

# Gratis AVG-Checklist

Is jouw organisatie AVG-proof?

# Maak jouw bedrijf AVG-proof met de checklist van Speak!



Het kan je bijna niet zijn ontgaan: op 25 mei 2018 treedt de Algemene Verordening Gegevensbescherming in werking. Ook wel bekend onder de naam General Data Protection Regulation (GDPR). Hoe kun je je als organisatie het beste voorbereiden op de officiële invoering, zodat je op 25 mei 2018 niet voor verrassingen komt te staan? Volg de AVG-checklist van Speak!

## ALGEMENE AANDACHTSPUNTEN:

### BEWUSTWORDING

Informeer al je werknemers, collega's, vrijwilligers en andere betrokkenen over de nieuwe privacyregels. Zorg dat er bewustwording is in je onderneming en zorg dat er binnen het bedrijf bewust wordt omgegaan met data. Kun je aangeven hoe dat is gedaan?

### PERSOONSGEGEVENS VERWIJDEREN

Controleer alle huidige opgeslagen persoonsgegevens. Heb je de beschikking over persoonsgegevens die niet noodzakelijk zijn en/of niet meer worden gebruikt? De AVG verplicht je deze gegevens te verwijderen, tenzij je hier nadrukkelijk (en aantoonbare) toestemming voor hebt gekregen.

### VERWERKERSOVEREENKOMSTEN

Werk jij samen met een andere partij (verwerker)? Dan ben je verplicht om een verwerkersovereenkomst af te sluiten. Ga na met welke verwerkers jij samenwerkt en controleer of die overeenkomst voldoet aan de eisen die de AVG daar aan stelt. [Bekijk hier wat er in een verwerkersovereenkomst moet staan:](#)



### PRIVACY BY DESIGN / PRIVACY BY DEFAULT

Maak je organisatie vertrouwd met de termen *privacy by design* en *privacy by default*. Dit houdt in dat je bij het ontwerpen van producten en diensten ervoor zorgt dat persoonsgegevens goed worden beschermd en dat je alleen noodzakelijke persoonsgegevens verwerkt.

### RECHT OP INZAGE, CORRECTIE EN VERWIJDERING

Personen krijgen in de nieuwe wet extra rechten, waaronder recht op inzage, correctie en verwijdering. Zorg dat personen hun gegevens eenvoudig kunnen opraven/ verkrijgen en doorgeven aan een andere organisatie als ze dat willen.

# Databeveiliging

## □ VERWERKINGSREGISTER

Stel een verwerkingsregister op waarin iedere verwerking van persoonsgegevens gedocumenteerd wordt. Het register mag zowel in elektronische vorm als schriftelijke vorm worden bijgehouden. [Bekijk hier wat er in een verwerkingsregister moet staan:](#)



## □ FUNCTIONARIS VOOR DE GEGEVENSBESCHERMING (FG) NODIG?

Ga na of je als organisatie verplicht bent om een Functionaris voor de Gegevensbescherming aan te stellen. Dit is iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de AVG. [Lees meer:](#)



## □ UP-TO-DATE SOFTWARE

De omgeving waaruit je medewerkers toegang hebben tot persoonsgegevens moet goed beveiligd zijn. Let dus op dat werksystemen voorzien van de laatste (Windows) beveiligingsupdates, de laatste versie van geïnstalleerde programma's, antivirus- en firewallsoftware.

## □ TOEGANG DATABESTANDEN

Inventariseer hoe de toegang tot de databestanden is beveiligd. Wie binnen de organisatie kan persoonsgegevens inzien en/of wijzigen? Neem maatregelen om de persoonsgegevens te beveiligen en inbreuk te voorkomen. Denk na over autorisatie en leg dit goed vast.

## □ REGELMATIGE BACK-UP

Hoe is gewaarborgd dat persoonsgegevens niet verloren gaan bij een computerstoring, inbraak, brand of een andere noodsituatie? Het is noodzakelijk om regelmatig een back-up te maken. Ga na of dat geregeld is en of de back-ups veilig worden bewaard.

## □ PAPIEREN DOCUMENTEN

Hoewel de nadruk ligt op de omgang met en het beveiligen van digitale informatie, geldt de AVG ook voor geprinte data en papieren documenten. Hoe en waar wordt informatie op papier bewaard zodat de wet hier geen bezwaar tegen maakt?

## □ BELEID BIJ DATALEKKEN

Wat doe je om te voorkomen dat persoonsgegevens 'op straat' komen te liggen? Dat kan bijvoorbeeld een klantenlijst zijn of een deelnemerslijst aan een bijeenkomst. Heb je een plan klaar als het datalekket toch gebeurt? Denk aan tijd, aard en maatregelen die dan genomen moeten worden.

## □ DATA PROTECTION IMPACT ASSESSMENT, DPIA

Is er een waarschijnlijkheid dat de gegevensverwerking door je bedrijf een hoog privacy risico oplevert voor de betrokkenen? Denk bijvoorbeeld aan het evalueren van persoonlijke aspecten of het volgen van mensen in een publiek toegankelijk gebied, dan is een [Data Protection Impact Assessment \(DPIA\) verplicht](#). [Lees meer:](#)



Je voldoet daarmee aan de verplichting om vooraf de risico's van gegevensverwerking in kaart te brengen.

