

**Handreiking privacy**

# **Do's & Don'ts**

**Persoonsgegevens in  
de uitzendbranche  
onder de AVG**



Algemene Bond  
Uitzendondernemingen

# Uitzendondernemingen en de Algemene verordening gegevensbescherming

**Als uitzendonderneming bent u verantwoordelijk voor correcte verwerking van persoonsgegevens. Het is belangrijk dat u zorgvuldig omgaat met de persoonsgegevens van kandidaten en uitzendkrachten.**

Door technologische ontwikkelingen en globalisering is in Europa behoefte ontstaan aan krachtiger bescherming van persoonsgegevens en strengere handhaving door toezichthouders. Dit gebeurt in de nieuwe privacywet, de *Algemene verordening gegevensbescherming* (AVG of GDPR in het Engels), die vanaf 25 mei 2018 de oude *Wet bescherming persoonsgegevens* vervangt.

Door de nieuwe privacywet krijgt u meer verplichtingen, krijgen betrokkenen meer rechten en heeft de nationale toezichthouder, de Autoriteit Persoonsgegevens, meer bevoegdheden.

Deze uitgave is aangepast op de AVG, dus op de regels die vanaf 25 mei 2018 gelden. Wij hebben hierin de belangrijkste uitgangspunten en wettelijke verplichtingen voor u op een rij gezet. **Deel 1** van deze handreiking gaat over de algemene privacyverplichtingen. In **deel 2** vindt u een aantal praktische do's & don'ts die van toepassing zijn op uitzendkrachten in verschillende situaties (ingeschreven, werkzaam en niet meer werkzaam). Let erop dat u de **do's en don'ts** altijd in samenhang moet zien met de algemene privacyverplichtingen.

# Inhoud

<b>Deel 1</b>	<b>Algemene verplichtingen AVG voor de uitzendbranche</b>	<b>4</b>
<b>Deel 2</b>	<b>Do's &amp; don'ts met persoonsgegevens in de uitzendbranche</b>	<b>10</b>
Situatie 1	Ingeschreven uitzendkracht	10
Situatie 2	De werkzame uitzendkracht	12
Situatie 3	De niet meer werkzame uitzendkracht	14
	<b>Over deze handreiking</b>	<b>16</b>
	Heeft u nog vragen?	16

# Deel 1 Algemene verplichtingen

In dit deel zijn de belangrijkste uitgangspunten en verplichtingen van de privacywet AVG voor u op een rij gezet.

---

## Uitgangspunten bij het verzamelen en verwerken van persoonsgegevens

### **Rechtmatig, eerlijk en transparant**

Uitzendkrachten en kandidaten worden altijd vooraf in eenvoudige taal geïnformeerd over het verzamelen en verwerken van persoonsgegevens en het doel daarvan.

### **Doelbinding**

Gegevens worden alleen gebruikt voor duidelijk omschreven doelen.

### **Minimale gegevensverwerking (dataminimalisatie)**

Er worden alleen gegevens verwerkt die noodzakelijk zijn voor het doel. Bovendien moet de toegang tot gegevens beperkt worden tot de werknemers/derden voor wie dit voor hun taak noodzakelijk is.

### **Juistheid**

De uitzendonderneming moet ervoor zorgen dat de gegevens juist zijn en blijven, bijvoorbeeld door periodiek aan uitzendkrachten en kandidaten te vragen of de verstrekte gegevens nog correct zijn.

### **Bewaartermijnen**

Gegevens worden zolang bewaard als nodig is voor het doel, daarna moeten ze verwijderd worden.

### **Technische en organisatorische maatregelen**

Gegevens moeten worden beveiligd tegen verlies en ongeoorloofde toegang of gebruik. Zie voor meer informatie de [Richtsnoeren beveiliging persoonsgegevens van de Autoriteit Persoonsgegevens](#).

### **Verantwoordingsplicht**

De uitzendonderneming moet kunnen aantonen dat de privacywet wordt nageleefd.

