

Werkwijzer gegevensverwerking de zieke werknemer



Disclaimer

Wij menen onze stellingname binnen deze werkwijzer te kunnen onderbouwen met zorgvuldig eigen onderzoek en motivatie, mede door de inschakeling van een aantal AVG-specialisten en juristen. Een bindend oordeel over hetgeen in deze werkwijzer opgenomen is echter voorbehouden aan de Autoriteit Persoonsgegevens.

De huidige juridische kaders zijn breed voor interpretatie vatbaar, waarmee wij niet kunnen uitsluiten dat deze werkwijzer in de toekomst moet worden bijgesteld, bijvoorbeeld door een nader standpunt van de Autoriteit Persoonsgegevens. Tips, aanvullingen, opmerkingen, aanbevolen correcties zijn van harte welkom. De werkwijzer is een dynamisch document en kan met hulp van de lezers verder worden geoptimaliseerd.

Stuurgroep AVG

info@stuurgroepavg.nl

Inhoudsopgave

Voorwoord.....	6
1. Inleiding AVG.....	7
1.1 Doel van de AVG	7
1.2 Rollen binnen de AVG	7
1.3 Ruimere scope dan Wbp	8
1.4 Persoonsgegevens.....	8
1.4.1. Toets op type data.....	9
1.4.2. Werknemersadministratie bij de arbodienst.....	10
1.5 Wijze van uitwisseling persoonsgegevens.....	10
1.6 Algemeen verwerkingsverbod en de uitzonderingen	10
1.7 Vrijwillig gedeelde gegevens.....	13
1.8 Bewustwording en overige stappen in organisaties t.a.v. de AVG	13
2. Verwerkersovereenkomsten en Register van verwerkingsactiviteiten voor arbodiensten en verzuim-/casemanagementbedrijven	16
2.1 Wie zijn zelfstandige verwerkersverantwoordelijken?	16
2.2 Register van verwerkingsactiviteiten	16
2.3 Data protection impact assessment (DPIA).....	17
2.4 Heeft een organisatie een Functionaris Gegevensbescherming nodig?	18
2.4.1 Wat moet de FG doen?.....	18
2.4.2 Aan welke eisen moet een FG voldoen?	19
2.5 Meldplicht datalekken.....	19
3. Beleidsregels AP ‘De zieke werknemer’	20
3.1 Aanleiding.....	20
3.2 Verwerking van persoonsgegevens op grond van de arbeidsovereenkomst.....	20
3.3 Controleer de personeelsdossiers: leg geen aard en oorzaak van ziekte vast	21
3.4 Gezondheidsgegevens.....	21
3.5 Noodzakelijke gegevens voor de loondoorbetalingsplicht en re-integratie	21
4. Rechten en plichten in de Wet verbetering poortwachter (WVP) en de WIA	23
4.1 Rechten en plichten in de WVP.....	23
4.2. Rechten en plichten in de WIA.....	24
4.3 Werknemer ziek melden in verband met claim op de inkomensverzekering	24

4.4 Wat mag de werkgever vragen en registreren bij een ziekmelding?.....	24
4.4.1 Gegevens die een werknemer vrijwillig verstrekt.....	25
4.4.2 Vermoedelijke duur van het verzuim	25
4.4.3 Over te nemen werkzaamheden.....	26
4.4.4 Vangnetbepaling	26
4.4.5 Functionele beperkingen.....	26
4.5 Welke gegevens mag de bedrijfsarts/arbodienst met werkgever delen?.....	26
4.5.1. Werknemersbestanden	28
4.6. Stroomlijnen verplichtingen WVP en de grondslagen van de AVG.....	29
4.6.1 Hoofdpijnen	29
4.6.2 Aandachtspunten	30
4.6.3 Standpunt verzuimprofessionals.....	31
4.6.4 Samenwerking met UWV.....	31
4.7. Onderscheid tussen verschillende soorten casemanagers	32
4.7.1 Casemanagers voor of namens de werkgever.....	32
4.7.2 De casemanager taakdelegatie onder auspiciën van de bedrijfsarts.....	32
5. Informatiestromen en rollen inkomensverzekeraar en bij re-integratie	34
5.1 Diverse rollen en functionarissen rondom de zieke werknemer.....	36
5.2 Soorten (bijzondere) persoonsgegevens.....	36
5.2.1 Categorie A-gegevens.....	36
5.2.2 Categorie B-gegevens.....	38
5.2.3 Bijzonderheden WIA-verzekeringen.....	39
5.2.4 Categorie C-gegevens.....	39
5.2.5 Categorie D-gegevens.....	42
5.3 Schema verwerking categorie persoonsgegevens per rol.....	42
5.4. Matrix onderlinge uitwisseling persoonsgegevens.....	43
5.5 Rol van de adviseur zorg- en inkomensverzekeringen.....	43
5.5.1 De inkomensverzekeraar	43
5.5.2 Rolscheiding.....	44
5.5.3 Rol van de medewerker acceptatie en prolongatie inkomensverzekeringen	44
5.5.4 Rol van de claimbehandelaar inkomensverzekeringen.....	45
5.5.5 Rol van de gevolmachtigde agent	45
5.5.6 Rol van het re-integratiebedrijf en de re-integratieadviseur	46

