



Privacy versus transparantie

HANDREIKING BIJ RAPPORTEREN

OVER INCLUSIEF WERKGEVEN

Inhoudsopgave

Inleiding	3
<hr/>	
1 Gegevens verwerken	4
1.1 PERSOONSgegevens	
1.2 BIJZONDERE PERSOONSgegevens	
1.3 WERKNEMER INFORMEREN	
1.4 AUTORITEIT PERSOONSgegevens INFORMEREN	
1.5 GEGEVENS DIE U ZONDER MEER MAG ADMINISTREREN	
<hr/>	
2 Gegevens over inclusief werkgeven	9
2.1 DOELGROEPREGISTER	
2.2 INSPANNINGEN INCLUSIEF WERKGEVEN	
2.3 UITKERINGSVERLEDEN	
2.4 ETNICITEIT EN GEBOORTELAND	
<hr/>	
3 Toegang tot gegevens	11
3.1 TOEGANG	
3.2 ANONIMISEREN	
3.3 DERDEN	
<hr/>	

Inleiding

Steeds meer werkgevers maken in hun organisatie ruimte voor mensen met een afstand tot de arbeidsmarkt. Inclusief werkgeven heeft voordelen voor beide partijen. Het personeel op alle niveaus van de organisatie krijgt een evenwichtige, diverse samenstelling.

Werkgevers komen niet alleen in contact met loyale, betrouwbare, gemotiveerde en betrokken arbeidskrachten, maar kunnen ook alvast invulling geven aan een mogelijk wettelijk quatum. Daarnaast is het goed voor het imago van uw organisatie. De arbeidskrachten op hun beurt krijgen de kans om werkervaring op te doen en zich te ontwikkelen.

Veel werkgevers willen hun inspanningen op het gebied van inclusiviteit meten en inzichtelijk maken. Bijvoorbeeld om deze informatie op te nemen in een MVO- of duurzaamheidsrapportage, te voldoen aan een social-returnverplichting of inzicht te krijgen in de invulling van de banenafpraak.

Het is belangrijk dat u hierbij rekening houdt met de privacy-wetgeving. Per 25 mei 2018 is de Algemene Verordening Gegevensbescherming van kracht ('AVG'), met daaraan verbonden de Uitvoeringswet AVG en Richtlijnen van de toezichthouder Autoriteit Persoonsgegevens.¹ Transparantie en privacy kunnen immers op gespannen voet staan met elkaar. Deze handreiking geeft praktische informatie over hoe u uw activiteiten op het gebied van inclusief werkgeven binnen de kaders van de wet transparant kunt maken. Wat mag wel en wat mag niet?

1. Vanaf dat moment geldt dat organisaties structureel en doeltreffend maatregelen moeten treffen tegen nalatige verwerking van persoonsgegevens. De Wet bescherming persoonsgegevens geldt dan niet meer. Zie in de UAVG vooral artikel 30 en de AP-opinie 'De zieke werknemer'.

1 Gegevens verwerken

1.1 | Persoonsgegevens

Persoonsgegevens zijn gegevens die direct of indirect zijn te herleiden tot een bepaalde persoon. Alles wat u met die gegevens doet, wordt 'verwerken' genoemd: verzamelen, delen en opslaan bijvoorbeeld.

De AVG vereist een zorgvuldige verwerking van persoonsgegevens. Zo is ondubbelzinnige toestemming van de werknemer (op basis van goede informatie en in vrijheid gegeven) vereist. Het is verstandig om dit schriftelijk te regelen, omdat u de toestemming achteraf moet kunnen aantonen. Bovendien mag u de persoonsgegevens alleen verwerken als u hiermee een specifiek, concreet doel heeft, dat vooraf duidelijk is omschreven, bijvoorbeeld social-returnverplichtingen of een MVO-rapportage. Daarnaast mag u niet meer dan de benodigde gegevens verwerken en deze mogen ook niet voor andere doelen gebruikt worden (tenzij dat een verwant doel betreft). Verder mogen werknemers die geen toestemming geven daar geen nadelige gevolgen van ondervinden.

