AVG (GDPR) bij [uw Bedrijf]

[uw Bedrijf]
AVG team
22-3-2018
Document versie: 5
Document status: Concept

Inhoud

[1.1 Moeilijke woordenlijst 3](#_Toc509489845)

[2 Inleiding 4](#_Toc509489846)

[2.1 AVG-Team 4](#_Toc509489847)

[2.2 Leeswijzer 4](#_Toc509489848)

[3 Bewustwording AVG 5](#_Toc509489849)

[3.1 Persoonsgegevens 5](#_Toc509489850)

[3.2 De Betrokkene(n) 5](#_Toc509489851)

[3.3 Hoe mogen we persoonsgegevens verwerken 6](#_Toc509489852)

[3.4 Verwerkingsverantwoordelijke personen bij ABC 7](#_Toc509489853)

[3.5 Opslag van persoonsgegevens en beveiliging 8](#_Toc509489854)

[3.6 Privacyverklaring (privacy statement) 8](#_Toc509489855)

[3.7 De AVG regelhulp 8](#_Toc509489856)

[3.8 ABC gegevensverzamelingen 9](#_Toc509489857)

[4 Data protection impact assessment (DPIA) 10](#_Toc509489858)

[4.1 DPIA heeft lage prioriteit bij ABC 10](#_Toc509489859)

[5 Het [uw Bedrijf] Verwerkingsregister 11](#_Toc509489860)

[5.1 Het verwerkingsregister bij [uw Bedrijf] is verplicht 11](#_Toc509489861)

[5.2 Inhoud van het verwerkingsregister 11](#_Toc509489862)

[6 De Functionaris voor de Gegevensbescherming (FG) 12](#_Toc509489863)

[6.1 De FG bij [uw Bedrijf] is vooralsnog onnodig 12](#_Toc509489864)

[7 De Verwerkersovereenkomsten 13](#_Toc509489865)

[7.1 Verwerkers van [uw Bedrijf] 13](#_Toc509489866)

[8 Registratie en Meldplicht van datalekken 14](#_Toc509489867)

[8.1 Melden datalekken 14](#_Toc509489868)

[8.2 Beleidsregels meldplicht datalekken 14](#_Toc509489869)

[8.3 Registratie van datalekken 14](#_Toc509489870)

[8.4 Overzichten meldingen datalekken 14](#_Toc509489871)

[9 Verantwoordingsplicht 15](#_Toc509489872)

[10 Toestemming van de betrokkene 16](#_Toc509489873)

[10.1 Toestemming van vrijwilligers en werknemers 16](#_Toc509489874)

[11 Rechten van de betrokkene 17](#_Toc509489875)

[11.1 Voldoen aan het Recht op Inzage 18](#_Toc509489876)

[11.2 Voldoen aan het Recht op Correctie 19](#_Toc509489877)

[11.3 Voldoen aan het Recht op Vergetelheid 19](#_Toc509489878)

[12 Beveiligingsmaatregelen 20](#_Toc509489879)

[12.1 IT maatregelen 20](#_Toc509489880)

[12.2 Gebruik van @[uw Bedrijf].NL e-mailaccounts 20](#_Toc509489881)

[12.3 Aanmeldformulieren aanpassen 21](#_Toc509489882)

[12.4 Organisatorische maatregelen 21](#_Toc509489883)

[12.5 Gebruik [uw Bedrijf] briefpapier 21](#_Toc509489884)

[13 Frequently Asked Questions 22](#_Toc509489885)

[14 Bijlage: Overzicht [uw Bedrijf] gegevensverzamelingen 26](#_Toc509489886)

## Moeilijke woordenlijst

|  |  |
| --- | --- |
| Medewerkers | In het kader van de AVG wordt met de term “medewerkers“ alle vrijwilligers en werknemers van [uw Bedrijf] bedoeld.***Ook in dit document wordt deze term als zodanig gebruikt !*** |
| Bewerker / verwerker | Een verwerker is een persoon of organisatie aan wie de verantwoordelijke de gegevensverwerking heeft uitbesteed. Bijvoorbeeld een administratiekantoor, drukkerij of CRM provider. |
| Betrokkene | De betrokkene is degene van wie [uw Bedrijf] persoonsgegevens verwerkt. Dit is dus degene op wie de persoonsgegevens betrekking hebben, door AVG beschermd wordt, en is ook de rechthebbende is i.h.k.v. AVG.  |
| Verantwoordelijke | De verantwoordelijke is de persoon die het doel van en de middelen voor het gebruik van persoonsgegevens bepaalt. |
| GegevensverwerkenofGegevensverwerking | Onder het verwerken van persoonsgegevens worden alle handelingen verstaan die [uw Bedrijf] kan uitvoeren met die persoonsgegevens. Voorbeelden zijn:verzamelen, vastleggen, ordenen, bewaren, bewerken, wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen. |
| Dataportabiliteit | Het recht hebben om de eigen – digitale – persoonsgegevens makkelijk op te vragen in een standaard formaat. Zo kunnen betrokkenen hun gegevens makkelijk doorgeven aan een andere leverancier van dezelfde soort dienst. Bijvoorbeeld als zij zich willen uitschrijven bij de ene sociale netwerksite en zich inschrijven bij een andere, wisselen van verzekeraar of van InternetProvider. Betrokkenen kunnen zelfs eisen dat de organisatie hun persoonsgegevens direct doorstuurt aan de nieuwe dienstverlener, als dat (technisch) mogelijk is. |
| Doelbinding | Doelbinding houdt in dat persoonsgegevens alleen voor specifieke, uitdrukkelijke en legitieme doeleinden mogen worden verzameld en niet verder mogen worden gebruikt op een manier die onverenigbaar is met deze doeleinden. |
| Profiling  | Met profiling (profileren) wordt de techniek bedoeld waarmee personen op grond van de verzamelde persoonsgegevens een bepaald soort ‘stempeltje’ (kunnen) krijgen. Lees [hier](https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/big-data-en-profiling#wat-zijn-de-privacyrisico’s-van-profiling-2004) [[1]](#footnote-1)) meer over profiling. |
| AVGWbp | Algemene Verordening Gegevensbescherming is de wet die sinds 25 mei 2016 de oude “Wet Bescherming Persoonsgegevens” (Wbp) heeft vervangen. |
| AP | Zie [www.AutoriteitPersoonsgegevens.nl](http://www.AutoriteitPersoonsgegevens.nl)  |
| GDPR | De Engelse afkorting voor AVG: General Data Protection Regulation |
| DPIA | Toetsing om vooraf de privacy risico’s van een gegevensverwerking in kaart te brengen. |
| CRM | XYZ is de naam van het releatiebeheersysteem (Customer Relation Management systeem = CRM) waarmee de meeste persoonsgegevens van [uw Bedrijf] verwerkt (gaan) worden  |

# Inleiding

Per 24 mei 2016 is de nieuwe wetgeving Algemene verordening gegevensbescherming (AVG) ingegaan. Per 25 mei 2018 wordt deze nieuwe wet daadwerkelijk gehandhaafd en kunnen boetes worden uitgedeeld aan bedrijven die niet aan de nieuwe regels voldoen. Dit document heeft als doel om iedereen binnen [uw Bedrijf] op de hoogte te brengen van de nieuwe privacyregels.

Op vele plaatsen binnen [uw Bedrijf] wordt gecommuniceerd met museumbezoekers, leveranciers, klanten en dienstverleners. Binnen AVG worden zij “natuurlijke personen” of “betrokkenen” genoemd. Organisaties moeten beperkt, beveiligd en precies omgaan met persoonsgegevens en inzage verlenen aan de autoriteit persoonsgegevens èn aan de betrokkenen. De nadruk ligt - meer dan nu - op onze verantwoordelijkheid om te kunnen aantonen dat wij ons aan de wet houden. Lees daarom aandachtig de verschillende hoofdstukken door en stel je eventuele vragen aan het AVG team.

Zondermeer kan worden gesteld dat de AVG voor elk bedrijf in Europa grote gevolgen heeft: zo ook voor [uw Bedrijf]. Lijstjes met naam-adres-woonplaats gegevens of lijstjes met e-mailadressen mogen niet meer rondslingeren. Deze moeten volgens de wet allemaal geregistreerd zijn binnen het bedrijf. Voor elk lijstje zal iemand verantwoordelijk zijn en de toegang dient afgeschermd te zijn.

Privacy is een grondrecht van ons allemaal. Elke werknemer is ook een “natuurlijk persoon”. Privé ervaren we de voordelen van AVG door een respectvolle omgang met persoonsgegevens. Daarom moet [uw Bedrijf] als organisatie AVG compliant zijn en de privacy van relaties goed op orde hebben. Niet alleen omdat de wet dat vraagt, maar vooral omdat onze relaties dat van ons verlangen.

Bedenk dat, als de medewerkers van [uw Bedrijf] deze nieuwe wet niet naleven, [uw Bedrijf] aangeklaagd kan worden door de betrokkene, publiekelijk in een slecht daglicht kan worden geplaatst en/of een boete kan krijgen. De sancties die de AP kan opleggen zijn maximaal 20 miljoen euro of 4% van de omzet als men zich niet aan de nieuwe privacywetgeving houdt.