### **Noodzaak, proportionaliteit en subsidiariteit**

Inbreuk op belangen van een kandidaat of uitzendkracht mag bij gegevensverwerking niet onevenredig zijn in verhouding tot het doel van de verwerking. Ook moet altijd het minst ingrijpende alternatief worden gekozen dat beschikbaar is om legitieme doelen te bereiken.

## Hoge boetes bij niet naleven privacyregels

De Autoriteit Persoonsgegevens kan hoge boetes opleggen aan organisaties die de regels niet goed naleven. Boetes kunnen vanaf 25 mei 2018 oplopen tot 20 miljoen euro of 4% van de wereldwijde jaaromzet. De hoogte van de boetes moet volgens de AVG wel in verhouding staan tot de ernst van de overtreding.

---

## Belangrijke grondslagen voor verwerking persoonsgegevens

Volgens de privacywet mogen uitzendondernemingen persoonsgegevens verwerken als er een wettelijke grondslag is. De belangrijkste grondslagen zijn:

**Uitvoering van de uitzendovereenkomst**, waarbij de uitzendkracht partij is. **Let op:** de gegevensverwerking moet noodzakelijk zijn voor de uitvoering van de overeenkomst, bijvoorbeeld voor de bemiddeling of salarisverwerking.

**Nakomen wettelijke plicht door de uitzendonderneming.** De verwerking moet strikt noodzakelijk zijn om de wettelijke verplichting na te komen. In sommige situaties is het bijvoorbeeld verplicht om het BSN en een kopie van het ID-document van een uitzendkracht te verwerken.

**Gerechtvaardigd belang van de uitzendonderneming.** Persoonsgegevens mogen ook verwerkt worden als dat noodzakelijk is voor het behartigen van een gerechtvaardigd belang van een uitzendonderneming. Hiervoor moet u kunnen aantonen dat uw belangen prevaleren boven het belang of de fundamentele rechten en vrijheden van de uitzendkracht.

**Toestemming van de uitzendkracht.** Doordat er tussen de uitzendkracht en uitzendonderneming een afhankelijkheidsrelatie bestaat, kan de uitzendkracht in beginsel de uitzendonderneming geen toestemming geven om persoonsgegevens te verwerken. In deze verhouding kan de toestemming namelijk vaak niet als in vrijheid gegeven worden beschouwd. Voor het verwerken van een foto heeft de Autoriteit Persoonsgegevens wel vastgesteld dat dit is toegestaan met toestemming van de uitzendkracht, mits die toestemming *natuurlijk vrijelijk* is gegeven.

## Persoonsgegevens

Wat zijn persoonsgegevens? Alle gegevens waarmee je een natuurlijk persoon kunt identificeren. Bijvoorbeeld: NAW-gegevens, e-mailadressen, telefoonnummers, personeelsnummers, geboortedata, geslacht, nationaliteit, werkervaring en opleidingen, IP-adressen, logingegevens etc.

## Bijzondere persoonsgegevens

Bijzondere persoonsgegevens zijn gegevens waaruit iemands **ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, gezondheid, strafrechtelijk gedrag, seksuele leven** of het **lidmaatschap van een vakbond** blijken. Ook **genetische gegevens** en **biometrische gegevens** voor unieke identificatie van een persoon vallen hieronder.

Voorbeelden hoe u hier als uitzendonderneming mee te maken kunt krijgen: het gegeven of een uitzendkracht of kandidaat een hoofddoek draagt, een pasfoto met gegevens over huidskleur of afkomst of een reden van ziekmelding van de uitzendkracht.

Bijzondere persoonsgegevens mogen in principe niet verwerkt worden, tenzij een wettelijke uitzondering van toepassing is en het strikt noodzakelijk is om ze hiervoor te verwerken. Meer informatie hierover staat op de website van de [Autoriteit Persoonsgegevens](#).

## Verwerken

Onder het verwerken van persoonsgegevens wordt elke handeling met betrekking tot persoonsgegevens verstaan. Voorbeelden zijn: verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken d.m.v. doorzending, verspreiding of op andere wijze ter beschikking stellen, combineren, afschermen, wissen of vernietigen.

