

Nieuwsbrief

PRIVACY ARBEIDSRECHT-SPECIAL

INHOUDSOPGAVE

De zieke werknemer Caro Mennen, Utrecht	1
Controle en het monitoren van werknemers. Mag dan niets meer? Elif Barioglu, Rotterdam	3
Hoe zit het ook alweer met identificatie, kopietje paspoort en BSN Ellen Timmer, Rotterdam	5
Privacy in een sollicitatieprocedure Jeroen Belderok, Rotterdam	6
Opvragen van personeelsgegevens Xander Alders, Rotterdam	7

De zieke werknemer

Iedere onderneming krijgt te maken met zieke werknemers. De werknemer vertelt bij zijn of haar ziekmelding vaak uit zichzelf wat hem of haar mankeert. De werkgever op haar beurt stelt vragen en verwerkt alle informatie in haar (verzuim) systemen. Wanneer de relatie tussen werkgever en werknemer goed is, zal het contact over de ziekte van de werknemer en het delen van informatie daarover plaatsvinden vanuit wederzijdse betrokkenheid. Dit neemt echter niet weg dat de wet grenzen stelt aan de gegevens die een werkgever over een zieke werknemer mag verwerken. Veel werkgevers zijn zich hier niet of onvoldoende van bewust. Reden om in dit artikel de hoofdlijnen van gegevensverwerking van zieke werknemers nog eens kort op een rijtje te zetten.

ZIEKMELDING

Wanneer een werknemer zich ziek meldt, mag een werkgever alleen die gegevens registreren, die

noodzakelijk zijn voor de beoordeling van de impact die de ziekmelding heeft op de gang van zaken binnen de onderneming van de werkgever. Dit is slechts de volgende informatie: vermoedelijke duur van het verzuim, telefoonnummer en (verpleeg)adres, stand van werkzaamheden en lopende afspraken. Een werkgever mag niet vragen naar informatie over (de aard van) de ziekte. Wel mag de werkgever vragen of de ziekte ertoe leidt dat de werknemer onder een van de vangnetbepalingen van de Ziektewet valt (maar niet onder welke bepaling), of de ziekte verband houdt met een arbeidsongeval en of er sprake is van een (verkeers)ongeval waarbij een derde betrokken is. Deze vragen zijn voor de werkgever relevant vanwege de mogelijkheid een verzekering of derde aan te spreken voor de schade die de werkgever door het verzuim lijdt.

De werknemer kan die informatie natuurlijk wel uit eigen beweging verstrekken. De werkgever mag die informatie echter nergens registreren. Dit is niet anders wanneer de werknemer daarvoor toestemming geeft. In de relatie tussen een werkgever en een werknemer wordt toestemming zelden of nooit gezien als een rechtmatige grondslag om gegevens van een werknemer te verwerken, omdat de werknemer in een (financieel) afhankelijke positie verkeert ten opzichte van de werkgever.

ZIEKTEVERZUIMBEGELEIDING

Wanneer een werknemer langdurig(er) ziek is, zal een arbodienst of bedrijfsarts worden ingeschakeld. Een werknemer is verplicht om de vragen van de bedrijfsarts te beantwoorden. Bedrijfsartsen moeten op hun beurt terughoudend zijn met het verstrekken van die informatie aan werkgevers. Een werkgever mag uitsluitend die informatie krijgen die noodzakelijk is voor een beslissing over loondoorbetaling, verzuimbegleiding en re-integratie. Over de ziekte van de werknemer mag de bedrijfsarts uitsluitend de volgende informatie verstrekken: de werkzaamheden die de werknemer kan uitvoeren of juist niet meer kan uitvoeren, de verwachte duur van het verzuim, de mate van arbeidsongeschikt-

PRIVACY ARBEIDSRECHT-SPECIAL

heid en eventueel advies over aanpassingen en werkvoorzieningen die de werkgever voor de re-integratie van de werknemer moet treffen. Een werkgever mag deze gegevens van de arbodienst of bedrijfsarts wel verwerken in haar administratie. Alle andere gegevens over de zieke werknemer zoals de diagnose, specifieke klachten, afspraken met therapeuten etc. mag een werkgever niet verwerken.