De website [www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl) geeft aan wat we binnen [uw Bedrijf] wel of niet mogen doen in het kader van AVG. Dit document is bedoeld om je daarbij te helpen.

## AVG-Team

Vragen omtrent de AVG binnen [uw Bedrijf] kunnen jullie en buitenstaanders stellen aan het AVG-team, Dit team is te bereiken via e-mailadres avg@[uw Bedrijf].nl en is samengesteld uit:

* Eindverantwoordelijkheid: xxxx
* Organisatorische verantwoordelijkheid: yyyy
* Technische verantwoordelijkheid: zzzz

## Leeswijzer

Weet je nog weinig van AVG begin dan met het lezen van hoofdstuk 3. De hoofdstukken 4, 5, 6 en 7 geven achtergrond informatie over hoe we AVG binnen [uw Bedrijf] opzetten.

Hoofdstuk 8 gaat over hoe we moeten omgaan met het melden van datalekken.

Hoofdstuk 9 gaat over de verantwoordingsplicht van [uw Bedrijf].

Hoofstuk 10 en 11 geven informatie over de betrokkenen. Als we zelf een mailing van een ander bedrijf ontvangen zijn we zelf ook een “Betrokkene”. Deze hoofdstukken geven meer informatie over de rechten die je als betrokkene hebt en de toestemming die je voortaan expliciet gegeven moet hebben voordat een ander bedrijf jouw gegevens in hun bestand mogen opnemen.

Hoofdstuk 12 gaat over de te nemen technische en organisatorische beveiligingsmaatregelen.

Tenslotte in hoofdstuk 13 vind je antwoorden voor veel gestelde vragen.

# Bewustwording AVG

De AVG wetgeving betreft persoonsgegevens over betrokkenen. De nieuwe wet heeft betrekking op de privacy van personen en is op 24 mei 2016 ingegaan met een overgangstermijn van 2 jaar. Per 26 mei 2018 gaat deze wet daarom ook gehandhaafd worden.
Kernbegrippen van deze wet zijn aldus samen te vatten:

* Persoonlijke vrijheid, persoonlijk leven;
* Onbespied en onbewaakt kunnen leven;
* Mogelijkheid om vertrouwelijk te communiceren;
* Zelf bepalen wie welke informatie over je krijgt.

Deze wet heeft twee hoofddoelen:

* Bescherming persoonsgegevens;
* De betrokkenen het recht van Dataportabiliteit geven binnen de EU. (Zie blz. 1.13).

De wet maakt een afweging tussen:

* Het privacybelang van personen
* Het belang van degenen (bijvoorbeeld bedrijven) die persoonsgegevens verwerken.

Door deze wet gaan flink wat zaken veranderen en sommige veranderingen kunnen grote gevolgen hebben. Deze veranderingen zijn onder andere:

* Versterking privacyrechten van natuurlijke personen (oftewel de betrokkenen);
* Meer verantwoordelijkheden en plichten voor organisaties om aan AVG-eisen te voldoen;
* Meer regelgeving voor samenwerkingen;
* Stevige bevoegdheden voor alle Europese privacytoezichthouders. De Nederlandse toezichthouder is hier te bereiken: [www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl).

Uitleg wat wordt verstaan onder persoonsgegevens, betrokkenen, verantwoordelijken en de andere begrippen is daarom nodig.

## Persoonsgegevens

Voor de AVG is de term persoonsgegevens heel ruim. Dit kunnen zijn:

* Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon
(“de betrokkene”).
Merk op: De voormalige Wpb gaat enkel over **levende** natuurlijke personen. De EU-AVG sluit overleden personen ook uit mits een EU-land op dit punt geen eigen wetgeving instelt. (zie hoofdstuk13 over de - op 6 april 2017 - in NL voorgestelde wetgeving).
* Kan in de vorm van: tekst (registratie), beeld (foto’s, video’s) of zelfs (stem)geluid.

Voorbeelden:
NAW gegevens zoals: naam, adres, woonplaats, postcode+huisnr, telefoonnr,
Bijzondere gegevens zoals: e-mailadres, IP-adres, BSN, inlogcodes, publicaties, meningen, medisch dossier, foto, filmbeelden, röntgenfoto, e-mails, opleiding, beroep, geluidsopname, gezinssamenstelling, geboortedatum, lidmaatschappen.

## De Betrokkene(n)

De **betrokkene(n)** is/zijn degene(n) van wie [uw Bedrijf] persoonsgegevens verwerkt. Het gaat steeds om de gegevens van “Natuurlijke Personen”. Dit zijn dus degenen op wie de persoonsgegevens betrekking hebben. Zoals:

* **Scholen en/of leerlingen**
De (contact)-personen van scholen zijn betrokkenen, maar de leerlingen en begeleiders – mits we niets van hun registreren – zijn dat niet. Echter, zodra we bijvoorbeeld foto’s maken van de aanwezigen, dan vallen deze weer wel in de categorie “betrokkenen”. Maakt iemand anders foto’s (die niet voor- of in opdracht van- [uw Bedrijf] werkt) dan zijn de aanwezigen niet “onze” betrokkenen.
* **Verenigingen, vriendenclubs en hun leden**
De (contact)-personen van verenigingen of clubs zijn betrokkenen, maar de leden van die verenigingen – mits we niets van hun registreren – zijn dat niet. Echter, zodra wij bijvoorbeeld foto’s maken van de mensen, dan vallen ze weer wel in de categorie “betrokkenen”. Maakt iemand anders foto’s (die niet voor- of in opdracht van- [uw Bedrijf] werkt) dan zijn de mensen niet “onze” betrokkenen.
* **Zaalhuurders en hun gasten / bezoekers**
De (contact)-personen die zelf of namens iemand anders een zaal huren zijn betrokkenen, maar de bezoekers van het gezelschap – mits we niets van hun registreren – zijn dat niet. Echter, zodra wij bijvoorbeeld foto’s maken van de bezoekers vallen deze weer wel in de categorie “betrokkenen”. Maakt iemand anders foto’s (die niet voor- of in opdracht van- [uw Bedrijf] werkt) dan zijn de bezoekers niet “onze” betrokkenen.
* **Museumkaarthouders**
De museumkaarthouders worden – in principe – niet bij ons maar bij Museum/kaart\ geregistreerd. De museumkaarthouders zijn daarom betrokkenen van het bedrijf Museum/kaart\.
* **Museumbezoekers**
De meeste museumbezoekers zijn – mits door ons niets over ze wordt geregistreerd – geen betrokkenen. Ook als een postcode zonder huisnummer wordt geregistreerd, is een museumbezoeker geen betrokkene. Echter, schrijft deze museumbezoeker zich in voor een nieuwsbrief of prijsvraag of reserveert deze een rondleiding, dan is dit een betrokkene.
* **[uw Bedrijf] vrijwilligers en werknemers**
Elke [uw Bedrijf] vrijwilliger en werknemer is een betrokkene: immers de persoonsgegevens van ons allen worden opgeslagen in de medewerkersdatabase en gebruikt om het kwartaalblad Meer-Historie (via de post) te kunnen versturen, de MeerNieuws en MeerFlits per e-mail rond te sturen en het ‘smoelenboek’ samen te stellen.
* **Vereniging Vrienden van de Cruquius**
De vrienden van de Cruquius die bij ons voorkomen in één van de bestanden zijn betrokkenen.
* **Leveranciers, afnemers, verwerkers**
De contactpersonen die we van leveranciers, afnemers, bruikleenverstrekkers, donateurs en verwerkers registreren zijn voor de AVG wet ook betrokkenen.

## Hoe mogen we persoonsgegevens verwerken

Onder het verwerken van persoonsgegevens worden alle handelingen verstaan die [uw Bedrijf] kan uitvoeren met die persoonsgegevens. Voorbeelden zijn:

verzamelen, vastleggen, ordenen, bewaren, bewerken, wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen.

De nieuwe AVG wet stelt simpel dat het gebruik van persoonsgegevens mag, mits ondubbelzinnig beschreven is welke gegevens voor welk proces binnen het bedrijf worden gebruikt. Dit alles dient vastgelegd te zijn in het verwerkingsregister. Op de website van AP wordt beschreven welke gegevens beslist niet mogen (ras, godsdienst, etc). Ook geboorteplaats valt daaronder omdat daarmee soms het ras kan worden bepaald.

De verwerking van persoonsgegevens moet voldoen aan de volgende principes:

* Moet rechtmatig, behoorlijk en transparant zijn;
* Op basis van te voren uitdrukkelijk omschreven en gerechtvaardigde doelen;
* Niet meer gegevens verwerken dan nodig;
* Gegevens moeten relevant zijn;
* Niet langer bewaren dan noodzakelijk;
* Passende en voldoende beveiliging (zowel organisatorisch als technisch).

