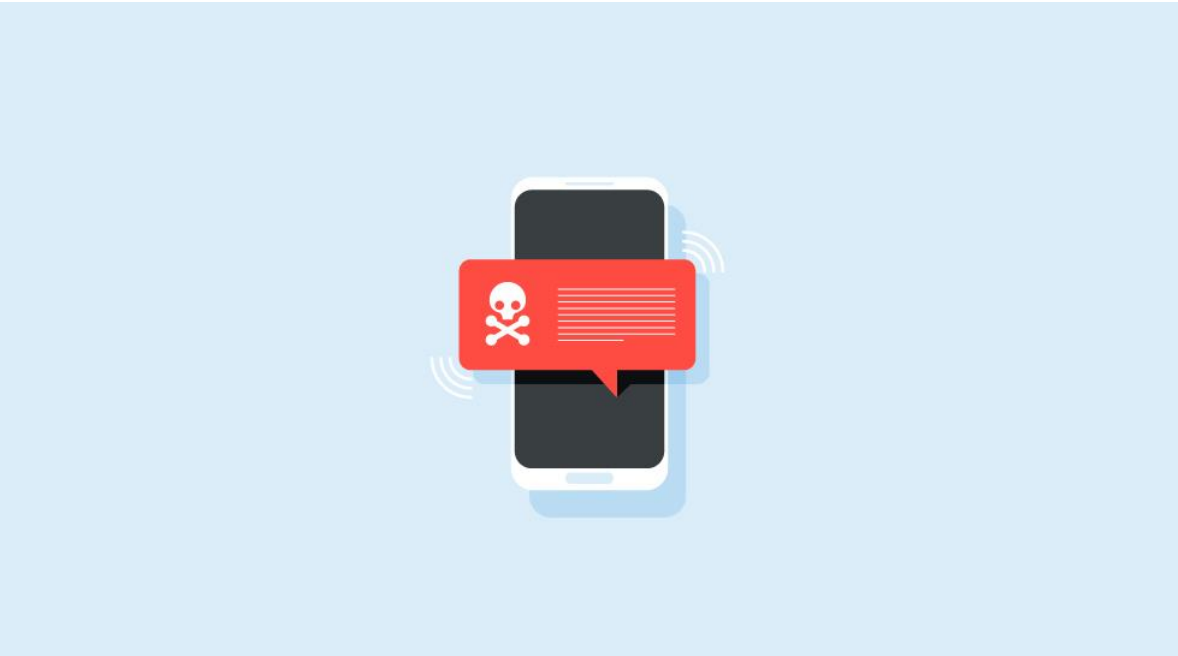
Nieuwe AVG wetgeving, we praten je bij!



Misschien heb je er al wat over gehoord. Vanaf 25 mei 2018 verandert er een hoop op gebied van de nieuwe privacywetgeving ofwel de Algemene Verordening Gegevensbescherming (AVG). Wij zijn natuurlijk het allerliefst bezig met het uitdenken van een pakkende communicatieboodschap of het oplossen van een technisch vraagstuk voor onze klanten, maar hebben desalniettemin al een behoorlijke tijd dit onderwerp op onze dagelijkse agenda staan. En nu willen we je graag meenemen in wat het betekent voor jou als klant / partner en wat wij hieraan doen.

Waarom zou je dit eigenlijk moeten weten?
Het klinkt als nogal saaie kost, dat klopt. Maar de AVG is van toepassing op iedere organisatie die persoonsgegevens verwerkt. Kunnen mensen bij jou producten bestellen? Heb je een online community of melden mensen zich aan voor een bijeenkomst? Al gauw ben je in het bezit van meer informatie dan je denkt. En heb je eigenlijk wel in kaart welke informatie je opslaat en waar? Je hebt er dus eerder mee te maken dan je denkt!

