E-book 17 vragen over de AVG

Inhoudsopgave

Inleiding

De reden voor dit ebook is gelegen in het feit dat er veel onjuiste informatie wordt verspreid over ISO27001 en de Algemene Verordening Gegevensbescherming (AVG), Zaken worden vaak onnodig moeilijk gemaakt, een voorbeeld is bijvoorbeeld dat elke onderneming een Functionaris Gegevensbescherming indienst moet hebben, dit is pertinent niet het geval.
Door het lezen van dit ebook verwachten wij dat u antwoorden kunt vinden op een aantal vragen, om te voldoen aan de Algemene Verordening Gegevensbescherming (AVG).
Het ebook bevat een aantal vragen naar voren kwamen tijdens onze presentatie bij Fingerspitz op 22 maart 2018 in Breda.
De vragen zijn in samenwerking met Fingerspitz beantwoord.

Fingerspitz is een online marketing buro, gevestigd aan de Torenallee 3 te 5617 BA Eindhoven.

inTECHrity is een belangrijke speler op de markt voor certificering en ACP partner van BSI. Wij begeleiden niet alleen organisaties bij het verkrijgen van een certificaat, maar ondersteunen ook daarna. Weliswaar is ISO 27001 het keurmerk dat uw organisatie de informatieprocessen continue beheerst, maar hoe kunt u dit nu eenvoudig aantonen? Wij maken hiervoor gebruik van de door ons ontwikkelde softwaretool en begeleiden u hierin.

Wie is de AP?

De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving. Het is het voormalige College Bescherming Persoonsgegevens (Cbp) en en een toezichthouder net als bijvoorbeeld ACM Autoriteit Consument en Markt

Hoe hoog zijn de boetes?

Zwaar - **boete van 20 miljoen euro of 4 procent van de omzet**.
Voor het overtreden van de basisbeginselen van de AVG zoals de voorwaarden voor het vragen van toestemming.
Voor het overtreden van de verplichtingen met betrekking tot de rechten van de individuen, zoals het recht op dataportabiliteit of recht van verzet.
Minder zwaar - **boete van 10 miljoen euro of 2 procent van de omzet**
Voor het niet (of te weinig) implementeren van maatregelen in verband met privacy by design of privacy by default.
Voor het inschakelen van een verwerker zonder de wettelijke verplichtingen voor een verwerkersovereenkomst.

Wat zijn persoonsgegevens?

De Wet bescherming persoonsgegevens (Wbp) geeft aan dat een persoonsgegeven elk gegeven is over een geïdentificeerde of identificeerbare natuurlijke persoon.
Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Dat het om een natuurlijke persoon moet gaan, houdt in dat gegevens van overleden personen of van organisaties geen persoonsgegevens zijn.Er zijn 3 soorten persoonsgegevens.

1) Persoonsgegevens zoals NAW-gegevens, locatie en IP-adres. Voor bijzondere persoonsgegevens zoals BSN-nummer, religie, medische gegevens, ethische etc. is er een aparte regelgeving.
2) Pseudo-anonieme data; persoonsgegevens die dusdanig verwerkt worden dat ze niet langer herleid kunnen worden zonder gebruik van aanvullende informatie, maar die wel een persoon individueel maken, zoals een versleuteld e-mailadres of gebruikers-ID.
3) Anonieme data; data die niet herleidbaar is naar een individu.

Wat wordt precies verstaan onder het verwerken van persoonsgegevens?

Verwerken is: alle handelingen die een organisatie kan uitvoeren met persoonsgegevens, van verzamelen tot en met vernietigen. Dit is dus een zeer ruim begrip. Handelingen die er volgens de Wet bescherming persoonsgegevens (Wbp) in ieder geval onder vallen, zijn: het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen

van gegevens. Als je gegevens gebruikt om te analyseren, dan is dat dus ook verwerken. Bij digitale marketing ben je dus al heel snel aan het verwerken

Gaan die boetes echt uitgedeeld worden?

Er zijn vooralsnog geen geluiden dat ze coulant omgaan met deze regeling. De verwachting is dus dat deze boetes ook echt uitgedeeld gaan worden. Er is niet te zeggen welke bedrijven het meest risico lopen.

De AP is verplicht om klachten van individuen in behandeling te nemen en zal dus meer gaan opereren op basis van die klachten van consumenten.

Toestemming vragen om gegevens te verwerken moet nu ook al. Wat is het verschil?

Je moet duidelijk aan kunnen geven waar je welke gegevens voor gebruikt met het bijbehorende doel. Nu wordt vaak alles over 1 kam geschoren. Maar nu moet je dus afzonderlijk voor ieder doel toestemming gaan vragen. Die toestemming moet ook net zo makkelijk ingetrokken kunnen worden. Voorbeeld; nu wordt er vaak in de cookiebar aangegeven:

Vallen b2b-gegevens ook onder de AVG?

Ja. Een werk e-mailadres kan een persoonsgegeven zijn. Het risico op klachten is minder groot, omdat het minder invloed heeft op iemands persoonlijke leven dan een privé 06-nummer. De wetgeving blijft van toepassing.

Wat moet ik veranderen in mijn privacystatement?