**Rechtmatige verwerking / Grondslag**

Van Rechtmatige Verwerking van ‘gewone’ persoonsgegevens is alleen sprake [mits dit gebaseerd is op minimaal één](https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/mag-u-persoonsgegevens-verwerken#wanneer-mag-u-zich-baseren-op-de-grondslag-algemeen-belang-of-openbaar-gezag-6329) van de zes in de AVG limitatief opgesomde gronden:

1. Nodig voor uitvoering van een overeenkomst (met de betrokkene)
2. Nodig ter uitvoering wettelijke verplichting
3. Nodig ter vrijwaring vitaal belang betrokkene
4. Nodig voor behartiging gerechtvaardigd belang
5. Nodig voor goede vervulling publiekrechtelijke taak
6. Ondubbelzinnige toestemming betrokkene

Met andere woorden: Alleen als een betrokkene een ‘ondubbelzinnige toestemming’ geeft mogen wij zijn of haar persoonsgegevens verwerken (zie ook hoofdstuk 10). In alle andere gevallen mogen we pas persoonsgegevens verwerken als vastgesteld is dat e.e.a. beslist nodig is (zie punten 1 t/m 5 hierboven).

## Verwerkingsverantwoordelijke personen bij [uw Bedrijf]

De **verwerkingsverantwoordelijke** is de persoon die het doel van en de middelen voor het gebruik van persoonsgegevens binnen [uw Bedrijf] bepaalt. Deze verantwoordelijke kan dit alleen doen of samen met anderen. Het houdt in dat de verantwoordelijke uiteindelijk beslist of de persoonsgegevens t.b.v. [uw Bedrijf] worden verwerkt, en zo ja:

* om welke verwerking het gaat (welke bestand(en)? welke processen?);
* welke persoonsgegevens hierbij verwerkt worden;
* voor welk doel [uw Bedrijf] dit doet (waarvoor wordt dit bestand gebruikt?);
* op welke manier [uw Bedrijf] dit doet (hoe gebeurt dit? wie heeft er toegang toe?).

Al deze informatie wordt vastgelegd in het **[uw Bedrijf]** **verwerkingsregister** (zie hoofdstuk 5). Het verwerkingsregister wordt onder andere gebruikt om eventuele vragen van de betrokkene omtrent zijn/haar registratie binnen [uw Bedrijf] te kunnen beantwoorden.

Kortom, houd je binnen [uw Bedrijf] een adreslijst en dus persoonsgegevens bij, dan ben je een “verantwoordelijke” volgens de AVG wet. Denk hierbij aan persoonsgegevens in Excel bestanden, e‑mails met namenlijstjes (let op een outlookarchief kan jaren oud zijn); aan reserveringsformulieren, visitekaartjes, genodigden- of contactlijsten, op papier bij de balie, in de voorraadkast. Denk ook aan filmpjes van de machine in beweging waarop herkenbare scholieren, groepen, voormalig rondleiders staan.
Omdat jij je ook aan de AVG wet moet houden is het belangrijk dat je weet wat je mag en niet mag doen met die gegevens. Uiteraard gaat verantwoordelijkheid en aansprakelijkheid samen.

**Taken van de Verwerkingsverantwoordelijke**

* Bijhouden van het verwerkingsregister;
* Meewerken aan de Privacy Impact Assessment (DPIA) (risico analyse);
* Privacy by design (dit houdt in dat al in een vroeg stadium zowel technisch als organisatorisch een zorgvuldige omgang met persoonsgegevens moet worden afgedwongen);
* Privacy by default (dit houdt in dat de standaard instellingen voor teksten op formulieren of in programma’s altijd zo privacy-vriendelijk mogelijk moeten zijn: bijvoorbeeld bij de vraag of de betrokkene een e-mail wil ontvangen deze NIET vooraf al aanvinken);
* Zorgen voor passende beveiliging van informatie;
* Verplicht melden van data datalekken;
* Overeenkomsten bij samenwerking, denk aan Ring biënnale;
* Verwerkingsovereenkomst bij uitbesteding (o.a. drukkerij, perfectview, boekhouding);
* Deelnemen aan certificering.

## Opslag van persoonsgegevens en beveiliging

Volgens de AVG wet dient ook [uw Bedrijf] vast te leggen wie toegang heeft tot persoonsgegevens. Ook dient [uw Bedrijf] te voorkomen dat persoonsgegevens gedeeld worden met medewerkers die – volgens het verwerkingsregister – geen toegang hebben.

Voorbeelden zijn:

* Anneloes Achternaam krijgt geen toegang tot de persoonsgegevens van de mensen die zich aangemeld hebben voor rondleidingen in het museum omdat deze door Klasina Achternaam vanuit Secretariaat worden beheerd.
* De persoonsgegevens van de mensen die de digitale nieuwsbrief via de website ontvangen zijn alleen toegankelijk voor de Geertje Achternaam.

Met andere woorden: elk bedrijf moet volgens de AVG wet vastgelegd hebben wie toegang heeft tot welke gegevens en ook wie de gegevens mag wijzigen of de gegevens alleen mag bekijken.

**Relatiebeheersysteem / CRM**

Om aan de AVG wet te kunnen voldoen gaat [uw Bedrijf] voor de opslag van persoonsgegevens een relatiebeheersysteem gebruiken. Dit is één van de beveiligingsmaatregelen (zie ook hoofdstuk 12.1).

## Privacyverklaring (privacy statement)

[uw Bedrijf] zal verschillende privacy-verklaringen opstellen, toegespitst op bijvoorbeeld: websitebezoek, digitale nieuwsbrief abonnees, Meer-Historie abonnees of vrijwilligers. Dit zijn verplicht op te stellen documenten die worden gepubliceerd via de website of uitgedeeld op papier bij offertes, bij aanmelding als vrijwilliger, als bijlage bij e-mail. Je kunt onze privacy verklaring [hier](https://www.haarlemmermeermuseum.nl/privacyverklaring) op de website lezen.

In de privacy verklaring is opgenomen:

* Persoonsgegevens (van wie, waar, en wanneer);
* Contactgegevens verantwoordelijke;
* Doel (uitvoeren overeenkomst, aanvullende diensten, verbeteren dienstverlening, marketing, etc.);
* Afgifte op grond van wettelijke verplichting;
* Doorgifte aan derden;
* Bewaartermijn;
* Rechten betrokkene (inzage, verbetering, verwijdering, overdraagbaarheid;
* Bijzonderheden.

## De AVG regelhulp

Op deze website: <https://rvo.regelhulpenvoorbedrijven.nl/avg/welkom> vind je de vragenlijst die eenvoudig te doorlopen is en advies geeft omtrent de eigen situatie.

Doorloop zelf deze website en de stappen eens aandachtig en merk op of we en waar we als [uw Bedrijf] nog tekort schieten.

Kijk ook op pagina 22 van dit document bij de “veel gestelde vragen” (FAQ).

## [uw Bedrijf] gegevensverzamelingen

Voor wat betreft AVG heeft [uw Bedrijf] verschillende (persoons)gegevensverzamelingen. Een gegevensverzameling kun je zien als een bestand dat voor een bepaald doel wordt gebruikt. Elke gegevensverzameling heeft slechts 1 verantwoordelijke.

In bijlage 14 vind je het overzicht van de gegevensverzamelingen die we bij [uw Bedrijf] zijn tegengekomen. Op basis van deze informatie wordt ook ons verwerkingsregister (zie hoofdstuk 5) samengesteld. Mocht je jouw bestand hieronder niet terugvinden, laat het ons dan weten.

# Data protection impact assessment (DPIA)

Onder de AVG kan [uw Bedrijf] verplicht zijn een zogeheten data protection impact assessment (DPIA) uit te voeren. Dat is een toetsing om vooraf de privacyrisico’s van een gegevensverwerking bij o.a. verhuur, verkoop, mailing e.d., in kaart te brengen en vervolgens maatregelen te kunnen nemen om de risico’s te verkleinen.

In de Nederlandse vertaling van de AVG wordt de term data protection impact assessment (DPIA) gegevensbeschermingseffectbeoordeling genoemd.

Organisaties hoeven, zodra de AVG geldt, niet voor elke gegevensverwerking een DPIA uit te voeren. Een DPIA is alleen verplicht als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de betrokkenen (de mensen van wie de organisatie gegevens verwerkt). Dat is in ieder geval zo indien [uw Bedrijf]:

* systematisch en uitvoerig persoonlijke aspecten evalueert, waaronder profiling (zie kader);
* op grote schaal bijzondere persoonsgegevens verwerkt;
* op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

Buiten deze drie situaties geeft de AVG geen overzicht van verwerkingen met een hoog risico. De Europese privacytoezichthouders hebben [criteria opgesteld om het risico te bepalen](https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving/data-protection-impact-assessment-dpia#in-welke-gevallen-moet-ik-een-dpia-uitvoeren-5879). Daarnaast publiceert de Autoriteit Persoonsgegevens (AP) op termijn een lijst van verwerkingen waarvoor een DPIA verplicht is.

