# Algemene Verordening Gegevensbescherming

Per 25 mei 2018 geldt de Algemene Verordening Gegevensbescherming (AVG), deze wetgeving wordt van kracht in de hele EU.

GDPR staat voor General Data Protection Regulation. In het Nederlands is dat AVG, Algemene Verordening Gegevensbescherming. Het is een nieuwe Europese wet die de verouderde Data Protection Directive van 1995 vervangt. De wet werd in 2016 goedgekeurd, maar pas vanaf 25 mei 2018 zal deze gecontroleerd worden. De nieuwe wet handelt over hoe bedrijven persoonsgegevens mogen verkrijgen, gebruiken, opslaan en verwijderen. De wet is toepasbaar op bedrijven uit alle sectoren die persoonsgegevens behandelen van EU-burgers.

Persoonsgegevens zijn data die direct of indirect te herleiden zijn tot een persoon. Voorbeelden hiervan zijn namen, e-mailadressen, posts op social media, IP-adressen. Voor gevoelige data gelden nog striktere regels. Gevoelige data kunnen gaan over ras, genetische info en dergelijke, maar ook een BSN-nummer hoort hierbij. De meeste bedrijven behandelen alleen persoonsgegevens en kunnen daarom de gevoelige data buiten beschouwing houden.

**Wat verandert er voor u?**

Elke organisatie legt adressenbestanden aan van klanten en (toe-)leveranciers. Welke informatie u precies vastlegt, hangt af van het gebruik: voor het verzenden van e-letters aan prospects volstaat het e-mailadres. Onder het credo ‘ken je klant’ heeft u van goede relaties wellicht meer informatie opgeslagen; volledige adressen, mobiele nummers en misschien zelfs privézaken zoals verjaardagen.

De regels rond het verzamelen en gebruiken van persoonsgegevens worden vanaf 25 mei 2018 strenger. Op die datum treedt namelijk de AVG in werking. Dit heeft betrekking op alle persoonsgegevens die u vastlegt. Zelfs als dit enkel het e-mailadres is van iemand die zichzelf ooit heeft aangemeld voor bijvoorbeeld uw nieuwsbrief.

De boetes die kunnen worden opgelegd als u de nieuwe regels niet naleeft, kunnen oplopen tot 20 miljoen euro of 4 procent van uw jaaromzet. Het is daarom belangrijk u ervan bewust te zijn wat de AVG inhoudt. In dit document zetten wij de belangrijkste regels op een rijtje.

**Begrippenlijst**

| Basisbegrip | Definitie | Voorbeeld |
|---|---|---|
| Persoonsgegevens | Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon | E-mailadressen, NAW-gegevens, persoonlijke gegevens etc. |
| Verantwoordelijke | Een natuurlijke of rechtspersoon die het doel en de middelen voor verwerking van persoonsgegevens vaststelt | U, uw organisatie, Van Erkelens Accountants \| Belastingadviseurs B.V. |

| | | |
|---|---|---|
| Verwerker | Natuurlijke of rechtspersoon die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt | U, uw organisatie;<br>Van Erkelens Accountants \| Belastingadviseurs B.V. |
| Betrokkene | De natuurlijke persoon wiens persoonsgegevens worden verwerkt | Uw klant of relatie |
| Verwerken | Praktisch elke handeling met een persoonsgegeven | Verzamelen, vastleggen, structureren, opslaan, raadplegen, verstrekken, gebruiken etc. |
| Bijzondere persoonsgegevens | Bijzondere kenmerken van personen | Bijv. gezondheidsgegevens, godsdienst of levensovertuiging, ras, politieke voorkeur, seksuele leven, lidmaatschap vakbond, strafrechtelijk verleden, BSN nummer |

## De belangrijkste regels voor verwerking van persoonsgegevens

***Openheid van zaken aan uw klanten en relaties***

Persoonsgegevens mogen alleen verwerkt worden voor een vooraf bepaald en omschreven doel en alleen als de betrokkene daartoe nadrukkelijk toestemming geeft. U mag de persoonsgegevens bovendien alleen verwerken als en zolang als:

- Dit noodzakelijk is om een overeenkomst met de betrokkene uit te voeren (zoals het toesturen van informatie, een offerte of bestelling)
- Dit noodzakelijk is voor de behartiging van een gerechtvaardigd belang van u of een derde (het verkopen van een product of dienst)
- Dit noodzakelijk is om te voldoen aan een wettelijke verplichting

De betrokkene moet vooraf geïnformeerd worden over wat u met zijn gegevens doet. Ook dient u, als de betrokkene daarom vraagt, een kopie van zijn/haar gegevens te verstrekken, onjuiste gegevens te wijzigen en gegevens (deels of helemaal) te verwijderen.