---

## Overige verplichtingen op basis van de privacywet

### Verwerkingsregister

Vanaf 25 mei 2018 bent u verplicht om een register bij te houden van de verwerking van persoonsgegevens. Het register is voor eigen gebruik en moet op verzoek aan de Autoriteit Persoonsgegevens worden verstrekt. Uitzendkrachten hebben geen recht op inzage.

Met betrekking tot verwerkingsactiviteiten moet het volgende geregistreerd worden:

- de naam en contactgegevens van de verantwoordelijke en indien van toepassing de functionaris voor gegevensbescherming (de FG);
- de doeleinden van gegevensverwerking;
- een beschrijving van de categorieën betrokkenen (op wie de gegevens betrekking hebben) en categorieën persoonsgegevens;
- de (voorgenomen) categorieën ontvangers;
- aan welke derde landen (landen buiten de EER en Zwitserland) de gegevens worden verstrekt;
- voor zover mogelijk de (voorgenomen) bewaartermijnen;
- voor zover mogelijk een algemene beschrijving van de beveiligingsmaatregelen.

### **Rechten van betrokkenen en transparantie**

De rechten van betrokkenen worden vanaf 25 mei 2018 uitgebreid. Daardoor hebben betrokkenen:

- recht op inzage;
- recht op correctie als gegevens niet juist of niet actueel zijn;
- recht op verwijdering (ook wel recht op vergetelheid). Indien gegevens verstrekt zijn aan derden, moeten die hierover geïnformeerd worden;
- recht op overdraagbaarheid van gegevens, ook wel dataportabiliteit genoemd. Dit houdt in dat zij het recht hebben om de persoonsgegevens te ontvangen die een organisatie van hen heeft.

Betrokkenen moeten vooraf op de juiste wijze worden geïnformeerd over de verwerking van hun persoonsgegevens. U kunt dit onder andere doen door middel van een privacystatement. Op grond van de privacywet moet u de betrokkenen informeren over:

- wie verantwoordelijk is voor de verwerking;
- wat de doeleinden zijn van de verwerking;
- wat de wettelijke grondslagen zijn voor de verwerking;
- of er sprake is van geautomatiseerde besluitvorming;
- wat de bewaartermijnen zijn;
- hoe de gegevens zijn beveiligd;
- welke rechten betrokkenen hebben;
- waar betrokkenen in de onderneming een klacht kunnen indienen over de verwerking van hun persoonsgegevens;
- de mogelijkheid tot het indienen van een klacht bij de Autoriteit Persoonsgegevens.

### **Meldplicht datalekken**

We spreken van een datalek als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben.

Alle inbreuken op de beveiliging moeten worden gemeld aan de Autoriteit Persoonsgegevens, tenzij het niet waarschijnlijk is dat deze leiden tot een

privacyrisico van betrokkenen. De melding moet uiterlijk binnen 72 uur na ontdekking van de inbreuk worden gedaan. De inbreuk moet ook worden gemeld aan betrokkenen als er sprake is van een waarschijnlijk hoog privacyrisico.

Om het privacyrisico te beoordelen, zijn onder andere de aard en de omvang van de verwerking van belang. Het privacyrisico is bijvoorbeeld groter als veel en/of bijzondere persoonsgegevens worden verwerkt. U bent als verwerkingsverantwoordelijke verplicht om alle inbreuken, de gevolgen daarvan en de getroffen maatregelen te documenteren. Dit geldt ook als het een inbreuk betreft die u niet hoeft te melden aan de Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens kan u verzoeken de documentatie van alle inbreuken te verstrekken.

### **Functionaris Gegevensbescherming**

Uitzendondernemingen die op grote schaal bijzondere persoonsgegevens verwerken, zijn vanaf 25 mei 2018 verplicht een Functionaris Gegevensbescherming (FG) aan te wijzen. U dient zelf in te schatten of u hiertoe verplicht bent.