5.5.7 Rol van de werkgever (en haar intern/extern HR-adviseur).....	46
5.5.8 Rol verzekeringsadviseur en bewustwording klantrelatie (werkgever) van AVG	47
5.5.9 Advies-, offerte- en aanvraagtraject	47
5.5.10 Naverrekeningstraject	49
5.5.11 Schadetraject	49
5.5.12 Overeenkomst inkomensverzekeraar en arbodienst/bedrijfsarts	50
5.5.13 Ongevraagd informatie ontvangen die men in zijn rol niet mag hebben.....	51
5.5.14 Samenwerking/contact met UWV in de keten inkomensverzekeringen.....	51
6. Mogelijkheden inzet interventie en de facturering	53
7. Eisen omtrent verzuimsystemen	56
8. Bewaartermijnen ziekteverzuimgegevens.....	57
8.1 Richtlijnen.....	57
Bijlage 1 brief AP – geen combifunctie werkgever casemanager en cmttd.....	63
Bijlage 2 : brief AP – een werkgever mag niet vragen naar de taken.....	65
Bijlage 3: Publicatie met gezamenlijke uitleg beleidsregels door ministerie Sociale Zaken en Werkgelegenheid met (onbekende) stakeholders	66
Bijlage 4 : vragenbrief van werkgroep Gegevensverwerking verzuim aan AP	68
Bijlage 5: Toelichting op artikel 30 UAVG : verwerken van gezondheidsgegevens.....	75
Bijlage 6: Datalekken nader uitgeschreven	77
Bijlage 7: Rechten van betrokkene – artikelnummers AVG.....	81
Bijlage 8: Toelichting derden – bewerkers/verwerkers	88
Bijlage 9: Verwerkingsverplichtingen	90
Bijlage 10. Criteria of uw organisatie een DPIA moet uitvoeren	94
Bijlage 11: Beveiligingsbeleid	96
Bijlage 12: Vragen werknemers en werkgevers en antwoorden AP	100
Bijlage 13: veel voorkomende vragen uit de praktijk beantwoord door de werkgroep	107
Bijlage 14. Tijdslijn Wet verbetering poortwachter.....	112

Voorwoord

Voor veel werknemers, werkgevers en betrokken partijen die gegevens over de gezondheid van (zieke) werknemers verwerken, is nog te vaak onduidelijk hoe zij gezamenlijk actief aan verzuimbegeleiding en re-integratie kunnen werken conform de aangescherpte privacyregels. Ook voor bedrijfsartsen zijn er uitdagingen om de gewenste of noodzakelijke ondersteuning te geven, terwijl hun agenda al onder druk staat.

In het voorjaar 2018 is de Werkgroep Gegevensverwerking rondom de (zieke) werknemer samengesteld om te onderzoeken hoe de verschillende partijen in de praktijk met de regels van de AVG en de Autoriteit Persoonsgegevens moeten omgaan. De Werkgroep bestaat uit een afvaardiging van professionals uit het gehele werkveld van arbeid en gezondheid. Deze professionals zijn werkzaam bij of als: arbodienstverlener, zelfstandig bedrijfsarts, re-integratiebedrijf, ICT-leverancier van HR-, Arbo- en verzuimsystemen, arbeidsjurist, opleider casemanagers procesbewaking en taakdelegatie, arbeidsdeskundige, register casemanager, functionaris gegevensverwerking, HR-adviseur en inkomensverzekeraar. Daarnaast is het merendeel van deze professionals werkgever dan wel werknemer.

