Leidraad **Bedrijfsarts en privacy** anno 2019

De situatie na invoering van de AVG

HOE OM TE GAAN MET PRIVACYGEVOELIGE INFORMATIE IN DE BEDRIJFSGEZONDHEIDSZORG EN IN HET BIJZONDER MET MEDISCHE GEGEVENS BIJ ZIEKTEVERZUIMBEGELEIDING.

OVAL

Nederlandse Vereniging voor Arbeids- en Bedrijfsgeneeskunde nvab

14 OKTOBER 2019

Inhoud

Inleiding

In alle lidstaten van de Europese Unie is sinds 25 mei 2018 de Algemene verordening Gegevensbescherming (AVG)[1] rechtstreeks van toepassing. De AVG en de bijbehorende Uitvoeringswet AVG (UAVG)[2] hebben de Wet bescherming persoonsgegevens (Wbp) vervangen. De AVG is onder andere bedoeld om de bescherming van natuurlijke personen in verband met de verwerking van hun gegevens te waarborgen. Behalve de AVG zijn voor de bedrijfsgezondheidszorg in verband met privacy van de werknemer ook de Wet geneeskundige behandelingsovereenkomst (WGBO)[3] en de Wet beroepen individuele gezondheidszorg (Wet BIG)[4] onverminderd relevant. De in deze wetten beschreven rechten en plichten inzake dossierplicht, patiënten-rechten en beroepsgeheim zijn ook na invoering van de AVG van toepassing.
De AVG en enkele andere wijzigingen noopten tot herziening van de leidraad Bedrijfsarts en privacy (NVAB, BoaBorea; 2011).

De aandacht voor de privacy van de werknemer en de (on)mogelijkheden van de werkgever in het bijzonder bij ziekteverzuimbegeleiding zijn flink toegenomen sinds de inwerkingtreding van de AVG. De bedrijfsarts wordt geconfronteerd met deze (on)mogelijkheden en is zich nog meer dan voorheen bewust van de grenzen van zijn beroepsgeheim. Met regelmaat rijzen er vragen over wat wel en wat niet geoorloofd is wanneer het bijzondere persoonsgegevens betreft. Voor de bedrijfsarts en ook voor de werkgever (leidinggevende en/of personeelsfunctionaris en/of andere vertegenwoordigers) en de werknemer is niet altijd duidelijk welke informatie wanneer mag worden uitgewisseld en met wie. Andere vragen die spelen zijn bijvoorbeeld: maakt het verschil of de betrokken medewerker ziek is of niet? Hoe verhoudt privacy zich tot de verplichtingen op basis van de Wet verbetering poortwachter (Wvp)[5] en de Regeling Procesgang 1e en 2e ziektejaar[6]?

De Autoriteit Persoonsgegevens (AP) geeft in de publicatie 'De zieke werknemer' richtlijnen voor de voor re-integratie benodigde informatie-uitwisseling. Deze richtlijnen blijven ook na invoering van de AVG en de uitvoeringswet AVG van kracht. Net zoals de AP zijn NVAB en OVAL van mening dat de privacy van de werknemer en het zorgvuldig omgaan met het medisch beroepsgeheim belangrijk zijn. Naleving van wet- en regelgeving hieromtrent is dan ook van belang, maar in de praktijk is hier regelmatig verwarring over.

Hoewel in diverse stukken[7] aandacht wordt besteed aan en regels worden gegeven over het omgaan met privacygevoelige informatie is er behoefte aan één duidelijke leidraad die het onderwerp privacygevoelige (medische) informatie op een praktische wijze behandelt, in het bijzonder voor bedrijfsartsen.
De Nederlandse Vereniging voor Arbeids- en Bedrijfsgeneeskunde (NVAB) heeft samen met OVAL deze leidraad tot stand gebracht.

De AVG in een notendop
(zie voor meer info Deel 2 'Achtergronddocument-AVG')

De AVG zorgt onder meer voor:
- versterking en uitbreiding van privacyrechten van betrokkenen;
- meer verantwoordelijkheden voor organisaties;
- stevige bevoegdheden voor de toezichthouder.

De AVG geldt in alle landen van de Europese Unie. Lidstaten hebben de mogelijkheid om ten aanzien van bepaalde onderwerpen specifieke bepalingen in de

1 de Algemene verordening Gegevensbescherming (AVG)
2 Uitvoeringswet Algemene verordening gegevensbescherming (UAVG)
3 Wijzigingswet Burgerlijk Wetboek, enz. (geneeskundige behandelingsovereenkomst) (WGBO)
4 Wet op de beroepen in de individuele gezondheidszorg (wet BIG)
5 Wet verbetering poortwachter (Wvp)
6 Regeling procesgang eerste en tweede ziektejaar
7 Niet uitputtende lijst:
- KNMG-richtlijn Omgaan met medische gegevens, (KNMG, mei 2018)
- De zieke werknemer, Beleidsregels voor de verwerking van persoonsgegevens over de gezondheid van zieke werknemers (AP, 2016)
- De inrichting van bedrijfsgeneeskundige dossiers (KNMG, 2008)
- Code gegevensverkeer en samenwerking bij arbeidsverzuim en re-integratie (KNMG, dec. 2007)

nationale wetgeving op te nemen. In Nederland zijn die opgenomen in de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG).

Op hoofdlijnen zijn er twee thema's te onderscheiden, namelijk de privacyrechten van het individu (de betrokkene) inzake de verwerking van zijn persoonsgegevens en de plichten voor organisaties die persoonsgegevens verwerken. Voor zover het gaat om de gegevensverwerking zelf zijn er slechts een paar nieuwe items. Het recht op dataportabiliteit en het recht om vergeten te worden zijn twee nieuwe rechten voor het individu. Voor de rechten van cliënten/werknemers in de individuele bedrijfsgezondheidszorg zijn de veranderingen minimaal temeer daar de reeds geldende patiëntenrechten mede op grond van de WGBO al uitgebreider waren dan in de Wet bescherming persoonsgegevens (Wbp) beschreven. Deze waren al vergelijkbaar met het niveau dat de AVG verlangt met uitzondering van de nieuwe rechten.

Het vernieuwende is vooral gelegen in de regels waaraan organisaties die persoonsgegevens verwerken moeten voldoen om naleving van de regels structureel te borgen en daarover verantwoording af te leggen. De sanctiemogelijkheden van de toezichthouders (voor Nederland de Autoriteit Persoonsgegevens) zijn flink verruimd. De Autoriteit Persoonsgegevens (AP) mag boetes opleggen tot maximaal € 20 miljoen of 4% van de (wereldwijde) jaaromzet indien dat cijfer hoger is dan € 20 miljoen.

In deze leidraad staan de gegevensverwerking en de rechten van cliënten (hier bedoelen we de werknemers; zij zijn betrokkenen in de zin van de AVG) centraal. De verplichtingen voor organisaties (arbodiensten, maatschappen en andere samenwerkingsverbanden dan wel zelfstandige bedrijfsartsen) worden op hoofdlijnen vermeld in *deel 2*. Voor uitgebreide informatie verwijzen we naar de website van de AP.[8]

Leeswijzer

Deel 1 beschrijft het doel van de leidraad, verantwoordelijkheden van bedrijfsarts en werkgever, de rechten van cliënten (in deze ook patiëntenrechten genoemd) en geeft praktische handvatten voor de dagelijkse praktijk. Aan de hand van drie hoofdonderwerpen wordt uitgewerkt hoe de bedrijfsarts dient om te gaan met privacygevoelige informatie, in het bijzonder met medische persoonsgegevens. Tevens wordt aandacht besteed aan een aantal bijzondere situaties.

In *deel 2* vindt u juridische achtergrondinformatie met een beknopte uitleg over de meest relevante elementen van de AVG.
Een begrippenlijst vindt u in *bijlage 1*.

8 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving

DEEL 1
De Leidraad

In dit deel van de leidraad vindt u in *hoofdstuk 1* informatie over doelstelling en reikwijdte van de leidraad en over de verantwoordelijkheden van bedrijfsarts en werkgever wanneer het gaat om het uitwisselen van medische gegevens. Vervolgens worden in *hoofdstuk 2* drie essentiële onderwerpen toegelicht die in de praktijk bepalend zijn voor het al of niet mogen verstrekken van gegevens aan derden. In *hoofdstuk 3* wordt een aantal praktijksituaties besproken die knelpunten kunnen opleveren. Tenslotte komt in *hoofdstuk 4* het digitaal verzenden van vertrouwelijke informatie aan bod.

Hoofdstuk 1

1.1 Doelstelling

Het doel van deze leidraad is om duidelijkheid te geven over hoe bedrijfsartsen dienen om te gaan met privacygevoelige medische informatie en in het bijzonder met informatie die noodzakelijk is in verband met re-integratie van een arbeidsongeschikte werknemer.

1.2 Doelgroep

De leidraad is primair bedoeld voor bedrijfsartsen en andere artsen werkzaam in de bedrijfsgezondheidszorg. Ook voor andere hulpverleners, voor werkgevers en werknemers is het interessant om van deze leidraad kennis te nemen.

Uitgangspunten zijn

- dat de re-integratie van de arbeidsongeschikte werknemer wordt bevorderd en niet belemmerd mag worden vanwege onvoldoende informatie of het ontbreken daarvan;
- dat gegevensverwerking en dat gegevensverstrekking plaats dient te vinden binnen de wettelijke kaders ter bescherming van de privacy.

1.3 Reikwijdte

Deze leidraad beperkt zich tot informatie-uitwisseling met werkgevers of voor deze werkzame personen die door de werkgever zijn ingeschakeld met het oog op de re-integratie van de werknemer en informatie-uitwisseling met re-integratiebedrijven. Informatie-uitwisseling met het UWV is ook zonder toestemming van de werknemer toegestaan[9]. Voor overige derden zoals verzekeraars, advocaten en gemachtigden geldt dat informatie-uitwisseling alleen met uitdrukkelijke en gerichte (ondubbelzinnige) toestemming is toegestaan. De specifieke regelgeving over uitwisseling met deze derden valt buiten de reikwijdte van deze leidraad.
In de uitgave 'De zieke werknemer'; beleidsregels (AP, 2016), is uitgebreide informatie te vinden over informatie-uitwisseling met andere partijen. De 'Code gegevensverkeer en samenwerking bij arbeidsverzuim en re-integratie' (KNMG, 2006) is van belang voor gegevensuitwisseling tussen artsen (curatief werkende artsen, bedrijfsartsen en verzekeringsartsen).