De werkgever kan ook een re-integratiebedrijf inschakelen. Ook aan een re-integratiebedrijf mag een werkgever geen gezondheidsgegevens over de werknemer verstrekken.

Dit kan anders zijn wanneer die gegevens noodzakelijk zijn voor de re-integratieactiviteiten die het re-integratiebedrijf gaat uitvoeren. In zo'n geval ontvangt het re-integratiebedrijf uitsluitend die informatie die zij in dat kader nodig heeft.

Een werkgever is verplicht om het ziekteverzuim en de re-integratieactiviteiten bij te houden in het re-integratiedossier. Hierin zijn onder meer het advies van de bedrijfsarts, het plan van aanpak dat werkgever en werknemer samen opstellen en een weergave van de re-integratieactiviteiten opgenomen. Indien re-integratie niet succesvol is, dan stelt de werkgever in overleg met de werknemer uitsluitend het eerste deel van het re-integratieverslag op. Het tweede deel bevat de medische gegevens en wordt dan ook door de bedrijfsarts opgesteld, zodat de werkgever niet over die gegevens kan beschikken.

BEVEILIGING

Ziekteverzuim wordt vaak geadministreerd in digitale verzuimsystemen. Ook hiervoor gelden een aantal aandachtspunten. Privacy wetgeving vereist dat er passende technische en organisatorische beveiligingsmaatregelen worden getroffen. Wanneer

die systemen via het internet toegankelijk zijn, moet de portal beveiligd zijn met een zogenaamde tweefactor-authenticatie. Dit betekent dat naast het wachtwoord ook een andere toegangscode moet worden ingevoerd, bijvoorbeeld een code die per sms wordt toegestuurd. Daarnaast dienen beveiligingsrisico's periodiek in kaart te worden gebracht. Dit kan door middel van een penetratietest of securityscan.

BEWAARTERMIJNEN

Uitgangspunt is dat persoonsgegevens niet langer dan noodzakelijk voor de doeleinden waarvoor ze werden verzameld, mogen worden bewaard. De bewaartermijn van de administratieve verzuimgegevens en het re-integratiedossier bedraagt voor de werkgever in beginsel twee jaar na afloop van de arbeidsrelatie. Uitzonderingen hierop zijn de werkgevers die eigenrisicodrager voor de Ziektewet of WGA zijn. In die gevallen is de bewaartermijn respectievelijk vijf en tien jaar na afloop van de arbeidsrelatie. Van de bewaartermijn tot twee jaar na afloop van de arbeidsrelatie kan worden afgeweken wanneer er sprake is van een (juridisch) conflict waarvoor deze gegevens belangrijk zijn. Na afloop van de bewaartermijn moeten de gegevens door een werkgever worden vernietigd.



Controle en het monitoren van werknemers. Mag dan niets meer?

In de 'wandelgangen' horen we steeds meer geluiden over de vergaande privacy en bescherming van werknemers. Privacy van werknemers zou steeds de voorkeur krijgen boven het belang van de werkgever om hen te controleren en te monitoren. De werkgever zou altijd aan het kortste eind trekken. Is dit wel het geval? Mag dan echt niets meer?

ALGEMEEN

In deze tijd van ver ontwikkelde technologie en computersystemen, zijn er verschillende mogelijkheden om (al dan niet automatisch) allerlei gegevens en informatie over het eigen personeel te verzamelen. Denk daarbij bijvoorbeeld aan cameratoezicht, toegangspoorten en telefooncentrales. Maar met welk doel? Vaak wordt vorenbedoelde informatie gebruikt om het personeel te controleren. Is dit op grond van de Wet bescherming persoonsgegevens toegestaan? Wat mag wel en wat niet?

CAMERATOEZICHT

Een camera is een vorm van een personeelsvolgsysteem, zelfs als de camera niet als zodanig wordt gebruikt. Indien een werkgever van plan is een camera te gaan gebruiken, dan dient dit eerst aan de ondernemingsraad (indien aanwezig) te worden voorgelegd. Zonder toestemming van de ondernemingsraad is het gebruik van een personeelsvolgsysteem niet toegestaan. Daarnaast dient separaat en expliciet te worden vastgelegd wat het doel van het betreffende personeelsvolgsysteem is. Is het bijvoorbeeld bedoeld om personeel te kunnen aanspreken op hun functioneren? Dan dient dit vooraf duidelijk te zijn bij het personeel. Personeelsleden kunnen niet aan de hand van camerabeelden op hun functioneren worden aangesproken, als ze ervan uitgingen dat de camera's enkel uit veiligheidsoverwegingen waren opgehangen.

