OOB adviseurs en accountants

Ondernemerszaken!

# Algemene Verordening Gegevens-bescherming

## Is uw organisatie voorbereid op de nieuwe privacyregelgeving?

# *Inhoudsopgave*

# Inleiding

Per 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van kracht binnen de gehele Europese Unie. De AVG is een Unierechtelijke verordening die rechtstreeks toepasselijk is in de lidstaten van de Europese Unie, waardoor omzetting van de bepalingen naar nationaal recht niet nodig is. De AVG vervangt de Wet bescherming persoonsgegevens (Wbp).

De nieuwe regels houden enerzijds in een toename van de verplichtingen van organisaties die persoonsgegevens verwerken en anderzijds krijgen personen meer controle over hun persoonsgegevens.

Organisaties die persoonsgegevens verwerken moeten per 25 mei 2018 aan de nieuwe privacyregels uit de AVG voldoen. Met deze whitepaper informeren wij u over de betekenis van de nieuwe privacyregelgeving voor uw organisatie. Daarnaast geven wij u praktische tips om uw organisatie privacy-proof te maken.

# *Heeft u te maken met de AVG?*

De AVG definieert persoonsgegevens als alle informatie over een geïdentificeerde of identificeerbare natuurlijk persoon (de betrokkene). Het kan gaan om digitale gegevens, maar ook om gegevens op papier. Persoonsgegevens zijn onder andere: naam, adres, geboortedatum, titulatuur, geslacht, e-mailadres, telefoonnummer, zakelijk adres, huisadres, werkgever, functie, personeelsnummer, loopbaan, opleidingen, competenties, medische dossiers, publicaties, inhoud van e-mails, surfgedrag, veroordelingen, loginnamen, wachtwoorden, identificatienummers, IP-adressen, tracking cookies, RFID-nummers en MAC-adressen en foto's en video-opnamen van personen. Gegevens over bedrijven zijns soms ook persoonsgegevens, namelijk als het gaat over een eenmanszaak, vennootschap onder firma, commanditaire vennootschap of maatschap.

**De conclusie is dat als u bijvoorbeeld een bestand bijhoudt met e-mailadressen van uw klanten, u moet voldoen aan de vereisten van de AVG.**

Alle handelingen die worden uitgevoerd met persoonsgegevens gelden als een verwerking. Denk bijvoorbeeld aan het verzamelen, vastleggen, ordenen, structureren, opslaan, gebruiken, doorzenden, opvragen, raadplegen, bijwerken, wijzigen en wissen van persoonsgegevens. Van verwerken is dus al snel sprake.

Alle organisaties (of personen) die gevestigd zijn in de Europese Unie en persoonsgegevens verwerken, vallen onder AVG. Alleen wanneer in huiselijk of privéverband gegevens worden verwerkt, dan is de AVG niet van toepassing.

De AVG onderscheidt twee belangrijke rollen, namelijk de verwerkingsverantwoordelijke en de verwerker. De verwerkingsverantwoordelijke (de naam zegt het al) is verantwoordelijk voor de verwerking van persoonsgegevens. De verwerkingsverantwoordelijke kan voor de verwerking van persoonsgegevens andere partijen inschakelen, die we verwerkers noemen.

## Tips

1) Onderzoek wie uw mogelijke betrokkenen zijn (klanten, werknemers, relaties).

2) Weet welke gegevens u van hen heeft en of dat persoonsgegevens zijn.

3) Kijk vervolgens naar wat u daadwerkelijk met de persoonsgegevens doet en niet naar wat u op papier zou moeten doen met de persoonsgegevens.

# Basisbeginselen

Persoonsgegevens moeten (net als onder de Wbp) worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. Meer specifiek gelden de basisbeginselen van ‘doelbinding’, ‘minimale gegevensverwerking’, ‘juistheid’, ‘opslagbeperking’ en ‘integriteit en vertrouwelijkheid’. Gegevensverwerking mag niet in strijd zijn met het Europese en nationale recht. Ook moet gegevensverwerking behoorlijk zijn. Dit betekent dat, ook indien er nergens in de AVG een concrete bepaling staat die wordt overtreden, er nog steeds sprake kan zijn van onvoldoende behoorlijke gegevensverwerking. Denkt u hierbij bijvoorbeeld aan de situatie waarin een organisatie toestemming van een betrokkene eist voor gegevensverwerking als voorwaarde voor het leveren van een dienst, terwijl de gegevens daarvoor niet nodig zijn.