Voornaamste taken van een FG zijn:

- de directie te informeren en adviseren;
- zorgdragen voor bewustwording en opleiding van personeel t.a.v. gegevensbescherming;
- de onderneming assisteren bij uitvoeren van een *Data Protection Impact Assessment*;
- toezien op naleving van de privacywet;
- het samenwerken met en fungeren als aanspreekpunt voor de Autoriteit Persoonsgegevens.

### **Data Protection Impact Assessment**

Als u vanaf 25 mei 2018 gegevens gaat verwerken die waarschijnlijk een hoog privacyrisico opleveren voor de betrokkenen, dan bent u verplicht een Data Protection Impact Assessment (DPIA) uit te voeren. Met een DPIA kunt u vooraf de privacyrisico's en impact daarvan op betrokkenen in kaart brengen en de maatregelen benoemen die de risico's verkleinen.



# Verwerker en verwerkersovereenkomst

Een verwerker verwerkt persoonsgegevens in opdracht van de uitzendonderneming. Hij mag geen beslissingen nemen over het gebruik van gegevens. Verwerkers zijn bijvoorbeeld:

- Salarisverwerkingsbedrijf/backoffice
- Leverancier personeelsadministratiesysteem
- (Website)hosting en cloudopslagdiensten
- Leverancier systeem voor verzuimafhandeling

*Tip! Voor u een verwerker inschakelt, is het raadzaam eerst te beoordelen of de verwerker zijn systemen zo heeft ingericht dat de do's & don'ts van deze handreiking (voor zover mogelijk) automatisch worden nageleefd. Zo worden risico's op fouten met onrechtmatig verwerkte gegevens zoveel mogelijk beperkt.*

## Verplichte verwerkersovereenkomst

U bent verplicht om met een verwerker een verwerkersovereenkomst te sluiten. Zo kunt u aantonen dat de verwerker voldoet aan de verplichtingen onder de privacywet en dat u tijdig kunt voldoen aan het melden van een datalek.

## Wat zijn de belangrijkste zaken om in de verwerkersovereenkomst te regelen?

Leg allereerst de omschrijving van de dienstverlening vast. Welke persoonsgegevens worden verwerkt en welke (categorieën) werknemers van de verwerker hebben toegang tot de persoonsgegevens en verwerkingshandelingen. Verder zijn deze aandachtspunten zeker van belang:

- het doel van verwerking
- geheimhouding
- betrouwbaarheidseisen
- bewaartermijnen
- beveiliging en rapportage
- auditrechten van de uitzendonderneming
- meldplicht datalekken van bewerker aan uitzendonderneming (o.a. inhoud van de melding, criteria voor het melden, de snelheid hiervan, verplichting van de bewerker om mee te werken, zodat de uitzendonderneming aan de meldplicht datalekken kan voldoen)
- het inschakelen van sub-bewerkers
- doorgifte persoonsgegevens naar landen buiten de Europese Economische Ruimte (EER)
- gevolgen beëindiging, heronderhandeling en noodplan.

Daarnaast kunt u ook denken aan onderwerpen zoals:

- aansprakelijkheid
- vrijwaring
- rechten van intellectueel eigendom
- looptijd

**U kunt gebruikmaken van een model verwerkersovereenkomst op het [ABU-ledennet](#)**

# Deel 2 Do's & don'ts met persoonsgegevens in de uitzendbranche

De volgende specifieke situaties van gegevensverwerkingen zijn vanuit de AVG relevant voor uitzendondernemingen:

1. **Ingeschreven uitzendkracht:** een persoon heeft zich ingeschreven als uitzendkracht, maar is nog niet werkzaam geweest voor uw uitzendonderneming.
2. **Werkzame uitzendkracht:** een persoon die voor uw uitzendonderneming werkzaam is en met wie u een uitzendovereenkomst bent aangegaan.
3. **Niet meer werkzame uitzendkracht:** een persoon die voor uw uitzendonderneming heeft gewerkt, maar nu niet meer in dienst is.

---

## Situatie 1 Ingeschreven uitzendkracht

Welke gegevens mogen wel of niet worden verzameld?

