

**Handreiking privacy
Do's & Don'ts**

Persoonsgegevens in de uitzendbranche onder de AVG

Inhoudsopgave

Deel 1 Algemene verplichtingen AVG voor de uitzendbranche	4
Basisbeginselen	4
Grondslagen	5
Deel 2 Do's & don'ts met persoonsgegevens in de uitzendbranche	9
Situatie 1 Ingeschreven uitzendkracht	10
Situatie 2 De werkzame uitzendkracht	11
Situatie 3 De niet meer werkzame uitzendkracht.	12
Over deze handreiking	13

Inleiding

Uitzendondernemingen en de Algemene verordening gegevensbescherming

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

Door technologische ontwikkelingen en globalisering ontstond in Europa behoefte aan een krachtigere bescherming van persoonsgegevens en strengere handhaving door toezichthouders. Om die reden is sinds 25 mei 2018 de Algemene verordening gegevensbescherming (AVG of GDPR in het Engels) ingevoerd. Hiermee is de Wet bescherming persoonsgegevens komen te vervallen.

Met deze nieuwe Privacywet heeft u meer verplichtingen gekregen, hebben betrokkenen meer rechten en heeft de nationale toezichthouder, de Autoriteit Persoonsgegevens, meer bevoegdheden.

In deze uitgave hebben wij de belangrijkste uitgangspunten en verplichtingen uit de AVG 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.

Deel 1

Algemene verplichtingen

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

Basisbeginselen

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 het thema '[Beveiliging van persoonsgegevens](#)' op de website van de Autoriteit Persoonsgegevens en 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 sinds 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.

Grondslagen

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-bewijs 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

Een van de grondslagen in de AVG is dat iemand toestemming geeft om zijn of haar persoonsgegevens te verwerken. Doordat er tussen de uitzendkracht en uitzendonderneming een afhankelijkheidsrelatie bestaat, wordt in principe aangenomen dat de toestemming niet 'vrijelijk' kan worden gegeven. De toestemming kan in beginsel dus niet worden gebruikt als grondslag om persoonsgegevens te verwerken. Slechts in uitzonderlijke gevallen kunt u de toestemming wél gebruiken. Toestemming voor het gebruik van een foto in een smoelenboek is hiervan een voorbeeld.

Let op dat deze toestemming altijd vrijelijk, ondubbelzinnig, geïnformeerd en specifiek is gegeven. Het weigeren van de toestemming mag geen negatieve gevolgen hebben voor de uitzendkracht.

Vraag ook niet 'voor de zekerheid' toestemming, als er een andere grondslag mogelijk is. Trekt de uitzendkracht de toestemming in, dan vervalt daarmee namelijk de grondslag van de verwerking.

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

U bent 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 om dit register in te zien.

Met betrekking tot verwerkingsactiviteiten moet het volgende geregistreerd worden:

- de naam en contactgegevens van de verantwoordelijke binnen uw onderneming en indien van toepassing de functionaris voor gegevensbescherming (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 (indien aan de orde);
- voor zover mogelijk de (voorgenomen) bewaartermijnen;
- voor zover mogelijk een algemene beschrijving van de beveiligingsmaatregelen.

Rechten van betrokkenen en transparantie

De rechten van betrokkenen zijn sinds 2018 uitgebreid. Daardoor hebben betrokkenen nu:

- recht op inzage
- recht op correctie

Als gegevens niet juist of niet actueel zijn:

- recht op verwijdering
Ook wel recht op vergetelheid genoemd.
- recht op informatie
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.
- recht op beperking van de verwerking
Dit houdt in dat zij u kunnen vragen om tijdelijk te stoppen met het gebruik van hun persoonsgegevens (bijvoorbeeld omdat de betrokkene u heeft gevraagd om een gegeven te wijzigen, maar u dat verzoek nog moet beoordelen).
- recht van bezwaar
Dit houdt in dat zij u kunnen vragen persoonsgegevens niet meer te gebruiken.
- recht op een menselijke blik
Dit betekent dat zij een nieuw, door een persoon genomen besluit, kunnen vragen als zij van u een geautomatiseerd besluit hebben gekregen.