Werkgevers dienen zich voor het ophangen van de camera's de volgende vragen te stellen: (i) heb ik een gerechtvaardigd belang (bijvoorbeeld het tegengaan van diefstal)? en (ii) is het noodzakelijk? Als het doel (het tegengaan van diefstal) op een andere, minder ingrijpende manier kan worden bereikt, dan zal de werkgever die andere manier moeten gebruiken. Daarnaast moet de werkgever de betrokken belangen tegen elkaar afwegen, het voornemen met de ondernemingsraad afstemmen en het personeel informeren. De camerabeelden mogen vervolgens niet langer dan noodzakelijk worden bewaard.

E-MAILVERKEER

Mag een werkgever de emailberichten in de zakelijke emailaccount van werknemers lezen?

E-mailberichten behoren tot het privé domein van een werknemer, zelfs al zijn deze gedurende werktijd verstuurd vanaf de werkplek met het zakelijke e-mailadres.

Vanwege het privé karakter van de mailberichten van de werknemer en het recht op privacy mag de werkgever zich slechts in uitzonderlijke gevallen toegang verschaffen tot de e-mailbox van een werknemer. De werkgever mag dit alleen indien: (i) er een gerechtvaardigd belang is om de mailberichten te controleren, (ii) de werknemers op de hoogte zijn van de mogelijke controle en (iii) er voldaan is aan de proportionaliteits eis.



Van een gerechtvaardigd belang kan sprake zijn indien bijvoorbeeld het vermoeden is ontstaan dat een medewerker fraudeert, bedrijfsgeheimen aan de concurrent onthult of zich onheus over de werkgever uit. De proportionaliteits eis houdt in dat de inbreuk op de privacy van de werknemers in verhouding moet staan met het belang van de werkgever.

Sommige werkgevers stellen een reglement op waarin wordt bepaald in welke situaties (zakelijke) e-mailberichten kunnen worden gecontroleerd. Dit is zeker aan te bevelen. Een dergelijk reglement komt immers de duidelijkheid ten goede en daarin kan aandacht worden besteed aan de bovenstaande vragen en antwoorden. Uit de rechtspraak volgt dat indien er geen reglement is opgesteld, de belangenafweging tussen het belang van de werkgever om mails te controleren en het recht op privacy van de medewerker strenger zal worden getoetst.

Overigens mag een werkgever emailberichten in een tijdens werktijd gebruikt privé account van een werknemer in geen enkel geval lezen.

ALCOHOL-EN DRUGSCONTROLE

Op de website van de Autoriteit Persoonsgegevens (AP) is te lezen dat Energiebedrijf Uniper (tot 1 januari 2016 E.ON) na onderzoek van de AP haar alcohol- en drugscontrolebeleid voor werknemers heeft ingetrokken. Uniper was van plan gegevens over de gezondheid van medewerkers te verwerken. De AP heeft geconstateerd dat dit beleid in strijd is met de Wbp. Uniper voldeed niet aan de proportionaliteitstoets en kon haar gerechtvaardigd belang om dergelijke testen te verrichten onder haar personeel niet aantonen.

Door het inzetten van alcohol- en drugstesten worden medische gegevens van werknemers verwerkt. Medische gegevens zijn bijzondere persoonsgegevens en zijn per definitie privacygevoelig. Bijzondere persoonsgegevens mogen maar in een beperkt aantal gevallen worden verwerkt. Denk in dit kader bijvoorbeeld aan drugstesten voor vliegtuig-personeel.

TOT SLOT

Werkgevers mogen hun personeel niet zomaar monitoren en/of controleren. Werkgevers dienen steeds rekening te houden met de privacy van de werknemers. Controle van personeel is toegestaan als dit af en toe gebeurt, de werkgever daar een gerechtvaardigd belang bij heeft en de werkgever voldoet aan de voorwaarden uit de Wet bescherming persoonsgegevens. Bij heimelijk controleren gelden er extra regels.