- **Wat moet u doen?**
  *Per 25 mei 2018 dient u van alle betrokkenen toestemming te hebben voor het verwerken van hun persoonsgegevens. Dit kan consequenties hebben voor onder meer de e-mailformulieren op uw website verwerken, klantgegevens en personeelsgegevens die u bewaart. Het moet duidelijk zijn waarvoor de gegevens worden gebruikt. Ook mogen niet méér gegevens gevraagd worden dan nodig is voor het vooraf omschreven doel.*

***Inrichten van een privacy-administratie***

De betrokkene heeft het recht om te weten welke gegevens er verwerkt worden, met welk doel, wie er toegang hebben tot zijn/haar gegevens, hoe u aan die gegevens komt en hoe lang deze worden bewaard.

- **Wat moet u doen?**
  *Per 25 mei 2018 dient u te beschikken over een privacy-administratie waarin dit voor elke betrokkene is vastgelegd.*

***Advies: stel een verwerkingsregister op***

Het is voor uw onderneming goed om allereerst in beeld te krijgen welke diensten u verricht en vooral welke persoonsgegevens u daarbij verwerkt. Daarbij is het van belang om de daarbij gebruikte applicaties en eventuele verwerkers in beeld te brengen. Ook het helder krijgen wie toegang heeft tot verwerkte persoonsgegevens is belangrijk. Wanneer u deze informatie verwerkt in een overzichtelijk register (bijvoorbeeld een Excel-bestand) dan is dat niet alleen handig en praktisch voor het overzicht voor uzelf. Voor organisaties met minder dan 250 werknemers is dit niet verplicht, maar wel raadzaam. Ook voor uw kleinere (MKB-)organisaties is het vrij waarschijnlijk dat de verwerking een risico inhoudt voor de rechten van betrokkenen, de verwerking niet incidenteel is of de verwerking (bijzondere) persoonsgegevens betreft. Het is dus altijd zinvol om een dergelijk register bij te houden, ook als dat niet verplicht is. Vermeld in het register ook uw diensten, contactgegevens, de verwerkingsdoeleinden en eventueel de grondslag(en), bewaartermijnen en indien mogelijk de getroffen beveiligingsmaatregelen. Op onze website is een voorbeeld van een verwerkingsregister te downloaden.

***Waarborgen dataveiligheid***

U dient persoonsgegevens afdoende te beveiligen, zowel technisch als organisatorisch. Voor passende veiligheidsmaatregelen kunt u kijken naar algemeen aanvaarde beveiligingsstandaarden, voorbeelden hiervan zijn de normen gesteld in ISO 27001 en ISO 27002. Denk aan het versleuteld verzenden van persoonsgegevens, encrypten van uw pc's en beveiligen van uw telefoons e.d. Mocht er sprake zijn van een mogelijk 'datalek', waarbij de kans bestaat dat er persoonsgegevens in handen van onbevoegden terechtgekomen zijn, dan bent u in sommige gevallen verplicht dit te melden aan de Autoriteit Persoonsgegevens (en soms aan de betrokkenen zelf).

- **Wat moet u doen?**
  *Per 25 mei 2018 moet u schriftelijk kunnen aantonen dat u de juiste (technische en organisatorische) veiligheidsmaatregelen genomen heeft. Ook moet er schriftelijk worden vastgelegd hoe uw organisatie omgaat met beveiligingsincidenten. Elke werknemer moet weten wat hij/zij moet doen in geval van een incident of datalek.*

***Kennisoverdracht personeel***

- **Wat moet u doen?**
  *Per 25 mei 2018 moet iedereen binnen uw organisatie die zich bezighoudt met de verwerking van persoonsgegevens op hoofdlijnen bekend zijn met de nieuwe regels, verantwoordelijkheden en het beleid voor de wettelijke 'meldplicht datalekken'.*

***Tekenen verwerkersovereenkomst***

Voorafgaand aan de uitwisseling van persoonsgegevens moet er een overeenkomst getekend worden door beide partijen.