1.2 | Bijzondere persoonsgegevens

Voor het verwerken van zo genoemde bijzondere persoonsgegevens gelden nog strengere regels. Deze gegevens hebben een gevoelig karakter, omdat zij de persoonlijke levenssfeer van de werknemer raken. Denk aan gezondheid, godsdienst, levensovertuiging, ras, politieke gezindheid, seksueel leven, lidmaatschap van een vakvereniging of strafrechtelijke achtergrond. Op grond van de AVG is het verwerken van bijzondere persoonsgegevens in beginsel verboden. Er zijn enkele uitzonderingen, die bespreken we hieronder.

Gezondheid: re-integratie arbeidsongeschikte werknemers

Gezondheidsgegevens mogen alleen worden verwerkt door personen die uit hoofde van hun ambt of beroep tot geheimhouding zijn verplicht. Denk aan een bedrijfsarts, huisarts en medisch specialist. Werkgevers mogen deze persoonsgegevens alleen verwerken voor zover dit noodzakelijk is voor de re-integratie of begeleiding van arbeidsongeschikte werknemers. Een arbeidsongeschiktheidspercentage, een 'vangnet-recht' en andere administratieve gegevens zijn vaak ook persoonsgegevens over 'gezondheid'.

Burgerservicenummer: controle doelgroepregister

Het Burgerservicenummer (BSN) is om een andere reden een bijzonder persoonsgegeven. Het gebruik is geregeld in de Wet algemene bepalingen Burgerservicenummer. Alleen de daar genoemde doelen gelden als gebruiksgrond. Het BSN is een uniek en tot de persoon herleidbaar nummer. Dit nummer maakt het mogelijk om informatie uit verschillende bestanden te koppelen. Werkgevers mogen het BSN gebruiken om te controleren of iemand in het doelgroepregister is opgenomen. U mag het nummer niet verstrekken aan derden, tenzij dit noodzakelijk is voor de uitvoering van een wettelijke verplichting, bijvoorbeeld in het kader van salarisverwerking. Onzorgvuldig gebruik van het BSN kan grote privacyrisico's met zich meebrengen, zoals identiteitsfraude. Overleg bij twijfel dus altijd eerst met de Autoriteit Persoonsgegevens of met de Functionaris Gegevensbescherming van de partij met wie u handelt (alle overheden en grote zorginstellingen zijn verplicht een FG aan te stellen). Social-returnverplichtingen vallen niet onder een wettelijke verplichting. Om in het kader van een social-returnverplichting het BSN te rapporteren, heeft u goedkeuring van de Autoriteit Persoonsgegevens nodig.

Strafrechtelijk verleden: VOG

U mag werknemers of sollicitanten niet vragen naar hun strafrechtelijke verleden. Het is wel toegestaan om te vragen om een verklaring omtrent gedrag (VOG). Iemand krijgt een VOG als uit onderzoek blijkt dat hij geen strafbare feiten op zijn naam heeft staan die relevant zijn voor de functie waarvoor de VOG is aangevraagd. Voor een leraar bijvoorbeeld zijn andere strafbare feiten van belang dan voor een accountant. Werkgevers die strafrechtelijke gegevens van werknemers willen verwerken, bijvoorbeeld in het kader van MVO- of inclusierapportages, moeten hiervan nadrukkelijk melding doen bij de Autoriteit Persoonsgegevens. Die stelt vervolgens een uitgebreid onderzoek in.

Werkgevers die zogenoemde pre-employmentscreenings voor opdrachtgevers uitvoeren, zijn verplicht een vergunning bij het Ministerie van Veiligheid en Justitie aan te vragen (Wet particuliere beveiligingsorganisaties en recherchebureaus). Er vindt dan geen voorafgaand onderzoek plaats, tenzij er redenen zijn om dit wel te doen.

Zie de website AP: onderwerpen → werk en uitkering → screening.

Etniciteit/ geboorteland: voorkeursbeleid

Vanwege het gevoelige karakter is het slechts in zeer uitzonderlijke gevallen toegestaan om gegevens over ras, huidskleur, afkomst, culturele achtergrond of nationale en etnische afstamming te verwerken. Het is alleen toegestaan als onvermijdelijk de identiteit van een werknemer vastgesteld moet worden, bijvoorbeeld in het kader van de Wet arbeid vreemdelingen, of om voorkeursbeleid te voeren.