In dit rapport geven wij onze bevindingen weer. De werkgroep heeft de AP verzocht om op bepaalde standpunten een visie te geven. Hierop is echter, ook na herhaaldelijke reminders, geen antwoord gekomen.

Werkgroep Gegevensverwerking rondom de (zieke) werknemer

Bonnie Bleij, Ruben Colijn, Monique van de Graaf, Brenda Damkat, Leon Floris, Irene van der Linden (ons helaas komen te overlijden najaar 2018), Irma van Lieshout, Marjol Nikkels en Carmen Schrader.

1. Inleiding AVG

Vanaf 25 mei 2018 is de General Data Protection Regulation (GDPR) van toepassing in de gehele Europese Unie. In Nederland is de GDPR beter bekend onder de naam Algemene Verordening Gegevensbescherming (AVG).

De AVG vervangt de Privacyrichtlijn uit 1995, die in Nederland vorm heeft gekregen in de Wet bescherming persoonsgegevens (Wbp). Aangezien de Privacyrichtlijn stamt uit de tijd dat het internet nog maar net bestond, was deze dringend aan vernieuwing toe. De AVG is al in mei 2016 in werking getreden, maar door de implementatieperiode van twee jaar was hij pas van toepassing vanaf 25 mei 2018. Tot die tijd gold dus de Wbp.

1.1 Doel van de AVG

De Verordening heeft tot doel het niveau van bescherming van persoonsgegevens te verhogen door:

- versterking van de rechten van betrokkenen en;
- een gelijkwaardig niveau van bescherming in alle lidstaten van de EU te bewerkstelligen.

Bescherming van persoonsgegevens is een grondrecht en de verwerking van de gegevens moet ten dienste staan aan de mens. Het recht op bescherming is echter geen absoluut recht. Het moet conform het evenredigheidsbeginsel worden afgewogen tegen andere grondrechten.

De administratieve sancties en aansprakelijkheid zijn bij de AVG anders dan bij de richtlijn Wbp. De boetes zijn zeer hoog; het niet voldoende informeren van een klant of het verwerken van persoonsgegevens zonder rechtsgeldige grondslag, kan een boete opleveren van 20 miljoen Euro of 4% van de wereldwijde jaaromzet in het voorafgaande jaar (hierbij wordt aansluiting gezocht bij art 2:377 lid 6 BW – de netto omzet van een rechtspersoon).

1.2 Rollen binnen de AVG

De Verordening is van toepassing op de verwerking van persoonsgegevens in het kader van activiteiten door een verwerkingsverantwoordelijke (zoals een bank/verzekeraar en werkgever) en degene die de gegevens daadwerkelijk verwerkt. De Verordening bevat specifieke regels voor de contractuele verhouding tussen verwerkingsverantwoordelijke en verwerkers.

Er zijn drie hoofdrollen te onderscheiden:

1. Verwerkingsverantwoordelijke (Engels: controller): bepaalt doel en middelen voor de verwerking van persoonsgegevens;
2. Verwerker (Engels: processor): verwerkt ten behoeve van de verwerkingsverantwoordelijke;
3. Betrokkene (Engels: datasubject): de geïdentificeerde of identificeerbare natuurlijke persoon van wie persoonsgegevens worden verwerkt.

1.3 Ruimere scope dan Wbp

De Verordening geeft regels ter bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en is in tegenstelling tot de Wbp ook buiten de EU van toepassing bij activiteiten van een EU-partij.

De Verordening is van toepassing op:

- a. Verwerkingsverantwoordelijken en verwerkers die in de EU gevestigd zijn, ongeacht of de verwerking binnen de EU plaatsvindt. Uiteraard betreffende individuen binnen de EU.
- b. Niet EU-gevestigde verwerkingsverantwoordelijken en verwerkers die diensten leveren aan betrokkenen die zich binnen de EU bevinden óf die gedrag monitoren van betrokkenen die zich in de EU bevinden.

Alle organisaties buiten de EU die data verzamelen via websites van EU-betrokkenen kunnen dus onder de Verordening vallen.