## DPIA heeft lage prioriteit bij [uw Bedrijf]

Hoewel het voor [uw Bedrijf] onnodig is om een DPIA uit te voeren stelt de AP:

“Het is aan te raden om vrijwillig een DPIA te doen. Dit komt niet alleen de gegevensbescherming ten goede, maar ook voor de organisatie zelf levert een [DPIA voordelen](https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacycheck/privacy-impact-assessment-pia) op.“

**Profiling**

Met profiling (profileren) wordt de techniek bedoeld waarmee personen op grond van de verzamelde persoonsgegevens een bepaald soort ‘stempeltje’ krijgen.

Door middel van profiling kan een organisatie het gedrag van mensen voorspellen of een beslissing over hen nemen. Iemand kan op die manier – op basis van een algemeen gedrags- of risicoprofiel – individueel beoordeeld worden. Soms met alle gevolgen van dien. Bijvoorbeeld dat diegene in eerste instantie niet de gevraagde lening krijgt en moeite moet doen om de organisatie te overtuigen dat zijn profiel niet klopt. Of dat die persoon niet wordt uitgenodigd voor een sollicitatiegesprek.

Profiling is toegestaan maar organisaties moeten zich bij profiling aan de privacywetgeving houden. Voor het bedrijfsleven en de overheid gelden niet altijd dezelfde privacyregels. Risicoprofilering door politie en justitie voor politietaken en opsporing (waaronder grenscontrole op luchthaven Schiphol door de Koninklijke Marechaussee) mag wanneer daarvoor een wettelijke basis bestaat.

Lees [hier](https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/big-data-en-profiling#wat-zijn-de-privacyrisico’s-van-profiling-2004) meer over profiling.

# Het [uw Bedrijf] Verwerkingsregister

Onder de AVG heeft [uw Bedrijf] een verantwoordingsplicht, wat inhoudt dat [uw Bedrijf] moet kunnen aantonen dat de organisatie in overeenstemming met de AVG handelt. Het bijhouden van een register van verwerkingsactiviteiten (verwerkingsregister) is onderdeel van de verantwoordingsplicht.

**Het opstellen van een register van verwerkingsactiviteiten is onder de AVG vaak een verplichte maatregel. In het register staat informatie over de persoonsgegevens die [uw Bedrijf] verwerkt. Of een dergelijk register moet worden opgesteld, hangt af van de omvang van [uw Bedrijf] en het type gegevens dat [uw Bedrijf] verwerkt.**

Let op: Voor de AVG wet tellen vrijwilligers en werknemers samen mee
bij de berekening van het aantal “medewerkers”.

#### Organisaties met meer dan 250 medewerkers

Heeft de organisatie meer dan 250 medewerkers? Dan is het **verplicht** om een register van verwerkingsactiviteiten bij te houden.

#### Organisaties met minder dan 250 medewerkers

Heeft de organisatie minder dan 250 medewerkers? Dan is het register slechts verplicht, wanneer de volgende persoonsgegevens worden verwerkt:

* waarvan de verwerking niet incidenteel is. In de praktijk zijn verwerkingen zelden incidenteel. Denk bijvoorbeeld aan de persoonsgegevens van medewerkers die worden verwerkt. Of van scholen, museumbezoekers, zaalhuurders en/of;
* die een hoog risico inhouden voor de rechten en vrijheden van de personen van wie je persoonsgegevens verwerkt en/of;
* die vallen onder de categorie [bijzondere persoonsgegevens](https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/wat-zijn-persoonsgegevens). Zoals gegevens over godsdienst, gezondheid en politieke voorkeur of strafrechtelijke gegevens.

Is het bedrijf verplicht om een register van verwerkingsactiviteiten op te stellen? Dan moet dit register kunnen worden verstrekt wanneer de Autoriteit Persoonsgegevens daar om vraagt. **Dit register is een intern document en wordt niet gepubliceerd.**

## Het verwerkingsregister bij [uw Bedrijf] is verplicht

Gezien dat het aantal [uw Bedrijf] medewerkers rond de 250 m/v ligt, en het verwerken van persoonsgegevens van de medewerkers, bezoekers etc. niet incidenteel is, is een verwerkingsregister verplicht. Het opstellen heeft dan ook prioriteit.

Het verwerkingsregister bevat informatie over de gegevens die worden opgeslagen en wie de verwerkingsverantwoordelijke is voor die gegevens.

## Inhoud van het verwerkingsregister

In het verwerkingsregister worden alle (persoons)gegevensverzamelingen (zie hoofdstuk 3.8 ) opgenomen. Per gegevensverzameling bevat het verwerkingsregister:

* De naam van de Verantwoordelijke(n);
* De beschrijving van de categorieën van betrokkenen en persoonsgegevens ;
* De verwerkingsdoeleinden;
* De wettelijke grondslag voor de gegevensverwerking
(zie hoofdstuk 3.3 onder het kopje “Rechtmatige verwerking / Grondslag);
* De categorieën van ontvangers van de persoonsgegevens;
* De bewaartermijnen van persoonsgegevens i.h.k.v. diensten, producten en verwerkingen;
* De beschrijving van technische en organisatorische beveiligingsmaatregelen.

# De Functionaris voor de Gegevensbescherming (FG)

Per 25 mei 2018 geldt de Algemene verordening gegevensbescherming (AVG). Vanaf dit moment kunnen organisaties verplicht zijn een Functionaris voor de Gegevensbescherming (FG) aan te stellen. Dit is iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de AVG. Op grond van artikel 37 van de AVG is een FG in drie situaties verplicht.

* Bij overheden en publieke organisaties
* Bij profilering van mensen
* Bij verwerken van bijzondere persoonsgegevens

EU-lidstaten kunnen ook andere situaties benoemen waarin een FG verplicht is. Het is nog niet bekend of dit in Nederland gaat gebeuren. Doordat het onduidelijk is of wij verplicht zijn om een FG aan te stellen, moeten wij goed kunnen onderbouwen waarom wij ervoor gekozen hebben om dat wel of niet te doen.

## De FG bij [uw Bedrijf] is vooralsnog onnodig

Gezien de regelgeving is een apart aan te stellen FG bij [uw Bedrijf] vooralsnog onnodig.

Wel is er een AVG team bij [uw Bedrijf] samengesteld waarvan elk lid een eigen onderwerp voor zijn, haar rekening neemt en verantwoordelijk is. Zie hoofdstuk “2.1 AVG-Team”.

# De Verwerkersovereenkomsten

Als je een verwerker inschakelt, moet je volgens de AVG een verwerkersovereenkomst afsluiten. Dit is niet nieuw, want dat moest volgens de voormalige Wpb ook al. Een verwerker is een persoon of organisatie aan wie de verantwoordelijke de gegevensverwerking heeft uitbesteed. Bijvoorbeeld een administratiekantoor, externe boekhouding, drukkerij of het bedrijf waar de klantgegevens zijn opgeslagen.

De AVG geeft een vast lijstje met onderwerpen dat je moet behandelen in de verwerkersovereen-komst. Bijvoorbeeld afspraken over de doeleinden van de verwerking, de manier van beveiliging van gegevens, de hulp bij het uitvoeren van rechten van individuen en de manier waarop je omgaat met persoonsgegevens buiten de EU.

Een verwerker is niet zelfstandig verantwoordelijk voor de verwerking van de persoonsgegevens. Maar de bewerker heeft wel een aantal afgeleide verplichtingen, voor onder meer beveiliging en geheimhouding van de gegevens.

## Verwerkers van [uw Bedrijf]

De verwerkers die voor [uw Bedrijf] persoonsgegevens gebruiken zijn nog niet allemaal vastgesteld. In elk geval zijn het de volgende bedrijven:

* Drukkerij m.b.t. de adreslijsten om het kwartaal blad te kunnen laten bezorgen;
* CRM hoster m.b.t. de verwerking van persoonsgegevens t.a.v. het verzenden van reserveringsbevestigingen naar scholen, zaalhuurders, museum bezoek in groepsverband, en het verzenden van e-mailingen naar werknemers en andere klanten;
* Unit4 m.b.t. de financiële administratie;
* Accountant m.b.t. salarisverwerking;
* Pensioenfonds;
* IT provider m.b.t. Sharepoint en Adlib;
* MailChimp m.b.t. abonnees digitale nieuwsbrief.

Mindere prioriteit / uitsluiten

* Mollie m.b.t. donaties via de website;
* Verzekering;
* webdesigner m.b.t. Drupal, webhost;
* XYZ m.b.t. toegang online bezoekers van de website.

**Taken van de verwerker**

* Alleen verwerken conform de instructies van [uw Bedrijf];
* Eigen systemen moet AVG proof zijn;
* [uw Bedrijf] waarschuwen als opdracht in strijd is met AVG;
* [uw Bedrijf] waarschuwen i.g.v. datalek;
* Voorafgaande toestemming [uw Bedrijf] bij subverwerking;
* Voldoende informatiebeveiliging;
* Verwerkingsregister bijhouden;
* Goede verwerkingsovereenkomst met [uw Bedrijf] hebben.