In je privacy statement moet het volgende staan:

1) Identiteit: de bedrijfsnaam
2) Doeleinden en rechtsgronden (bijvoorbeeld toestemming vragen voor een marketingdoel)
3) Als de verwerking van de persoonsgegevens een wettelijke of contractuele verplichting is, of noodzakelijke voorwaarde, dan moet je ook aangeven wat de gevolgen zijn als je het niet doet.
4) Je moet aangeven hoe lang gegevens bewaard worden óf welke criteria bepalen hoe lang het opgeslagen zal worden.
5) Recht op inzage, rectificatie of wissen van de gegevens. De betrokkene heeft recht en je moet dat opnemen in het statement. Je moet dus ook vermelden hoe dat gedaan kan worden (per e-mail/formulier).
6) Aangeven dat ze het recht hebben om een klacht in te dienen bij de AP (Autoriteit Persoonsgegevens).

Moet ik altijd een verwerkersovereenkomst

Alleen als je gegevens laat verwerken door een andere partij (Google, Hotjar).

Moet ik een data privacy officer of functionaris gegevensbescherming aanstellen?

Het is in 3 situaties verplicht:
ten eerste -Bij overheden en publieke organisaties.
ten tweede -Wanneer je een organisatie bent die vanuit je kernactiviteiten op grote schaal individuen volgt (profilering van mensen, risico-inschattingen, iemands gezondheid via wearables meet)
ten derde als je op grote schaal bijzondere persoonsgegevens verwerkt, zoals informatie over iemands gezondheid, ras, politieke opvatting, geloofsovertuiging etc.

Wat verandert er als mijn organisatie in meerdere landen actief is?

De AVG wet is voor alle landen die lid zijn van de EU van toepassing. Hierdoor is het juist makkelijker om te voldoen aan de regelgeving van andere landen.

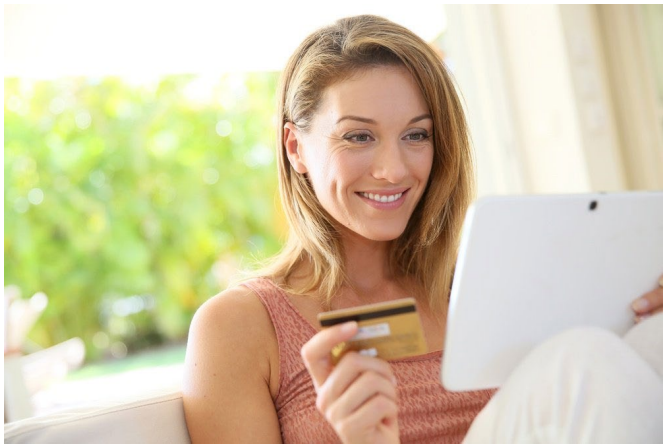
Cookiemelding worden aangepast

Je moet ervoor zorgen dat je je toestemming net zo makkelijk kan intrekken als dat je toestemming geeft.
Voorbeeld; https://www.cookieinfo.net/

Waar moet ik gebruikers over informeren als ik data verzamel?

Je bent verplicht je klanten te informeren over de verwerking van hun persoonsgegevens. Je moet aangeven wat de doeleinden zijn waarvoor je de gegevens verwerkt, welke rechten de mensen hebben en hoe ze daar gebruik van kunnen maken.

Dit kun je natuurlijk doen in een privacy statement maar ook door extra informatie te tonen bij het invoeren van een formulier



Moet je opnieuw toestemming vragen aan de klant wanneer je al gegevens hebt verwerkt.

Indien de toestemming voldoet aan de eisen van de AVG, dan hoef je geen aanpassingen meer door te voeren. Wijken ze af, dan dien je alsnog aanpassingen te maken.

Moet ik mijn orderdata kunnen verwijderen?

De orderdata mag blijven bestaan zolang de directe persoonsgegevens maar gewist worden die aan de order gekoppeld zijn. De definitie van persoonsgegeven is namelijk "alle informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon". De bestelling van een product dus niet. Maar die zijn wel gekoppeld aan een persoon/klantnummer en dat is dus herleidbaar naar een persoon.

In hoeverre moet je echt overal je klantdata kunnen verwijderen (backups, etc)?

Een organisatie is verplicht binnen 4 weken schriftelijk of per e-mail te reageren op een correctieverzoek. Besluit je de klantgegevens te corrigeren, dan moet dit zo snel mogelijk gebeuren. U moet het recht op vergetelheid ook toepassen op digitale back-upbestanden. Vraagt iemand u om zijn gegevens te wissen? Dan moet u zijn persoonsgegevens dus ook zo snel mogelijk uit uw back-ups verwijderen.

Contactinformatie

Bezoekadres: Papendorpseweg 100,
3528 BJ Utrecht
Telefoon: +31 (0)85 130 1281
E-mail: info@intechrity.nl

inTECHrity is een belangrijke speler op de markt voor certificering. Wij begeleiden niet alleen organisaties bij het verkrijgen van een certificaat, maar ondersteunen ook daarna. Weliswaar is ISO 27001 het keurmerk dat uw organisatie de informatieprocessen continue beheerst, maar hoe kunt u dit nu eenvoudig aantonen?
Wij maken hiervoor gebruik van de door ons ontwikkelde softwaretool en begeleiden u hierin.