Betrokkenen moeten vooraf ook op de juiste wijze worden geïnformeerd over de verwerking van hun persoonsgegevens (recht op informatie). U kunt dit onder andere doen door middel van een privacyverklaring. Op grond van de Privacywet moet u de betrokkenen in elk geval 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;
- de mogelijkheid tot het indienen van een klacht bij de Autoriteit Persoonsgegevens.

Meldplicht datalekken

Van een datalek is sprake als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben. Dit kan bijvoorbeeld ontstaan door:

- een lek van persoonsgegevens naar onbevoegden (inbreuk op de vertrouwelijkheid);
- verlies of vernietiging van persoonsgegevens (inbreuk op de beschikbaarheid);
- ongewenst wijzigen van persoonsgegevens (inbreuk op de integriteit).

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. U moet zelf een risico-inschatting maken om na te gaan of u een datalek wel of niet moet melden bij de Autoriteit Persoonsgegevens. Het raadplegen van de [website](#) van de Autoriteit Persoonsgegevens kan u mogelijk helpen bij het maken van een goede afweging. Twijfelt u of u het datalek moet melden? Dan kunt u het beste het zekere voor het onzekere nemen en het datalek wél melden.

Komt u tot het oordeel dat u het datalek moet melden, dan moet de melding uiterlijk binnen 72 uur na ontdekking van de inbreuk worden gedaan bij de Autoriteit Persoonsgegevens.

De inbreuk moet ook worden gemeld aan betrokkenen, als u tot het oordeel komt dat het datalek waarschijnlijk een hoog privacyrisico oplevert voor de betrokkene(n).

Om het privacyrisico te beoordelen, zijn onder andere de volgende factoren van belang:

- de aard van de inbreuk;
- de aard en gevoeligheid van de persoonsgegevens en de hoeveelheid;
- het gemak waarmee personen kunnen worden geïdentificeerd;
- de ernst van de gevolgen voor de betrokkenen;
- de kenmerken van de onbevoegde ontvanger;
- bijzondere kenmerken van de persoon;
- bijzondere kenmerken van uw organisatie;
- aantal betrokkenen.

Het privacy-risico is bijvoorbeeld groter als veel en/of bijzondere persoonsgegevens zijn betrokken bij het datalek.

U bent als verwerkingsverantwoordelijke verplicht om alle inbreuken, de gevolgen daarvan en de getroffen maatregelen te documenteren in een datalekregister. Dit geldt ook als het een datalek betreft dat u niet hoeft te melden aan de Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens kan u verzoeken de documentatie van alle inbreuken te verstrekken.

Meer informatie over datalekken vindt u op de [website van de Autoriteit Persoonsgegevens](#).

Functionaris Gegevensbescherming

Uitzendondernemingen die op grote schaal bijzondere persoonsgegevens verwerken (en waarbij deze verwerking hun kernactiviteit is), zijn sinds 25 mei 2018 verplicht een Functionaris Gegevensbescherming (FG) aan te wijzen. U dient zelf in te schatten of u hiertoe verplicht bent.

De voornaamste taken van een FG zijn:

- de directie informeren en adviseren;
- zorgdragen voor bewustwording en opleiding van personeel t.a.v gegevensbescherming;
- de onderneming assisteren bij het 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 persoonsgegevens 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.

Er is pas sprake van een verwerker, als deze partij de persoonsgegevens niet voor eigen doeleinden gebruikt. Deze partij mag dus geen beslissingen nemen over het gebruik van gegevens. Verwerkers zijn bijvoorbeeld:

- Salarisverwerkingsbedrijf/backoffice
- Leverancier personeelsadministratiesysteem
- (Website)hosting en cloudopslagdiensten
- Leveranciersysteem 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 verwerking van persoonsgegevens zoveel mogelijk beperkt.