Hoe zit het ook alweer met identificatie, kopietje paspoort en BSN

Aangezien het kopiëren en overnemen van persoonsgegevens vermeld op identificatiebewijzen risico's kan opleveren op het gebied van identiteitsfraude, is het voor werkgevers en opdrachtgevers belangrijk de regels goed in de gaten te houden.

Om een bepaald persoon te identificeren is het vaak voldoende om het identiteitsbewijs in te zien. Vervolgens is het - behoudens uitzonderingen - verboden om:

- het identiteitsbewijs te kopiëren en te bewaren.
- het burgerservicenummer (BSN) op te nemen in de administratie.

Belangrijke uitzonderingen op het bovenstaande verbod gelden (onder andere) in de sfeer van arbeid.

WERKGEVER

Een werkgever is op grond van de fiscale wetgeving verplicht om bij het aangaan van de arbeidsovereenkomst een kopie van het identiteitsbewijs te maken en deze in de loonadministratie op te nemen. Ook mag de werkgever uiteraard het BSN in de loonadministratie opnemen.

De kopie van het identiteitsbewijs hoeft niet actueel te worden gehouden (dus het mag ook niet). Uitzondering: van werknemers van buiten de Europese Economische Regio (EER) moet de werkgever wél altijd een kopie van een geldig identiteitsbewijs in het personeelsdossier bewaren.

INLENER EN AANNEMER (OPDRACHTGEVER VAN DE ONDERAANNEMER)

Als personeel wordt ingeleend, is de formele werkgever (de uitlener) verantwoordelijk voor de fiscale verplichting een kopie van het identiteitsbewijs te bewaren. De inlener mag dat niet. De uitlener mag de kopieën ook niet aan de inlener geven. Ook hier is een uitzondering voor werknemers van buiten de EER. Voor onderaannemers geldt hetzelfde. Wel mag een inlener bepaalde gegevens van het identiteitsbewijs van een uitgeleende werknemer overnemen.

Op grond van per 1 januari 2017 gewijzigde fiscale wetgeving mogen uitlener en onderaannemer wel het BSN van de uitgeleende werknemers, respectievelijk door de onderaannemer ingezet personeel aan de opdrachtgever (inlener of aannemer) verstrekken.

OPDRACHTGEVER ZZP'ER

Degene die aan zzp'ers opdracht geeft, doet er goed aan om de identiteit van de zzp'er te verifiëren. Het kopiëren van het identiteitsbewijs en het registreren van het BSN is niet toegestaan.

OVERIGE UITZONDERINGEN

Het kopiëren van een identiteitsbewijs en het registreren van een BSN is alleen toegestaan als de wet dat bepaalt. Zo mogen financiële instellingen op grond van de wet een kopie van het identiteitsbewijs maken om te kunnen bewijzen dat zij aan de identificatieplicht hebben voldaan. Zorgverleners moeten het BSN in hun administratie opnemen.



Privacy in een sollicitatieprocedure

Indien een werkzoekende met een potentiële werkgever in contact komt om bij hem in dienst te treden, worden er uiteraard veel persoonsgegevens verwerkt. Ten eerste stuurt een werkzoekende een sollicitatiebrief en zijn curriculum vitae, waarin hij (vrijwillig) bepaalde gegevens verstrekt. Vervolgens wordt de werkzoekende wellicht op een sollicitatiegesprek uitgenodigd, waarbij de potentiële werkgever gegevens over hem kan noteren. Tot slot kunnen een medische of psychologische keuring, dan wel een assessment of andersoortige screening, onderdeel uitmaken van een sollicitatieprocedure. Maar tot op welke hoogte mag de potentiële werkgever, gelet op de Wet bescherming persoonsgegevens ('Wbp'), die persoonsgegevens opslaan en onder zich houden? En in hoeverre mag de potentiële werkgever een werkzoekende screenen?

