Auteur: **Anneloes Korremans**

Privacy van zieke werknemers

Terwijl privacy bijna dagelijks aandacht krijgt in de media, blijkt het bij veel bedrijven nog te schorten aan de benodigde aandacht voor dit onderwerp. Met name als het gaat om gegevensverwerking binnen de arbeidsrelatie. Werkgevers verwerken grote hoeveelheden persoonsgegevens over hun werknemers, waaronder gegevens over de gezondheid van werknemers. Gezondheidsgegevens zijn zeer privacy gevoelig en kwalificeren daarom als 'bijzondere persoonsgegevens' in de zin van de Wet bescherming persoonsgegevens (Wbp). Deze gegevens zijn wettelijk goed beschermd en mogen niet zomaar verwerkt worden. Het verwerken van persoonsgegevens omvat vrijwel iedere denkbare handeling met betrekking tot persoonsgegevens, waaronder vastleggen, bijwerken, wijzigen, opvragen, gebruiken en verstrekken.

Privacy is steeds belangrijker en de verwerking van persoonsgegevens wordt daarom steeds verder gereguleerd. Zo publiceerde de Autoriteit Persoonsgegevens (AP) op 21 april 2016 Beleidsregels voor de verwerking van persoonsgegevens over de gezondheid van zieke werknemers en is per 25 mei 2018 de Europese Algemene verordening gegevensbescherming (AVG) van toepassing, ook op arbeidsrelaties.

Ziekmelding

Een werknemer die ziek is en daardoor de bedongen arbeid niet kan verrichten, moet dat zo snel mogelijk melden bij zijn werkgever. Bij de ziekmelding mag de werkgever slechts een beperkt aantal vragen stellen aan de werknemer en een beperkt aantal gegevens verwerken:

- het telefoonnummer en (verpleeg)adres;
- de vermoedelijke duur van het verzuim;
- de lopende afspraken en werkzaamheden;
- of de werknemer onder een van de vangnetbepalingen van de Ziektewet valt (niet onder welke);
- of de ziekte verband houdt met een ongeval;
- of er sprake is van een verkeersongeval met regresmogelijkheid.

Bij een kortdurende ziekteperiode worden vaak niet meer dan bovenstaande (administratieve) gegevens verwerkt. Bij (mogelijke) langdurige arbeidsongeschiktheid moet de werkgever zorgen voor adequate re-integratie en zal een werkgever zich laten bijstaan door een geregistreerde bedrijfsarts of een gecertificeerde arbodienst (hierna zullen we alleen spreken over bedrijfsarts waar beide worden bedoeld).
De bedrijfsarts verwerkt veel gegevens over de gezondheid van de werknemer. Bedrijfsartsen moeten zich bij deze verwerking uiteraard ook aan bepaalde privacywetgeving houden. De bedrijfsarts mag aan de werkgever slechts de volgende gegevens over de gezondheid van de zieke werknemer verstrekken:

- de werkzaamheden waartoe de werknemer nog wel of niet meer in staat is (functionele beperkingen, restmogelijkheden en implicaties voor het soort arbeid dat de werknemer nog kan verrichten);
- de verwachte duur van het verzuim;
- de mate waarin de werknemer arbeidsongeschikt is;
- de eventuele aanpassingen of werkvoorzieningen die de werkgever in het kader van de re-integratie moet treffen.

Alle mogelijke overige gegevens over de gezondheid van werknemers zijn voor de werkgever niet noodzakelijk

Uitklapveld

De Autoriteit Persoonsgegevens (AP) heeft in 2015 een tip ontvangen over een werkgever die in geval van een ziekmelding zelf besloot of een werknemer daadwerkelijk ziek werd gemeld en voor welk percentage. Uit het onderzoek van de AP bleek dat het verzuimsysteem dat de werkgever gebruikte een uitklapveld bevatte waarin de verzuimreden kon worden opgegeven, zoals 'Verkoudheid/griep'. Naast deze mogelijkheid, bood het verzuimsysteem ook de mogelijkheid vast te leggen voor welk percentage de werknemer arbeidsongeschikt was, zonder dat dit percentage werd overgenomen uit een rapportage van een bedrijfsarts. De werkgever kon hiermee meer persoonsgegevens vastleggen dan noodzakelijk. Met enkel het bieden van deze mogelijkheid werd de wet al overtreden, hetgeen voor deze werkgever tot een dwangsom van maximaal € 50.000 heeft geleid.

voor de loondoorbetalingsverplichting, noch voor de re-integratie/verzuimbegeleiding. Deze overige gegevens mogen dan ook niet worden verwerkt door de werkgever.
Het voorgaande betekent dat de werkgever in ieder geval de volgende persoonsgegevens van zieke werknemers niet mag verwerken, ongeacht of deze (spontaan) van de werknemer zelf of van de bedrijfsarts afkomstig zijn:

- diagnose, de naam van de ziekte, specifieke klachten of pijnaanduidingen;
- waarnemingen, zowel over geestelijke als lichamelijke gezondheidstoestand, van de werkgever zelf of van anderen;
- gegevens over therapieën, afspraken met artsen, fysiotherapeuten, psychologen en andere behandelaars;
- overige situationele problemen zoals relatieproblemen, problemen uit het verleden, enzovoort.