OKÉ, WAT JE MOET WETEN EN REGELEN:

Deze wet is niet nieuw maar vanaf 25 mei 2018 wordt de AVG gehandhaafd en vervangt deze de huidige Wet bescherming persoonsgegevens (Wbp). Bedrijven hebben dan voldoende tijd gehad om maatregelen te treffen. De wet geldt voor de hele Europese Unie. De nieuwe wetgeving is wat strenger. Er wordt meer verantwoordelijkheid gelegd bij partijen die persoonsgegevens verwerken. Bijvoorbeeld: Wat te doen bij een datalek? En sla je alleen benodigde data op? Boetes zijn serieus bij nalatigheid, vandaar dat je je maar beter goed kunt voorbereiden.

De AVG is in de basis een afgeleide van de ISO-27001 norm. Groot verschil is dat je voor ISO gecertificeerd mag worden en AVG is de wet, daar moet je je gewoon aan houden.

Het doel hiervan is om de gegevens van jouw bezoekers beter te gaan beschermen. Kortom: onze privacyrechten. Dit voorkomt dat gegevens op straat komen te liggen omdat ze niet beschermd zijn, onnodig bewaard worden of voor andere doeleinden gebruikt worden dan jij vooraf wist.

Super! Aangezien jij ook zelf een burger bent zal je hier blij mee zijn. Want jouw gegevens liggen immers ook op meer plekken dan je denkt. Dus dit is de basis voor een betere wereld!

Dat klopt helemaal. Maar aangezien dat jij daarnaast vanuit je beroep ook persoonsgegevens verwerkt ben jij "Verwerkingsverantwoordelijke" en zal ook jouw organisatie haar steentje bij moeten dragen aan deze betere wereld. En dat is best een pittige opgave.

De wet schrijft je niet in alle gevallen exact voor wat je moet doen op detailniveau. Ze leggen daarvoor veel verantwoordelijkheid bij jou zelf neer.

Hoe je die verantwoordelijkheid moet dragen? Laten we er eens een mooie term tegenaan gooien: ISMS ofwel: Information Security Management System. Nee, dit is geen "systeem" zoals een applicatie maar een organisatorisch systeem waarin een aantal zaken samenkomen en daardoor een beveiligingssysteem van jouw organisatie vormen.

De term mag je nu weer vergeten. Plat geslagen komt het op een paar zaken neer:

1. Zorg voor een beleid op het gebied van informatiebeveiliging vanuit de directie.
2. Inventariseer welke gegevens je verzamelt, met welk doel en wat je ermee doet.
3. Inventariseer waar je risico's ziet en wat de kans en impact van deze risico's zijn.
4. Geef aan welke maatregelen je neemt om deze risico's te beperken. Denk hierbij zowel aan mens, techniek als proces.
5. Informeer je personeel en leveranciers over de maatregelen die voor hen van toepassing zijn, zorg voor bewustwording en maak duidelijke afspraken over de naleving hiervan.
6. Controleer of de maatregelen in de praktijk daadwerkelijk aanwezig zijn en werken.
7. Verbeter jezelf continu middels de Plan Do Check Act cyclus.

OM WELKE GEGEGEVENS GAAT HET NU PRECIES?

Partijen die gebruikersgegevens verwerken zijn verplicht om te documenteren welke persoonsgegevens dat precies zijn en om aan dataminimalisatie te doen.
Je mag niet allerlei extra persoonsgegevens opslaan zonder deze ook concreet ergens voor in te zetten. Bij persoonsgegevens spreken we over alle gegevens die tot een individu te herleiden zijn zoals:

- NAW gegevens
- Uiterlijke kenmerken, maatvoering, Geslacht, Geboortedatum
- Contactgegevens zoals telefoonnummer en e-mailadres
- IP adres, browser- en apparaat gegevens
- Profielgegevens
- Interesses, Surfgedrag
- Bankinformatie
- Locatiegegevens

Maar binnen de AVG is er extra aandacht voor bijzondere of gevoelige persoonsgegevens. Denk hierbij aan:

- Ras, godsdienst of levensovertuiging
- Politieke voorkeur of lidmaatschap vakbond
- Gezondheid
- Seksuele leven
- Strafrechtelijk verleden
- Kredietwaardigheid
- Gegevens van jongeren onder 16 jaar
- BSN nummer
- Biometrische of genetische gegevens.