In de algemene Wet gelijke behandeling staat dat voorkeursbeleid alleen mag worden gevoerd voor vrouwen, etnische minderheden en chronisch zieken en gehandicapten. Werkgevers moeten aantonen dat de bewuste groep een achterstand heeft binnen het bedrijf, bijvoorbeeld aan de hand van statistische gegevens. Volgens de Autoriteit Persoonsgegevens is het niet nodig om in deze statistische overzichten ook de namen van de medewerkers op te nemen. U moet de sollicitanten beoordelen aan de hand van vooraf op schrift gestelde, zakelijke criteria. Het is dus belangrijk om te werken met schriftelijke functiebeschrijvingen en duidelijke functie-eisen.

Een kandidaat mag alleen voorrang krijgen bij 'gelijke' geschiktheid - en dus niet bij 'voldoende' of 'gebleken' geschiktheid. Verder moet de voorkeursmaatregel in redelijke verhouding staan tot het doel: de maatregel mag geen onevenredig zwaar middel zijn om de achterstand mee te bestrijden. Het beleid moet ook kenbaar zijn. Het is dus verstandig om in de vacaturetekst te vermelden dat u voorkeursbeleid voert.

Expliciete toestemming

Als u de bijzondere persoonsgegevens uit een van deze uitzonderingscategorieën wilt vastleggen, moet de werknemer expliciet laten weten dat hij hiermee instemt. Stilzwijgende of impliciete toestemming is onvoldoende. Met andere woorden: de werknemer moet in woord, geschrift of gedrag zijn toestemming uitdragen. Voor BSN-gebruik geldt dat organisaties buiten de overheid een BSN alleen mogen gebruiken als dit in een wet staat, en dan is er vaak een wettelijke verplichting waarbij individuele toestemming niet nodig is.

Hoe gevoeliger de gegevens, hoe gedetailleerder u de medewerker moet informeren over het doel en de wijze waarop de gegevensverwerking plaatsvindt. Gezien de gezagsrelatie tussen een werkgever en werknemer neemt de Autoriteit Persoonsgegevens niet snel aan dat de werknemer vrijwillig toestemming heeft gegeven om (bijzondere) persoonsgegevens te verwerken.

Voorheen moest u de verwerking van persoonsgegevens altijd vooraf melden bij de Autoriteit Persoonsgegevens. Deze verplichting is in het najaar 2017 reeds vervallen.

1.3 | Werknemer informeren

Werkgevers hebben een informatieplicht: u moet uw medewerker(s) informeren over welke persoonsgegevens u gaat verwerken, wat het doel daarvan is en hoe u zorgt dat dit zorgvuldig gebeurt. Eenmaal verkregen persoonsgegevens mogen niet worden verwerkt voor een ander doel. U moet ook 'passende technische en organisatorische maatregelen' nemen om de verzamelde persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking. Daarnaast mag u de persoonsgegevens niet langer bewaren dan noodzakelijk is om het doel te verwezenlijken.

De werknemer heeft op grond van de wet het recht om de werkgever te vragen of, en zo ja welke persoonsgegevens worden verwerkt en voor welk doel. In dat geval moet u hem een overzicht van deze gegevens sturen. De werknemer kan u vervolgens vragen om bepaalde gegevens aan te passen of te verwijderen. Hij kan u ook vragen om helemaal te stoppen met bepaalde vormen van verwerking. Dat dient u dan te doen. De medewerker kan uw handelen in dezen ter toetsing voorleggen aan de Autoriteit Persoonsgegevens.

1.4 | Autoriteit Persoonsgegevens informeren

Als verwerker van persoonsgegevens heeft de werkgever, zoals gezegd, onder de AVG niet langer de plicht de verwerking te melden bij de Autoriteit Persoonsgegevens.

1.5 | Gegevens die u zonder meer mag administreren

Werkgevers mogen algemene persoonsgegevens over hun medewerkers registreren, zoals naam, adres, woonplaats, geslacht, geboortedatum en opleidingsniveau, mits u voldoet aan de eisen van de AVG. Daarnaast mag u een aantal zaken registreren die van belang zijn voor de toepassing van wettelijke regelingen. U mag dus bijvoorbeeld vastleggen of een werknemer tot de doelgroep van de banenafpraak behoort en of de no-riskpolis en premiekorting van toepassing zijn.

Let op: u mag alleen die gegevens administreren die noodzakelijk zijn voor de uitvoering van de wettelijke regeling. Waarom een werknemer tot de doelgroep voor de banenafpraak behoort en onder welke no-riskpolis hij valt, mag dus niet in de boeken staan.