1.4 Vooraf

De AVG vereist dat verwerking van algemene en bijzondere persoonsgegevens berust op een van de grondslagen zoals opgenomen in art. 6 AVG[10]. Het verwerken van bijzondere persoonsgegevens is niet toegestaan tenzij een van de uitzonderingssituaties die in art. 9 AVG[11] staan genoemd van toepassing is. In de AVG[12] is specifiek benoemd dat verwerking van gezondheidsgegevens waaronder die voor preventieve en arbeidsgeneeskunde en de beoordeling van arbeidsgeschiktheid van de werknemer is toegestaan.

1.5 Verantwoordelijkheid bedrijfsarts

De verantwoordelijkheden van de bedrijfsarts zijn uitgebreid beschreven in Kernwaarden van de Bedrijfsarts (NVAB, 2012) en het Professioneel Statuut. Voor taken en verantwoordelijkheden bij arbeidsverzuim bestaat een aparte richtlijn[13]. De verantwoordelijkheden die van belang zijn in verband met informatieverstrekking aan werkgever en re-integratiebedrijf zijn:

- De bedrijfsarts is adviseur voor zowel werknemer als werkgever. Hij houdt op zorgvuldige wijze een medisch dossier bij (WGBO, artikel 7:454 BW)[14].
- De bedrijfsarts dient de werknemer te informeren over zijn conclusie en advies. Hij dient zich een oordeel te vormen over welke gegevens hij aan wie verstrekt en of hij de gerichte toestemming van de werknemer nodig heeft om zijn beroepsgeheim te mogen doorbreken. De bedrijfsarts informeert de werknemer voorafgaand aan de feitelijke informatieverstrekking aan derden ongeacht of toestemming nodig is of niet.
  Het toestemmings- en noodzakelijkheidsvereiste vormen een belangrijk kader voor de afweging van de bedrijfsarts.

9 Artikel 54 Wet structuur uitvoeringsorganisatie werk en inkomen

10 Art. 6 AVG "Rechtmatigheid van de verwerking"

11 Art. 9 sub b en Art. 9 sub h AVG en Art. 30 UAVG

12 Art.9 AVG lid 2 sub h AVG

13 Taken en verantwoordelijkheden van de bedrijfsarts in het kader van de verzuimbegeleiding en re-integratie (KNMG, 2009)

14 De bedrijfsarts is adviseur voor zowel werknemer als werkgever. Hij houdt op zorgvuldige wijze een medisch dossier bij (WGBO, artikel 7:454 BW).

- De bedrijfsarts verstrekt aan de werkgever die informatie die deze nodig heeft
  - om het recht van de arbeidsongeschikte werknemer op loondoorbetaling te kunnen vaststellen en
  - om aan zijn re-integratieverplichtingen te kunnen voldoen.
- Indien vereist in het kader van het uitwisselen van gezondheidsgegevens dient de cliënt zijn toestemming vrijwillig en doelgericht, schriftelijk of mondeling te geven (informed consent). De cliënt geeft zijn toestemming bij voorkeur schriftelijk[15]. Van mondeling verkregen toestemming maakt de bedrijfsarts een aantekening in het dossier van de betreffende werknemer.

1.6 Patiëntenrechten

In de AVG zijn de rechten voor betrokkenen omschreven. Deze zijn uitgebreider dan onder de Wet bescherming persoonsgegevens (Wbp). In de WGBO zijn rechten voor patiënten beschreven die in lijn zijn met de rechten op basis van de AVG en derhalve ook onder de AVG van toepassing blijven. In de praktijk van de individuele gezondheidszorg zijn de veranderingen op dit punt minimaal.

Het gaat om onder meer de volgende rechten:

- Recht op informatie
- Recht op inzage en verbetering
- Recht op verwijdering en vergetelheid
- Recht op dataportabiliteit (overdraagbaarheid)
- Recht op bezwaar en beperken van de verwerking

Zie *deel 2* voor meer informatie over deze rechten.

15 Zie deel C sub 1 van de Code gegevensverkeer en samenwerking bij arbeidsverzuim en re-integratie (KNMG, 2007). Informatie-uitwisseling waarvoor de werknemer gerichte toestemming dient te geven vereist een schriftelijke vraagstelling (machtiging). Voor mondeling overleg is apart schriftelijke toestemming noodzakelijk. Hier wordt bedoeld informatie-uitwisseling met de curatieve sector.

Hoofdstuk 2

In dit hoofdstuk komen de verschillende situaties waarin de bedrijfsarts privacygevoelige gegevens verwerkt ter sprake. Om vast te stellen hoe om te gaan met die privacygevoelige gegevens dient de bedrijfsarts in ieder geval rekening te houden met onderstaande onderwerpen:

- Vrijwillig of verplicht spreekuurcontact
- De vereiste toestemming, doelbinding en minimale gegevensverwerking
- Noodzakelijke informatie voor derden (bijv. werkgever) in het kader van verzuimbegeleiding en re-integratie

In het navolgende deel worden deze items uitgewerkt zodat de bedrijfsarts in staat is zelf te beoordelen hoe in een concrete situatie te handelen.

2.1 Vrijwillig of verplicht spreekuurcontact

De wijze waarop privacygevoelige gegevens verkregen zijn is belangrijk om vast te stellen of de WGBO onverkort van toepassing is of beperkt. Dat laatste houdt in voor zover het in de specifieke relatie arts-cliënt past[16].

2.1.1 Vrijwillig contact

Wanneer sprake is van een vrijwillig contact met de werknemer geldt de WGBO onverkort. De bedrijfsarts mag op grond van zijn medisch beroepsgeheim (art. 7:457 BW)[17] geen informatie met de werkgever of andere derden uitwisselen. Dit mag hij alleen doen met de uitdrukkelijke, gerichte en vrijwillig gegeven toestemming van de werknemer.

Van een vrijwillig contact is sprake als een werknemer zelf om dat contact verzoekt zoals bij:

- een arbeidsomstandighedenspreekuur óf
- als de werknemer vrijwillig deelneemt aan een PMO óf
- bij andere vrijwillige spreekuurcontacten.

Let op: Soms is er sprake van een vrijwillig spreekuurcontact tijdens een ziekteverzuimperiode[18]. De wegens ziekte verzuimende werknemer kan op eigen verzoek komen:

- met een vraag die niet te maken heeft met zijn ziekteverzuim óf
- hij komt op eigen verzoek voordat de werkgever opdracht heeft gegeven voor een consult.

Als de werknemer een afspraak in het kader van de ziekteverzuimbegeleiding verzet of de bedrijfsarts raadpleegt in verband met zijn ziekteverzuim nadat de ziekteverzuimbegeleiding is gestart is dit een consult in opdracht.

Een spreekuur op verzoek van de werkgever vanwege frequent verzuim van de werknemer of om andere redenen vindt veelal plaats buiten de verzuimperiodes. Dit spreekuur is dan te beschouwen als een vrijwillig spreekuurcontact aangezien de werknemer niet arbeidsongeschikt gemeld is.

2.1.2 Verplicht contact

Van een verplicht contact is sprake wanneer de werknemer de bedrijfsarts bezoekt in opdracht van de werkgever zoals bij ziekteverzuimbegeleiding of verplichte medische keuringen. De WGBO is dan beperkt van toepassing. Dit betekent in de praktijk dat de bedrijfsarts het beroepsgeheim niet volledig en onverkort handhaaft, hij mag beperkt informatie uitwisselen ook zonder toestemming van werknemer.

Wanneer de werknemer zichzelf arbeidsongeschikt heeft gemeld en de werkgever accepteert de ziekmelding niet en stuurt die werknemer naar het spreekuur, dan valt dat onder een verplicht contact.

Toelichting op verschillende situaties

Ziekteverzuimbegeleiding

De bedrijfsarts dient zich steeds te beperken tot datgene wat noodzakelijk is in verband met het doel waarvoor de gegevens worden uitgewisseld, ook als

16 Artikel 464 Burgerlijk Wetboek Boek 7 'Indien in de uitoefening van een geneeskundig beroep of bedrijf anders dan krachtens een behandelingsovereenkomst handelingen op het gebied van de geneeskunst worden verricht, zijn deze afdeling alsmede de artikelen 404, 405 lid 2 en 406 van afdeling 1 van deze titel van overeenkomstige toepassing voor zover de aard van de rechtsbetrekking zich daartegen niet verzet.'

17 Artikel 457 Burgerlijk Wetboek Boek 7

18 CTG 2007/153, beschreven in artikel 'één casus, 2 bedrijfsartsen, 8 lessen geleerd'; TBV, jan. 2009

hij toestemming heeft van de werknemer. De bedrijfsarts dient zich ook dan in te spannen het medisch beroepsgeheim zoveel mogelijk te bewaren, bijvoorbeeld door in algemene bewoordingen te verwijzen naar behandelaren en interventies, zelfs al betaalt de werkgever deze.

Het gaat bij ziekteverzuimbegeleiding doorgaans om verplichte contacten op verzoek van de werkgever. De bedrijfsarts mag in dat kader bepaalde gegevens doorgeven die van belang zijn voor de inzetbaarheid van de werknemer zoals beperkingen, mogelijkheden en verwachte duur van verzuim. Het gaat om gegevens die de werkgever nodig heeft om het recht op loondoorbetaling vast te stellen en de re-integratie vorm te geven.

Ook al hoeft de werknemer niet akkoord te gaan met de inhoud van dit bericht aan de werkgever, aangezien dit het professioneel oordeel van de bedrijfsarts betreft, is het zeker wel de bedoeling dat de werknemer op de hoogte is van de strekking/inhoud van dit advies. De bedrijfsarts dient de strekking van zijn advies met werknemer te bespreken vóór verzending aan de werkgever en de werknemer. Het vaststellen van de belastbaarheid blijft een professioneel oordeel.
Gerichte toestemming is nodig wanneer de bedrijfsarts:

- nadere onderbouwing van zijn advies wil geven en daarvoor het verstrekken van gezondheidsgegevens nodig is;
- interventies adviseert die al dan niet door de werkgever worden betaald, voor zover en indien uit de aard van de interventie de aard van de achterliggende problematiek te herleiden is;
- vangnetsituaties of regresmogelijkheden wil melden.

Vangnetsituaties

Ten aanzien van het melden van vangnetsituaties geldt het volgende.
De bedrijfsarts heeft geen wettelijke plicht de werkgever over een mogelijke vangnetsituatie te informeren. Hij kan volstaan om de werknemer te wijzen op diens meldplicht zodra zich het vermoeden voordoet dat een vangnetsituatie van toepassing is (of kan zijn). Zelf melding maken van een mogelijke vangnetsituatie aan de werkgever mag de bedrijfsarts alleen na expliciete toestemming van de werknemer. Zelfs met toestemming mag de bedrijfsarts de werkgever niet vertellen welke vangnetsituatie van toepassing is of zou kunnen zijn.