Daarnaast moet een betrokkene op de hoogte worden gesteld van het feit dat een verwerking van zijn persoonsgegevens plaatsvindt, waarbij aangegeven wordt wat de doeleinden van deze verwerking zijn. In de praktijk kunt u aan deze verplichting voldoen door deze informatie in een privacyverklaring op te nemen.

Op grond van de AVG moet de verwerkingsverantwoordelijke de naleving van voornoemde basisbeginselen voortaan ook kunnen aantonen (de verantwoordingsplicht).

# Tips

1) De wet geeft bepaalde richtlijnen voor een transparante, behoorlijke en rechtmatige verwerking van persoonsgegevens. Voer de verwerking naar de bedoeling van de wet uit.

2) Wees naar de betrokkenen open over uw redenen om de persoonsgegevens te verwerken en gebruik daarvoor de (juiste) grondslagen.

# Grondslagen

De verwerking van persoonsgegevens is slechts rechtmatig indien u deze kunt baseren op een van de onderstaande zes grondslagen:

- **De verwerking is nodig om een overeenkomst met de betrokkene voor te bereiden of uit te voeren;**
- **De verwerking is nodig om aan een wettelijke verplichting te voldoen;**
- **De verwerking is voor iemand van levensbelang;**
- **De verwerking is nodig om een overheidstaak goed te vervullen;**
- **De verwerking is voor u van zodanig belang, dat de verwerking zwaarder weegt dan de belangen van de betrokkenen;**

  Of

- **De betrokkene heeft zijn toestemming gegeven voor de verwerking.**

## Tip

Aan de grondslag toestemming zitten veel bijkomende voorwaarden, probeer daarom (indien mogelijk) een andere grondslag te gebruiken.

## Let op!

**Het werken met toestemming als grondslag moet aan verschillende vereisten voldoen.**

U moet de betrokkene duidelijk vertellen waarvoor u zijn toestemming vraagt, daarbij moet u de betrokkene erop wijzen dat hij zijn toestemming altijd mag intrekken.

De toestemming mag niet vaag of algemeen van aard zijn, maar moet zien op een specifiek omlijnde verwerking.

De betrokkene moet vrij zijn om zijn toestemming te weigeren.

De toestemming is niet geldig als u die als voorwaarde stelt voor het aangaan van een overeenkomst met de betrokkene, terwijl de gegevensverwerking daarvoor niet nodig is.

De toestemming moet gegeven worden door middel van een duidelijke actieve handeling, zoals het aanvinken van een vakje op een website. Van een duidelijke actieve handeling is geen sprake in het geval van stilzwijgen of het gebruikmaken van al aangevinkte vakjes. Het is enkel nodig dat uit de handeling van betrokkene de wil van de betrokkene eenduidig is af te leiden (bijvoorbeeld het invullen van een e-mailadres op een inschrijfformulier voor een nieuwsbrief).

U moet kunnen aantonen dat de betrokkene zijn toestemming heeft gegeven.

De betrokkene moet zijn toestemming altijd weer in kunnen trekken en dat moet net zo eenvoudig zijn als het geven van toestemming.

# Bijzondere persoonsgegevens

De AVG benoemt een aantal bijzondere categorieën van persoonsgegevens, die als extra privacygevoelig worden beschouwd. Bijzondere persoons-gegevens zijn onder meer gezondheidsgegevens, genetische gegevens, biometrische gegevens en gegevens waaruit iemands ras, politieke opvattingen of religieuze overtuigingen blijken. De verwerking van bijzondere persoons-gegevens is verboden, tenzij een uitzondering op het verbod van toepassing is (bijvoorbeeld uitdrukkelijke toestemming van de betrokkene). De eerder in deze whitepaper genoemde basisbeginselen zijn ook van toepassing op bijzondere persoonsgegevens.

## Tip

Onderzoek of u bijzondere gegevens verwerkt en beoordeel of dit is toe-gestaan en of u de juiste maat-regelen heeft genomen (bijvoorbeeld of u uitdrukkelijke toestemming heeft gevraagd).

# Rechten van betrokkenen

Betrokkenen hebben op grond van de AVG bepaalde rechten die zij ten opzichte van de verwerkingsverantwoordelijke kunnen inroepen. Zo hebben betrokkenen bijvoorbeeld het recht op informatie, zij moeten op de hoogte worden gesteld van het feit dat verwerking van hun persoonsgegevens plaatsvindt of zal plaatsvinden en wat de doeleinden hiervan zijn. Ook hebben betrokkenen het recht op inzage van hun persoonsgegevens. Als betrokkenen daarom verzoeken, moet aan hen een kopie worden verstrekt van alle persoonsgegevens die van hen worden verwerkt.