# Registratie en Meldplicht van datalekken

Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat [uw Bedrijf] direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. En soms moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).

**Het melden van een datalek moet door de organisatie binnen 72 uur gebeuren.**

Wist je dat het gebruik van het Aan en CC veld bij het verzenden van een e-mail reeds als datalek kan worden opgevat. Gebruik altijd het BCC veld, waarbij de mailadressen voor anderen niet zichtbaar zijn.

Ook het verliezen of uitlenen aan derden van een usbstick of laptop met persoonsgegevens uit de bedrijfsvoering van [uw Bedrijf] zijn datalekken.

## Melden datalekken

Organisaties die een datalek willen melden bij de Autoriteit Persoonsgegevens kunnen dat doen via deze link: het [meldloket datalekken](https://datalekken.autoriteitpersoonsgegevens.nl/).

In het [privacystatement formulier meldplicht datalekken](https://autoriteitpersoonsgegevens.nl/nl/privacystatement-formulier-meldplicht-datalekken) is te vinden hoe de Autoriteit Persoonsgegevens omgaat met de persoonsgegevens van degene die een datalek meldt.

Hoewel de meldplicht datalekken blijft bestaan, verandert er mogelijk ook wat. Lees meer over de [meldplicht datalekken in ons AVG-dossier](https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving/voorbereiding-op-de-avg#stap-7-meldplicht-datalekken-5897).

## Beleidsregels meldplicht datalekken

De Autoriteit Persoonsgegevens heeft [beleidsregels meldplicht datalekken](https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken_0.pdf) opgesteld. Deze beleidsregels zijn bedoeld om organisaties te helpen bij het bepalen of er sprake is van een datalek dat zij moeten melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

## Registratie van datalekken

[uw Bedrijf] dient alle datalekken te documenteren. Met deze documentatie moet de AP kunnen controleren of we aan de meldplicht hebben voldaan.

## Overzichten meldingen datalekken

De AP publiceert in 2017 elk kwartaal een totaaloverzicht van alle gemelde datalekken. Daarnaast gaat de AP in een aantal sectorspecifieke overzichten dieper in op de datalekken uit bepaalde sectoren. Zie: [Overzichten meldingen datalekken](https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken/overzichten-meldingen-datalekken).

De Europese privacytoezichthouders hebben in oktober 2017 [guidelines gepubliceerd over de meldplicht datalekken](http://ec.europa.eu/newsroom/document.cfm?doc_id=47741) onder de AVG. Deze guidelines zijn nog niet definitief,

**Conclusie**

Duidelijk is dat rond datalekken veel nog onduidelijk is. Wel is duidelijk dat zorgvuldigheid vereist is en een vermoeden van een datalek zo snel mogelijk aan het AVG team moet worden doorgegeven om de situatie te beoordelen en te kunnen voldoen aan de 72 uur eis.

# Verantwoordingsplicht

De AVG legt volledige verantwoordelijkheid bij [uw Bedrijf] om aan te tonen dat aan de privacyregels voldaan wordt. Door te voldoen aan de verantwoordingsplicht (accountability) wordt een belangrijke bijdrage geleverd aan de bescherming van het grondrecht van mensen op privacy.

De nieuwe regels dwingen om goed na te denken over hoe we als [uw Bedrijf] persoonsgegevens verwerken en beschermen. De verantwoordingsplicht houdt in dat we moeten kunnen aantonen dat de verwerkingen door ons ook aan de regels van de AVG voldoen. Dit is een van de taken van de verwerkingsverantwoordelijke.

Zo moeten we bijvoorbeeld kunnen aantonen dat een verwerking aan de belangrijkste beginselen van verwerking voldoet, zoals:

* rechtmatigheid;
* transparantie;
* doelbinding (zie kader);
* juistheid.

Ook moet aangetoond worden dat we de juiste technische en organisatorische maatregelen hebben genomen om de persoonsgegevens te beschermen.

Als [uw Bedrijf] zijn we verplicht verantwoording af te leggen over onze gegevensverwerkingen wanneer de Autoriteit Persoonsgegevens daar om vraagt.
Zorg daarom dat aan de verantwoordingsplicht kan worden voldaan.

Doelbinding

Doelbinding houdt in dat persoonsgegevens alleen voor specifieke, uitdrukkelijke en legitieme doeleinden mogen worden verzameld en niet verder mogen worden gebruikt op een manier die onverenigbaar is met deze doeleinden.

# Toestemming van de betrokkene

Als de betrokkene expliciet toestemming heeft gegeven voor gebruik van zijn of haar persoonsgegevens (zie ook hoofdstuk 3.3), dan mogen die gegevens worden gebruikt. Echter, de AVG stelt eisen aan de wijze waarop die toestemming is verkregen en is vastgelegd:

* De verantwoordelijke (zie verwerkingsregister), moet toestemming kunnen aantonen
* Toestemming moet blijken uit duidelijke actieve handeling (bijv. handtekening of vink);
* Toestemming voor een specifiek afgebakende verwerking;
* Toestemmingsverzoek moet kort en bondig zijn;
* Toestemming is niet geldig als die als voorwaarde wordt gesteld bij het aangaan van overeenkomst waarvoor die gegevens niet nodig zijn;
* De betrokkene moet toestemming altijd weer in kunnen trekken
(Intrekken moet net zo makkelijk zijn als het geven).

Zonder toestemming moeten de persoonsgegevens na afloop van de dienstverlening, binnen een bepaalde tijd (zoals opgenomen is in het verwerkingsregister), uit de [uw Bedrijf] systemen worden gewist. Slechts de gegevens die de belastingdienst nodig heeft mogen worden bewaard: naam, datum, bedrag, factuurnummer, rekeningnr.

Toch zijn er geldige mogelijkheden om de persoonsgegevens langer te bewaren mits die maar beschreven zijn. Bijvoorbeeld:

* Indien iemand achteraf na verlenen van de dienstverlening de persoonsgegevens nogmaals wil gebruiken, dan dient dit voorafgaand aan de dienstverlening aan de klant bekend gemaakt te worden. Dit kan bijvoorbeeld door in de omschrijving van de dienst op te nemen dat achteraf/naderhand een evaluatie plaatsvindt. Op deze wijze kan een klant vooraf besluiten om de dienst al dan niet door te laten gaan. Bij het toch afnemen van de dienstverlening geeft de klant impliciet toestemming voor het gespecificeerde gebruik, in dit geval evaluatie, van de persoonsgegevens op een later tijdstip.
* Incentives om e-mailadressen te vergaren mag. Immers voor wat hoort wat. Echter de degene die zijn mailadres afstaat is daarna vrij om te verzoeken dat zijn gegevens worden gewist uit de [uw Bedrijf] bestanden.

## Toestemming van vrijwilligers en werknemers

Voor de AVG wetgeving worden vrijwilligers, net als werknemers in vaste dienst, beschouwd als “medewerkers”. [uw Bedrijf] hoeft geen aparte toestemming aan medewerkers te vragen om persoonsgegevens op te slaan. De toestemming wordt verkregen bij het ondertekenen van de overeenkomst voor vrijwilligers of het arbeidscontract.
Je toestemming intrekken voor gebruik van je persoonsgegevens door [uw Bedrijf] komt eigenlijk overeen met het stoppen van vrijwilligerswerk bij [uw Bedrijf] of uit dienst gaan. Wel kunnen er afspraken worden gemaakt over persoonsgegevens door middel van “opt-out”:

* Vraag bezoekers van bijvoorbeeld de Zomerborrel om een rood lint om te hangen als ze niet op de foto willen (de foto’s met de rode linten worden dan naderhand gewist);
* Bijvoorbeeld de naam plus foto wel tonen in de medewerkerslijst/smoelenboek maar zonder het privé (e-mail)adres of telefoonnummer.

# Rechten van de betrokkene

Bij aanvang verwerking – dus bij de registratie – moet de betrokkene geïnformeerd worden over:

* Identiteit verwerkingsverantwoordelijke (voorstel = per gegevensverzameling vastleggen in het verwerkingsregister);
* Doel en rechtsgrond van de verwerking;
* Periode van opslag of criteria daarvoor;
* Het recht op inzage;
* Recht op correctie en verwijdering of beperking verwerking. PerfectView houdt bij wie een record als laatste heeft aangepast en op welk moment (nog te controleren);
* Recht op dataportabiliteit (zie moeilijke woordenlijst);
* Recht om toestemming in te trekken;
* Klachtrecht bij AP;
* Verstrekking gegevens aan derden;
* Verwerking voor een ander doel of voornemens voor profilering
(betrokkene mag bezwaar maken).

Dit soort informatie kan als aanhangsel bij de beschrijving van de dienstverlening worden meegestuurd.

Als je de persoonsgegevens van iemand anders of een ander bedrijf ontvangt (dus niet van de betrokkene zelf), dan ben je verplicht om:

* Uiterlijk binnen een maand de betrokkene te informeren over de hierboven genoemde rechten;
* De bron te melden waar je de gegevens vandaan hebt.

