

Je e-mail database met klantgegevens moet verder voorzien worden van extra informatie:

- Is er gebruik gemaakt van een opt-in? (ja/nee)
- Hoe en waar de opt-in is verkregen? (website, pop-up, link, etc)
- Wanneer de opt-in is verkregen? (datum en tijd)
- Welke toestemming is gegeven? (de tekst die bij de opt-in stond)

Voor bestaande klantrelaties (er is een aankoop geweest en daar heeft geld tegenover gestaan) gelden deze regels niet. Wel is een opt-out/uitschrijfmogelijk te allen tijde verplicht.

Ik voorzie voor de meeste ondernemers een groot probleem met de mailingslijsten omdat dergelijke informatie meestal niet wordt bijgehouden op dit moment.

Data opslag in de cloud

Als je in de cloud werkt bij de grote aanbieders (bijvoorbeeld Google, Microsoft) dan word je data waarschijnlijk buiten Europa opgeslagen. Je bent dan verplicht te onderzoeken of de vereiste contracten zijn gesloten en of deze partijen gecertificeerd zijn.

Je kunt er ook voor kiezen om je privacy gevoelige data op te slaan in een cloudserver gevestigd in Europa/Nederland. Een bedrijf dat voldoet aan de nieuwe privacy eisen zal ISO 27001 gecertificeerd zijn. Afspraken over opslag dienen te worden vastgelegd in een verwerkersovereenkomst.

Hoe bereid je je voor op de AGV?

In elk geval zo snel mogelijk!

Voor alle bedrijven, ongeacht de grootte geldt: start met een **inventarisatie** van álle processen en systemen waar privacy gevoelige informatie wordt vastgelegd, om welke informatie het gaat en wie toegang hebben tot deze informatie.

Voor een zelfstandig ondernemer is dit ongetwijfeld een makkelijker uit te voeren klus dan voor een multinational, maar desalniettemin essentieel om mee te beginnen.

Leg al deze informatiestromen vast. Niet alleen welke bestanden, systemen en processen er gebruikt worden, maar ook wélke (privacy gevoelige) informatie.

10 stappenplan van de Autoriteit Persoonsgegevens (AP)

De Autoriteit Persoonsgegevens heeft een 10 stappenplan gemaakt ter voorbereiding op de AVG (hier te downloaden: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/in_10_stappen_voorbereid_op_de_avg.pdf)

Stap 1: Bewustwording
Zorg ervoor dat alle relevante mensen in het bedrijf op de hoogte zijn van de nieuwe regels zodat zij de consequenties voor het bedrijf kunnen inschatten.

Stap 2: Rechten van betrokkenen
De personen van wie de privacy gevoelige data wordt vastgelegd hebben het recht tot inzage, verwijdering, correctie en het meenemen (dataportabiliteit). Een bedrijf moet dit organisatorisch en technisch zo inrichten dat dit uit te voeren is.

Stap 3: Overzicht verwerkingen
Breng alle persoonsgegevens in beeld, waar deze gegevens vandaan komen en met wie ze worden gedeeld. Alle gegevens moeten goed gedocumenteerd worden mét reden waarom je die gegevens vastlegt (geldt voor bedrijven met meer dan 250 medewerkers).

Stap 4: Privacy Impact Assessment (PIA)
Inventariseer welke privacyrisico's het verwerken van persoonsgegevens tot gevolg hebben. Groot risico? Dan ben je verplicht een PIA uit te laten voeren en af te stemmen met de AP.

Stap 5: Privacy by design & privacy by default
Voer nu al die maatregelen in voor nieuwe en bestaande processen en systemen zodat er alleen maar die gegevens worden vastgelegd die echt noodzakelijk zijn voor het specifieke doel. Let op ook bij opt-in formulieren, contactformulieren, ed.

Stap 6: Functionaris voor de gegevensbescherming
Nodig voor je bedrijf? Ga dan al snel zoeken hoe je deze functie wilt inrichten (eigen personeel of inhuur). Let goed op certificeringen en opleidingen die nodig zijn.

Stap 7: Meldplicht datalekken
Zorg voor goede documentatie en zit er bovenop als er iets mis gaat met een datalek.