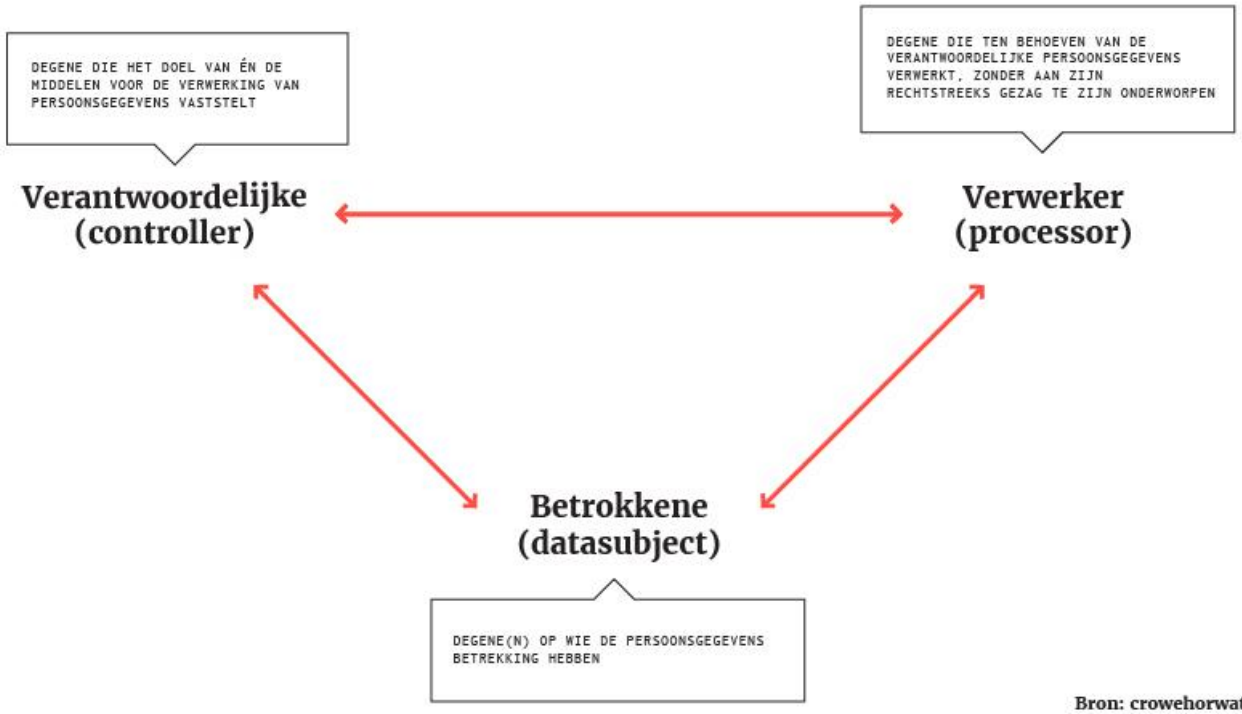
Voor deze gegevens gelden strenge(re) voorwaarden en regels en moet je gericht aangeven met welk doel je deze verwerkt.

DE ROLVERDELING

Het is erg belangrijk om te weten wie de betrokkenen zijn. Er is een partij verantwoordelijk is en die bepaalt welke gegevens verzameld worden bijvoorbeeld een kledingwebshop.

Er zijn partijen die gegevens verwerken, The Cre8ion.Lab bijvoorbeeld doordat we gegevens voor de webshop in een database verzamelen en deze hosten. Maar dit kan ook een mailingprovider, datacenter of de accountant zijn. Tot slot is er de betreffende persoon van wie de gegevens verwerkt worden.