**Voorbeeld**
Stel iemand van ons ontvangt een e-mail van een bedrijf. De e-mail is bestemd voor alle scholen in de omgeving en ook organisaties die educatief bezig zijn. Met die mail worden de contactpersonen gewaarschuwd voor een virus dat op verschillende scholen in de regio actief is. Ook bevat de e-mail (hoe aardig) een aanbieding – met korting – voor hun hulp tegen dat virus.
De e-mailadressen van alle geadresseerden staan in het Aan-veld van de e-mail.

Er zijn nu verschillende mogelijkheden:

1. Als de ontvanger van de e-mail aan de afzender **nooit toestemming heeft gegeven**, dan heeft de ontvanger het recht om:
	* te weten wie verantwoordelijk is voor de verwerking binnen dat bedrijf;
	* te weten waarom de gegevens worden opgeslagen (doel en grondslag van verwerking);
	* te weten wat de bewaartermijn van die gegevens is;
	* te weten welke persoonsgegevens het bedrijf van de ontvanger opslaat (recht van inzage);
	* te weten hoe zijn/haar e-mailadres bij dat bedrijf is terecht gekomen;
	* te eisen dat de eigen gegevens worden verwijderd (toestemming in te trekken).

Vervolgens kan de ontvanger het bedrijf en/of de afzender aanklagen wegens:

* ongeoorloofd gebruik van zijn/haar persoonsgegevens.
* het niet binnen een maand geïnformeerd te zijn over de herkomst
* verstrekking van gegevens aan derden, datalek (het Aan-veld wordt gebruikt)
1. Als de ontvanger **wel is geabonneerd op de digitale nieuwsbrief** maar niet op de aanbiedingen van dat bedrijf, dan kan de ontvanger van de e-mail het bedrijf en/of de afzender aanklagen wegens:
	* “Verwerking voor een ander doel”, dus onjuiste “doelbinding”: immers melding maken van een virus kan heel goed via de nieuwsbrief, maar de aanbieding met korting past daar niet in.
	* Verstrekking van gegevens aan derden (het Aan-veld wordt gebruikt).
2. Ook als de ontvanger aan het bedrijf **wèl toestemming heeft gegeven** om aanbiedingen te doen, dan kan de ontvanger het bedrijf alsnog aanklagen wegens:
	* verstrekking van gegevens aan derden, datalek (het Aan-veld wordt gebruikt).
3. Afhankelijk van het soort afzenderadres dat werd gebruikt (bedrijf e-mailadres of persoonlijk e-mailadres) kun je overwegen of je het bedrijf gaat aanklagen of de persoon (immers het bedrijf kan stellen dat de e-mail ongevraagd door de persoon is verstuurd).

## Voldoen aan het Recht op Inzage

Mensen hebben recht op inzage in hun persoonsgegevens. Dat houdt in dat zij [uw Bedrijf] mogen vragen of deze persoonsgegevens van hen heeft vastgelegd en zo ja, welke. Zij hoeven geen reden te geven voor een inzageverzoek.

Vraagt iemand om inzage, dan moet [uw Bedrijf] diegene op een duidelijke en begrijpelijke manier binnen vier weken schriftelijk laten weten:

* of de organisatie  zijn persoonsgegevens gebruikt, en zo ja:
* om welke gegevens het gaat;
* wat het doel is van het gebruik;
* aan wie de organisatie de gegevens eventueel heeft verstrekt;
* wat de herkomst is van de gegevens, als deze bekend is.

**Reikwijdte inzagerecht**

Het recht op inzage betreft alleen inzage in iemands eigen gegevens. Mensen hebben dus geen recht op informatie over anderen.

Gebruikt een organisatie persoonlijke werkaantekeningen als geheugensteuntje? Dan vallen deze aantekeningen niet onder het inzagerecht. Maar slaat de organisatie de aantekeningen vervolgens op in een dossier of verstrekt de organisatie deze aan anderen? Dan heeft degene over wie het gaat ook recht op inzage in deze aantekeningen.

**Hoe kunnen betrokkenen inzage krijgen**

In de privacyverklaring – die op de website staat (of komt te staan) – worden de betrokkenen geïnformeerd op welke wijze men bij [uw Bedrijf] de eigen persoonsgegevens kan opvragen, laten corrigeren of verwijderen. Zij kunnen daarvoor contact opnemen met de “klantenservice” van [Uw Bedrijf] via de volgende gegevens:

|  |  |
| --- | --- |
| Telefonisch | 012-345 6789Maandag tot en met vrijdag van 10:00 tot 16:00 uur |
| E-mail | Via e-mailadres avg@[uw Bedrijf].nl  |
|  Post | Stichting huppeldepup, afd. AVG-teamavgstraat 27, 1111 AA nergenshuizen |

Om misbruik te voorkomen dient altijd gevraagd te worden om ons een schriftelijk verzoek tot inzage te sturen waarbij de betrokkene zich adequaat dient te identificeren door een kopie van een geldig legitimatiebewijs mee te sturen. Aan de balie worden geen privacygegevens afgegeven.

## Voldoen aan het Recht op Correctie

Mensen hebben het recht om correctie van hun persoonsgegevens te vragen. Dat houdt in dat zij een organisatie mogen vragen hun persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen.

* Iemand kan om correctie vragen als zijn persoonsgegevens:
* feitelijk onjuist zijn;
* onvolledig zijn of niet ter zake doen voor het doel waarvoor ze zijn verzameld;
* op een andere manier in strijd met een wet worden gebruikt.

**Reikwijdte correctierecht**

Het correctierecht is niet bedoeld voor het corrigeren van professionele indrukken, meningen en conclusies waarmee iemand het niet eens is, voor zover deze ter zake doen. Wel mag diegene van de organisatie verwachten dat deze in ieder geval zijn schriftelijke mening toevoegt aan het dossier. Dat kan vooral een oplossing bieden bij situaties waarbij het om niet objectief vast te stellen feiten gaat.

## Voldoen aan het Recht op Vergetelheid

In de AVG is het zogeheten [recht op vergetelheid](https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/rechten-van-betrokkenen#wat-houdt-het-recht-op-vergetelheid-uit-de-avg-in-5976) opgenomen. Dit recht houdt in dat [uw Bedrijf] in een aantal gevallen iemands persoonsgegevens moet wissen als diegene daarom vraagt.

Het recht op vergetelheid lijkt op het huidige recht op correctie en verwijdering, maar is breder. Het recht is niet meer, zoals nu, beperkt tot het verwijderen van objectief onjuiste gegevens, onvolledige gegevens of gegevens die niet ter zake doen.

# Beveiligingsmaatregelen

De beveiligingsmaatregelen betreffen IT maatregelen en organisatorische maatregelen.

## IT maatregelen

Vanwege de AVG wetgeving dient de IT beveiliging op orde te zijn. Daarom worden in de komende maanden een aantal wijzigingen doorgevoerd.

**@[uw Bedrijf].nl accounts**

Om te voorkomen dat onbevoegden binnen en buiten [uw Bedrijf] ongeoorloofd de gegevens van betrokkenen kunnen inzien of – erger nog – kunnen wijzigen, worden de volgende maatregelen getroffen:

* [uw Bedrijf] wachtwoorden dienen elk half jaar aangepast te worden.
* Wachtwoord regels zijn: minimaal 8 teken waarvan 1 hoofdletter, 1 kleine letter, 1 cijfer en 1 ander teken (bijvoorbeeld !#$%&;:. )
* Geen gemeenschappelijk gebruik van accounts.
Indien bestanden of e-mail gemeenschappelijk (door meerdere medewerkers) gebruik moet worden, dan is SharePoint of een Shared Mailbox de aangewezen oplossing en niet het gemeenschappelijk gebruik van een account.

Het bestaande balie account blijft intact om te e-mailen en de agenda te raadplegen.

**@gmail accounts**

Het balie Google account wordt nu nog voor zowel voor de Google agenda als ook voor het communicatieblog gebruikt. Dit persoonlijke account werd tijdens het afgelopen jaar regelmatig door Google geblokkeerd wegens gebruik door meerdere personen.

Als poging om te voorkomen dat het account in de toekomst opnieuw door Google wordt afgesloten, wordt het communicatieblog verhuisd naar de mijn [uw Bedrijf].nl website. Het gebruik van het account zal daardoor verminderen en naar verwachting minder vaak worden afgesloten.

**@mijn[uw Bedrijf].nl accounts**

Hier vinden geen wijzigingen plaats

**Relatiebeheersysteem (CRM)**

[uw Bedrijf] gaat over tot centrale opslag van persoonsgegevens. Dit gaan we doen met de xyz toepassing. In de AVG is bepaald dat de toegang tot die gegevens wordt vastgelegd (wie kijkt of bewerkt de gegevens en wanneer gebeurt dat). . In dit computerprogramma worden alle personen opgenomen die in groepen e-mail of post krijgen van [uw Bedrijf]. Lijstjes met persoonsgegevens die niet geregistreerd zijn in het verwerkingsregister mogen niet meer worden gebruikt. De wet staat dat simpelweg niet meer toe.