Stap 8: Verwerkersovereenkomsten
Controleer bestaande contracten of stel nieuwe contracten op met derde partijen die privacy gevoelige gegevens verwerken van het bedrijf.

Stap 9: Leidende toezichthouder
Is het geval bij bedrijven met vestigingen in meerdere EU-lidstaten.

Stap 10: Toestemming
Het documenteren van de gegeven toestemming is essentieel onder de nieuwe wetgeving. Zorg dus dat hier mogelijkheden voor zijn (hoe ben je aan de toestemming gekomen, wanneer, met welke teksten/goedkeuringen).

Voorbeelden van mogelijke consequenties voor zelfstandig ondernemers

Ook de zelfstandig ondernemer heeft werk te verzetten als gevolg van deze wetswijzigingen. Een aantal voorbeelden:

- Het bestand met klantnamen, adressen, afspraken, e-mail adressen, etc. zal bekeken moeten worden: worden er geen gegevens vastgelegd die niet noodzakelijk zijn? Wie kan bij deze gegevens? Is de toegang en opslag goed geregeld? Zijn gegevens makkelijk te verwijderen of aan te passen? Hoe geef ik mijn klanten toegang tot het bekijken of meenemen van hun gegevens?
- De website: hoe worden nu gegevens verzameld, welke gegevens, hoe is de opt-in geregeld? In het opt-in formulier moet de (potentiele) klant kunnen aangeven waar hij/zij toestemming voor geeft. Die moeten ook goed nagekomen worden (dus indien retargetting niet aangevinkt wordt dan mogen de gegevens daar dus ook niet voor gebruikt worden).
- De e-maillijst met uitgebreid worden met extra informatie (wanneer en hoe ben je aan die informatie gekomen, waar ik de inschrijver mee akkoord gegaan).
- Er moeten overeenkomsten met derde partijen worden afgesloten (of aangepast) die gebruik maken van jouw data. Wat gebeurd er met de informatie ten behoeve van de boekhouding? Wordt dat uitbesteed? Dan is er ook daar werk aan de winkel (verwerkingsovereenkomst).
- In alle mailings moet een duidelijke opt-out functie aanwezig zijn. Die uitschrijving moet ook in alle systemen verwerkt worden (dus in je klantregistratie systeem, in de mailinglijst bij je assistente, etc.).
- Je privacyverklaring moet ‘transparant en eenvoudig toegankelijk’ zijn. Dat houdt dus in dat er in makkelijke bewoording staat wat jij met welke gegevens doet.

Voorbeelden van mogelijke consequenties voor MKB ondernemers

Voor grotere bedrijven adviseer ik een multidisciplinair team samen te stellen met alle mogelijke betrokken partijen (intern en extern). Vorm dit team met in elk geval met iemand van het management, een jurist, ICT'er, marketeer, HRM-medewerker. Aan de ene kant krijg je meer betrokkenheid als je alle betrokken afdelingen/personen betrekt, maar ook meer awareness binnen het bedrijf en bij alle medewerkers. Informatiestromen zijn sneller inzichtelijk te maken als iedereen vanuit zijn/haar expertise aan kan geven welke informatie nu wordt vastgelegd, noodzakelijk is en hoe aan deze gegevens wordt gekomen.

Denk in elk geval aan:

- Het CRM systeem moet geanalyseerd worden: welke gegevens worden vastgelegd, hoe kom je aan die gegevens, welke zijn noodzakelijk en welke niet, wie kan bij deze data en is dat noodzakelijk.
- Hoe makkelijk kan je klant zich uitschrijven uit je bestand(en) en data meenemen via bijv. een Excellijst?
- Zijn er voor elke samenwerking waarbij een derde partij data verwerkt vanuit jouw bedrijf goede contracten? Het administratiekantoor, online marketing bureau, leasemaatschappij, accountant, etc.
- Voldoet de website aan de eisen? Wordt er data verzameld via de website en zo ja, met een duidelijke opt-in functie? Klopt de privacyverklaring nog? En de Algemene voorwaarden? Laat hier vooral ook een jurist naar kijken die gespecialiseerd is in deze nieuwe wetgeving.
- Alle systemen en procedures moeten bekeken worden: waar wordt welke data vastgelegd, waarom en hoe ben je aan die data gekomen en wie heeft toegang nodig tot deze data?
- Werk je met grote hoeveelheden privacygevoelige data en/of heb je meer dan 250 medewerkers? Dan ben je vaak verplicht een PIA uit te voeren en een medewerker aan te stellen of te benoemen die belast wordt met privacy gevoelige zaken.
- Wie controleert of de gegevens veilig zijn en blijven? Wie signaleert een hack en rapporteert deze?