Verplichte verwerkersovereenkomst

U bent verplicht om met een verwerker een verwerkersovereenkomst te sluiten. In de verwerkersovereenkomst wordt vastgelegd hoe de gegevensverwerking in de praktijk gaat en wat de wederzijdse verantwoordelijkheden zijn. Ook wordt in dit document vastgelegd hoe om te gaan met 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 de volgende elementen in elk geval van belang om op te nemen in de verwerkersovereenkomst:

- het doel van verwerking;
- geheimhouding;
- betrouwbaarheidseisen;
- bewaartermijnen;
- beveiliging en rapportage;
- auditrechten van de uitzendonderneming;
- het melden van datalekken bij de verwerker aan u (o.a. inhoud van de melding, criteria voor het melden, de snelheid hiervan, verplichting van de verwerker om mee te werken, zodat u aan de meldplicht datalekken kan voldoen);
- het inschakelen van subverwerkers;
- 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](#). Wil de verwerker met een eigen model werken, controleer deze dan altijd goed, of laat dit doen door uw juridisch adviseur.

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 uitzend-onderneming 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 verwerken 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 identiteitsbewijs in uw administratie bewaren van een werkzoekende die nog niet aan een opdrachtgever ter beschikking is gesteld, maar daar wel voor in aanmerking komt. Het afschrift dient te

worden vernietigd, zodra het bewaren van dit afschrift niet meer noodzakelijk is, maar uiterlijk vier weken nadat het afschrift in de administratie is opgenomen. Deze termijn geldt niet, als er binnen die termijn een arbeidsovereenkomst tot stand komt met de uitzendkracht. In dat geval moet u de kopie van het identiteitsbewijs bewaren en dus niet vernietigen.

U mag de gegevens die op het identiteitsbewijs staan echter niet afzonderlijk registreren. Dit is slechts anders bij het BSN, indien het verwerken hiervan noodzakelijk is om bij UWV te controleren of de uitzendkracht behoort tot de doelgroep van de Wet banenafpraak en quotum arbeidsbeperkten. Hierover moet de ingeschreven uitzendkracht wel worden geïnformeerd. Na deze toetsing dient het BSN weer verwijderd te worden.

Bijzondere persoonsgegevens

De AVG maakt onderscheid tussen 'gewone' en 'bijzondere' persoonsgegevens. Bijzondere persoonsgegevens zijn gegevens die vanwege hun gevoelige aard extra privacyrisico's met zich meebrengen. Onzorgvuldige verwerking van deze gegevens kan aanzienlijke gevolgen hebben voor de betrokkene. Daarom biedt de AVG hiervoor extra bescherming.

Volgens de AVG zijn dit bijzondere persoonsgegevens:

- Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt;
- Persoonsgegevens waaruit iemands politieke opvattingen blijkt;
- Persoonsgegevens waaruit iemands religie of levensovertuiging blijkt;

- Gegevens over iemands gezondheid;
- Gegevens over iemands seksuele gedrag of gerichtheid;
- Genetische en biometrische gegevens;
- Persoonsgegevens waaruit het lidmaatschap van een vakbond blijkt.

Bijzondere persoonsgegevens mogen in beginsel niet worden verwerkt, tenzij sprake is van een van de tien uitzonderingen uit de AVG.

Gezondheidsgegevens

Gezondheidsgegevens zijn een voorbeeld van bijzondere persoonsgegevens. Deze gezondheidsgegevens, zoals over aandoeningen, verzuim, ziekteverleden, arbeidshandicap en andere beperkingen, mogen in principe niet worden verwerkt. U mag de uitzendkracht hier dus ook niet naar vragen.

Meer informatie over welke gezondheidsgegevens u wel of niet mag verwerken, vindt u op de website van de Autoriteit Persoonsgegevens.

Als de uitzendkracht twee maanden in dienst is, mag u vragen of deze in aanmerking komt voor een van de volgende twee vangnetregelingen van de Ziektewet: de no-riskpolis of de Compensatieregeling oudere werknemers.

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 persoonsgegevens moeten in ieder geval op (mondeling) verzoek van de uitzendkracht worden verwijderd.
- De kopie van het identiteitsbewijs van de uitzendkracht mag worden opgeslagen zolang dit noodzakelijk is voor de bemiddeling, met een

maximum van vier weken na het verstrekken hiervan. Na deze vier weken moet de kopie worden vernietigd (tenzij de uitzendkracht in dienst is getreden). Deze termijn kan ook niet worden verlengd met toestemming van de sollicitant.