- ***Als verwerker heeft Van Erkelens Accountants | Belastingadviseurs een rechtsgeldige verwerkersovereenkomst opgesteld die voldoet aan de wettelijke vereisten van de AVG. Binnenkort ontvangt u deze per mail van ons.***

## Meer in detail

**Het spamverbod**

De Telecommunicatiewet uit 1998 omvat onder meer een spamverbod. Hierin wordt het verboden overlast te veroorzaken met ongevraagde e-mails. Ook via sms, apps en social media kan spam worden verzonden.

Er is geen sprake van spam als:

- De ontvanger vooraf toestemming heeft gegeven
- De ontvanger kan zien wie de afzender is
- De ontvanger zich kan afmelden (opt-out)

De regels betreffende spam gelden binnen de Europese Economische Ruimte en hebben betrekking op de gehele Europese Unie, alsmede IJsland, Noorwegen en Liechtenstein.

**Opnieuw toestemming vragen of niet**

Als iemand een product of dienst heeft gekocht is hij/zij klant. De regel voor klanten is dat zij voor reclamedoeleinden digitale informatie toegestuurd mogen krijgen. Wel moet deze voorzien zijn van een opt-out.

**Prospects mag dat wel of niet**

Voor prospects geldt dat zij niet zonder meer benaderd mogen worden met behulp van Electronic Direct Mail (EDM). Alleen wanneer zij zelf een opt-in hebben uitgevoerd, of er in een eerste gesprek toestemming is gevraagd (schriftelijke vragenlijst, door sales/binnendienst), mag het prospect benaderd worden.

Een manier voor het verkrijgen van e-mailadressen is de registratie van het downloaden van Whitepapers. In de nieuwe wetgeving is dit e-mailcontact geen vrijwaring voor het toevoegen van dit adres aan een e-mailbestand voor het verstrekken van informatie, er wordt namelijk niet expliciet toestemming gegeven. Dit betekent dat het doel duidelijk moet zijn en dat deze adressen alleen dan gebruikt mogen worden als zij via een opt-in worden verkregen (het liefst via double opt-in).

Ontvangers van EDM moeten dus vooraf toestemming hebben gegeven en het bewijs hiervan moet na afloop tenminste vijf jaar bewaard worden.

**Splitsing adresgegevens**

Adresgegevens zijn er in verschillende niveaus. De gegevens van personen vallen onder de nieuwe wet. Hiermee ook de gegevens van eenmanszaken, vennootschappen onder firma (V.O.F.'s), maatschappen, medewerkers, leden van verenigingen of kerkgenootschappen, bestuurders van rechtspersonen etc. Dit zijn adressen die altijd persoonsgebonden zijn.

Voor adresgegevens van B.V.'s of N.V.'s en Stichtingen geldt de wet niet. Voor deze categorieën gelden andere regels.

Uiteraard moet bovenstaande ook voor de prospects in kaart worden gebracht.

**NAWTE-gegevens**

De gegevens die te vinden zijn in CRM-systemen of databases zijn zogeheten NAWTE-gegevens, dit staat voor

- Naam
- Adres
- Woonplaats
- Telefoon
- E-mailadres

Dit zijn tevens de gegevens waarvoor regels zijn opgesteld. Zo zal er een bewaartermijn geformuleerd moeten zijn en zaken als hoe op te slaan en wie autorisatie heeft ze in te zien. De betrokkenen mogen deze gegevens opvragen. Ook geldt het recht dat personen in uw bestanden 'vergeten' mogen worden. U moet dan kunnen aantonen wat u hebt gedaan om deze data te verwijderen.

**Gebruik in E-marketing**

De NAWTE-gegevens worden naast de normale bedrijfsvoering, ook gebruikt voor sales- en marketingdoeleinden.