- ✓ Bij het inschrijven van een uitzendkracht mag u alleen die gegevens inschrijven die nodig zijn voor de arbeidsbemiddeling. Denk bijvoorbeeld aan: naam, adres, contactgegevens en de relevante werkervaring en opleiding van de betreffende persoon ten behoeve van de bemiddeling.

### **BSN, nationaliteit, (pas)foto en kopie-identiteitsbewijs**

- ✓ Per 1 januari 2018 mag u ook een kopie van het identiteitsdocument in uw administratie bewaren van een werkzoekende die nog niet aan een opdrachtgever ter beschikking is gesteld, maar daar wel voor in aanmerking komt. Dat betekent dat bij ingeschreven uitzendkrachten de gegevens die op de kopie van het identiteitsbewijs staan, verwerkt mogen worden. Zoals het BSN, nummer van het identiteitsbewijs, nationaliteit en de pasfoto.
- ✗ U mag deze gegevens echter niet afzonderlijk registreren. Een uitzondering hierop vormt het **BSN** voor het nagaan bij UWV of iemand in het doelgroepregister vermeld staat. Hierover moet de ingeschreven uitzendkracht wel worden geïnformeerd. Na deze toetsing dient het BSN weer verwijderd te worden. Voor de **pasfoto** geldt dat deze niet alleen via de kopie van het identiteitsdocument mag worden verwerkt, maar ook als de uitzendkracht hiervoor uitdrukkelijk toestemming heeft gegeven en hierover voldoende is

geïnfomeerd. Het moet ook geheel vrijstaan om deze toestemming niet te geven. Als een uitzendkracht geen toestemming geeft, mogen hier geen negatieve consequenties aan verbonden zijn (zoals geen verdere bemiddeling of plaatsing).

### **Gezondheidsgegevens**

- ✘ Gezondheidsgegevens zoals over aandoeningen, verzuim, ziekteverleden, arbeidshandicap en andere beperkingen mogen niet worden verwerkt. Tenzij dit noodzakelijk is ter bescherming van een belang dat voor het leven van de betrokkene essentieel is (een vitaal belang). Bijvoorbeeld bij ernstige epilepsie.

### **Godsdienst**

- ✘ Godsdienstgegevens (o.a. of iemand een hoofddoek/keppeltje draagt of gemoedsbezwaren heeft) mogen niet worden verwerkt. Ook als een uitzendkracht werkzaam is, mogen godsdienstgegevens niet worden verwerkt.

### **Hoe lang mogen persoonsgegevens bewaard worden?**

- ✔ Zolang een ingeschreven uitzendkracht bemiddeld wil worden naar werk door de uitzendonderneming, mogen relevante gegevens bewaard worden.
- ✔ De kopie van het identiteitsdocument van de kandidaat mag worden opgeslagen zolang dit noodzakelijk is, met een maximum van vier weken.
- ✘ De gegevens moeten in ieder geval op (mondeling) verzoek van de uitzendkracht worden verwijderd.
- ✘ Als een uitzendkracht niet heeft gewerkt en niet opnieuw heeft aangegeven bemiddeld te willen worden, mogen sollicitatiegegevens maximaal vier weken bewaard worden. Aan uitzendkrachten kan uitdrukkelijke toestemming worden gevraagd om de gegevens maximaal één jaar na de sollicitatie te bewaren. Het is aan te raden om uitzendkrachten periodiek te vragen of zij nog bemiddeld willen worden.

**Let op:** indien noodzakelijk en legitiem kunnen gegevens langer bewaard worden. Bij een concrete klacht of claim mogen relevante gegevens worden bewaard voor zover dat noodzakelijk is voor de afhandeling van een klacht/claim of tot het moment dat de klacht/claim verjaard is.

## Situatie 2 Werkzame uitzendkracht

### Verwerken van BSN

#### Wanneer mag/moet het BSN verwerkt worden?

- ✓ Als een uitzendovereenkomst met de uitzendkracht wordt aangegaan, mag een uitzendonderneming het BSN van de uitzendkracht verwerken voor specifieke doelen (zie hieronder).
- ✓ Het BSN dient voor aanvang van de werkzaamheden in de administratie te zijn opgenomen.