1.4 Persoonsgegevens

Onder de Verordening hebben we nu vier categorieën van persoonsgegevens:

- a) Persoonsgegevens;
- b) Anonieme gegevens;
- c) Pseudonieme gegevens;
- d) Bijzondere persoonsgegevens.

a) Persoonsgegevens

Onder de Verordening is de definitie van Persoonsgegevens verruimd:

“Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene)”

Daaronder vallen nu ook locatiegegevens, online identificatoren en andere elementen die kenmerkend zijn voor de identiteit van de natuurlijke persoon. Natuurlijke personen kunnen gekoppeld worden aan online identificatoren via hun apparatuur, applicaties en protocollen zoals een internetprotocol (IP-adressen), identificatie-cookies of andere identificatoren. Achtergelaten sporen kunnen gecombineerd worden met andere informatie (bijvoorbeeld andere unieke identificatoren), waardoor profielen opgesteld kunnen worden en natuurlijke personen herkend kunnen worden.

Op overleden personen is, net als bij de Wbp, de Verordening niet van toepassing.

b) Anonieme gegevens

Anonieme gegevens zijn niet herleidbaar tot een individu en dus is de Verordening daarop niet van toepassing.

c) Pseudonieme gegevens

Een nieuwe categorie is de pseudonieme gegevens. Dit is het verwerken van persoonsgegevens op zodanige wijze dat deze gegevens niet meer aan bepaalde betrokkenen gekoppeld kunnen

worden zonder dat aanvullende gegevens worden gebruikt. Deze aanvullende gegevens moeten apart worden bewaard en er moeten technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.

d) Bijzondere persoonsgegevens

Bijzondere persoonsgegevens zijn gegevens die door hun aard bijzonder gevoelig zijn voor wat betreft fundamentele vrijheden (ras of etnische afkomst, maar ook gegevens waaruit ras of afkomst blijkt). Deze verdienen specifieke bescherming gelet op de risico's.

De Verordening breidt de categorie bijzondere gegevens uit met genetische en biometrische gegevens. Het gaat dan specifiek om gegevens waaruit ras of etnische afkomst blijkt, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid en gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Let op: foto's zijn dat niet persé, tenzij deze vallen onder biometrische gegevens met het oog op de unieke identificatie van een persoon. Uit een foto kan mogelijk het ras of de etnische afkomst worden herleid.

In de Verordening zijn definities opgenomen van genetische en biometrische gegevens en gegevens over gezondheid. Onder gezondheidsgegevens wordt verstaan: persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijk persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over de gezondheidstoestand wordt gegeven.

De strafrechtelijke gegevens worden apart benoemd in art 10 AVG.

1.4.1. Toets op type data

Het is dus belangrijk om voor de verschillende type data die worden verwerkt te toetsen of het persoonsgegevens zijn. Een IP-adres is dit sowieso, maar locatiegegevens en identifiers zijn nu ook persoonsgegevens. Ook het kunnen combineren van informatie kan inhouden dat de gegevens te herleiden zijn tot een natuurlijk persoon. Dat geldt ook voor biometrische data.

Wellicht kan pseudonimisering gunstig zijn: met pseudonimiseren worden persoonsgegevens getransformeerd in een dataset die niet meer direct herleidbaar is tot een persoon. Om dit te doen worden de direct identificeerbare elementen van een persoonsgegeven, zoals de naam, weggehaald. Of de dataset wordt omgecodeerd tot een nummer. Vervolgens worden de gepseudonimiseerde dataset en de (sleutel tot de) brondata apart bewaard en zijn er waarborgen aanwezig die re-identificatie voorkomen. De originele identificerende elementen zijn dus nog wel aanwezig.

Pseudonimiseren vermindert het privacyrisico van betrokkenen, maar ook het risico voor organisaties die met deze gegevens werken. De Verordening is wel van toepassing, maar er gelden dan minder strikte vereisten. Te denken valt aan geen inzagerechtigingen, etc.

1.4.2. Werknemersadministratie bij de arbodienst

In het verleden was het gebruikelijk dat het HR-systeem van een werkgever werd gekoppeld aan de verzuimadministratie van de arbodienst. Het doorgeven van werknemersbestanden aan de arbodienst is op aandringen van de Autoriteit Persoonsgegevens niet meer toegestaan. De arbodienst mag geen actieve werknemersadministratie voeren. Pas op het moment van de ziekmelding, of op het moment dat een werknemer vrijwillig een beroep doet op de arbodienstverlener of bedrijfsarts, mogen er persoonsgegevens verwerkt worden.