Voor e-marketing zijn nodig

- Persoonsgegevens
  *Naam en e-mailadres*
- Overeenkomst
- Aanmelding voor nieuwsbrief ofwel opt-in waarin de ontvanger toestemming geeft mails te willen ontvangen (formulier op de website)
- Duidelijkheid over vorm van informatie
  *Informatieverstrekking in de vorm van nieuwsbrieven, marketingboodschappen of aanbiedingen – afhankelijk van de soort opt-in*
- Verwerking
  *Verantwoordelijk voor de verwerking van adressen – het aanleveren voor gebruik voor campagnes op dit niveau is de afdeling communicatie, marketing of het secretariaat*
- Bewaartermijn
  *Nadat een ontvanger zich heeft uitgeschreven, mogen de gegevens nog maximaal 3 maanden bewaard worden.*

**Klant en leverancier**

De regels voor contracten zijn:
Zolang het contract loopt kunnen de gegevens worden bewaard. Na afloop van het contract nog eens zeven jaar. De gegeven mogen dan uitsluitend hiertoe worden gebruikt en niet zomaar voor andere doeleinden.

**Kruisen van doelen**

Persoonsgegevens die voor het 'ene doel' verkregen zijn, mogen niet gebruikt worden voor een ander doel.

Een voorbeeld:
Iemand schrijft zich in voor een algemene nieuwsbrief, dan mag dit adres niet gebruikt worden voor (digitale) direct marketing. De ontvanger zal voor een andere dienst namelijk opnieuw toestemming voor moeten geven.

**Opvolging door sales**

In het CRM-systeem zal aangegeven moeten worden voor welk doel de gegevens verkregen zijn. Dit betekent ook dat in gesprekken met klanten en prospects, bijvoorbeeld door de binnendienst of de accountmanager steeds een checklist gebruikt moet worden waarin expliciet gevraagd wordt om toestemming van het gebruik van de gegevens.

**Website Privacy policy**

De privacy policy van een organisatie moet voor iedereen vindbaar zijn. Deze zal te vinden zijn in de footer van de website van de organisatie. Het gaat echter verder dan dat. In alle overeenkomsten (documenten waarin persoonsgegevens gevraagd worden) moet een verwijzing staan naar de privacy policy.

Niet alleen documenten maar ook alle formulieren in een website moeten voorzien zijn van een link naar de privacy policy op de website. En ook EDM's zullen in de footer voorzien moeten zijn van een link naar de privacy policy.

**Hieronder treft een voorbeeld van een privacy policy aan:**
*{Organisatie} hecht veel waarde aan de bescherming van uw persoonsgegevens. In deze Privacy policy willen we heldere en transparante informatie geven over hoe wij omgaan met persoonsgegevens. Wij doen er alles aan om uw privacy te waarborgen en gaan daarom zorgvuldig om met persoonsgegevens. {Organisatie} houdt zich in alle gevallen aan de toepasselijke wet- en regelgeving, waaronder de Algemene Verordening Gegevensbescherming. Dit brengt met zich mee dat wij in ieder geval:*

- *Uw persoonsgegevens verwerken in overeenstemming met het doel waarvoor deze zijn verstrekt, deze doelen en type persoonsgegevens zijn beschreven in dit Privacy policy;*
- *Verwerking van uw persoonsgegevens beperkt is tot enkel die gegevens welke minimaal nodig zijn voor de doeleinden waarvoor ze worden verwerkt;*
- *Vragen om uw uitdrukkelijke toestemming als wij deze nodig hebben voor de verwerking van uw persoonsgegevens;*
- *Passende technische en organisatorische maatregelen hebben genomen zodat de beveiliging van uw persoonsgegevens gewaarborgd is;*
- *Geen persoonsgegevens doorgeven aan andere partijen, tenzij dit nodig is voor uitvoering van de doeleinden waarvoor ze zijn verstrekt;*
- *Op de hoogte zijn van uw rechten omtrent uw persoonsgegevens, u hierop willen wijzen en deze respecteren.*