Voorts moeten de persoonsgegevens van de betrokkenen worden verbeterd indien betrokkenen terecht aangeven dat ze onjuist zijn. Bovendien hebben betrokkenen in een aantal gevallen het recht dat hun gegevens op verzoek worden verwijderd. Een bijzondere vorm van het recht op verwijdering is het recht om vergeten te worden. In het geval dat u persoonsgegevens openbaar heeft gemaakt en die gegevens op grond van een verzoek van de betrokkene moeten worden gewist, dan moet u, binnen redelijke grenzen, uw best doen om anderen te informeren dat de betrokkene wil dat iedere koppeling naar (of kopie van) de gegevens gewist wordt.

Op grond van het beginsel van behoorlijke rechtsverwerking moet de andere partij serieus met het verzoek van de betrokkene omgaan. Het recht op verwijdering en het recht om vergeten te worden zijn echter niet van toepassing indien u gegevens verwerkt omdat het nodig is, bijvoorbeeld om een wettelijke verplichting na te komen. In aanvulling op het bovenstaande moeten de betrokkenen ook worden gewezen op hun rechten en hierover geïnformeerd worden, hetgeen betekent dat u verschillende privacyverklaringen op kunt stellen, bijvoorbeeld een verklaring voor uw klanten, websitebezoekers en relaties maar ook een verklaring voor uw werknemers.

## Tips

1) Informeer uw betrokkenen beknopt, open, begrijpelijk, toegankelijk en in duidelijke en eenvoudige taal over hun rechten.

2) Zorg voor privacyverklaringen voor uw verschillende betrokkenen (klanten, websitebezoekers, werknemers).

3) Controleer regelmatig of de persoonsgegevens die u verwerkt juist zijn.

# Verwerkingsregister

Als verwerkingsverantwoordelijke moet u een register van verwerkings-activiteiten bijhouden (de documentatieplicht) waarin u minimaal opneemt welke persoonsgegevens verwerkt worden, voor welk doel, waar ze worden opgeslagen en met wie ze worden gedeeld.

De documentatieplicht is niet van toepassing op organisaties die minder dan 250 werknemers in dienst hebben, tenzij het waarschijnlijk is dat de verwerking die zij verrichten een risico inhoudt voor de rechten en vrijheden van de betrokkenen, de verwerking niet incidenteel is, of de verwerking bijzondere categorieën van gegevens of strafrechtelijke gegevens betreft.

U kunt hierbij bijvoorbeeld denken aan fysiotherapie- en huisartsenpraktijken die gezondheidsgegevens verwerken. De genoemde uitzonderingen leiden er in de praktijk toe dat ook veel kleine en middelgrote organisaties niet zullen ontkomen aan het bijhouden van een verwerkingsregister.

## Tip

Stel vast of u een register van verwerkingsactiviteiten moet aanleggen.

# *Functionaris van de gegevensbescherming*

Een Functionaris voor de Gegevensbescherming (FG) houdt binnen een organisatie toezicht op de toepassing en naleving van de AVG. U bent verplicht om een FG aan te stellen indien uw organisatie als kerntaak grote hoeveelheden persoonsgegevens verwerkt op basis van regelmatige en stelselmatige observatie. Denkt u hierbij bijvoorbeeld aan een beveiligingsbedrijf dat openbare gelegenheden bewaakt of een marketingbureau dat persoonsgegevens verwerkt om gepersonaliseerde reclame aan te kunnen bieden (profilering).

Daarnaast bent u verplicht een FG aan te stellen indien één van de kernactiviteiten van uw organisatie het grootschalig verwerken van bijzondere persoonsgegevens (bijvoorbeeld ras, gezondheid of politieke voorkeur) of strafrechtelijke gegevens is. Hierbij kunt u bijvoorbeeld denken aan een ziekenhuis.