Regres

Het melden van een mogelijkheid voor regres is niet de verantwoordelijkheid van de bedrijfsarts. De werkgever mag zelf aan de werknemer vragen of er sprake is of kan zijn van regres naar aanleiding van een verkeersongeval.

Keuringen

Aanstellingskeuring[19]

Op aanstellingskeuringen is de Wet op de medische keuringen van toepassing. Deelname aan een aanstellingskeuring geschiedt op vrijwillige basis.
De uitslag mag uitsluitend met toestemming van de keurling wordt meegedeeld aan opdrachtgever (de potentiële werkgever) in termen van geschikt, ongeschikt of geschikt onder voorwaarden.

Verplichte medische keuringen van werknemers tijdens hun dienstverband[20]

De verplicht medische keuringen van werknemers tijdens hun dienstverband zijn gebaseerd op wet- of regelgeving of op bepalingen in cao's. De uitslag mag ook zonder toestemming van de keurling worden meegedeeld aan opdrachtgever (werkgever) in termen van geschikt, ongeschikt of geschikt onder voorwaarden.

De definitie van verplichte medische keuringen is als volgt: ieder medisch onderzoek van een werknemer tijdens zijn dienstverband dat is gebaseerd op een wettelijke verplichting of verplichting op basis van een cao waaraan een werknemer zich in opdracht van zijn werkgever dient te onderwerpen en waaraan rechtsgevolgen zijn verbonden en dat niet wordt verricht in het kader van ziekteverzuimbegeleiding.

Andere keuringen, PMO, intredeonderzoeken, vaccinaties

Bij de overige keuringen gaat het om vrijwillige contacten/onderzoeken. Daarop is de WGBO onverkort

19 Artikel 10 Wet op de medische keuringen

20 Leidraad Verplichte medische keuringen van werknemers tijdens hun dienstverband, NVAB, 2007

van toepassing. Er mag geen uitslag naar de werkgever tenzij met toestemming van de werknemer.

Andere opdrachtsituaties

Een voorbeeld van een andere opdrachtsituatie is het verplichte medische onderzoek van een ambtenaar waar het bevoegd gezag om vraagt. Op basis van wetgeving kan het bevoegd gezag in bepaalde situaties om een dergelijk onderzoek vragen. Meestal is de werknemer/ambtenaar verplicht mee te werken aan een dergelijk onderzoek en mag de uitslag aan de opdrachtgever worden meegedeeld. Wanneer u wordt verzocht een dergelijk onderzoek te doen vraag de opdrachtgever dan op basis van welke regelgeving hij tot zijn verzoek komt. Raadpleeg de betreffende regelgeving (bijvoorbeeld het Algemeen Rijksambtenarenreglement (ARAR)). De vermelding van een verplichting om deel te nemen aan een gezondheidskundig onderzoek in een intern beleidsstuk vormt daarentegen een onvoldoende wettelijke basis.

2.2 Toestemming, doelbinding en minimale gegevensverwerking

De vereisten toestemming, doelbinding en minimale gegevensverwerking bepalen of en welke informatie de bedrijfsarts mag verwerken en of en welke informatie hij mag uitwisselen met werkgevers of andere hulpverleners.

Hieronder volgt per item een toelichting. In paragraaf 2.2.1 worden achtereenvolgens de vereisten voor het verwerken (zoals het verzamelen, vastleggen en gebruiken) en voor het verstrekken van persoonsgegevens aan derden nader omschreven en toegelicht. Voor iedere verwerking gelden de beginselen van eisen voor doelbinding (paragraaf 2.2.2) en minimale gegevensverwerking (paragraaf 2.2.3).

*2.2.1 **Toestemming** als grondslag voor de verwerking van persoonsgegevens, met name het verwerken van bijzondere persoonsgegevens, zoals gezondheidsgegevens*

Het verstrekken van (bijzondere) persoonsgegevens ook een vorm van verwerken is maken we daar in paragrafen 2.2.1.A en 2.2.1.B een onderscheid, aangezien in de toestemmingsvereisten enkele verschillen zitten.

2.2.1.A Het verwerken van bijzondere persoonsgegevens

Het verwerken van bijzondere persoonsgegevens bij vrijwillige contacten

De toestemming van de werknemer is niet nodig om de gegevens te mogen verwerken (zoals verzamelen en vastleggen) met uitzondering van het verstrekken van deze gegevens aan derden.

Om persoonsgegevens te mogen verwerken moet aan een van de grondslagen uit art. 6 AVG voldaan zijn. Bijzondere persoonsgegevens mogen niet worden verwerkt tenzij een van uitzonderingen beschreven in art. 9 AVG van toepassing is. Zowel de algemene grondslag (art.6 AVG)[10] als de uitzonderingssituatie op het verwerkingsverbod (art.9 AVG en art 30 UAVG)[11] zijn dus van belang voor een rechtmatige verwerking van gezondheidsgegevens.

In de hiervoor besproken situaties van vrijwilligheid van contact vormt het aangaan door de werknemer van de behandelingsovereenkomst de grondslag uit art 6.1.b en 6.1.c AVG[21] voor het mogen verwerken van persoonsgegevens van de betrokken werknemer. Het aangaan van de behandelingsovereenkomst heeft tot gevolg dat op de bedrijfsarts een wettelijke dossierplicht rust op grond van de WGBO[14]. Voor de dossiervoering heeft een bedrijfsarts dus geen toestemming nodig van de werknemer.

Het verwerken van bijzondere persoonsgegevens bij vrijwillige contacten berust op de noodzaak goede zorg te verlenen aan de werknemer dan wel op het beheer van de beroepspraktijk[22]. Deze noodzaak levert tevens de uitzondering op waarop gezondheidsgegevens mogen worden verwerkt als bedoeld in art. 9 lid 2 sub h AVG.[23]

21 Art. 6.1.b en 6.1.c AVG "Rechtmatigheid van de verwerking"; De verwerking is noodzakelijk voor de uitvoering van de geneeskundige behandelingsovereenkomst en "de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust'

22 Artikel 30.3.a UitvoeringswetAVG

Het verwerken van bijzondere persoonsgegevens bij verplichte contacten

Ook bij niet-vrijwillige contacten is geen expliciete toestemming nodig om de gegevens te mogen verwerken (zoals verzamelen en vastleggen) met uitzondering van het verstrekken van deze gegevens aan derden.

De verwerking van persoonsgegevens in het kader van verplichte contacten zoals bij ziekteverzuimbegeleiding berust op een wettelijke grondslag[24]. Ook in dit geval is geen expliciete toestemming nodig om de gegevens te mogen vastleggen. De dossierplicht berust op de wettelijke verplichting tot het bijhouden van een dossier en de plicht tot het leveren van goede en verantwoorde zorg uit de WGBO[14] die bij niet-vrijwillige contacten van overeenkomstige toepassing is. Deze noodzaak levert tevens de uitzondering op waarop gezondheidsgegevens mogen worden verwerkt als bedoeld in art. 9.2 sub h AVG[23].

Toestemmingsvereiste

Toestemming kan nodig zijn als de bedrijfsarts meer of andere bijzondere persoonsgegevens wil vastleggen dan strikt noodzakelijk is voor het doel van het vrijwillige dan wel het verplichte contact.

We doelen hier op de toestemming als bedoeld in de AVG en UAVG als grondslag om bijzondere persoonsgegevens te mogen **verwerken** in de zin van verzamelen, vastleggen, gebruiken e.d. (met uitzondering van verstrekken[25]) (art.9.2.a AVG en art.22.2.a UAVG).

Dit kan het geval zijn wanneer de bedrijfsarts vanuit een PMO weet heeft van een essentieel gezondheidsgegeven dat ook van belang is voor de ziekteverzuimbegeleiding. De AVG hanteert als definitie voor toestemming van betrokkene: 'elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt' (art.4 sub 11 AVG).
In deze definitie ligt een aantal eisen besloten waaraan toestemming dient te voldoen om van een rechtsgeldige toestemming te kunnen spreken. In de praktijk betekent dit het volgende;

De werknemer dient bekend te zijn met:
- doel, aard en omvang van de te verwerken dan wel de te verstrekken gegevens;
- de reden waarom die informatie wordt verwerkt dan wel verstrekt aan derden;
- eventuele consequenties van het al dan niet verwerken dan wel verstrekken van die informatie;
- aan wie de informatie wordt verstrekt;
- hoe lang de gegevens worden bewaard.

De bedrijfsarts dient zorg te dragen dat deze toestemming aantoonbaar is.

De werknemer dient daarnaast zijn toestemming in vrijheid, met andere woorden zonder dwang of drang te kunnen geven. Als dit niet het geval is, is er geen sprake van een rechtsgeldige toestemming en kan de verwerking dus onrechtmatig zijn. Bedrijfsarts kan werknemer er expliciet op wijzen dat deze niet verplicht is om toestemming te verlenen.

2.2.1.B Communicatie (verstrekken van gegevens aan derden)

Hoewel het verstrekken van gegevens ook een vorm van verwerken is gelden onderstaande specifieke regels met betrekking tot communicatie met derden.

Vrijwillige contacten

In verband met het verstrekken van gegevens aan derden heeft de bedrijfsarts bij vrijwillige contacten toestemming nodig om het beroepsgeheim te mogen doorbreken. Deze toestemming berust op de WGBO (art. 7:457 BW).[26]

23 Art.9 lid 2 sub h AVG; 'de verwerking is noodzakelijk voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten, op grond van Unierecht of lidstatelijk recht, of uit hoofde van een overeenkomst met een gezondheidswerker en behoudens de in lid 3 genoemde voorwaarden en waarborgen'

24 art. 30.1.b UAVG, art. 9.2.b AVG en art. 6.1.c AVG

25 Zie daarover paragraaf 2.2.1.B over Communicatie.

26 Artikel 457 Burgerlijk Wetboek Boek 7

Verplichte contacten

Voor communicatie van de bedrijfsarts met de werkgever inzake verplichte medische contacten heeft de bedrijfsarts geen expliciete toestemming nodig voor zover het gegevens betreft die de werkgever nodig heeft in het kader van het doel van het verplichte contact.