1.5 Wijze van uitwisseling persoonsgegevens

Voor het uitwisselen van persoonsgegevens zijn er de volgende mogelijkheden:

- Via mondeling gesprek (live of telefonisch);
- Via chat apps;
- Via e-mail, maar alleen als het veilig is (bijvoorbeeld door encryptie).
Het is niet zo dat het verboden is persoonsgegevens te mailen. Dit is afhankelijk van het beveiligingsniveau;
- Via fax;
- Via portals (verzuimvolgsystemen, HR-systemen, schademeldingssystemen, brancheloketten etc.);
- Via datadragers (USB);
- Via Cloud en Sharepoint omgeving;
- Via post (briefgeheim).

1.6 Algemeen verwerkingsverbod en de uitzonderingen

Op het verwerken van bijzondere categorieën van persoonsgegevens rust, gezien hun gevoelige aard, een algemeen verwerkingsverbod. Hierop zijn echter wel een aantal uitzonderingen geformuleerd. Een deel van de uitzonderingen is geregeld in de Verordening en van toepassing op alle bijzondere categorieën van persoonsgegevens (artikel 9 AVG). De Uitvoeringswet (UAVG) bevat daarnaast specifieke uitzonderingen per categorie (artikelen 22 tot en met 30 UAVG).

Let op: Als er sprake is van een uitzondering op het verbod om de bijzondere persoonsgegevens te verwerken, is er nog altijd wel een grondslag nodig om te kunnen verwerken, zoals opgesomd in art 6 AVG!

De Verordening biedt in artikel 9 tien verschillende algemene uitzonderingsgronden op het verwerkingsverbod op bijzondere categorieën persoonsgegevens. Denk hierbij aan de uitdrukkelijke toestemming van betrokkene. De uitzonderingen kennen specifieke voorwaarden, regels en beperkingen, die nader zijn uitgewerkt in de Uitvoeringswet en zijn onderverdeeld in:

- 1) algemene uitzonderingen
- 2) specifieke uitzonderingen op basis van de Verordening en ons nationaal recht.

1) Algemene uitzonderingsgronden UAVG

De Uitvoeringswet onderscheidt de volgende algemene uitzonderingsgronden (artikelen 22 tot en met 24 UAVG):

- a. **Uitdrukkelijke toestemming:** De eis van uitdrukkelijke toestemming is strenger dan de eis van ondubbelzinnige toestemming bij het verwerken van niet-bijzondere categorieën van persoonsgegevens. Er mag geen enkele twijfel over bestaan of de persoon in kwestie toestemming heeft gegeven. De handeling waarmee uitdrukkelijke toestemming wordt gegeven moet specifiek zijn gericht op het geven van toestemming.
- b. **Vitale belangen:** Wanneer een betrokkene fysiek of juridisch niet in staat is zijn toestemming te geven (bijvoorbeeld omdat hij niet bij bewustzijn is, maar het verwerken van persoonsgegevens noodzakelijk is voor de bescherming van zijn vitale belangen), mogen bijzondere categorieën persoonsgegevens worden verwerkt.
- c. **Verwerkingen door instanties actief op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied:** Denk hierbij aan bijvoorbeeld de ledenadministratie van een vakbond of politieke partij. De persoonsgegevens mogen niet zonder de toestemming van de betrokkenen buiten die instantie worden verstrekt.
- d. **Gegevens die kennelijk openbaar zijn gemaakt:** Dit zijn nog steeds bijzondere categorieën van persoonsgegevens, maar ze mogen onder deze omstandigheden wel worden verwerkt, aangezien de betrokkene de persoonsgegevens zelf duidelijk openbaar heeft gemaakt. Let op dat ook hiervoor geldt dat de verwerking noodzakelijk moet zijn in het licht van een gerechtvaardigd doel.
- e. **Instelling, uitoefening of onderbouwing van een rechtsvordering:** Het is toegestaan om in een gerechtelijke procedure bijzondere categorieën van persoonsgegevens te verwerken, zoals bijvoorbeeld van de wederpartij.
- f. Als verwerking noodzakelijk is om te kunnen voldoen aan een **volkenrechtelijke verplichting**, bijvoorbeeld een verplichting vanuit staats- en gerechtsdeurwaarders of vanuit internationale verdragsafspraken, bijvoorbeeld de overdracht van persoonsgegevens van personen die in verband staan met terroristische aanslagen.
- g. **Verwerking door de AP of ombudsman**, indien dat noodzakelijk is voor de uitvoering van de aan hen opgedragen wettelijke taken.
- h. Als de verwerking noodzakelijk is in aanvulling op de verwerking van **persoonsgegevens van strafrechtelijke aard**. Van deze uitzondering kan echter alleen gebruikt worden gemaakt ten behoeve van de doelen waarvoor de persoonsgegevens van strafrechtelijke aard worden verwerkt.
- i. Als de verwerking noodzakelijk is voor **wetenschappelijk of historisch onderzoek of statistische doeleinden**. Dit mag echter alleen als het onderzoek een algemeen belang dient, het vragen van uitdrukkelijke toestemming onmogelijk blijkt en er voldoende waarborgen zijn getroffen om zo min mogelijk risico's voor de persoonlijke levenssfeer van de betrokkene te creëren.