Deze medische gegevens mag een werkgever dus ook niet bijhouden in een (intern of extern) verzuimsysteem. Ook mag een bedrijfsarts deze medische gegevens niet opslaan in het verzuimsysteem, als de werkgever dit verzuimsysteem zelf beheert.
Een uitzondering op deze hoofdregel geldt voor gegevens die om een andere reden noodzakelijk zijn om te verwerken. Hierbij kan gedacht worden aan een ziekte waarvan collega's op de hoogte moeten zijn zodat zij (eerste) hulp kunnen verlenen, bijvoorbeeld epilepsie of een ernstige allergie. Deze gegevens mogen wel worden verwerkt door de werkgever.

Bewaartermijnen

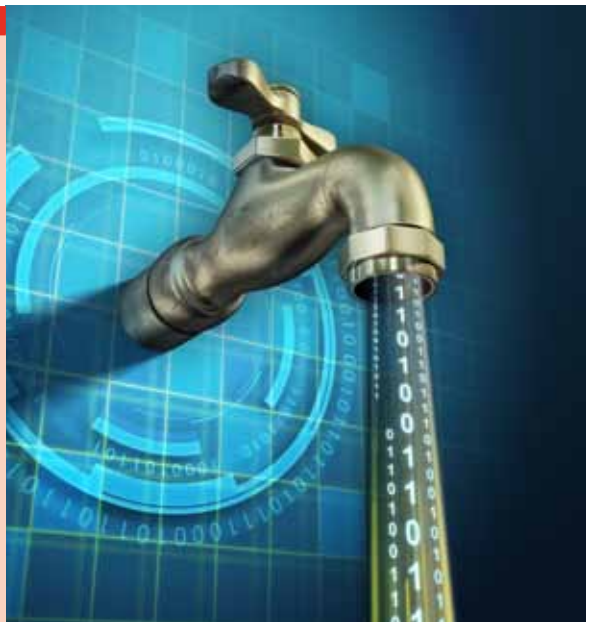
De Wbp verbiedt de werkgever persoonsgegevens van werknemers langer te bewaren dan noodzakelijk voor het doel waarvoor deze zijn verwekt. De AP meent dat bij een korte periode van ziekte – waarbij doorgaans enkel sprake is van administratieve verzuimgegevens – deze niet langer dan twee jaar na afloop van de arbeidsrelatie bewaard hoeven worden. Bij een langdurige periode van ziekte – waarbij een re-integratiedossier is bijgehouden – is de bewaartermijn niet langer dan twee jaar na afronding van de re-integratie. Voor eigenrisicodragers geldt een langere bewaartermijn, omdat zij ook na uitdiensttreding verantwoordelijk blijven voor de re-integratie.

Beveiliging

Veel werkgevers gebruiken verzuimsystemen voor het verwerken van medische gegevens van werknemers. De Wbp verplicht werkgevers de persoonsgegevens van werknemers te beveiligen tegen verlies en onrechtmatige verwerking, door middel van 'passende technische en organisatorische maatregelen'. Ten aanzien van een verzuimsysteem betekent dit onder meer dat naast identificatie via een gebruikersnaam en een wachtwoord, ie-

Meldplicht datalekken

Een datalek moet (ook) door een werkgever binnen 72 uur worden gemeld bij de AP. Een datalek is iedere schending van het technische beveiligingsbeleid of het organisatorische beveiligingsbeleid. Er is al snel sprake van een datalek als persoonsgegevens betrokken zijn. Bijvoorbeeld bij een virus of als een onbevoegd persoon inzage krijgt in het verzuimsysteem of personeelsdossier. Een datalek is ook het verliezen van een USB-stick met daarop persoonsgegevens. Het niet naleven van deze meldplicht kan grote (financiële) gevolgen hebben en vraagt daarom om permanente aandacht binnen de organisatie.



mand ook nog op een andere manier zijn identiteit moet aantonen om toegang te krijgen tot het systeem (meerfactorauthenticatie). In de Richtsnoeren beveiliging persoonsgegevens gaat de AP nader in op de beveiligingsmaatregelen die in acht moeten worden genomen.