Wanneer de bedrijfsarts andere of meer bijzondere persoonsgegevens wilt verstrekken heeft hij daarvoor wel expliciete, gerichte toestemming nodig van de werknemer.

Vereisten voor toestemming bij communicatie

De vereisten voor toestemming zijn voor zowel vrijwillige als verplichte contacten als volgt. Het verstrekken van (bijzondere) persoonsgegevens, zoals gezondheidsgegevens, aan derden mag alleen als aan de volgende criteria is voldaan[27];

- De werknemer geeft zijn toestemming schriftelijk of mondeling. Van mondeling gegeven toestemming maakt de bedrijfsarts een aantekening in het medisch dossier[28]. Voor uitwisseling van informatie met de curatieve sector is schriftelijke toestemming nodig[29].
- De toestemming dient in vrijwilligheid te worden gegeven.
- De werknemer begrijpt waarvoor hij toestemming geeft en de consequenties daarvan[30].
- De bedrijfsarts dient de werknemer vooraf in te lichten over het doel, de inhoud en de mogelijke consequenties van de gegevensverstrekking.

Voor deze toestemming geldt dat vrijwilligheid in een arbeidsrelatie niet snel mag worden aangenomen[31] aangezien er sprake is van een afhankelijkheidsrelatie van de werknemer tot de werkgever. Ook met toestemming van de werknemer dient de bedrijfsarts daarom terughoudend te zijn met het verstrekken van gezondheidsgegevens / medische informatie.

Om ondubbelzinnig aantoonbaar te maken dat een werknemer toestemming heeft gegeven om informatie uit te wisselen met derden zoals de werkgever verdient het aanbeveling deze toestemming door middel van een schriftelijke machtiging te laten geven. Draag er zorg voor dat uit die machtiging tenminste duidelijk blijkt om welke informatie het gaat, wie de ontvanger is, wat het doel van de informatieverstrekking is en de datum.

Samenvattend voor de praktijk

We maken onderscheid in toestemming voor het verwerken van (bijzondere) persoonsgegevens en het verstrekken daarvan. In de toestemmingsvereisten zitten enkele verschillen. Voor communicatie met de werkgever of een andere derde die niet valt onder de uitzonderingssituatie (onderzoek in opdracht; **zie hoofdstuk 2.1.2**) of die niet noodzakelijk is op basis van een wettelijke verplichting dient de bedrijfsarts:

- de werknemer goed te informeren en
- zich te vergewissen van de actieve, vrijwillige toestemming van betrokken werknemer
- geen informatie uit te wisselen wanneer hij geen toestemming heeft of twijfelt over de rechtsgeldigheid van de gegeven toestemming
- zijn eigen afweging te maken over relevantie van de te verstrekken informatie. Met andere woorden: toestemming is geen vrijbrief om alle beschikbare informatie prijs te geven.
- aan de hand van de criteria doelbinding en dataminimalisatie de omvang van de te verstrekken informatie te bepalen.

27 Zie 'De zieke werknemer, Beleidsregels voor de verwerking van persoonsgegevens over de gezondheid van zieke werknemers (AP, 2016) p. 15 en 25

28 Door aantekening te maken in het dossier wordt de mondelinge toestemming 'aantoonbaar' (art. 7.1 AVG).

29 Richtlijn het omgaan met medische gegevens (KNMG, jan 2018)

30 Art. 7.2 AVG 'Indien de betrokkene toestemming geeft in het kader van een schriftelijke verklaring die ook op andere aangelegenheden betrekking heeft, wordt het verzoek om toestemming in een begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal zodanig gepresenteerd dat een duidelijk onderscheid kan worden gemaakt met de andere aangelegenheden. Wanneer een gedeelte van een dergelijke verklaring een inbreuk vormt op deze verordening, is dit gedeelte niet bindend.' grond 42 'Toestemming mag niet worden geacht vrijelijk te zijn verleend indien de betrokkene geen echte of vrije keuze heeft of zijn toestemming niet kan weigeren of intrekken zonder nadelige gevolgen.'

31 Zie 'De zieke werknemer, Beleidsregels voor de verwerking van persoonsgegevens over de gezondheid van zieke werknemers' (AP, 2016)

2.2.2 Doelbinding

Het doel bepaalt welke informatie noodzakelijk is om te verwerken dan wel te verstrekken of op te vragen. Gegevens die niet noodzakelijk zijn voor het vastgestelde doel mogen niet worden verwerkt (art. 5 lid 1 sub b AVG)[32]. Gegevens verzameld voor het ene doel mogen alleen met toestemming van betrokkene, dan wel onder een van de andere voorwaarden zoals genoemd in artikel 6 lid 4 AVG[10] voor een ander doel worden verwerkt.[33]

Persoonsgegevens mogen alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verwerkt. De persoonsgegevens mogen dan voor dat doel of die doelen gebruikt worden.

Persoonsgegevens mogen verder worden verwerkt voor andere doelen, als die doelen verenigbaar zijn met het oorspronkelijke verzameldoel (art. 6 lid 4 AVG[10]). Om te bepalen of een nieuw doel verenigbaar is met het oorspronkelijke doel, moet worden gekeken naar een aantal elementen:

- het verband tussen het nieuwe doel en het oorspronkelijke doel. Hoe dichter de twee doelen bij elkaar liggen, hoe eerder de verdere verwerking van persoonsgegevens verenigbaar is met het oorspronkelijke doel.
- de context waarin de persoonsgegevens zijn verzameld. Hierbij moet met name worden gekeken naar de relatie tussen u en de betrokkene in kwestie en de redelijke verwachtingen die de betrokkene heeft ten aanzien van het verdere gebruik van zijn persoonsgegevens door u. Verwacht de betrokkene bijvoorbeeld dat gegevens die zijn verzameld in de context van ziekteverzuimbegeleiding hergebruikt worden om zijn verzekeringspremies te berekenen?
- de aard van de persoonsgegevens. Wanneer het bijvoorbeeld bijzondere persoonsgegevens betreft, geldt dat deze een hoger beschermingsniveau verdienen en dat deze minder snel voor andere doelen mogen worden gebruikt.
- de mogelijke gevolgen van de verdere verwerking voor betrokkenen.
- het bestaan van passende waarborgen. Als u bijvoorbeeld de persoonsgegevens heeft versleuteld of gepseudonimiseerd zullen deze eerder voor andere doelen mogen worden gebruikt dan wanneer geen waarborgen zijn getroffen.

Ook wanneer de werknemer toestemming heeft gegeven voor verdere verwerking (ook in het geval dat het doel van de verdere verwerking niet verenigbaar is met het oorspronkelijke doel) mogen persoonsgegevens verder worden verwerkt, mits die toestemming 'vrij' is gegeven.

Een voorbeeld

Ziekteverzuimbegeleiding en een keuring dienen ieder een ander doel. Daarom zijn de persoonsgegevens die voor een van deze doelen zijn verzameld niet zonder meer uitwisselbaar. Met toestemming van betrokkene mogen persoonsgegevens van een keuring wel worden gebruikt voor ziekteverzuimbegeleiding of andersom wanneer die gegevens noodzakelijk zijn voor en verenigbaar zijn met ("niet onverenigbaar") het andere doel.

2.2.3 Minimale gegevensverwerking

Onder minimale gegevensverwerking wordt verstaan dat niet meer gegevens worden verwerkt dan strikt noodzakelijk voor het beoogde doel en dat deze niet langer dan de wettelijke bewaartermijn worden bewaard.

Voorheen was dit het noodzakelijkheidsvereiste. Onder de AVG wordt ook wel gesproken van dataminimalisatie. In het kader van ziekteverzuimbegeleiding betekent dataminimalisatie dat alleen gegevens mogen worden verwerkt die noodzakelijk zijn voor een goede diagnosestelling/behandeling of begeleiding en re-integratie van de arbeidsongeschikte werknemer en voor beantwoording van de vraag of er zich een uitzondering op de loondoorbetalingsverplichting voordoet conform art 7:629 lid2 BW.[34]

32 Art. 5 AVG "Beginselen inzake verwerking van persoonsgegevens"

33 Handleiding Algemene verordening gegevensbescherming en UAVG (Ministerie van Justitie en Veiligheid, 2018)

34 Artikel 629 Burgerlijk Wetboek Boek 7

2.3 Noodzakelijke informatie voor derden in het kader van verzuimbegeleiding en re-integratie

In de communicatie over noodzakelijke adviezen ten behoeve van arbeidsongeschikte werknemers is het gebruik van algemeen gebruikelijke termen toegestaan mits die niet specifiek naar een bepaalde aandoening verwijzen en geen specifieke overige privacygevoelige informatie verschaffen en die in de dagelijkse omgang gebruikelijk zijn (termen als ziekenhuis, medische behandeling, bezoeken behandelaar).

De bedrijfsarts adviseert in het kader van verzuimbegeleiding en re-integratie om de werkgever en werknemer in staat te stellen om deze zo optimaal mogelijk vorm te geven. De vraag is echter welke informatie voor de werkgever strikt noodzakelijk is om als goed werkgever aan zijn re-integratie-verplichtingen te voldoen, terwijl anderzijds recht wordt gedaan aan het privacybelang van de werknemer.

Noodzakelijke informatie om op verantwoorde wijze de re-integratie vorm te geven omvat:

- functionele beperkingen en implicaties daarvan voor het soort arbeid dat de werknemer nog kan verrichten (functionele mogelijkheden).
- werkzaamheden waartoe de werknemer nog wel, of juist niet meer in staat is.
- het verwachte einddoel van de re-integratie (geschiktheid voor eigen werk, passend werk of re-integratie tweede spoor) met zo mogelijk een indicatie van de verwachte duur van de beperkingen of arbeidsongeschiktheid.
- eventuele aanpassingen, werkvoorzieningen of activiteiten die in het belang zijn van de re-integratie.
- advies over technische interventies die door de werkgever worden gefaciliteerd zoals bijvoorbeeld werkplekonderzoek en/of –aanpassingen, inschakelen arbeidsdeskundige of re-integratiebedrijf.
- aanwezigheid van verstoorde arbeidsrelatie welke oplossing behoeft om de re-integratie te bevorderen.
- werkgerelateerde oorzaken voor de arbeidsongeschiktheid, die bij terugkeer in de eigen werksituatie opnieuw arbeidsongeschiktheid of gezondheidsschade kunnen opleveren. De werkgever zal in staat gesteld dienen te worden passende maatregelen te nemen.

De werknemer is zelf verantwoordelijk voor het melden van:

- een ander verblijf- of verpleegadres;
- mogelijkheid van regres;
- vangnetsituatie.