2) Specifieke uitzonderingen per categorie UAVG

De Uitvoeringswet onderscheidt de volgende specifieke uitzonderingen per categorie van bijzondere persoonsgegevens (artt 25 tot en met 30 UAVG):

a. **Gezondheidsgegevens (artikel 30 UAVG)**

Pas wanneer verstrekking van gezondheidsgegevens niet in strijd is met het medisch beroepsgeheim, gelden volgens artikel 30 UAVG vijf specifieke uitzonderingsgronden op het verwerkingsverbod voor gezondheidsgegevens. Voor verzekeraars is de uitzonderingsgrond van art 30 lid 3 onder b UAVG van belang: gezondheidsgegevens mogen wel verwerkt worden indien dit nodig is voor de beoordeling van het door de verzekeraar te verzekeren risico. Een toelichting hierop is gegeven in bijlage 5.

b. **Data Protection Impact Assessment (DPIA)**

Het op grote schaal verwerken van bijzondere persoonsgegevens, zoals medische gegevens, valt onder een hoog privacyrisico waarvoor een DPIA nodig is. Zie verder Hoofdstuk 2.3.

c. **Gevoelige gegevens**

Ook gegevens die niet 'bijzonder' zijn in de zin van de Verordening, kunnen volgens de AP gevoelig zijn. Denk hierbij bijvoorbeeld aan financiële data of locatiegegevens. De te nemen maatregelen om de persoonsgegevens te beschermen, zijn mede afhankelijk van de gevoeligheid van de gegevens en het risico dat zij kunnen vormen voor de betrokkene bij verkeerd gebruik of misbruik.

d. **Burgerservicenummer | BSN (artikel 87 AVG en artikel 46 UAVG)**

Het BSN wordt onder de Verordening en in de Uitvoeringswet niet aangemerkt als een bijzonder persoonsgegeven, anders dan wel werd aangenomen onder de Wbp. Afgezien hiervan worden geen veranderingen voorgesteld voor het verwerken van het BSN.

- Artikel 87 van de Verordening geeft een grondslag om bij lidstatelijk recht specifieke voorwaarden te stellen aan de verwerking van een nationaal identificatienummer (BSN).
- Artikel 46 van de Uitvoeringswet regelt dat een nummer dat ter identificatie van een persoon bij de wet is voorgeschreven, bij de verwerking van persoonsgegevens slechts gebruikt wordt ter uitvoering van de betreffende wet dan wel voor doeleinden bij de wet bepaald.

Overheidsorganen kunnen bijvoorbeeld bij het verwerken van persoonsgegevens - in het kader van de uitvoering van hun publieke taak - gebruikmaken van het BSN, zonder dat daarvoor nadere regelgeving vereist is (artikel 10 Wet algemene bepalingen burgerservicenummer (Wabb)). Voor instellingen die geen beroep kunnen doen op artikel 10 Wabb, dient het gebruik te zijn voorgeschreven in sectorale wetgeving. Zo geldt bijvoorbeeld voor verzekeraars en banken dat zij het BSN mogen gebruiken voor uitwisseling van gegevens met de Belastingdienst.

In de praktijk bestaat soms de wens het BSN ook voor andere doelen te gebruiken dan ter uitvoering van de wet waarin het voorschrift over het nummer is opgenomen. Dit is alleen mogelijk als aan twee vereisten is voldaan:

- Ten eerste geldt het algemene vereiste dat persoonsgegevens alleen verder mogen worden verwerkt als dat verenigbaar is met de doeleinden waarvoor ze zijn verkregen.
- Ten tweede bepaalt artikel 46 UAVG dat verwerking van persoonsnummers voor andere doeleinden dan de uitvoering van de betreffende wet alleen mogelijk is voor zover dat bij de wet is bepaald.