GERECHTVAARDIGDE DOELEINDEN

Het doel van een sollicitatieprocedure is uiteraard om de geschiktheid van een werkzoekende te beoordelen voor de functie waarop diegene solliciteert. In beginsel mogen in een sollicitatieprocedure daarom slechts persoonsgegevens worden verwerkt voor (i) het beoordelen van de werkzoekende op zijn kwaliteiten voor de opengevallen functie, (ii) de afhandeling van de door de werkzoekende gemaakte onkosten en (iii) het - indien nodig - toegang verlenen aan de werkzoekende tot het gebouw van de potentiële werkgever. De potentiële werkgever behoeft dus in principe niet meer informatie dan nodig is voor bovenstaande doeleinden. Een verdergaande verwerking van persoonsgegevens moet de potentiële werkgever kunnen onderbouwen en moet bij de Autoriteit Persoonsgegevens worden gemeld.

BIJZONDERE PERSOONSGEGEVENS

Let in dit verband op met het verwerken van bijzondere persoonsgegevens. Bijzondere persoonsgegevens zijn gegevens betreffende (onder meer) iemands godsdienst, ras, politieke gezindheid en gezondheid. Dergelijke gegevens zijn niet nodig om de geschiktheid van een werkzoekende te beoordelen voor de functie waarop diegene solliciteert, zodat deze in beginsel niet mogen worden verwerkt. Een potentiële werkgever mag tijdens een sollicitatiegesprek bijvoorbeeld niet vragen naar de gezondheid van een werkzoekende of naar het feit of een werkzoekende zwanger is (of wil worden).

Een werkzoekende dient wel in een sollicitatieprocedure zelf mededelingen te doen over zijn gezondheid, indien dit rechtstreeks van belang is voor de functie waarop diegene solliciteert. Als hij dit niet doet en op een later moment (als werknemer) arbeidsongeschikt uitvalt als gevolg van de verzwegen beperking, kan dit gevolgen hebben voor de rechtspositie van de werknemer (zoals de loondoorbetaling tijdens ziekte). Daarnaast mag een potentiële werkgever in twee gevallen wel vragen naar de gezondheid van de werkzoekende: tijdens de sollicitatieprocedure om te controleren of een werkzoekende behoort tot de doelgroep van de Wet banenafpraak en quotum arbeidsbeperkten (hiertoe mag ook naar het burgerservicenummer worden gevraagd) en na twee maanden dienstverband om te controleren of de werknemer in aanmerking komt voor de no-riskpolis van de Ziektewet.



SCREENING

Ook voor een screening geldt dat een potentiële werkgever slechts die informatie mag verwerken om de geschiktheid van de werkzoekende te beoordelen voor de functie waarop diegene solliciteert. Daarnaast dient een screening proportioneel te zijn. Voor een schoonmaker is op zich geen uitgebreide screening noodzakelijk, maar voor een schoonmaker op Schiphol of voor een beveiligingsmedewerker wellicht wel.

Voor sommige vertrouwensfuncties geldt een wettelijke verplichting tot screening, omdat het voor die functies extra relevant is dat werknemers geen misbruik maken van hun machtspositie of geen strafbare feiten hebben gepleegd die relevant zijn voor de functie. Hierbij kan bijvoorbeeld worden gedacht aan functies in de kinderopvang.

BEWAARTERMIJNEN

Tot slot mogen in het kader van een sollicitatieprocedure verwerkte persoonsgegevens niet tot in lengte van dagen door de potentiële werkgever worden bewaard. De verwerkte persoonsgegevens dienen te worden verwijderd zodra de werkzoekende daarom verzoekt en in ieder geval uiterlijk vier weken nadat de sollicitatieprocedure is geëindigd. Uiteraard kunnen de persoonsgegevens met toestemming van de werkzoekende langer worden bewaard, waarbij een termijn van één jaar redelijk is.

Een potentiële werkgever dient dus goed na te gaan welke informatie hij in een sollicitatieprocedure mag opvragen en verwerken en hoelang hij die informatie mag bewaren.



Opvragen van personeelsgegevens

Iedere werkgever houdt (als het goed is) een personeelsdossier bij van zijn werknemers en verzamelt daarnaast ook andere gegevens over zijn werknemers. Maar heeft een werknemer met een beroep op de Wet bescherming persoonsgegevens ('Wbp') volledige inzage in die gegevens en moet de werkgever die gegevens op verzoek ook aan de werknemer overhandigen? En verandert dit onder de Algemene Verordening Gegevensbescherming ('AVG')?