De bedrijfsarts bespreekt met de werknemer dat het van belang is voor de werkgever om bovenstaande informatie van de werknemer te verkrijgen. Voor zover de bedrijfsarts inzicht heeft in de consequenties van het al dan niet melden aan de werkgever bespreekt hij die met de werknemer.

Wanneer de bedrijfsarts het noodzakelijk vindt de werkgever andere en meer dan de toegestane informatie te verschaffen ten behoeve van de re-integratie dan bespreekt hij dit met de werknemer. Daaronder valt ook het advies over interventies die door de werkgever worden gefaciliteerd (o.a. financieel, mogelijkheid bieden om andere deskundigen/hulpverleners in het bedrijf te consulteren). De bedrijfsarts vraagt de werknemer gericht toestemming om die informatie die hij noodzakelijk acht aan de werkgever mee te delen.
De werknemer dient zijn toestemming vrijwillig en doelgericht, schriftelijk of mondeling te geven (informed consent). De schriftelijke machtiging bewaart hij in het dossier.
Van mondeling verkregen toestemming maakt de bedrijfsarts een aantekening in het dossier van de betreffende werknemer.

Hoofdstuk 3

Aandachtspunten en bijzondere situaties

3.1 Voor de dagelijkse praktijk is een aantal aandachtspunten te benoemen

In alle hieronder besproken situaties geldt voor het verstrekken van gegevens dat, indien vereist, de werknemer zijn toestemming vrijwillig en doelgericht, schriftelijk of mondeling dient te geven (informed consent). Van mondeling verkregen toestemming maakt de bedrijfsarts een aantekening in het dossier van de betreffende werknemer.

1. Arbeidsongeschiktheid ten gevolge van zwangerschap, vangnetsituaties en regres

De bedrijfsarts mag zonder toestemming van betrokkene niet melden aan diens werkgever dat er sprake is van een vangnetsituatie. De voor de werkgever financieel nadelige gevolgen hiervan zijn geen reden het beroepsgeheim te doorbreken.
Voor een vangnetsituatie in verband met zwangerschap geldt dat de werkgever de mogelijkheid heeft met terugwerkende kracht deze te melden zodra hij kennis krijgt van deze situatie.
Dit recht heeft de werkgever niet wanneer er andere redenen zijn voor een beroep op vangnet. Voor regreszaken gelden vergelijkbare beperkingen. De bedrijfsarts mag geen mededelingen doen tenzij met gerichte, uitdrukkelijke en in vrijheid gegeven toestemming van betrokkene. In deze situaties is de werkgever niet uitsluitend van de bedrijfsarts afhankelijk om de benodigde informatie te verkrijgen. De werknemer dient zelf de werkgever te informeren. Kiest hij ervoor om dat niet te doen vanwege voor hem of haar moverende redenen, dan is dat voor de bedrijfsarts geen reden dat voor de werknemer te doen.

2. Projecten die de werkgever financiert bijvoorbeeld interventies door andere hulpverleners zoals fysiotherapeut, psycholoog en/of bedrijfsmaatschappelijk werker

De bedrijfsarts mag geen mededelingen doen over de aard van de in te zetten interventie. Voor de werkgever is dit veelal niet acceptabel. Deze wil weten waarvoor hij betaalt en tenminste enig inzicht hebben in de plausibiliteit van het advies. En hij zal rekeningen willen kunnen controleren. Echter alleen met expliciete toestemming van werknemer mag bedrijfsarts werkgever hierover informeren.
De bedrijfsarts dient zich ook in deze situatie te realiseren dat toestemming mogelijk niet in vrijheid is gegeven. Ook als de bedrijfsarts met expliciete toestemming informatie betreffende een interventie met de werkgever deelt, betekent dat niet dat de specifieke interventie in combinatie met de naam van betrokkene op een factuur mag komen te staan.

3. Wat nu als de werkgever al door de werknemer zelf is geïnformeerd?

Ook in die situatie mag de bedrijfsarts geen mededelingen doen over aard en inhoud van het medische probleem. Indien er sprake is van een toegevoegde waarde kan de bedrijfsarts expliciet toestemming vragen om de werkgever te mogen informeren.
De bedrijfsarts kan werknemer er expliciet op wijzen dat toestemming verlenen niet verplicht is.

4. De bedrijfsarts heeft wel toestemming van de werknemer om de werkgever te informeren

Desondanks behoudt de bedrijfsarts toch een eigen verantwoordelijkheid om te bepalen welke gegevens hij verstrekt aan derden. De bedrijfsarts dient steeds rekening te houden met het doel waarvoor hij de gegevens heeft ontvangen en weer verstrekt én het vereiste van data-minimalisatie. Toestemming en verstrekken van nadere gegevens kan gebruikt worden voor draagvlakverbreding om maatregelen te doen nemen met het doel re-integratie te bevorderen en verder verzuim te voorkomen.

5. Probleemanalyse

In de probleemanalyse behoort geen medische informatie te worden vermeld.

6. Werken met een standaard verklaring van toestemming of het geen-bezwaarsysteem tenzij de werknemer dit expliciet kenbaar maakt

Bij deze vormen van toestemming is niet zonder meer aan te nemen dat de toestemming gericht en in vrijheid wordt gegeven. Tevens houdt op deze wijze omgaan met toestemming in dat er een automatisme kan ontstaan en onvoldoende informatie over doel en noodzaak wordt verstrekt.

7. ERD-ziektewet

Begeleiding geschiedt op een vergelijkbare wijze als

voor werknemers die nog wel een dienstverband met de werkgever hebben. Voor de communicatie met de werkgever of derden gelden dan ook dezelfde regels als bij verzuimbegeleiding voor einde dienstverband. Let op: er zijn enkele bijzonderheden, zie de Werkwijzer 'Handelen van de bedrijfsarts op verzoek van eigenrisicodragers Ziektewet'[35].

8. ERD-WGA

In deze situatie doet de bedrijfsarts meestal een herbeoordeling na 1 of meer jaren na een WIA-keuring. De bedrijfsarts mag met opdrachtgever zijn conclusie over de duurzaamheid van de beperkingen, de beperkingen en mogelijkheden met opdrachtgever communiceren. Medische informatie valt hier niet onder. Zie de Werkwijzer 'Handelen van de bedrijfsarts op verzoek van eigenrisicodragers WGA'[36].

9. Informatie verstrekken aan UWV in het kader van DO/WIA-aanvraag

De bedrijfsarts is in deze situaties verplicht[37] die gerichte medische informatie aan het UWV te verstrekken die de verzekeringsarts nodig heeft om het benodigde onderzoek te doen. Betrokkene dient hierover te worden geïnformeerd maar hoeft geen toestemming te verlenen. In overige situaties is het goed na te gaan wat precies de opdracht is en of er sprake is van een wettelijk opgedragen taak waarvoor de informatie van de bedrijfsarts noodzakelijk is.[38]

10. Overige situaties zoals bijvoorbeeld keuringen in het kader van de Participatiewet, WMO e.a.

Deze worden hier niet verder besproken vanwege verschillende regimes die van toepassing zijn. Wanneer de bedrijfsarts in opdracht van een gemeente of verzekeraar keuringen of medische onderzoeken uitvoert is het aan te raden vooraf na te gaan welke regelgeving van toepassing is en wat de consequenties zijn voor de rechten van betrokkene en de communicatie met opdrachtgever.

3.2 Bijzondere situaties

In een aantal bijzondere situaties kan de werkgever de bedrijfsarts vragen of deze op de hoogte was van de medische situatie. Moedwilligheid of bewust niet vermelden van medische problemen wordt in de rechtspraak niet snel aangenomen: een goede onderbouwing is noodzakelijk.
Dit betekent dat de bedrijfsarts zich **zéér terughoudend** dient op te stellen wanneer het gaat om het verstrekken van informatie aan de werkgever in de hieronder genoemde situaties.

- Bij een aanstellingskeuring bewust verzwijgen van zodanige informatie die, als de keurend arts hiermee bekend was geweest, tot een andere uitkomst van de aanstellingskeuring zou hebben geleid.[39] [40] [41]
- Moedwillig niet meewerken of zelfs tegenwerken herstel.
- Verzwijgen van medische problemen bij een sollicitatie terwijl betrokkene wist of redelijkerwijs kon weten dat deze in de weg staan aan een goede uitoefening van de functie.

35 Werkwijzer 'Handelen van de bedrijfsarts op verzoek van eigenrisicodragers Ziektewet' (NVAB, 2014)

36 Werkwijzer 'Handelen van de bedrijfsarts op verzoek van eigenrisicodragers WGA (NVAB, 2014)

37 Artikel 54 Wet structuur uitvoeringsorganisatie werk en inkomen

38 Artikel 13.2 sub e AVG

39 Zie www.aanstellingskeuringen.nl

40 Wet op de medische keuringen

41 Artikel 629 lid 3 sub a Burgerlijk Wetboek Boek 7

Hoofdstuk 4

Digitaal verwerken en verstrekken van privacy-gevoelige informatie

Situatieschets

De bedrijfsarts verstuurt naar aanleiding van een spreekuurcontact meestal gelijktijdig een advies naar de werknemer, diens leidinggevende en/of personeelsfunctionaris. Dit gebeurt schriftelijk per post en/of per e-mail via internet of intranet.

Juridisch is onderscheid maken tussen verzenden van bijzondere persoonsgegevens per post of per e-mail in feite niet relevant: met bijzondere persoonsgegevens dient te allen tijde zorgvuldig te worden omgegaan. In beide situaties is een aantal vergelijkbare risico's te benoemen. Voor e-mailverkeer bestaan er daarnaast nog enkele bijkomende risico's. Denk bijvoorbeeld aan inzage al dan niet bewust door onbevoegden, verkeerde adressering, e-mails zijn gemakkelijk door te sturen en te hacken. Verifiëren van echtheid van afzender en ontvanger kan zeker bij e-mail problematisch zijn. Indien deze gegevens door onbevoegden kunnen worden ingezien betekent dit een datalek en schending van de privacy die de bedrijfsarts kan worden aangerekend. Hij is tuchtrechtelijk aansprakelijk, en kan ook civielrechtelijk worden aangesproken om de geleden schade te verhalen.

Mogelijke oplossingen

In de AVG is vastgelegd dat moet worden voorzien in voldoende technische en organisatorische maatregelen om een passend beveiligingsniveau voor de verwerking van persoonsgegevens te bereiken. Zowel bij verzending per post als bij emailverkeer dient een voldoende beveiligingsniveau te zijn gerealiseerd en geborgd. Verzending van gezondheidsgegevens valt in een verhoogde tot hoge risicoklasse en vereist dan ook een hoog beveiligingsniveau.