#### Waarvoor mag de uitzendonderneming het BSN verwerken?

- ✓ Voor het uitvoeren van de (inhoudingen) loonbelasting en de salaris- en pensioenadministratie (inclusief loonaangifte bij de Belastingdienst).
- ✓ Vaststellen van de identiteit van de uitzendkracht.
- ✓ Wanneer de uitzendonderneming eigenrisicodragers is volgens de Ziektewet.
- ✓ Gegevensverstrekking aan UWV in verband met ziekte en re-integratie.
- ✓ Verstrekking aan de bedrijfsarts in het kader van re-integratie van de uitzendkracht.
- ✓ Ten behoeve van een aanvraag over vermelding in het doelgroepregister van UWV.

#### Mag het BSN aan de inlener worden verstrekt?

- ✓ Het BSN mag aan de opdrachtgever worden verstrekt, mits wordt voldaan aan de zogeheten disculpatieregeling.

### Verwerken kopie ID-document

#### Wanneer mag/moet een kopie van het identiteitsdocument worden verwerkt?

- ✓ Bij een werkzame uitzendkracht bestaat er een wettelijke grondslag om een kopie te maken en het verwerken van het ID-document.
- ✗ Een kopie van het ID-document moet vóór aanvang van de werkzaamheden zijn opgenomen in de administratie.

#### Waarvoor moet de uitzendonderneming de kopie verwerken?

- ✓ Om identiteit en nationaliteit van de uitzendkracht vast te stellen (inclusief of het gaat om een buitenlandse uitzendkracht volgens de *Wet arbeid vreemdelingen*).
- ✓ Om te voldoen aan de wettelijke plicht om een kopie te bewaren voor de loonadministratie. Hierop mag geschreven worden of een markering zijn aangebracht, zolang de gegevens duidelijk leesbaar zijn.

### **Mag de kopie aan de inlener worden verstrekt?**

- ✘ In beginsel mag dit niet. Alleen wanneer is vastgesteld dat het gaat om een buitenlandse uitzendkracht (niet-EER of inwoner van Zwitserland), dan mag de kopie aan de inlener worden verstrekt.

## **Verwerken van ziekteverzuim- en gezondheidsgegevens**

### **Welke gegevens mogen geregistreerd worden bij ziekmelding?**

- ✔ Het telefoonnummer en (verpleeg)adres, zolang de ziekte daaruit niet herleidbaar is.
- ✔ De vermoedelijke duur van het verzuim.
- ✔ Lopende afspraken en werkzaamheden.
- ✔ Of de werknemer valt onder een van de vangnetbepalingen van de Ziektewet. Dit is na twee maanden dienstverband toegestaan. Er mag niet worden gevraagd onder welke vangnetbepaling de werknemer valt.
- ✔ Of de ziekte verband houdt met een arbeidsongeval.
- ✔ Of sprake is van een verkeersongeval met verhaalsmogelijkheid.

**Let op:** overige gezondheidsgegevens mogen niet verzameld of verder verwerkt worden, omdat die niet noodzakelijk zijn voor de loondoorbetalingsverplichtingen of re-integratie. Zij vallen onder het medisch beroepsgeheim. De bedrijfsarts mag deze gegevens van de uitzendkracht dus ook niet aan de uitzendonderneming verstrekken.

### **Welke gegevens mogen bijvoorbeeld niet worden verwerkt?**

- ✘ De aard en oorzaak van verzuim, waaronder de naam van ziekten en specifieke klachten. Het is voldoende om kennis te hebben van functionele beperkingen: wat de uitzendkracht wel en niet kan.
- ✘ Eigen subjectieve waarnemingen over de geestelijke of lichamelijke gezondheidstoestand van de uitzendkracht.
- ✘ Of een ziekte werk gerelateerd is of bijvoorbeeld te maken heeft met relatieproblemen.
- ✘ Gegevens over therapieën, afspraken met artsen, fysiotherapeuten, psychologen.