RECHT OP INZAGE

Iedere werknemer heeft het recht om inzage te krijgen in de verwerking van zijn persoonsgegevens door zijn werkgever. Binnen vier weken na een dergelijk verzoek van de werknemer moet de werkgever onder meer een

overzicht van de verwerkte persoonsgegevens van de werknemer, de redenen waarom die gegevens worden verwerkt en de partijen aan wie die gegevens zijn verstrekt, aan de werknemer verstrekken.

PRIVACY EN SECURITY

De werkgever kan dit verzoek normaal gesproken alleen weigeren ter bescherming van de werknemer of van de rechten of vrijheden van anderen (waaronder de werkgever zelf).

REIKWIJDTE

Moet een werkgever dan alle gegevens aan de werknemer verstrekken? Nee, de werkgever moet slechts die informatie verstrekken die nodig is voor de werknemer om na te gaan of de gegevensverwerking onjuist, onnodig of in strijd met de wet is. In principe is daarvoor voldoende dat een overzicht van de verwerkte persoonsgegevens wordt verstrekt, dus niet de gegevens zelf. Met name indien het gaat om gevoelige gespreksverslagen of juridische adviezen (die al dan niet ook andere werknemers betreffen) zal een werkgever die gegevens liever niet willen overleggen. De werkgever zal daarnaast steeds moeten beoordelen of belangen van anderen niet in het gedrang komen door de werknemer inzage te geven. Ook kan een zwaarwichtig belang van de werkgever om geen inzage te verlenen voorrang krijgen boven het belang bij inzage, maar dat zal niet snel aan de orde zijn.

Steeds moet in gedachten worden gehouden dat het inzagerecht uit de Wbp alleen ziet op persoonsgegevens die geautomatiseerd worden verwerkt of (als niet geautomatiseerd wordt verwerkt) in een bestand zijn opgenomen (dan wel bestemd zijn om daarin te worden opgenomen).

Zo heeft de hoogste bestuursrechter geoordeeld dat een juridisch advies dat alleen op papier beschikbaar

is, niet onder het inzagerecht valt. Hetzelfde geldt voor documenten die geen persoonsgegevens bevatten of voor notities van medewerkers die alleen voor intern overleg zijn bedoeld. Let daarbij wel op de ruime reikwijdte van het begrip 'persoonsgegevens'. Zijn laatstgenoemde notities namelijk in een rapport opgenomen, dan is de Wbp en daarmee het inzagerecht wel weer van toepassing.

De werknemer kan de Wbp dus niet zo maar gebruiken/misbruiken om bijvoorbeeld in een (voorgenomen) ontslagtraject het hele dossier en de (zwakke punten van de) juridische onderbouwing van het voorgenomen ontslag op te vragen. Daar staat tegenover dat werknemers (en betrokkenen in het algemeen) in de Wbp aanzienlijke bescherming genieten en rechters in het verleden regelmatig de kant van de werknemer hebben gekozen in een procedure daarover.

DE ALGEMENE VERORDENING GEGEVENSBESCHERMING

Na inwerkingtreding van de AVG wordt het recht op inzage nog verder uitgebreid, in die zin dat nog meer informatie omtrent de gegevensverwerking aan de werknemer moet worden verstrekt en dat in principe een kopie van de persoonsgegevens moet worden verstrekt. Een overzicht volstaat dan niet meer.

Indien een werkgever een verzoek om inzage krijgt, dan moet hij dus goed nagaan welke gegevens hij kan overhandigen, op welke wijze hij dat dient te doen en of belangen van anderen in het spel zijn.

Pellicaan Advocaten adviseert u graag over de onderwerpen die in deze nieuwsbrief worden behandeld.

ROTTERDAM
Postbus 23161
3001 KD Rotterdam
Tel. +31 (0)88 627 22 87
Fax +31 (0)88 627 22 80
rotterdam.advocaten@pellicaan.nl

AMSTERDAM
Delflandlaan 1
1062 EA Amsterdam
Tel. +31 (0)88 627 22 20
Fax +31 (0)88 627 22 21
amsterdam.advocaten@pellicaan.nl

UTRECHT
Orteliuslaan 1051
3528 BE Utrecht
Tel. +31 (0)88 627 22 60
Fax +31 (0)88 627 22 61
utrecht.advocaten@pellicaan.nl