- Persoonsgegevens die een uitzendkracht bij zijn sollicitatie/inschrijving heeft verstrekt, mogen in principe maximaal vier weken worden bewaard, als de uitzendkracht niet heeft gewerkt en niet opnieuw heeft aangegeven bemiddeld te willen worden.
- Indien de uitzendkracht uitdrukkelijk toestemming geeft voor een langere bewaartermijn, mogen de sollicitatiegegevens langer worden bewaard. Hierbij is het van belang dat de toestemming voldoet aan de eisen van de AVG: de toestemming moet vrijwillig, specifiek, geïnformeerd en ondubbelzinnig worden gegeven. De redelijkheid van de (nieuwe) bewaartermijn moet wel altijd kunnen worden onderbouwd.

Let op: indien noodzakelijk en legitiem kunnen gegevens langer bewaard worden, ook zónder expliciete toestemming. Bij bijvoorbeeld een concrete klacht of claim, mogen relevante gegevens worden bewaard voor zover dat noodzakelijk is voor de afhandeling van deze klacht/claim.

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?

- 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 eigenrisico-drager 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, als deze het BSN nodig heeft om een beroep te doen op matiging van de inleners- of ketenaansprakelijkheid (wat in principe altijd het geval is) en daarom verzoekt.

Verwerken kopie ID-bewijs

Wanneer mag/moet een kopie van het identiteitsbewijs worden verwerkt?

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

Waarvoor moet de uitzendonderneming de kopie verwerken?

- Om de 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?

Nee, dit mag niet. Dit is alleen anders, als het gaat om een buitenlandse uitzendkracht (niet-EER of inwoner

van Turkije en Zwitserland). In dat geval bent u wettelijk verplicht een kopie van het ID-bewijs aan de inlener te verstrekken.

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 vier vangnetbepalingen van de Ziektewet. Er mag niet worden gevraagd onder welke vangnetbepaling de werknemer valt. Na twee maanden mag u de werknemer wél vragen of hij mogelijk valt onder de no-riskpolis of de Compensatieregeling oudere werknemers.
- 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. Deze overige gezondheidsgegevens 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 de ziekte 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 werkgerelateerd is of bijvoorbeeld te maken heeft met relatieproblemen.
- Gegevens over therapieën, afspraken met artsen, fysiotherapeuten, psychologen.

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

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 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 het uitvoeren 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 uitzendkrachten die uit dienst zijn, moeten in beginsel twee jaar na de dag waarop de uitzendkracht nog werkzaam was, worden verwijderd. Het gaat hier om gegevens waarbij niet in de wet staat hoe lang u die moet bewaren. Het gaat bijvoorbeeld om de volgende gegevens:

- verslagen van functionerings- en beoordelingsgesprekken;
- arbeidsovereenkomsten en wijzigingen hierin;
- correspondentie over benoeming, promotie, degradatie en ontslag;
- afspraken over werkzaamheden voor de ondernemingsraad;

- getuigschriften;
- verzuimfrequentie.

Bepaalde gegevens moeten langer worden bewaard als sprake is van een specifieke wettelijke minimumbewaartermijn (zie hieronder).

Welke gegevens moeten langer worden bewaard?

Een aantal relevante wettelijke minimumbewaartermijnen zijn de volgende:

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, salarisafspraken en voor zover noodzakelijk pensioenverplichtingen) geldt een bewaartermijn van zeven jaar.

Uitvoeringsregeling loonbelasting 2011 (ID-bewijzen en loonheffingskorting)

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

Uitvoeringsregeling loonbelasting 2011 (gegevens werknemer)

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

BW boek 2, artikel 10 (boekhoudplicht, administratie vermogenstoestand)

Zeven jaar.

Let op: indien noodzakelijk en legitiem kunnen gegevens langer worden bewaard. Bijvoorbeeld als er een arbeidsconflict is (geweest) met een (ex-)werknemer of als er een rechtszaak loopt.

Over deze handreiking

Deze handreiking (uitgave juni 2025) is zorgvuldig door juristen opgesteld en geeft een globaal beeld van de privacyverplichtingen voor uitzend-ondernemingen, 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 altijd 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 of 020 - 655 82 30 (9.00-12.30 uur) of uw eigen juridisch adviseur.

ABU

Algemene Bond Uitzendondernemingen

Singaporestraat 74
1175 RA Lijnden

020-655 82 55

info@abu.nl
www.abu.nl