- Technische maatregelen zijn de logische en fysieke maatregelen in en rondom de informatiesystemen (zoals toegangscontroles, vastlegging van gebruik en back-up). Onder technische maatregelen worden tevens verstaan de voorzieningen die bekend staan onder de verzamelnaam Privacy-Enhancing Technologies (PET). Technische maatregelen betreffende het netwerk omvatten:
  - diverse beveiligingsschillen aanbrengen, (firewall, up-to-date virusscanner, recente patches voor de gebruikte software).
  - Zo mogelijk gebruik maken van Virtual Private Networks en een 'secure' verbinding.
  - Logfile aanleggen zodat kan worden nagegaan wie, wanneer een dossier of document heeft geraadpleegd dan wel verwerkt.

  Zie voor meer informatie 'De Nederlandse Technische Afspraak (NTA) 7516', de veldnorm die kaders stelt voor e-mailen in de zorg.[42]
- Organisatorische maatregelen zijn maatregelen ten behoeve van de inrichting van het systeem zoals (logische processen die helpen fouten te voorkomen) en voor het verwerken van persoonsgegevens zoals toekenning en deling van verantwoordelijkheden en bevoegdheden, instructies, trainingen en calamiteitenplannen.
- Verder valt te denken aan het geven van voorlichting in de organisatie hoe om te gaan met privacygevoelige informatie waarbij aandacht voor onderwerpen als toegang, opslaan en bewaren van gegevens, rechten van werknemers betreffende de over hem/haar opgeslagen gegevens.
- Alle medewerkers (vast, tijdelijk, ingeleend) in de eigen organisatie laten tekenen van een document waarin de geheimhoudingsplicht is vastgelegd kan hierbij ondersteunen. Zo ook periodiek instructie geven als een reminder.
- Communiceren via een beveiligd domein waarbij de cliënt een eigen (tijdelijke) toegang heeft tot een afgeschermd deel van de server met aldaar het voor hem bestemde bericht. De toegang kan geregeld zijn met een wachtwoord of bij voorkeur via twee-factor authenticatie.
- Alleen gebruik maken van veilig e-mail[42].
- Zie ook de Richtlijn online arts-patiëntcontact (herziene versie, KNMG 2007)
- Zie ook de website AVG Helpdesk Zorg en Welzijn[43].

42 NTA 7516:2019, Hoofdstuk 6, Richtlijnen voor professionals

43 https://www.avghelpdeskzorg.nl/onderwerpen/e-mail-om-persoonsgegevens-te-delen

Door de bedrijfsarts zelf te nemen voorzorgsmaatregelen

De bedrijfsarts dient zich ook in zijn dagelijkse praktijk bewust te zijn van mogelijke privacyrisico's en de mogelijkheden deze risico's te minimaliseren. Van de individuele bedrijfsarts − indien niet zijnde de verwerkingsverantwoordelijke in de zin van de AVG − mag worden verwacht dat hij zich op de hoogte stelt of die maatregelen zijn genomen, die redelijkerwijs verwacht kunnen worden volgens de stand der techniek om voor het systeem een afdoende beschermingsniveau te realiseren.

Voor zowel bedrijfsarts of voor hem werkende personen als ontvanger gaat het om de volgende mogelijkheden die al dan niet in combinatie toepasbaar zijn:

- instellen van schermbeveiliging met wachtwoord
- controleren en verifiëren van adres- en e-mailgegevens
- documenten voorzien van wachtwoord
- encryptie
- digitale handtekening
- verifiëren van zender en ontvanger
- ontvangstbevestiging instellen.

De ontvanger is verantwoordelijk voor zijn eigen e-mailaccount en de beveiliging daarvan. Voor de opslag van bijzondere persoonsgegevens gelden dezelfde eisen als voor de papieren verslagen.

DEEL 2

Achtergrond-document

Algemene verordening gegevensverwerking (AVG)

Hoofdstuk 5

Algemene informatie AVG
De Algemene verordening gegevensverwerking (AVG) is een Europese verordening die in alle lidstaten van de Europese Unie rechtstreeks van toepassing is sinds 25 mei 2018. De AVG vervangt in Nederland de Wet bescherming persoonsgegevens, deze is dan ook niet meer geldig. De AVG is bedoeld om in alle lidstaten van de Europese Unie (EU) twee belangen te waarborgen: de bescherming van natuurlijke personen in verband met de verwerking van hun gegevens en het vrije verkeer van persoonsgegevens binnen de EU. In iedere lidstaat is eenzelfde niveau van bescherming op basis van de AVG gegarandeerd, aan specifieke bepalingen mogen lidstaten een eigen invulling geven door middel van een Uitvoeringswet. De uitvoeringswetten kunnen dan ook per land verschillen.

Dit achtergronddocument is geschreven vanuit de Nederlandse situatie en rekening houdend met de alhier geldende uitvoeringswet.

De AVG is waar het gaat om de rechten van betrokkenen vooral een neerslag van hetgeen al gold op basis van voorgaande EU-richtlijnen en jurisprudentie. Enkele rechten zijn toegevoegd. Voor de gezondheidszorg zijn de veranderingen ten aanzien van de patiëntenrechten beperkt. De WGBO en wet BIG gingen verder dan de eisen op basis van de Wbp. In *hoofdstuk 5.1* zijn de rechten van betrokkenen beschreven.
De meest ingrijpende veranderingen betreffen de eisen die aan organisaties die persoonsgegevens verwerken, worden gesteld. In *hoofdstuk 5* treft u hierover meer informatie aan.

Rechten betrokkenen zijn het recht op:
- Toegang tot gegevens, inzage in gegevens
- Rectificatie van gegevens
- Vergetelheid
- Beperking van verwerking
- Kennisgeving
- Dataportabiliteit

Privacymanagement of wel de belangrijkste verplichtingen voor organisaties in trefwoorden
- Accountability ofwel de verantwoordingsplicht
- Het nemen van technische en organisatorische maatregelen
- Data protection impact assessment (DPIA)
- Functionaris gegevensbescherming (FG)
- Procedure afhandeling datalekken

De sanctiemogelijkheden van de toezichthouder
- Aanscherping van de maatregelen

De in dit document gebruikte term organisaties staat voor verwerkingsverantwoordelijke in zowel arbodiensten als maatschappen of andere vormen van samenwerkingsverbanden van bedrijfsartsen.
De verwerkingsverantwoordelijke is degene die doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Hij dient zorg te dragen dat aan de AVG wordt voldaan. Dit kan ook de individuele zelfstandige bedrijfsarts (de ZZP'er) zijn.
De in dit deel verstrekte informatie is informatie op hoofdlijnen, bedoeld om de lezer attent te maken op de kern en aandachtspunten van en voor het omgaan met persoonsgegevens in het kader van de bedrijfsgezondheidszorg. Wat betreft de verplichtingen voor de verwerkingsverantwoordelijke is het zeker geen uitputtende handleiding hoe te voldoen aan de eisen die de AVG stelt. Wel zijn de beginselen en maatregelen beschreven. Het hangt van de specifieke situatie af hoe het beleid en management inzake het omgaan met privacy van cliënten dient te worden ingericht.

Hoofdstuk 6

Toelichting op de verschillende rechten

Het recht op informatie (Art. 13 en 14 AVG)
Dit recht omvat het recht informatie te krijgen over de volgende items

- voor welke doeleinden de persoonsgegevens worden verwerkt;
- hoe lang zij worden bewaard;
- van wie de organisatie de persoonsgegevens ontvangt;
- aan wie de organisatie de persoonsgegevens verstrekt;
- de eventuele automatische verwerking van de persoonsgegevens.

Toegang, inzage (art.15 AVG)
Betrokkene heeft het recht om kennis te kunnen nemen van de gegevens die over hem zijn verwerkt (opgeslagen). Hij heeft recht op een afschrift van die gegevens.

Rectificatie (art.16 AVG)
Betrokkene heeft het recht onjuiste gegevens te doen corrigeren en onvolledige gegevens aan te vullen voor zover nodig en passend bij de doeleinden van de verwerking. Hij mag daartoe een aanvullende verklaring verstrekken.

Dataminimalisatie (Art. 5 AVG)
Dit betekent dat de bedrijfsarts niet meer gegevens verwerkt dan noodzakelijk voor het doel van de registratie. Dit is vergelijkbaar met doelbinding en noodzakelijkheidsvereiste onder Wbp.

Klachtrecht (Art. 77 AVG)
Betrokkene heeft het recht om over de vermeende onjuiste verwerking van zijn persoonsgegevens (zijn rechten zijn geschonden) of als zijn verzoeken niet goed zijn afgehandeld bij de Autoriteit Persoonsgegevens (AP) een klacht in te dienen. Of hij kan ervoor kiezen en rechtszaak te starten. De AP dient klachten in behandeling te nemen en betrokkene binnen drie maanden te informeren over de voortgang en de uitkomst daarvan.

De volgende rechten zijn nieuw in de AVG:

Recht op vergetelheid (art.17 AVG)
Het recht op vergetelheid is een nieuw recht in de AVG. Dit recht lijkt op het recht op correctie en verwijdering[44] uit de WGBO maar is breder. In de bedrijfsartsen-praktijk geldt het recht op vergetelheid niet voor medische dossiers.[45]

Recht op dataportabiliteit (art.20 AVG)
Dit houdt in dat betrokkene het recht heeft op zijn verzoek de vastgelegde gegevens te ontvangen en deze door te mogen geven naar een andere organisatie. Dataportabiliteit is het recht om in een gestructureerd, gangbaar, machineleesbaar en interoperabel formaat de verwerkte gegevens te verkrijgen en die aan een andere verwerkingsverantwoordelijke door te zenden. Het recht op dataportabiliteit geldt alleen onder de volgende voorwaarden:

- Gegevens zijn verwerkt op basis van toestemming van betrokkene
- of op basis van een overeenkomst met hem zoals gegevens ontleend aan vrijwillige deelname aan PMO (periodiek medisch onderzoek), aan vrijwillige spreekuurcontacten of aan vrijwillige keuringen.
- Betrokkene heeft de gegevens zelf verstrekt.

Het gaat om digitale gegevens, dus niet om papieren dossiers.