# Marketingtools



Ook op het gebied van digitale marketing heeft de AVG veel impact en raakt vrijwel alle vakgebieden: van analytics en conversie-optimalisatie tot social media en het versturen van nieuwsbrieven. Met onderstaande checklist ga je na wat de verplichtingen zijn van de nieuwe privacywet:

## ☐ EXTERNE SOFTWARE/TOOLS AVG-PROOF?

Maak een lijst van marketingtools die persoonsgegevens voor jouw bedrijf verwerkt. Controleer of de voorwaarden voldoen aan de nieuwe regels van de AVG. Denk aan e-mailmarketing software, chatfunctionaliteit, analyse en A/B testing tools. Mogelijk voldoen externe partijen wel aan de AVG, maar alleen met bepaalde instellingen of beperkte functionaliteiten. Zorg dan voor privacyvriendelijke instellingen die wel voldoen aan de AVG. Vaak is dit terug te vinden op de website van de aanbieder.

## ☐ VERWERKERSOVEREENKOMSTEN

Let ook bij je marketingsoftware en tools op dat je een verwerkersovereenkomst afsluit wanneer er persoonsgegevens verwerkt worden. In veel gevallen is dit namelijk zo. [Bekijk hier wat er in een verwerkingsovereenkomst moet staan:](#) 

## ☐ TOESTEMMING VRAGEN (OPT-IN)

Zorg ervoor dat je geldige (en aantoonbare) toestemming krijgt van bezoekers voor elk specifiek doel waarbij je niet noodzakelijke persoonsgegevens verwerkt. Bijvoorbeeld voor een nieuwsbrief inschrijving. Geef hierbij aan wat de bezoeker kan verwachten: hoe vaak verstuurt je de nieuwsbrief en wat is de inhoud? Let ook op dat je voor minderjarigen mogelijk toestemming nodig hebt van een ouder.

## ☐ UITSCHRIJFLINK

De AVG verplicht bedrijven dat elke commerciële mail een uitschrijflink bevat. Met deze uitschrijflink kunnen ontvangers zich op ieder moment uitschrijven.

## ☐ VOLDOEN EERDER VERZAMELDE GEGEVENS?

Alle eerder verzamelde persoonsgegevens moeten per 25 mei 2018 aan de nieuwe regels voldoen. Ook de bewijslast moet dan kloppen: heb je geen aantoonbare opt-in gegevens? Dan zul je deze persoonsgegevens moeten verwijderen voor 25 mei.

**Tip:** mailinglijsten zonder aantoonbare opt-in kun je een heractivatie mail sturen. De mail moet een even prominente 'ja' als 'nee' knop bevatten. Geen reactie voor 25 mei 2018 geldt ook als een nee.

# Website/webshop aandachtspunten



Ook voor je website of webshop moet je het een en ander nog doen om straks te voldoen aan de nieuwe privacywet.

## □ PRIVACYVERKLARING

Hierin moet je duidelijk en volledig beschrijven welke persoonsgegevens je verwerkt, waarom (doel), welke maatregelen je treft om deze te beveiligen en hoe lang deze gegevens bewaard worden. [Bekijk ook onze privacyverklaring tips en een basisopzet.](#) 

## □ COOKIEVERKLARING

Analyseer welke cookies door je website geplaatst worden en achterhaal of hier toestemming voor nodig is. In de cookieverklaring beschrijf je wat cookies zijn, welke cookies je gebruikt, waarvoor deze dienen en de bewaartermijn. [Bekijk onze cookieverklaring tips voor informatie en een basisopzet.](#) 

## □ COOKIEMELDING

Met een cookiemelding dien je bezoekers te informeren welke cookies geplaatst worden als zij toestemming geven (opt-in) en met welk doel. Zonder toestemming mag je niet cookies plaatsen die inbreuk hebben op de privacy, zoals remarketing en profiling cookies. Je moet kunnen aantonen wanneer, hoe, waarvoor en waarop toestemming is gegeven.

## □ HYPERLINKS

Als je privacyverklaring en cookieverklaring volledig AVG proof zijn, adviseren wij je beide verklaringen een geheel eigen pagina te geven. Daarnaast moeten ze eenvoudig terug te vinden zijn op je website, bijvoorbeeld middels hyperlinks in de footer.

## □ GOOGLE ANALYTICS

Gebruik je Google Analytics? Dan verwerk je met analytische cookies persoonsgegevens van websitebezoekers. Om aan de AVG voorwaarden te voldoen, moet de technische code aangepast worden zodat het IP-adres geanonimiseerd wordt. Daarnaast moet je Google Analytics account privacyvriendelijk instellen.

## □ FORMULIEREN

Het is volgens de AVG niet toegestaan om gegevens te vragen die niet noodzakelijk zijn voor het doel dat je wilt bereiken. Zorg dat je bij alle formulieren op je website enkel persoonsgegevens verwerkt die nodig zijn voor het doel dat je wilt bereiken.

## □ SSL-CERTIFICAAT

Zorg dat je website een SSL-certificaat heeft. Hiermee wordt alle data, die via de website verstuurd wordt, versleuteld. Elke website die structureel persoonsgegevens verwerkt is verplicht om een SSL-certificaat te hebben.

## □ UPDATES EN BEVEILIGING

Zorg ervoor dat je website CMS en eventuele plug-ins/extensies up-to-date zijn om beveiligingslekken te voorkomen. Controleer ook of er extensies zijn die (stiekem) informatie doorsturen naar de ontwikkelaars van de extensies.

# Disclaimer

Deze checklist bevat de hoofdpunten en is bedoeld als ondersteuning voor de beeldvorming van de globale inhoud van de AVG. Je kunt geen rechten ontleen aan deze checklist.

Het moment, 25 mei 2018, komt snel dichterbij. Werk systematisch en betrek medewerkers, collega's, vrijwilligers en andere betrokkene bij het implementeren van de AVG!



Voor meer informatie ga naar [www.speak.nl](http://www.speak.nl)  
of bel 0512 36 60 79