Voor sommige organisaties is een Data Protection Impact Assessment (DPIA), oftewel een gegevensbeschermingseffectbeoordeling, verplicht. Een DPIA is slechts verplicht als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de betrokkenen. Dat is in ieder geval zo als een organisatie:

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

## Tips

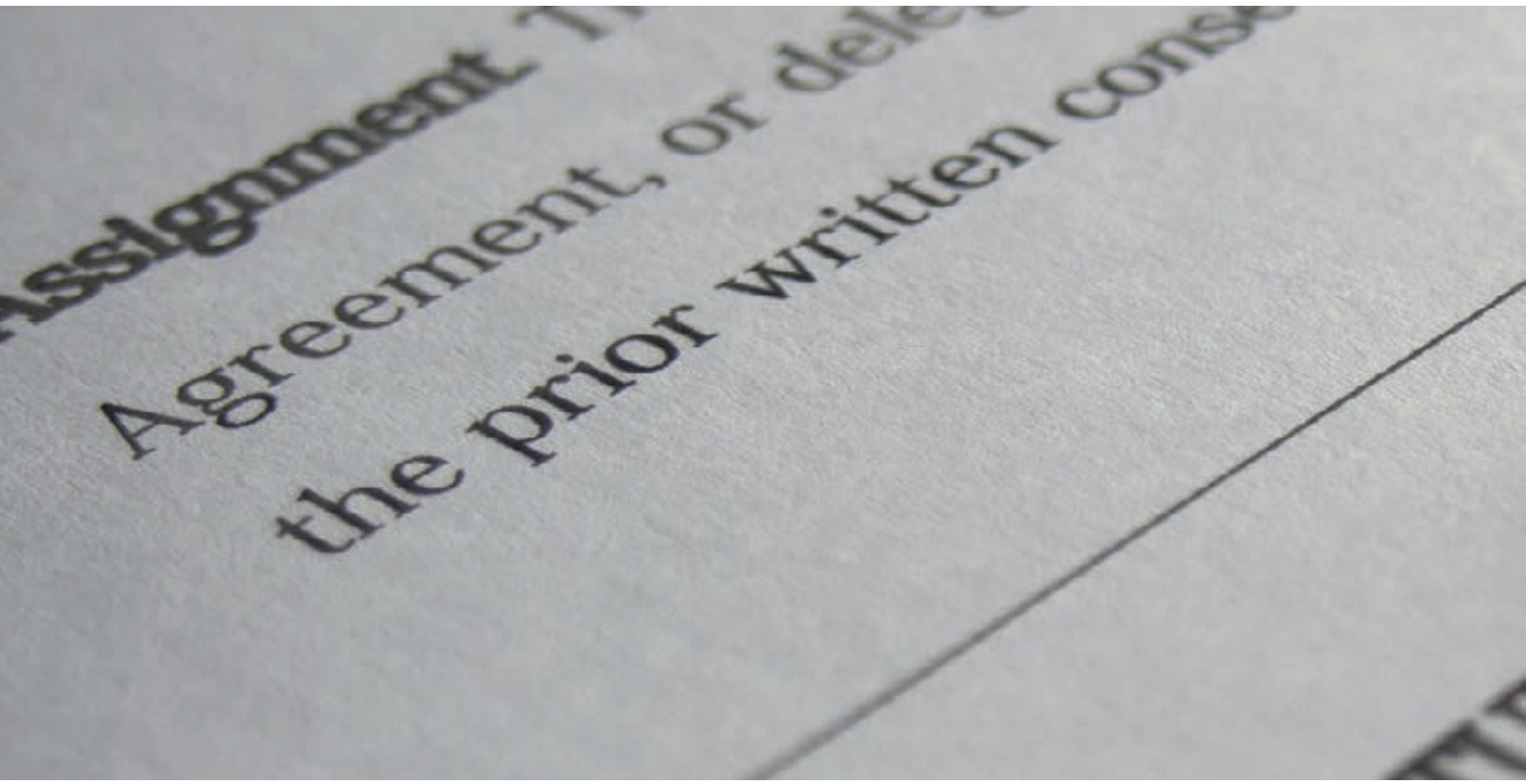
1) Stel vast of u verplicht bent een FG aan te stellen.

2) Stel vast of u een gegevensbeschermingseffectbeoordeling dient uit te voeren.

# Verwerkersovereenkomst

De verwerkingsverantwoordelijke kan voor de verwerking van persoonsgegevens andere partijen inschakelen, die we verwerkers noemen. U kunt hierbij denken aan arbodiensten, ICT-dienstverleners, pensioenfondsen en salarisverwerkers. Een verwerkingsverantwoordelijke moet ervan uit kunnen gaan dat de verwerker die hij inschakelt op een correcte wijze omgaat met de verstrekte gegevens. De verwerkingsverantwoordelijke moet daarom vaststellen of de verwerker aan de wettelijke eisen voldoet. De maatregelen die de verwerker hiervoor neemt kunnen worden vastgelegd in een verwerkersovereenkomst.