**Let op:** ook wanneer een uitzendkracht vrijwillig informatie geeft over de aard en oorzaak van het ziekteverzuim, mogen deze gegevens niet worden vastgelegd. Dit mag alleen als het noodzakelijk is ter bescherming van een belang dat voor het leven van de betrokkene essentieel is (dit is een vitaal belang).

# Verwerken gegevens Loonbeslag

## Wanneer mogen gegevens worden verwerkt over loonbeslag op de uitzendkracht?

- ✓ Dat mag alleen indien er loonbeslag is gelegd. Als het loonbeslag wordt opgeheven, mogen deze gegevens niet langer worden bewaard.

## Hoe mogen gegevens over loonbeslag worden verwerkt?

- ✓ Deze gegevens mogen alleen worden verwerkt voor zover dat noodzakelijk is voor de salarisadministratie en uitvoer van het loonbeslag.
- ✓ Of medewerkers van een uitzendbureau toegang mogen hebben tot gegevens over het loonbeslag is afhankelijk van de vraag of dit noodzakelijk is voor hun taak.

---

## Situatie 3 Niet meer werkzame uitzendkracht

Persoonsgegevens van een uitzendkracht die eerder gewerkt heeft, moeten in beginsel uiterlijk twee jaar na de dag waarop de uitzendkracht nog werkzaam was, verwijderd worden. Bepaalde gegevens moeten langer worden bewaard als daarvoor sprake is van een wettelijke minimumbewaartermijn.

### Welke gegevens moeten langer worden bewaard?

Een aantal relevante wettelijke minimumbewaartermijnen zijn:

#### **Algemene wet inzake rijksbelastingen, artikel 52 (fiscale bewaarplicht)**

Voor de administratie die noodzakelijk is voor de controle op de rijksbelasting en vennootschappelijke administratieplicht (bijvoorbeeld: salarisadministratie, uitzendovereenkomst en voor zover noodzakelijk pensioenverplichtingen) geldt een bewaartermijn van zeven jaar.

#### **Uitvoeringsregeling loonbelasting 2011 (ID-bewijzen en loonheffingskortingen)**

ID-bewijzen en loonheffingskortingen dienen ten minste vijf jaar te worden bewaard na het einde van het kalenderjaar waarin de dienstbetrekking is geëindigd.

#### **Uitvoeringsregeling loonbelasting 2011 (gegevens werknemer)**

De inhoudingsplichtige bewaart de bedoelde gegevens ten minste vijf jaar na het einde van het kalenderjaar waarin de dienstbetrekking is geëindigd. Deze gegevens betreffen: naam met voorletters, geboortedatum, BSN, adres met postcode, woonplaats en als iemand niet in Nederland woont: woonland en regio.

#### **BW boek 2, artikel 10 (Administratie vermogenstoestand o.a. jaarstukken)**

Zeven jaar.

**Regeling eigenrisicodragen ZW**

Een werkgever mag nooit over een medisch dossier beschikken. Ook niet bij eigen risicodragerschap Ziektewet. Dit is uitsluitend voorbehouden aan de arbodienst of bedrijfsarts.

**Let op:** indien noodzakelijk en legitiem kunnen gegevens langer worden bewaard. Zo mogen bij een claim de noodzakelijke gegevens tot verjaring van de claim worden bewaard.

# Over deze handreiking

Deze handreiking (uitgave december 2017) is zorgvuldig door juristen opgesteld en geeft een globaal beeld van de privacyverplichtingen voor uitzendondernemingen, maar behelst uitdrukkelijk geen (volledig) juridisch advies. Dit document is niet juridisch bindend, noch kunnen hier rechten aan worden ontleend of kan hier enige aansprakelijkheid of verplichting voor de ABU uit voortvloeien. De privacyregelgeving is momenteel op nationaal en Europees niveau enorm in beweging. Het is daarom raadzaam de ontwikkelingen goed te blijven volgen.

## Heeft u nog vragen?

Met vragen kunt u terecht bij de ABU-Helpdesk via [helpdesk@abu.nl](mailto:helpdesk@abu.nl) of 020 - 655 82 30 (9.00-12.30 uur) of uw eigen juridisch adviseur.