Handhaving

De AP is bevoegd tot het instellen van een onderzoek naar de verwerking van persoonsgegevens. Een onderzoek kan uit eigen beweging gestart worden, maar ook naar aanleiding van een ontvangen tip of actuele gebeurtenis. Constateert de AP tijdens een onderzoek een overtreding, dan is zij in beginsel verplicht tot handhaving over te gaan. De AP heeft de mogelijkheid boetes op te leggen tot maximaal € 820.000 of 10% van de netto jaaromzet. Voordat een boete wordt opgelegd, moet de AP in beginsel eerst een zogenoemde bindende aanwijzing geven.
In principe worden alle bevindingen van de AP openbaar gemaakt, zodat naast het boete risico ook een groot risico op reputatieschade op de loer ligt bij overtreding van privacywetgeving.

Algemene Verordening Gegevensbescherming

Vanaf 25 mei 2018 is de AVG van toepassing, als gevolg waarvan de Wbp komt te vervallen en er één privacywet is in de EU (i.p.v. 28 nationale wetten). Als de AVG van toepassing is, hebben organisaties die persoonsgegevens verwerken meer verplichtingen. Er wordt in de AVG meer nadruk gelegd op de verantwoordelijkheid van organisaties zelf om de wet na te leven én om te kunnen aantonen dat zij zich aan de wet houden (accountability). Hoewel de basisprincipes niet veel anders zijn dan de huidige Wbp, zijn er toch een aantal wijzigingen die ingrijpende gevolgen zullen hebben. Nieuw zijn onder meer het – in een groot aantal gevallen – verplicht aanwijzen van een functionaris gegevensbescherming (FG) en het uitvoeren van Privacy Impact Assessment (PIA). Een FG houdt binnen de organisatie toezicht op de toepassing en naleving van privacywetgeving en een PIA is een instrument om voorafgaand aan iedere verwerking de privacy risico's in kaart te brengen. Verder krijgen werknemers meer rechten ten aanzien van hun persoonsgegevens.
Nederland kiest vooralsnog voor een beleidsneutrale uitvoering van de AVG. Dat wil zeggen dat het bestaande recht over de verschillende bepalingen onder meer op het gebied van verwerking van persoonsgegevens in de arbeidsverhouding – zoals hierboven uiteengezet – zoveel mogelijk wordt gehandhaafd. Met de invoering van AVG wordt de AP bevoegd hogere boetes op te leggen: maximaal € 20.000.000 per overtreding of 4% van de wereldwijde jaaromzet. De AP is verder niet langer verplicht eerst een bindende aanwijzing te geven.

Conclusie

De werkgever verwerkt veel gegevens van (zieke) werknemers en is er voor verantwoordelijk dat de verwerking van deze persoonsgegevens aan de wettelijke vereisten voldoet. Met name van belang is dat niet méér gegevens worden verwerkt dan noodzakelijk en dat persoonsgegevens goed worden beveiligd. Het is aan te bevelen om de regels strikt na te leven, gelet op de (torenhoge) boetes van de AP. De boetes zijn veelal veel hoger dan de kosten van het vernieuwen van software en/of beleid. Ondernemingen hebben nog maar één jaar om zich op de AVG voor te bereiden. Het is verstandig om nu al met de voorbereidingen te starten en de OR daar tijdig bij te betrekken. Een goede voorbereiding is het immers het halve werk. ■

mr. A.M. Korremans, *De Clercq Advocaten Notariaat, www.declercq.com*

Rol ondernemingsraad

De ondernemingsraad (OR) heeft instemmingsrecht bij diverse regelingen op het gebied van ziekteverzuim en privacy van werknemers:
- **de keuze van de arbodienst;**
- **het afsluiten en wijzigen van het contract met de arbodienst;**
- **een regeling op het gebied het ziekteverzuim en re-integratiebeleid;**
- **een regeling omtrent het verwerken van alsmede de bescherming van de persoonsgegevens van de in de onderneming werkzame personen;**
- **het invoeren van personeelscontrolesystemen;**
- **het aanstellen/aanwijzen van een functionaris voor gegevensbescherming (FG).**

Wet: art. 10, 12, 16, 21, 23, 35, 60, 65 Wbp; art. 14, 20 Arbeidsomstandighedenwet; art. 5:2 lid 1 onder b Awb; art. 88 Wet BIG; Wet uitbreiding loondoorbetaling bij ziekte; art. 7:629 lid 3 BW; Algemene Verordening Gegevensbescherming (AVG); Uitvoeringswet Algemene Verordening Gegevensbescherming (AVG); Wet verbetering poortwachter; art. 27 WOR

Jurisprudentie: AP 6-10-2016, z2016-00165

Bron: Autoriteit Persoonsgegevens 21-04-2016, Beleidsregels voor de verwerking van persoonsgegevens over de gezondheid van zieke werknemers (Stcrt 2016, 21703)