In die overeenkomst staat onder meer dat de gegevens slechts op instructie van de verwerkingsverantwoordelijke verwerkt worden, dat de personen binnen de verwerkende organisatie vertrouwelijk met de gegevens omgaan, dat de verwerker passende maatregelen voor de beveiliging van de gegevens neemt, onder welke voorwaarden de verwerker de gegevens mag doorgeven, dat de verwerker er, voor zover mogelijk, voor zorgt dat de verwerkingsverantwoordelijke zich aan de rechten van de betrokkenen kan houden, dat de verwerker na afloop van de diensten de gegevens wist of teruggeeft aan de verwerkingsverantwoordelijke en dat de verwerker alle informatie die nodig is om het voldoen aan de wettelijke eisen te testen, aan de verwerkingsverantwoordelijke zal geven.



## Tips

1) Onderzoek of u voor de verwerking van persoonsgegevens andere partijen inschakelt en, zo ja;

2) Leg de afspraken met die andere partijen vast in verwerkersovereenkomsten.

3) Controleer regelmatig of de verwerker zich aan de afspraken houdt.

# Beveiliging

Het onderwerp beveiliging krijgt ruim de aandacht onder de AVG. De AVG stelt de norm van “passende maatregelen” ter beveiliging van persoonsgegevens. De AVG verlangt dat gegevensbescherming in het technische ontwerp van systemen wordt ingebouwd. Dit betekent dat systemen op een privacy-vriendelijke manier moeten worden ingericht Daarnaast moeten systemen zo zijn ontworpen en ingericht dat er zo min mogelijk persoonsgegevens worden verwerkt. Welke maatregelen zorgen voor een passend beveiligingsniveau moet van geval tot geval beoordeeld worden.

# Risico’s

De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de AVG. De AP kan op grond van de AVG naast of in plaats van corrigerende maatregelen, geldboetes opleggen tot maximaal € 20.000.000. Indien de boete aan een onderneming wordt opgelegd, dan kan de AP onder de AVG zelfs een hogere boete tot 4% van de totale wereldwijde jaaromzet opleggen.

Daarnaast bestaat de kans dat betrokkenen zich tegenover de verwerkingsverantwoordelijke op het standpunt stellen dat zij materiële en/of immateriële schade hebben geleden als gevolg van het niet-naleven van de AVG en schadevergoeding van de verwerkingsverantwoordelijke vorderen. Dit zal zich bijvoorbeeld voor kunnen doen bij onderhandelingen over een beëindigingsvergoeding in de relatie werknemer-werkgever.

## Tips

1) Enkele maatregelen die u zou kunnen treffen zijn de pseudonimisering en versleuteling van persoonsgegevens, het regelmatig testen van beveiligingssystemen en het zorgdragen voor back-up mogelijkheden.

2) Beperk de kring van werknemers die toegang hebben tot bepaalde persoonsgegevens tot die werknemers die de gegevens nodig hebben voor de uitoefening van hun werkzaamheden en verleen enkel toegang tot de persoonsgegevens die zij nodig hebben voor de uitoefening van hun werkzaamheden.

# Conclusie

Wat u moet doen om uw organisatie te laten voldoen aan de nieuwe privacy-regelgeving is afhankelijk van hetgeen hiervoor is besproken en hangt af van uw type onderneming. U kunt denken aan een privacyverklaring om uw klanten, werknemers en relaties te informeren over hoe u met hun persoonsgegevens omgaat. Werkt u samen met organisaties die namens uw organisatie persoons-gegevens verwerken, dan raden wij u aan met die partijen een verwerkersover-eenkomst sluiten. Deze verwerkersovereenkomsten dient u slechts éénmaal op te stellen. Daarnaast geldt voor veel organisaties een documentatieplicht. In dat geval dient tevens een verwerkingsregister te worden aangelegd. De op een organisatie van toepassing zijnde privacyregels zijn dus voor iedere organisatie verschillend.

# Stappenplan en bewaartermijnen

Het voorgaande laat zich samenvatten in het volgende stappenplan:

1) Ga na **welke persoonsgegevens** u verwerkt.

2) Zorg voor een **privacyverklaring** om klanten, werknemers en relaties te informeren over hoe u met hun persoonsgegevens omgaat:

- op uw website;
- in of bij uw opdrachtbevestiging;
- in of bij de arbeidsovereenkomst/ arbeidsvoorwaarden.