1.6 | Meldplicht datalekken

De Wet meldplicht datalekken is op 1 januari 2016 in werking getreden. Hij is per 25 mei 2018 verwerkt in de AVG. Op grond van deze wet zijn overheden en ondernemingen verplicht om bij de Autoriteit Persoonsgegevens direct melding te doen van een datalek dat mogelijk ernstige gevolgen heeft voor de bescherming van persoonsgegevens. Er is, kort gezegd, sprake van een datalek als onbevoegde derden persoonsgegevens in handen krijgen. Voorbeelden zijn een kwijtgeraakte usb-stick, een gestolen laptop of een inbraak in een databestand.

Als u ten onrechte geen melding maakt van een datalek, kan de Autoriteit Persoonsgegevens een hoge bestuurlijke boete opleggen. Deze boete kan oplopen tot 10 miljoen euro of 2 procent van de jaaromzet. Niet elk datalek hoeft te worden gemeld. Dit is afhankelijk van de ernst ervan. Volgens de wet is melding verplicht als het datalek leidt of kan leiden tot ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Als het datalek 'waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer', moet u ook de betrokken werknemer(s) informeren.

2 Gegevens over inclusief werkgeven

2.1 | Doelgroepregister

Soms is het nodig om na te gaan of een sollicitant of werknemer behoort tot het doelgroepregister. Is dat het geval, dan telt de werknemer mee voor de banenafpraak. De wet staat toe om na te gaan of een sollicitant of werknemer is opgenomen in het doelgroepregister. Met het BSN kunt u bij het werkgeversportaal van UWV nagaan of een sollicitant of werknemer is opgenomen in het doelgroepregister. Dit mag u ook vastleggen. UWV mag u echter geen informatie verstrekken over de reden van de opname in het doelgroepregister. Kortom: u kunt alleen checken óf een sollicitant of werknemer in het doelgroepregister staat, niet op grond waarvan. Voor uw huidige werknemers kunt u ook met het loonheffingnummer bij UWV nagaan of zij in dit register staan. Ook dan krijgt u geen inzicht in de reden van opname.

Als een werknemer langer dan twee maanden in dienst is, mag u hem vragen of hij in aanmerking komt voor de no-riskpolis op grond van de Ziektewet. Op deze vraag moet de werknemer antwoord geven. Zo kunt u beoordelen of u subsidies moet aanvragen. Op grond van de Beleidsregels voor de verwerking van persoonsgegevens over de gezondheid van zieke werknemers van de Autoriteit Persoonsgegevens mogen werkgevers in het kader van de no-riskpolis niet vragen naar het ziekte- of uitkeringsverleden van de werknemer. Dit mag ook niet worden geregistreerd. Daarbij geldt een uitzonderings situatie voor werknemers die onder de no-riskpolis vallen omdat ze 56 jaar of ouder waren toen ze in dienst traden en die direct voorafgaande aan het moment van in dienst treden tenminste 52 weken een WW-uitkering ontvingen. Voor deze categorie geldt dat de no-riskpolis pas na 13 weken ziekte tot uitbetaling komt. De werkgever moet daarom registreren als een werknemer tot deze categorie behoort. Voor werknemers uit deze categorie die tussen 1 januari 2018 en 31 december 2019 zijn aangenomen, geldt deze wachttijd van 13 weken niet.

2.2 | Inspanningen inclusief werkgeven

Uw inspanningen om werknemers met een afstand tot de arbeidsmarkt aan het werk te helpen en te houden, mag u in principe vastleggen. Dan gaat het bijvoorbeeld om informatie over ondersteunende maatregelen, zoals persoonlijke begeleiding, scholing en aanpassing van functie, werkplek, werktijden of productienorm. Over deze gegevens mag u echter niet zodanig rapporteren, intern noch extern, dat de informatie kan worden herleid tot een individuele werknemer. Bij werknemers die behoren tot de doelgroep van de banenafpraak is dit risico eerder aanwezig dan bij andere collega's, omdat het doorgaans om een vrij kleine groep gaat. Kortom: rapportage is alleen toegestaan als de gegevens niet individueel herleidbaar zijn.