Sommige partijen, die bijvoorbeeld op grote schaal gegevens verwerken, moeten een Functionaris Gegevensbescherming aanstellen. Deze persoon heeft binnen de organisatie de taak om bewustzijn te creëren en het personeel te informeren en in het geval van incidenten hier direct naar te handelen.

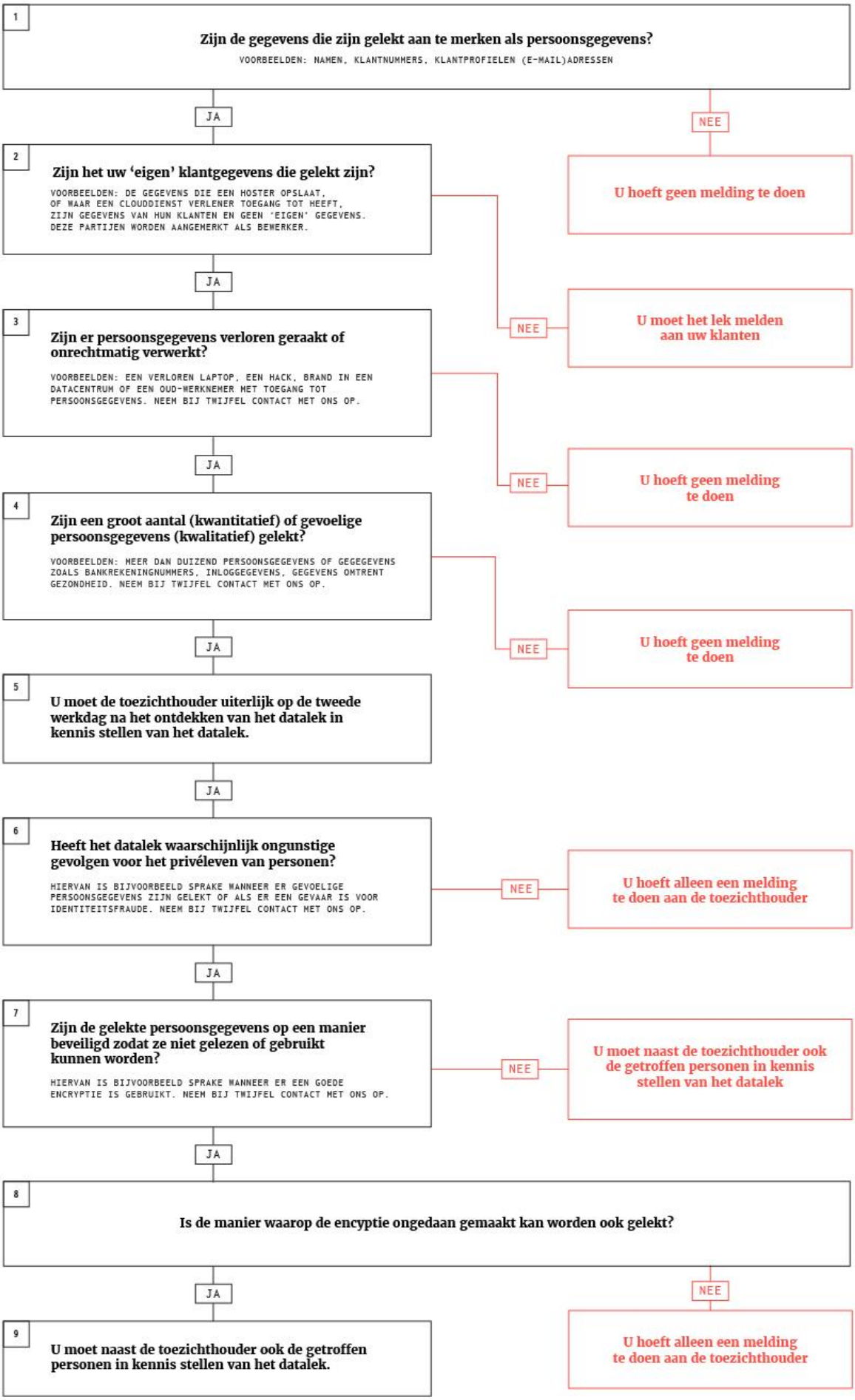


Bron: crowehorwathpeak.nl

MELD INCIDENTEN TIJDIG BIJ DE AUTORITEIT!

Als je je zaakjes goed op orde hebt verkleint dat de kans op datalekken natuurlijk enorm. Mocht je toch te maken krijgen met een lek, dan is het belangrijk dat je dit tenminste binnen 72 uur meldt bij de toezichthouder (meldpunt Autoriteit Persoonsgegevens). Niet ieder lek hoeft echter gemeld te worden. Onderstaande infographic geeft hier meer toelichting op.

Procedure melden datalekken



Bron: ictprivacyrecht.nl

LAAT JE KUNDIG ADVISEREN

Zoals bij iedere hype of actualiteit schieten de adviseurs en zelfbenoemde specialisten als paddenstoelen uit de grond. De kwaliteit van deze adviseurs verschilt enorm! Zo kunnen ze zaken van de wet anders interpreteren ofwel jou zaken laten organiseren die helemaal niet noodzakelijk zijn. Of ze kunnen een slaatje slaan uit jouw onrust en onzekerheid over dit thema door je onnodig veel adviesuren in rekening te brengen ofwel in zaken te investeren die niet noodzakelijk zijn.

Wij zijn ook geen juristen en ondanks dat we dit artikel en onze adviezen proberen op een zorgvuldige manier samen te stellen om jou zo wat handgrepen te geven kunnen er zaken zijn die we niet (afdoende) hebben belicht of niet 100% volledig of correct zijn. Ben dus bewust betrokken