Verbod op profilering (Art 22 AVG)
Van profilering is sprake wanneer een profiel van betrokkene opgesteld wordt op basis van verzamelde gegevens. Een dergelijk profiel kan allerlei persoonlijke aspecten betreffen. De verzamelde persoonsgegevens worden geanalyseerd en gebruikt om voorspellingen te doen over iemand (bijv. koopgedrag, interesses, gezondheid, economische situatie). Profilering aan de hand van bijzondere persoonsgegevens is verboden tenzij met uitdrukkelijke toestemming van betrokkene of op basis van een wettelijke regeling.

Als aan profilering rechtsgevolgen zijn verbonden of als profilering anderszins een grote impact voor betrokkene heeft, mag een besluit niet alleen op geautomatiseerde

44 Artikel 455 Burgerlijk Wetboek Boek 7

45 https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/gezondheid/medisch-dossier

verwerking gebaseerd worden. In die situatie is een menselijke tussenkomst (beoordeling) vereist, Dit is niet nodig wanneer verwerking geschied op basis van toestemming of een overeenkomst met betrokkene. Vraagt betrokkene toch om menselijke tussenkomst dan heeft hij daar recht op.

Het recht van bezwaar uit te oefenen (Art 21 AVG)
Betrokkenen hebben het recht bezwaar te maken tegen verwerking van hun persoonsgegevens wanneer een organisatie deze gegevens verwerkt op grond van een taak van algemeen (overheidstaak) of van een gerechtvaardigd belang. De organisatie moet dan de verwerking stoppen en/of een heroverweging van de belangen maken.

Beperking van verwerking (art.18 AVG)
In bepaalde situaties kan betrokkene de organisatie vragen de gegevens niet te verwerken. Met uitzondering van het opslaan mag de organisatie niets doen met deze gegevens zonder toestemming van betrokkene.

Toestemming

De verwerkingsverantwoordelijke moet kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens. Daarnaast moet de toestemming duidelijk worden onderscheiden van toestemming voor andere aangelegenheden. Het intrekken van de toestemming moet even eenvoudig zijn als het geven ervan.

Twee van de eisen die de AVG stelt aan 'toestemming' zijn dat deze 'geïnformeerd' en 'specifiek' gegeven is. Om geldige toestemming aan te tonen is het dan ook essentieel dat aantoonbaar is op basis van welke informatie betrokkene de toestemming heeft gegeven. Het is onvoldoende om alleen de toestemming zelf vast te leggen.

Voor een rechtsgeldige toestemming is het tevens noodzakelijk dat deze actief en in volledige vrijheid is gegeven. Dit wordt niet snel aangenomen omdat er een afhankelijkheidsrelatie is tussen werkgever en werknemer.[46]

Wat te verwachten van de verwerkingsverantwoordelijke als het gaat om het uitoefenen van de rechten?
De verwerkingsverantwoordelijke dient mogelijk te maken dat betrokkenen hun rechten kunnen uitoefen (art.12 AVG). Enkele aandachtspunten voor de organisatie in deze zijn:

- Het is belangrijk betrokkene goed en volledig te informeren over de verwerking van zijn persoonsgegevens en zijn rechten. De informatieverstrekking aan betrokkene dient
  - beknopt te zijn;
  - in duidelijke, begrijpelijke, eenvoudige taal;
  - en in een transparante, begrijpelijke en toegankelijke vorm te worden gegeven.
- Om welke informatie het gaat staat in art.13 en 14 AVG. Er wordt onderscheid gemaakt tussen informatie die van betrokkene zelf is verkregen en informatie over betrokkene die van derden is verkregen.
- Binnen maximaal 1 maand na ontvangst van het verzoek informeert de organisatie betrokkene over de afhandeling. Ook als de organisatie besluit geen gevolg te geven aan het verzoek dient deze betrokkene hierover met redenen omkleed te informeren.
- Voor het verschaffen van afschriften, vernietigen en uitoefenen van zijn overige rechten mogen geen kosten in rekening worden gebracht. In uitzonderlijke gevallen (bijv. excessieve verzoeken) mogen administratiekosten in rekening worden gebracht of mag de organisatie weigeren aan het verzoek te voldoen.
- De organisatie mag bij twijfel aan de identiteit van verzoeker om nadere informatie ter bevestiging van de identiteit (legitimatie) vragen.

46 Groep gegevensbescherming artikel 29 Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679

Hoofdstuk 7

Het gegevensverwerkende proces: welke eisen stelt de AVG aan privacy-management?
De AVG benoemt **een aantal beginselen, een zestal grondslagen en een aantal maatregelen** ten behoeve van de verwerking van persoonsgegevens. De beginselen en grondslagen zijn onder meer verwerkt in de maatregelen en behoren in het privacybeleid en -reglement dat organisaties hanteren terug te komen. In dit hoofdstuk vindt u een toelichting op genoemde items op hoofdlijnen en zoveel mogelijk gericht op de bedrijfsgezondheidszorg.

Beginselen
In de AVG zijn de beginselen opgenomen waaraan iedere verwerking van persoonsgegevens moet voldoen. Organisaties dienen aantoonbaar aan deze beginselen (art. 5 lid1en 2) te voldoen. Het gaat om de volgende beginselen:

- Rechtmatigheid: verwerken van persoonsgegevens heeft een gerechtvaardigde grondslag.
- Transparantie: betrokkene is op de hoogte en heeft − indien van toepassing − aantoonbaar toestemming gegeven voor het verwerken van zijn persoonsgegevens.
- Behoorlijkheid: een niet concreet omschreven eis die nauw verbonden is met rechtmatigheid en transparantie.
- Doelbinding: gegevens worden verzameld/verwerkt met een expliciet omschreven doel en worden niet zonder meer aangewend voor andere doeleinden.
- Gegevensbeperking (dataminimalisatie): er worden niet meer gegevens verwerkt dan strikt noodzakelijk voor het omschreven doel.
- Juistheid: correcte gegevens, periodieke actualisering kan nodig zijn.
- Bewaarbeperking: niet langer dan strikt noodzakelijk voor het doel, tenzij wettelijke plicht.
- De juiste organisatorische en technische maatregelen, privacy by design en privacy by default.
- De verwerkingsverantwoordelijke moet kunnen aantonen dat aan de wettelijke verplichtingen vanuit de AVG wordt voldaan (accountability).

De rechtsgronden voor verwerking
Iedere verwerking van persoonsgegevens dient op een van de in de art. 6 AVG genoemde zes rechtsgronden te zijn gebaseerd. Deze rechtsgronden zijn gelegen in:

1. een overeenkomst met betrokkene, ter voorbereiding of uitvoering daarvan
2. een wettelijke verplichting
3. het levensbelang voor iemand
4. de juiste vervulling van een overheidstaak
5. het belang van de verwerkingsverantwoordelijke dat zwaarder weegt dan het belang van betrokkenen
6. toestemming van betrokkene.

In art. 9 AVG lid 1 is een verbod opgenomen inzake het verwerken van bijzondere persoonsgegevens. Gegevens die een (bedrijfs)arts verzamelt over de gezondheid van een cliënt zijn dergelijke bijzondere persoonsgegevens. Niet alleen gegevens over iemands gezondheid maar ook over zijn ras en etnische afkomst, religie en een aantal andere aspecten vallen onder dit verbod.

In art. 9 lid 2 zijn uitzonderingen opgenomen op grond waarvan verwerking van bijzondere persoonsgegevens wel is toegestaan. Artikel 9 lid 2 sub b bevat een uitzondering om bijzondere persoonsgegevens te mogen verwerken ter uitvoering van verplichtingen op het terrein van het arbeidsrecht en sociale zekerheidsrecht. Onder art. 9 lid 2 sub h is specifiek opgenomen dat verwerking van gezondheidsgegevens waaronder die voor preventieve en Arbeidsgeneeskunde en de beoordeling van arbeidsgeschiktheid van de werknemer is toegestaan. Deze uitzonderingen zijn nader uitgewerkt in art. 30 UAVG.

Maatregelen
Organisaties hebben op grond van de AVG een aantal specifieke verplichtingen (maatregelen genoemd). De maatregelen geven uitvoering aan genoemde beginselen en zijn een noodzaak om aan te tonen hoe een organisatie met persoonsgegevens omgaat. De verplichte maatregelen die de AVG concreet noemt, zijn:

1. het bijhouden van een register van verwerkingsactiviteiten;
2. indien van toepassing het uitvoeren van een data protection impact assessment (DPIA);
3. het bijhouden van een register van datalekken die zijn opgetreden;
4. het aantonen dat een betrokkene daadwerkelijk toestemming heeft gegeven voor een gege-

vensverwerking wanneer voor een verwerking toestemming nodig is;
5. wanneer onduidelijk is of een organisatie verplicht is om een Functionaris gegevensbescherming aan te stellen, is een goede onderbouwing nodig waarom ervoor gekozen is al dan niet een FG aan te stellen.

Aanvullende maatregelen, niet verplicht wel sterk aanbevolen, zijn:
6. het aansluiten bij een gedragscode;
7. het behalen van een bepaald certificaat[47]; (nog niet ontwikkeld voor zover bekend)
8. het hanteren van een specifiek ICT-beveiligingsbeleid;
9. het afleggen van verantwoording over de verwerking van persoonsgegevens in uw jaarverslag of in een speciaal privacy-jaarverslag.

Toelichting bij een aantal begrippen en maatregelen

- **De verantwoordingsplicht (accountability)**
  Organisaties hoeven verwerkingen van persoonsgegevens niet meer te melden bij de Autoriteit Persoonsgegevens. Organisaties hebben daarentegen een grotere verantwoordingsplicht gekregen (accountability). Dit houdt in dat de verwerkingsverantwoordelijke met documenten moeten kunnen aantonen hoe wordt voldaan aan de AVG, bijvoorbeeld dat de juiste organisatorische en technische beveiligingsmaatregelen zijn genomen.

- Een van de verplichtingen in dit kader is ook het bijhouden van een **verwerkingsregister**. Een verwerkingsregister is verplicht voor alle organisaties met meer dan 250 medewerkers. Organisaties met minder dan 250 medewerkers dienen een register bij te houden wanneer de verwerking persoonsgegevens betreft:
  - die een hoog risico inhouden voor de rechten en vrijheden van de betrokkenen en/of;
  - waarvan de verwerking niet incidenteel is[48] en/of;
  - die vallen onder de categorie bijzondere persoonsgegevens, zoals gegevens over godsdienst, gezondheid en politieke voorkeur of strafrechtelijke gegevens.