3) Werkt u samen met andere bedrijven die namens uw bedrijf persoons-gegevens verwerken? Denkt u hierbij bijvoorbeeld aan uw ICT-dienstverlener. Sluit met die partijen dan **verwerkersovereenkomsten.**

4) Heeft u meer dan 250 werknemers, is de verwerking niet incidenteel of verwerkt u bijzondere/risicovolle persoonsgegevens, leg dan een **verwerkings-register** aan.

5) Controleer of u de persoonsgegevens voldoende heeft **beveiligd** (versleuteling, anonimisering, back-up mogelijkheden e.d.).

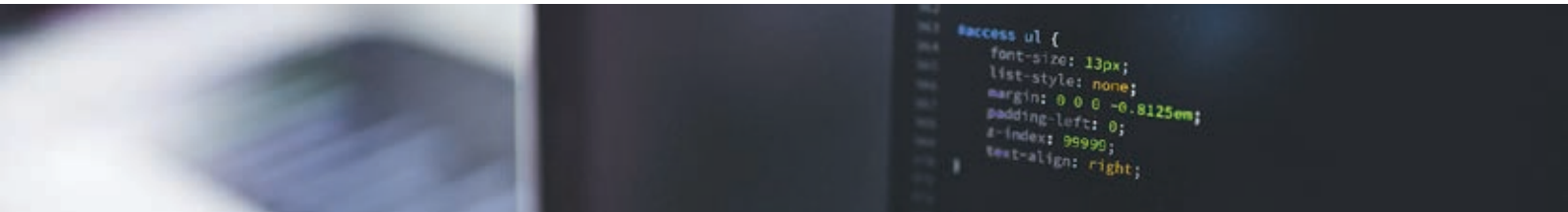
Tenslotte wijzen wij u nog op enkele bewaartermijnen waar u rekening mee dient te houden. Er zijn binnen uw organisatie diverse processen en activiteiten waarin verschillende categorieën van persoonsgegevens nodig zijn. De verwerkingsdoelen per proces verschillen, waardoor ook andere bewaartermijnen kunnen gelden. Denk aan salarisafspraken, facturen en verzuimbeheer. De bewaartermijn gaat lopen na bijvoorbeeld het einde van een dienstverband, het einde van een boekjaar of het doen van een registratie. Overigens kan het soms zo zijn dat de genoemde termijn wordt overruled door een andere wettelijke bewaarplicht, zoals fiscale wetgeving.

- Sollicitatieprocedures (CV's): zonder toestemming van de sollicitant bedraagt de maximale bewaartermijn 4 weken;
- Camerabeelden: maximale bewaartermijn 4 weken;
- Verzuimbeheer: maximale bewaartermijn 2 jaar;
- Personeelsdossier: maximale bewaartermijn 2 jaar na uitdiensttreding.

Is de bewaartermijn van persoonsgegevens verstreken of zijn de gegevens niet meer noodzakelijk voor het doel? Dan moeten de gegevens vernietigd worden. Denk bijvoorbeeld aan gegevens over loonbeslag als het loonbeslag is opgeheven. Vernietiging moet gebeuren onder controle van uw bedrijf. Vernietigen houdt in dat de gegevens niet langer meer bestaan of niet langer meer bestaan in een bruikbare vorm. De AVG stelt geen extra vereisten aan het vernietigen van persoonsgegevens.

**Wilt u hulp om uw organisatie privacy-proof te maken?**
Neem dan contact met ons op, wij helpen u graag. Wij stellen vast welke documenten en procedures uw organisatie nodig heeft om te voldoen aan de AVG en wij kunnen, indien gewenst, deze documenten en procedures ook voor u opstellen.





# Waar vindt u ons?

## Vestigingen
## OOvB adviseurs en accountants.

**Cuijk**
Gildekamp 12
5431 SP Cuijk
Telefoon: 0485-316844
Emailadres: cuijk@oovb.nl

**Heesch**
De La Sallestraat 8
5384 NK Heesch
Telefoon: 0412 - 612818
Emailadres: heesch@oovb.nl

**Wijchen**
Vijverlaan 21
6602 CX  Wijchen
Telefoon: 024 - 6412471
Emailadres: wijchen@oovb.nl

**Boekel**
De Vlonder 60
5427 DE Boekel
Telefoon: 0492-327327
Emailadres: boekel@oovb.nl

**Wanroij**
Bus 8
5446 PK Wanroij
Telefoon: 0485 - 452817
Emailadres: wanroij@oovb.nl

OOvB adviseurs en accountants

# Vertrouwen is goed, controle is beter.

Wel degelijk. OOB adviseurs en accountants