**Encryptie op de PC’s**

Waar nodig zal op PC’s encryptie worden aangezet waardoor de gegevens op de harde schijf versleuteld worden tegen onbevoegd gebruik.

## Gebruik van @[uw Bedrijf].NL e-mailaccounts

Als je gevraagd wordt om namens [uw Bedrijf] naar de buitenwereld te communiceren, dan dien je dat voortaan met een [uw Bedrijf] e-mailadres als afzender te doen en niet met een ander bedrijfse-mailadres of je privé e-mailadres. Overleg vooraf met de staf of de e-mailadressen die je wilt gebruiken (zeker als daar persoonlijke e-mailadressen tussen zitten) inderdaad gebruikt mogen worden. Op deze wijze weten andere bedrijven of personen (dus de ontvangers van de e-mail) dat [uw Bedrijf] inderdaad achter de intentie van het bericht staat en voorkomen we als [uw Bedrijf] de privacy discussie van de nieuwe AVG wetgeving.

Bedenk dat bij ongeoorloofd gebruik door werknemers en vrijwilligers van e-mailadressen [uw Bedrijf] strafbaar is. Ook als dit gebeurd door onzorgvuldigheid of onwetendheid. [uw Bedrijf] is door de AVG verder verplicht uit te zoeken waar en bij welke medewerker de fout is ontstaan en maatregelen te nemen om foutief handelen in de toekomst te ter voorkomen.

Als je niet wordt gevraagd om namens [uw Bedrijf] op te treden naar de buitenwereld, dan gebruik je natuurlijk je privé e-mailadres en niet een [uw Bedrijf] mailadres als afzender. De [uw Bedrijf] staf zal zich uiteraard distantiëren van privé e-mails ongeacht of hier privacy klachten over komen of niet.

Ook bij e-mailberichten tussen vrijwilligers kan het zijn dat een collega-vrijwilliger heeft aangegeven geen e-mailberichten te willen ontvangen. Respecteer dus iemands privacy!

Gebruik beslist het BCC veld als je voortaan een mailing rondstuurt naar meerdere personen buiten [uw Bedrijf]. Het niet gebruiken van het BCC veld (waarbij de mailadressen dus voor anderen zichtbaar worden) kan reeds als datalek worden opgevat.
Bij een mailing naar [uw Bedrijf] medewerkers (naar hun privé e-mailadressen) mag het Aan veld alleen worden gebruikt indien iedereen toestemming heeft gegeven. Indien slechts @[uw Bedrijf].nl e-mail-adressen worden gebruikt, mag zonder toestemming het Aan-veld gebruikt worden.

## Aanmeldformulieren aanpassen

Alle aanmeld formulieren op onze websites moeten worden aangepast volgens “Privacy by Default”. Ook moeten we kunnen aantonen dat mensen zelf toestemming hebben gegeven voor het opnemen van hun gegevens in onze bestanden.

## Organisatorische maatregelen

De organisatorisch maatregelen zijn in verschillende categorieën in te delen:

* + Check verwerkersovereenkomsten;
	+ Terugkerende AVG voorlichting aan de medewerkers ;
	+ Blijvende aandacht voor AVG met name zaken die door de AP nog worden aangepast;
	+ Schep duidelijkheid naar je klanten en laat weten of de communicatie namens [uw Bedrijf] dan wel privé plaatsvindt. Voor projecten als bijvoorbeeld Museum Komt Naar U Toe of het Kruikgenootschap is het goed dit proces te bekijken.

## Gebruik [uw Bedrijf] briefpapier

Als je gevraagd wordt om namens [uw Bedrijf] naar de buitenwereld te communiceren, dan dien je voortaan de [uw Bedrijf] briefpapier te gebruiken en geen ander bedrijfs-briefpapier of blanco briefpapier. Op deze wijze weten andere bedrijven of personen (dus de ontvangers van je brief) dat [uw Bedrijf] inderdaad achter de intentie van het bericht staat en voorkomen we als [uw Bedrijf] de privacy discussie van de nieuwe AVG wetgeving.

Als je niet wordt gevraagd om namens [uw Bedrijf] op te treden naar de buitenwereld, dan gebruik je natuurlijk niet het [uw Bedrijf] briefpapier.

# Frequently Asked Questions

#### [Mag ik post versturen en bellen zonder toestemming van de ontvanger?](https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/algemene-informatie-avg#mag-ik-onder-de-avg-aan-direct-marketing-doen-zonder-toestemming-van-de-ontvanger-5997)

* **Ja**, net als nu mag je straks onder de wet AVG een persoon of organisatie bellen (bel-me-niet register ?) of post sturen met een aanbod zonder dat je daarvoor toestemming hebt.
Maar….

Zodra je een aanbod verstuurt via een digitaal kanaal, zoals e-mail, fax of sms, **heb je wel voorafgaande toestemming** nodig.
Onder de nieuwe regels houden mensen het recht om bezwaar te maken tegen klassieke direct marketing. En het recht om hun toestemming in te trekken als het gaat om digitale kanalen. Wij moeten mensen in beide gevallen duidelijk informeren. Dit geldt zowel voor commerciële, ideële als charitatieve direct marketing.
<https://www.privacy-web.nl/vragen/mag-ik-onder-de-avg-aan-direct-marketing-doen-zonder-toestemming-van-de-ontvanger>

[**Moet ik onder de AVG nog steeds registreren (loggen) wie toegang heeft gehad tot gegevens?**](https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/algemene-informatie-avg#moet-ik-onder-de-avg-nog-steeds-registreren-loggen-wie-toegang-heeft-gehad-tot-gegevens-6071)

* Ja. We zijn nog steeds verplicht om vast te leggen [wie toegang heeft gehad](https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/beveiliging-van-persoonsgegevens#moet-ik-registreren-loggen-wie-toegang-heeft-gehad-tot-gegevens-6065) tot de persoonsgegevens die we verwerken.
<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/algemene-informatie-avg#moet-ik-onder-de-avg-nog-steeds-registreren-loggen-wie-toegang-heeft-gehad-tot-gegevens-6071>

#### [Moet ik betrokkenen laten weten wie toegang heeft gehad tot hun gegevens?](https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/algemene-informatie-avg#moet-ik-onder-de-avg-betrokkenen-nog-steeds-laten-weten-wie-toegang-heeft-gehad-tot-hun-gegevens-6073)

* **Ja**. Een betrokkene heeft nu en straks het recht om te vragen wie binnen [uw Bedrijf] toegang heeft gehad tot zijn gegevens.
<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/algemene-informatie-avg#moet-ik-onder-de-avg-betrokkenen-nog-steeds-laten-weten-wie-toegang-heeft-gehad-tot-hun-gegevens-6073>

#### Is ons restaurant volgens de AVG een verwerker?

* Indien persoonsgegevens (zoals bijvoorbeeld de naam van de betrokkene plus de dieetwensen) worden gedeeld met het restaurant, dan is volgens de AVG het restaurant een ‘verwerker’. [uw Bedrijf] dient dan vooraf aan de klant te vragen of de gegevens wel/niet met het restaurant gedeeld mogen worden. Een beter alternatief is om in een dergelijke situatie slechts de dieetwensen (zonder de namen van de betrokkenen) door te geven.

#### Hoe lang mag ik persoonsgegevens bewaren?

* Het uitgangspunt blijft dat je persoonsgegevens niet langer mag bewaren dan noodzakelijk voor het doel van je verwerking.
* Je bepaalt van tevoren hoe lang je de persoonsgegevens gaat bewaren per dienst of product en legt dat vast bij de beschrijvingen van de diensten/producten die door [uw Bedrijf] worden geleverd.
* Je neemt de bewaartermijnen ook op in het verwerkingsregister en in de verkoopvoorwaarden.
* Je informeert de betrokkene over de bewaartermijn als ze de dienst/product willen afnemen.
Bijvoorbeeld via een privacyverklaring op de website of door middel van de verkoopvoorwaarden die met een offerte of (aankoop)bevestiging wordt meegestuurd.

#### Hoe beschrijf ik een dienst of product?

* Maak per dienst of product een procesbeschrijving met de opsomming van alle activiteiten of stappen die er moeten gebeuren om de dienst of product uiteindelijk te kunnen leveren. Dus vanaf eerste aanmelding of vraag, opstellen, versturen, bevestigen offerte/bevestiging, etc. tot en met de levering inclusief de facturatie en ook (nog beter) een evaluatie achteraf;
* Maak per stap een korte beschrijving (één alinea is voldoende) wat er in die stap plaats vindt en waarom die nodig is;
* Als je transparant wilt zijn, dan beschrijf je ook wanneer en op welke gronden een korting kan worden gegeven. De prijzen veranderen hooguit per jaar, maar kortingen kun je altijd geven. Op deze manier is het niet erg als klanten onderling facturen vergelijken. Goede klanten kun je immers belonen door meer korting te geven.
* De AVG bewaartermijn laat je aflopen nadat de laatste stap in het proces is voltooid. Hoe later die laatste stap ligt, des te langer kun je de persoonsgegevens bewaren.
* Het facturatieproces heeft een eigen verwerking en ook een bewaartermijn die los staat van het leveren van de dienst of product. De bewaartermijn die daar wordt genoemd is als regel gekoppeld aan de belastingwetgeving.