  Verder is het verplicht logbestanden bij te houden.[49]

- Organisaties kunnen verplicht zijn een **data protection impact assessment (DPIA)** uit te voeren. Dit houdt in dat zij volgens een methodiek privacy-risico's van gegevensverwerking in kaart brengen. Daarop dient de organisatie maatregelen te baseren om de risico's te verkleinen.
  Er zijn 9 criteria om te beoordelen of een DPIA noodzakelijk is. Wanneer aan 2 van de 9 criteria wordt voldaan is een DPIA noodzakelijk, in overige situaties wordt het aangeraden maar niet verplicht. Voor de bedrijfsgezondheidszorg zijn de meest relevante criteria de volgende:
  - Bijzondere persoonsgegevens
  - Grootschalige gegevensverwerking;
  - Gegevens over kwetsbare personen. Personen die niet in vrijheid toestemming hebben kunnen geven vanwege ongelijke machtsverhoudingen (bijvoorbeeld werknemers, kinderen en patiënten).

Een DPIA is een continu proces. Deze dient dan ook regelmatig te worden herhaald. Aanleiding om een DPIA te herhalen bestaat onder andere als de omgeving wijzigt of het doel van de verzameling of technologie ingrijpend verandert.

- Organisaties kunnen verplicht zijn een **functionaris gegevensbescherming (FG)** aan te stellen. Een FG is verplicht voor organisaties die zorg verlenen en voor organisaties die op grote schaal bijzondere persoonsgegevens verwerken en dit een kernactiviteit is. Deze FG heeft een belangrijke taak bij gegevensbescherming. De FG is niet eindverantwoordelijk voor het privacybeleid.
  De FG heeft een onafhankelijke positie binnen de organisatie. Zijn taken zijn toezicht houden, signaleren en adviseren in het kader van privacy.

47 De AVG stimuleert het ontwikkelen van gedragscodes (bv per branche), die gecertificeerd worden door de AP. Art. 40-43 AVG

48 aldus geldt dus voor vrijwel alle verwerkingen dat ze in een register moeten worden opgenomen (behalve als ze echt incidenteel zijn), dus ook in organisaties met <250 medewerkers.

49 NEN7513:2018

De FG is contactpersoon voor de AP. Hij geniet ontslagbescherming vergelijkbaar met OR-leden.

Criteria op grote schaal

Criteria ter bepaling of er sprake is van verwerken op grote schaal:

- het aantal betrokkenen (de mensen van wie gegevens worden verwerkt);
- de hoeveelheid gegevens die worden verwerkt;
- de duur van de gegevensverwerking;
- de geografische reikwijdte van de verwerking.

Verwerking van bijzondere persoonsgegevens door individuele artsen (de eenpitters) valt niet onder grootschalige verwerking. De verwerking van persoonsgegevens door ziekenhuizen, huisartsenposten en zorggroepen interpreteert de Autoriteit Persoonsgegevens (AP) altijd als grootschalig. Voor alle overige zorgaanbieders geldt dat zij grootschalig persoonsgegevens verwerken als zij van meer dan 10.000 patiënten gegevens verwerken in één informatiesysteem.[50]

Datalekken

Een inbreuk op de beveiliging van persoonsgegevens kan bewust of onbewust / per ongeluk gebeuren.
Een hacker is bewust uit op het maken van een datalek, een verkeerd verstuurde mail is meestal een onbedoeld datalek. Elke organisatie of verwerkingsverantwoordelijke is verplicht een registratie van datalekken bij te houden en moet deze meestal melden aan de AP en in bepaalde gevallen ook aan betrokkene(n), namelijk wanneer het lek waarschijnlijk een hoog risico betekent voor diens rechten en vrijheden, bijvoorbeeld vanwege de mogelijkheid van chantage of identiteitsfraude.
De criteria om te beoordelen of er sprake is van een hoog risico zijn nog in ontwikkeling. Op de site van de AP zijn voorbeelden opgenomen die behulpzaam kunnen zijn bij de beoordeling of een datalek aan de AP en/of aan betrokkene(n) moet worden gemeld.[51]

Aanscherping van de maatregelen

Een **aanscherping van de maatregelen** die de AP kan opleggen bij overtreding (max. € 20 miljoen of 4% van de wereldwijde jaaromzet).

Voor meer gedetailleerde informatie zie de site van de AP: https://autoriteitpersoonsgegevens.nl

50 Bron: Autoriteit Persoonsgegevens, 'Uitleg begrip 'grootschalig' verduidelijkt voor alle zorgaanbieders'. Nieuwsbericht, 11 december 2018. https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/uitleg-begrip-%E2%80%98grootschalig%E2%80%99-verduidelijkt-voor-alle-zorgaanbieders.

51 Voorbeeldlijst wel/niet melden datalek (AP, 2019): https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/2019_voorbeeldlijst_wel_niet_melden_datalek_def.pdf

Bijlage 1
Definities

Definities (art.4 AVG)
Onderstaand een aantal voor de bedrijfsgezondheidszorg belangrijke definities in kernwoorden. Voor de letterlijke tekst zie genoemd artikel.

- **Bestand**: elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn
- **Betrokkene**: een identificeerbaar natuurlijk persoon
- **Bijzondere persoonsgegevens**: gevoelige gegevens genoemd in art.9 lid 1 AVG
- **Ontvanger**: degene of de organisatie aan wie persoonsgegevens worden verstrekt
- **Persoonsgegevens**: alle informatie over een geïdentificeerde of identificeerbare natuurlijk persoon
- **Toestemming van de betrokkene**: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt.
- **Verwerking**: alle bewerkingen m.b.t. persoonsgegevens zoals verzamelen, vastleggen, verwijderen al dan niet via geautomatiseerde procedés uitgevoerd.
- **Verwerker**: een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of ander orgaan die/dat ten behoeve van een verwerkingsverantwoordelijke persoonsgegevens verwerkt.
- **Verwerkingsverantwoordelijke**: een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of ander orgaan die/dat alleen of samen met anderen het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt

Overig
- **Client**: In deze leidraad bedoelen we met de term cliënt de werknemer. De werknemer/cliënt is de betrokkene in de zin van de AVG.

Bijlage 2
Lijst van afkortingen

AP	Autoriteit Persoonsgegevens
ARAR	Algemeen Rijksambtenarenreglement
AVG	Algemene Verordening Gegevensbescherming
BA	Bedrijfsarts
BIG	Beroepen in de individuele gezondheidszorg
CAO	Collectieve arbeidsovereenkomst
DO	Deskundigen oordeel
DPIA	Data protection impact assessment
ERD	Eigenrisicodrager
EU	Europese Unie
FG	Functionaris gegevensbescherming
ICT	Informatie- en communicatietechnologie
KNMG	Koninklijke Nederlandsche Maatschappij tot bevordering der Geneeskunst
NVAB	Nederlandse Vereniging voor Arbeids- en Bedrijfsgeneeskunde
OR	Ondernemingsraad
OVAL	Organisatie voor Vitaliteit, Activering en Loopbaan
PET	Privacy-Enhancing Technologies
PMO	Preventief medisch onderzoek
SUWI	Wet structuur uitvoeringsorganisatie werk en inkomen
UAVG	Uitvoeringswet Algemene Verordening Gegevensbescherming
UWV	Uitvoeringsinstituut werknemersverzekeringen
Wbp	Wet bescherming persoonsgegevens
WGA	Regeling werkhervatting gedeeltelijk arbeidsgeschikten
WGBO	Wet geneeskundige behandelingsovereenkomst
WIA	Inkomensvoorziening Volledig Arbeidsongeschikten
WMO	Wet maatschappelijke ondersteuning
Wvp	Wet verbetering poortwachter
ZZP	Zelfstandige zonder personeel

Bijlage 3
Literatuur/ geraadpleegde bronnen

- Grip op de AVG, de nieuwe privacywet voor niet-juristen; dr. Koen Versmissen CIPP/E; mr. Drs. Jeroen Terstegge CIPP-E/US; Natalja Krijgsman MSc CIPM; Wolters Kluwer, 2017
- Sdu Commentaar AVG, editie 2019; mr.drs. T.F.M. Hooghiemstra; mr.dr. S. Nouwt; Sdu Uitgevers bv Den Haag, 2019

Richtlijnen en leidraden

- Leidraad Verplichte medische keuringen van werknemers tijdens hun dienstverband (NVAB, 2007)
- Kernwaarden van de Bedrijfsarts (NVAB, 2012)
- Het Professioneel Statuut van de bedrijfsarts (NVAB, 2003)
- Richtlijn inzake het omgaan met medische gegevens (KNMG, 2018)
- Code gegevensverkeer en samenwerking bij arbeidsverzuim en reïntegratie (KNMG, 2007)
- Richtlijn online arts-patiëntcontact, herziene versie (KNMG, 2007)
- Taken en verantwoordelijkheden van de bedrijfsarts in het kader van de verzuimbegeleiding en re-integratie (KNMG, 2009)
- Werkwijzer 'Handelen van de bedrijfsarts op verzoek van eigenrisicodragers Ziektewet' (NVAB, 2014)
- Werkwijzer 'Handelen van de bedrijfsarts op verzoek van eigenrisicodragers WGA (NVAB, 2014)
- NTA 7516:2019, Hoofdstuk 6, Richtlijnen voor professionals
- NEN7513:2018

Bijlage 4
Wet- en regelgeving

m.b.t. AVG & UAVG:

- L 119/1 Publicatieblad van de Europese Unie (27 april 2016)
- Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming (Ministerie van Justitie en veiligheid, 2018) & Memorie van toelichting Uitvoeringswet Algemene verordening gegevensbescherming
- Uitvoeringswet Algemene verordening gegevensbescherming (UAVG)

m.b.t. AP:

- De zieke werknemer. Beleidsregels voor de verwerking van persoonsgegevens over de gezondheid van zieke werknemers (AP, 2016)
- Website van de Autoriteit Persoonsgegevens (AP); https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving
- AVG helpdesk; https://www.avghelpdeskzorg.nl/onderwerpen/e-mail-om-persoonsgegevens-te-delen

Overig:

- Wijzigingswet Burgerlijk Wetboek, enz. (geneeskundige behandelingsovereenkomst) (WGBO)
- Wet op de beroepen in de individuele gezondheidszorg (wet BIG)
- Wet verbetering poortwachter (Wvp)
- Regeling procesgang eerste en tweede ziektejaar
- Wet structuur uitvoeringsorganisatie werk en inkomen (wet SUWI)
- Wet op de medische keuringen
- Burgerlijk Wetboek Boek 7

OVAL

Nederlandse Vereniging voor Arbeids- en Bedrijfsgeneeskunde nvab

WWW.OVAL.NL
WWW.NVAB-ONLINE.NL