bij de keuzes die gemaakt worden en maatregelen en waak er voor dat jij zelf de eindverantwoordelijkheid blijft dragen. Maar ook als je zelf aan de slag gaat: maak gebruik van recente en betrouwbare bronnen. Een google actie levert op ieder onderwerp een hoop informatie op maar de vraag is of deze volledig en juist is.

Staat op 26 mei een controleur bij jou op de stoep? Waarschijnlijk niet.
De autoriteit persoonsgegevens die in het leven is geroepen om deze wet in Nederland te handhaven is simpelweg niet in staat om alle bedrijven in Nederland 1-op-1 proactief te controleren. Maar wanneer er een lek plaatsvindt waardoor de gegevens van jouw bezoekers op straat liggen dan zullen ze waarschijnlijk wel gaan controleren of jouw organisatie maatregelen heeft getroffen om dit te voorkomen.

Is dat niet het geval? Dan riskeer je hoge boetes en het risico dat je je klanten persoonlijk op de hoogte moet stellen dat hun gegevens mogelijk op straat liggen of voor doeleinden gebruikt worden die zij niet hadden voorzien. Dat kan natuurlijk imagoschade tot gevolg hebben.

MEER LEZEN?

Wil je meer de diepte in op dit onderwerp? Top! Er zijn een hoop bronnen online. Hieronder hebben we een aantal voor je opgesomd:

- Wettekst op wetten.nl
- Autoriteit persoongegevens
- Handleiding AVG door ministerie van Justitie en Veiligheid
- DDMA doorbreekt dagelijks mythes van de AVG

Enkele voorbeelden uit de praktijk:

- Autoriteit Persoonsgegevens lekt zelf
- Leasebedrijven moeten alle klanten inlichten door lek
- 50 miljoen facebookprofielen worden misbruikt
- 95.000 klanten van ANWB betrokken bij datalek webshop