*Als {Organisatie} zijn wij verantwoordelijk voor de verwerking van uw persoonsgegevens. Indien u na het doornemen van ons Privacy policy, of in algemenere zin, vragen heeft hierover of contact met ons wenst op te nemen kan dit via de contactgegevens onder aan dit document.*

**Websites**
Voor de meeste websites zijn de volgende zaken nodig:

- SSL-certificaat
  *Nodig om https:// te verkrijgen, naast veiligheid biedt dit ook een betere Google-ranking*
- Privacy statement
  *Hierin wordt verteld hoe het bedrijf omgaat met de privacy*
- Cookie melding nieuw
  *Waarbij nadrukkelijk vermeld wordt, welke data verzameld worden en met een verwijzing naar de privacyverklaring*
- Formulieren voorzien van opt-ins

Informeer tijdig bij uw websitebeheerder of uw website AVG-proof is.

## Welke maatregelen treft Van Erkelens

De volgende (categorieën) persoonsgegevens verwerkt Van Erkelens namens haar klanten:

| Categorie persoonsgegevens | Type verwerking | Duur van de verwerking | Aard en doel van de verwerking |
|---|---|---|---|
| Klantgegevens: naam, adres, woonplaats, telefoonnummers, e-mailadressen, geboortedata, BSN-nummers, kopie ID's en banknummers | Administratieve verwerkingen, fiscale aangiften, en door de wet verplichte gestelde publicaties | Doorlopende de duur van de opdracht | Financiële administratie, jaarrekeningen, fiscale aangiften, advisering, mediation, publicaties o.a. KvK en CBR, banken |
| Medewerkersgegevens: naam, adres, woonplaats, telefoonnummers, e-mailadressen, geboortedata, BSN-nummers, kopie ID's en banknummers | Salarisverwerking en arbeidsovereenkomsten en overige HRM documenten | Doorlopende de duur van het dienstverband. | Salarisadministratie, aangiften loonheffingen, pensioenopgaven en arbeidsrechtelijke zaken, (HRM-) advisering |
| Informatievoorzieningen | Nieuwsbrieven en overige algemene informatiecontacten, uitnodigingen, verjaardagskaarten | Gedurende de periode dat men is aangemeld | Geven van relevante informatie ten aanzien van de bedrijfsvoering |

**Functierollen/ functiegroepen en hun verwerkingen**

In de volgende tabel staan de functierollen en/of functiegroepen die toegang hebben tot bepaalde Persoonsgegevens en daarachter vermeld welke verwerkingen zij ten aanzien van de persoonsgegevens mogen uitvoeren.

| Functie(groep) | Categorie (persoonsgegevens) | Type verwerking |
|---|---|---|
| Alle medewerkers (behoudens huishoudelijke dienst) | NAW-gegevens, inclusief e-mailadressen, BSN-nummers, ID's en banknummers van klanten | Administratieve- en fiscale gegevensverwerking. |
| HRM-afdeling | Medewerkersgegevens van werknemers van opdrachtgevers | Salarisadministratie voor opdrachtgevers |

**Bewaartermijnen**

Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de uitvoering van onze werkzaamheden. Voor persoonsgegevens die worden verwerkt gelden de volgende bewaartermijnen:

- Administratieve- fiscale- en relatiegegevens 7 jaren (na de opdrachtperiode)
- Medewerkersgegevens van opdrachtgevers 7 jaren (na opdrachtperiode)
- E-mailadressen nieuwsberichten, na uitschrijven maximaal drie maanden

**Beveiligingsmaatregelen**

Van Erkelens treft verregaande technische maatregelen inzake de beveiliging van haar systemen, autorisaties en back-up procedures. Daarnaast worden de medewerkers getraind op het gebied van beveiliging en databescherming. Voorts is er een meldingsprocedure opgesteld in verband met mogelijke datalekken. Digitale communicatie met klanten waarbij persoonsgegevens worden verzonden zal beschermd worden door gebruik te maken van het huidige klantenportalen of een andere erkende verzendmogelijkheden waarbij de gegevens versleuteld worden verzonden.

Meer informatie kunt u vinden op www.autoriteitpersoonsgegevens.nl.

Een voorbeeld van het verwerkingsregister kunt u vinden op www.van-erkelens.nl.