Waarom dit document?

Ik ben ondernemer, online marketeer en projectmanager. Het is nu juli 2017, nog 10 maanden voor de start van de nieuwe wetgeving. In mijn omgeving krijg ik glazige blikken als ik aan ondernemers vraag hoeveel zij weten van de AVG ("wat is dat, toch een virusbeschermer?" is de meest gekregen reactie). Als ik dan uitleg wat het inhoudt, dan krijg ik steevast te horen "dat geldt niet voor mijn bedrijf".

Met dit document probeer ik ondernemers, van zelfstandig ondernemer tot MKB, een soort awareness mee te geven. Er verandert veel en het raakt álle ondernemers. Misschien is het een half dagje werk om de boel goed in te richten, misschien kost het maanden en tonnen om het goed door te voeren (vooral bij multinationals waarschijnlijk). Maar wachten tot mei 2018 en er dan achter komen dat er nog van alles en nog wat aangepast moet worden is zonde van de tijd, stress, foutgevoeligheid én het riskeren van een boete (4% van je jaaromzet is toch leuker te besteden en dan heb ik het niet eens over je reputatieschade).

Als projectmanager kan ik bedrijven ondersteunen bij het in actie komen, kennis en kunde mobiliseren en werkzaamheden coördineren.
Als online marketeer heb ik de kennis over gegevens ten behoeve van marketing acties.
Ik ondersteun bedrijven graag met deze kennis.
Maar hoewel ik ~~dagen~~ weken lang informatie aan het vergaren ben geweest over dit onderwerp, dikke rapporten heb doorgeworsteld en verschillende mensen over dit onderwerp heb gesproken, ben ik **geen** AVG specialist en heb niet de ambitie dit te worden. Ik ben niet gecertificeerd, niet in te zetten voor audits of als privacy vertegenwoordiger.
Toch interesse in een vrijblijvend gesprek over wat ik kan betekenen (op dit gebied) voor je bedrijf? Ik kom graag langs of je bent welkom bij mij.

Voor meer actuele informatie over AVG, raadpleeg dan vooral deze website:

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving/algemene-verordening-gegevensbescherming

Ik wens alle ondernemers heel veel succes toe bij het implementeren van deze wetgeving!

Willeke van den Heuvel
Mijn Gereedschapskist

www.mijngereedschapskist.nl
willeke@mijngereedschapskist.nl

Bovendijk 132
3045 PC Rotterdam (16Hoven)
Telefoon: 015-2010466
Gsm: 06-19635283

Geraadpleegde bronnen:

http://www.marketingonline.nl/achtergrond/marketeer-let-op-je-data-want-dit-gaat-er-allemaal-veranderen?utm_source=NB_MOL_mol_dag_20170724&utm_medium=email&utm_term=&utm_content=&utm_campaign=24-07-2017&mt=Rv2O9SiMIyPz0kJwT8LaSg&vk=8WuFPhstqnZTjjydRP2vWA&pub=1002

https://www.emerce.nl/research/zorgen-om-privacy

https://dutchitchannel.nl/563728/dell-komt-met-best-practices-om-aan-gpdr-te-voldoen.html

https://www.marketingonline.nl/achtergrond/cmos-nog-lang-niet-klaar-voor-praktijk-van-nieuwe-privacywetgeving

https://www.frankwatching.com/archive/2017/07/13/e-mailmarketing-zo-stoom-je-jouw-opt-in-klaar-voor-de-gdpr-wet/

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving/voorbereiding-op-de-avg

http://www.bno.nl/nieuws/meestgestelde-vragen-nieuwe-privacyverordening-avg

http://www.justitia.nl/privacy/europese-privacyverordening.html

https://www.mkb.nl/nieuws/mkb-slecht-voorgelicht-over-europese-privacywet