**Mag ik mijn bestaande klanten berichten sturen per e-mail, sms of app?**

* **Ja, dat mag. We mogen onze eigen, bestaande klanten aanbiedingen voor andere, vergelijkbare producten of diensten sturen per e-mail, sms of app. Onze klanten hoeven daarvoor niet eerst toestemming te geven. Maar we moet wél een makkelijke, gratis afmeldmogelijkheid bieden bij elk bericht dat we versturen!** <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/algemene-informatie-avg#mag-ik-onder-de-avg-mijn-bestaande-klanten-direct-marketing-sturen-per-e-mail-sms-of-app-6372>
* **Bestaande klant**
Iemand is een bestaande klant als deze persoon een product of dienst van ons heeft gekocht. Er moet sprake zijn van een koopovereenkomst, waarin wij verplicht zijn of waren om iets te leveren en de klant om daarvoor te betalen.
* **Geen bestaande klant**
Let op: We mogen iemand niet tot onze bestaande klanten rekenen als diegene (nog) niets heeft gekocht, maar zich alleen maar heeft aangemeld voor de nieuwsbrief, een enquête heeft ingevuld, meegedaan heeft aan een prijsvraag of spel of een gebruikersaccount heeft aangemaakt.
* **Potentiële klanten mailen**
Is iemand nog geen bestaande klant van ons? En wil je deze persoon mailen, sms-en of appen met aanbiedingen? Dan moet je diegene vóóraf eerst om toestemming vragen, bijvoorbeeld per post, via formulier op website, of tijdens een mondeling gesprek ondersteund door een formulier op papier (met handtekening).

[**Waar moet toestemming voor direct marketing per e-mail of sms aan voldoen?**](https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/algemene-informatie-avg#waar-moet-toestemming-voor-direct-marketing-per-e-mail-sms-of-app-aan-voldoen-onder-de-avg-6374)

* **Volgens de AVG moet toestemming ‘vrij’, ‘specifiek’, ‘geïnformeerd’ en ‘ondubbelzinnig’ zijn.**
* **Vrij**
Iemand moet vrij zijn om toestemming te geven, maar ook om deze te weigeren of in te trekken. Weigert iemand toestemming te geven? Dan mag dat er bijvoorbeeld niet voor zorgen dat je deze persoon een dienst weigert.
* **Specifiek**
Dit betekent dat er geen twijfel over mag bestaan voor welk specifiek gebruik van de gegevens iemand toestemming heeft gegeven. Het moet bijvoorbeeld duidelijk zijn welke gegevens je voor direct marketing wilt gebruiken.
* **Geïnformeerd**
We moeten mensen, vóórdat zij toestemming geven, duidelijk informeren over de verwerking van hun persoonsgegevens. Dit moeten we in begrijpelijke taal doen, zodat mensen ook echt weten waarvoor zij toestemming geven. We moeten dus heel open en transparant veel informatie geven op een overzichtelijke manier.
Let op: vraag je toestemming tegelijk met het verzoek om een overeenkomst te accepteren? Dan mogen we de toestemming niet ‘verstoppen’ als onderdeel van het contract. We moeten het deel dat over direct marketing gaat duidelijk en apart vermelden.
* **Ondubbelzinnig**
Er moet sprake zijn van een duidelijke actieve handeling. Bijvoorbeeld een (digitale) schriftelijke of een mondelinge verklaring. Het moet in elk geval volstrekt helder zijn dát er toestemming is verleend.
We mogen niet uitgaan van het principe ‘wie zwijgt, stemt toe’. Het gebruik van vooraf aangevinkte vakjes is dus niet toegestaan (privacy by default).
* **Verstrekken aan derde partijen**
Wil je de persoonsgegevens aan derde partijen verstrekken ? Dan moeten we mensen goed informeren over welke categorieën derde partijen dat zijn.
Ook moeten we apart toestemming vragen voor deze verstrekking aan genoemde soorten derde partijen. Dit geldt ook als we reclame van derde partijen aan onze klanten willen sturen.
* **Toestemming intrekken**
Mensen die toestemming hebben gegeven, moeten die kunnen intrekken via elk e-mail, sms of app die je verstuurt.
We moeten ervoor zorgen dat toestemming intrekken gratis is en net zo makkelijk gaat als toestemming geven. Het is dus verboden om mensen alleen de mogelijkheid te bieden hun toestemming per post of telefoon in te trekken.
* **Toestemming bewijzen**
We moeten kunnen [**aantonen dat we daadwerkelijk toestemming hebben gekregen**](https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/verantwoordingsplicht). Dit is onderdeel van de [**verantwoordingsplicht**](https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/verantwoordingsplicht) die je onder de AVG hebt.
Let op: om geldige toestemming aan te tonen, is het essentieel dat je kunt laten zien op basis van welke informatie iemand toestemming heeft gegeven. Het is dus niet genoeg om alleen de toestemming zelf vast te leggen.

[**Hoe lang mag ik klantgegevens bewaren onder de AVG?**](https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/algemene-informatie-avg#hoe-lang-mag-ik-klantgegevens-bewaren-onder-de-avg-6375)

* **In de AVG staan geen concrete bewaartermijnen genoemd. Het uitgangspunt is dat we persoonsgegevens niet langer mogen bewaren dan noodzakelijk is voor het doel van onze verwerking. Hoe lang je gegevens mag bewaren, verschilt dus per geval.**
* **Bewaartermijnen in andere wetten**
Is er wetgeving van toepassing die bepaalde bewaartermijnen voorschrijft? Dan moeten we deze termijnen hanteren. Bijvoorbeeld: de belastingwetgeving zegt dat je bepaalde gegevens 7 jaar moet bewaren.
* **Doel klantgegevens**
Denk na over waar we de gegevens van onze klanten precies voor nodig hebben. Ten eerste natuurlijk om aankopen van onze klanten te kunnen afronden. Maar misschien willen we ook wel contactgegevens van onze klanten gebruiken voor direct marketing.
Ga vervolgens bij elk van deze doelen na wanneer we dat doel hebben bereikt. Op het moment dat dit het geval is, hebben we de persoonsgegevens waarschijnlijk niet langer nodig.

Zo kun we voor elk doel waarvoor we klantgegevens bewaren, een bewaartermijn bepalen. We mogen de termijnen dus zelf vaststellen. Maar we moeten wel kunnen beargumenteren hoe lang we de klantgegevens bewaren.

* **Informeren**
We moeten de bewaartermijnen opnemen in onze privacyverklaring. Zodat onze klanten weten hoe lang we hun gegevens bewaren.
* **Na afloop bewaartermijn**
Is de bewaartermijn verlopen? Dan moeten we de klantgegevens vernietigen of anonimiseren. Of eerder, zodra een klant bezwaar maakt tegen direct marketing of zijn toestemming hiervoor intrekt.

**Geldt de AVG wetgeving ook voor overleden personen?**

* Dit is niet duidelijk in de wet opgenomen.
In het basis ontwerp EU-AVG uit mei 2016 is opgenomen: “De onderhavige verordening is niet van toepassing op de persoonsgegevens van overleden personen. De lidstaten kunnen regels vaststellen betreffende de verwerking van de persoonsgegevens van overleden personen.”
In het “Advies wetsvoorstel Uitvoeringswet Algemene verordening gegevens-bescherming” dd. april 2017 adviseert de AP in hoofdstuk 12c het volgende:

De AP acht het zinvol om de regels inzake bepaalde rechten van betrokkene (het recht van inzage en op rectificatie of gegevenswissing, het recht op overdraagbaarheid van gegevens en het recht van bezwaar) van overeenkomstige toepassing te verklaren op overleden personen dan wel te bepalen dat die rechten gedurende een bepaalde periode [[2]](#footnote-2)) na overlijden door de nabestaanden kunnen worden ingeroepen, in verband met onder meer het gebruik van dergelijke gegevens op social media.

De AP uitleg is: Met deze wetgeving is bijvoorbeeld mogelijk om personen/journalisten aan te klagen die foto’s maken van net overleden (verkeers)slachtoffers waarbij de nabestaanden nog geen weet hebben van het gebeurde.

Heb je nog onbeantwoorde vragen lees dan vooral [hier](https://ddma.nl/actueel/17-meest-gestelde-vragen-gdpr/) verder.

1. ) In de papieren versie van dit document kun je de links niet volgen. Gebruik daarvoor de .pdf. [↑](#footnote-ref-1)
2. De vervaltermijn die de AP voorstelt is overeenkomstig het erfrecht (5 jaar). [↑](#footnote-ref-2)