2.3 | Uitkeringsverleden

De werkgever mag in principe niet vragen en vastleggen of de werknemer in het verleden een specifieke uitkering heeft gehad, bijvoorbeeld een Wajong-uitkering. In verband met de wettelijke verplichting die de werkgever kan hebben op grond van de WIA mag de werkgever wel een beslissing van UWV verwerken. Wanneer een werknemer tijdens het dienstverband in aanmerking komt voor een WIA-uitkering, ontvangt de werkgever een kopie van de beslissing van UWV.

2.4 | Etniciteit en geboorteland

Gegevens over de etniciteit van medewerkers mag u niet verwerken in uw personeelsadministratie ('tenzij'; zie paragraaf 1.2). Een uitzondering is alleen mogelijk als deze gegevens nodig zijn om voorkeursbeleid te voeren. En dan nog slechts als de etnische of culturele minderheidsgroepering in uw bedrijf aantoonbaar een achterstand heeft. In het kader van het voorkeursbeleid mag u alleen gegevens over het geboorteland of dat van ouders of grootouders verwerken in uw personeelsadministratie, als de betrokkenen daartegen geen schriftelijk bezwaar hebben gemaakt. Zo'n bezwaar mogen zij op elk moment en zonder opgaaf van redenen indienen. In dat geval moet u de verwerking van de gegevens onmiddellijk beëindigen.

3 Toegang en rapportage

3.1 | Toegang

Als werkgever mag u een administratie bijhouden ten behoeve van de medewerkers uit de doelgroep van de banenafpraak. Deze registratie is alleen toegankelijk voor medewerkers die de gegevens nodig hebben om hun werkzaamheden uit te oefenen. Medewerkers personeelszaken of direct leidinggevendenden die de premiekorting moeten realiseren, bijvoorbeeld. Zij moeten een schriftelijke geheimhoudingsverklaring ondertekenen.

3.2 | Anonimiseren

Als het gaat om geanonimiseerde persoonsgegevens, bent u niet meer gebonden aan de Wet bescherming persoonsgegevens. Dit anonimiseren moet wel zorgvuldig gebeuren, zodat de gegevens nooit meer zijn te herleiden tot individuele medewerkers. Het gaat om het theoretische herkenningsrisico: iemand is identificeerbaar als zijn identiteit redelijkerwijs, zonder bovenmatige inspanning, kan worden vastgesteld. Als er een theoretisch herkenningsrisico bestaat, en er dus geen sprake is van werkelijke anonimisering, moet u de AVG toch in acht nemen.

3.3 | Derden

Soms vragen derden om privacygevoelige informatie over uw medewerker(s). Gemeenten die social-returnbeleid voeren bijvoorbeeld, of instellingen die willen beoordelen of uw organisatie in aanmerking komt voor een certificaat voor sociaal ondernemen. Hierbij moet u rekening houden met de privacywetgeving met alle beperkingen van dien, zoals hierboven uiteengezet. Bij twijfel is het verstandig om de zaak aan de Autoriteit Persoonsgegevens voor te leggen. Zo beperkt u het risico op een boete, aansprakelijkheid en imago-schade. Vooral het vereiste 'expliciete individuele toestemming op basis van goede informatie' is in de praktijk vaak een knelpunt.

Colofon

Dit is een uitgave van AWWN. De publicatie is totstandgekomen met steun van Start Foundation.

Postbus 93050
2509 AB Den Haag
www.awvn.nl

Tekst: AWWN
Vormgeving: titusvormgeving.nl
Druk: AWWN

© 2018. Alle rechten voorbehouden. Ondanks de zorgvuldigheid die aan deze uitgave is besteed, kan de uitgever geen aansprakelijkheid aanvaarden bij eventuele onjuistheden. Aan de inhoud van deze publicatie kunnen dus geen rechten worden ontleend.

The logo for AWWN, consisting of the letters 'AWVN' in a bold, blue, sans-serif font.

Gesteund door  Start
Foundation

The logo for VNO NCW, featuring the letters 'VNO' and 'NCW' in a teal, sans-serif font, with a horizontal line underneath.The logo for MKB Nederland, featuring the letters 'MKB' in a bold, black, sans-serif font with an orange wave-like graphic above it, and the word 'Nederland' in a smaller, orange, sans-serif font below it.The logo for DE NORMAALSTE ZAAK, featuring a stylized graphic of two overlapping circles (one blue, one red) on the left, and the text 'DE NORMAALSTE ZAAK' in a blue, sans-serif font on the right.