Eventuele andere gebruiksdoelen dienen dus door de formele wetgever zelf te worden vastgesteld. Er komt voor de verdere verwerking van het BSN geen eigen afweging toe aan de verwerkingsverantwoordelijke.

1.7 Vrijwillig gedeelde gegevens

Een werkgever mag geen vragen stellen over de gezondheidssituatie van de werknemer, maar wat als een werknemer zelf van alles vertelt? De wet geeft een verbod op het verwerken van bijzondere persoonsgegevens, tenzij er sprake is van een noodzakelijkheidsvereiste.

De werkgever heeft de verplichting om bij een ziekmelding de bedrijfsarts in te schakelen. Deze beoordeelt of en zo ja welke, mogelijkheden de werknemer nog heeft. Voor de werkgever is er dus geen noodzaak om te weten wat er precies aan de hand is en dus ook geen grondslag om deze gegevens te verwerken.

Bovendien wordt door de AP altijd in twijfel getrokken of informatie inderdaad vrijwillig gegeven is, gezien de gezagsverhouding tussen werkgever en werknemer. Ook kan de werknemer te allen tijde zijn gegeven toestemming weer intrekken. Met andere woorden: ook gegevens die een werknemer spontaan deelt, mogen niet verwerkt worden.

1.8 Bewustwording en overige stappen in organisaties t.a.v. de AVG

AP heeft een tienstappenplan uitgegeven om organisaties te helpen te werken conform de richtlijnen van de AVG.

Stap 1. Bewustwording van noodzakelijkheidseis en dataminimalisatie

Zorg ervoor dat de relevante mensen in de organisatie (zoals beleidsmakers) op de hoogte zijn van de nieuwe privacyregels, zodat zij zich doorlopend bewust zijn van de uitgangspunten van de AVG bij gegevensverwerking qua dataminimalisatie en noodzakelijkheid. Dit geldt ook voor de data-uitwisseling met andere partijen.

Stap 2. Rechten van betrokkenen (zie bijlage 7)

Zorg ervoor dat betrokkenen hun privacy-rechten goed kunnen uitoefenen:

- Recht op inzage;
- Recht op correctie;
- Recht op verwijdering;

- Recht op dataportabiliteit;
- Recht op bezwaar;
- Recht op menselijke blik;
- Recht op beperking van verwerking.

Wees ervan bewust dat mensen bij AP klachten kunnen indienen over de manier waarop de organisatie met hun gegevens omgaat. AP is verplicht deze klachten te behandelen.

Stap 3. Overzicht verwerkingen

Breng de gegevensverwerkingen in kaart. Documenteer welke persoonsgegevens de organisatie verwerkt en met welk doel dit wordt gedaan, waar deze gegevens vandaan komen en met wie ze worden gedeeld. De organisatie heeft een verantwoordingsplicht en moet kunnen aantonen dat deze organisatie in overeenstemming met de AVG handelt. Houd daarom een register van verwerkingsactiviteiten bij.

Stap 4. Data protection impact assessment (DPIA)

Komt uit een DPIA naar voren dat de beoogde verwerking een hoog risico oplevert? En lukt het de organisatie niet om maatregelen te vinden om dit risico te beperken? Dan moet er met AP overleg plaatsvinden voordat er met de verwerking gestart wordt.

Stap 5. Privacy by design en privacy by default

Maak de organisatie vertrouwd met de onder de AVG verplichte uitgangspunten van *privacy by design* en *privacy by default* en ga na hoe deze beginselen binnen de organisatie kunnen worden ingevoerd.

- Privacy by design: Zorg er al bij het ontwerpen van producten en diensten voor dat persoonsgegevens goed worden beschermd, er niet meer gegevens worden verzameld dan nodig en de gegevens niet langer worden bewaard dan nodig;
- Privacy by default: Neem technische en organisatorische maatregelen om ervoor te zorgen dat de organisatie, als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat zij willen bereiken.

Stap 6. Functionaris voor de gegevensbescherming

Bepaal of er sprake is van een verplichting om een functionaris voor de gegevensbescherming (FG) aan te stellen.

Stap 7. Meldplicht datalekken

De AVG stelt strengere eisen aan de eigen registratie van de datalekken die zich in de organisatie hebben voorgedaan. Alle datalekken moeten gedocumenteerd worden.

Stap 8. Verwerkersovereenkomsten

Heeft de organisatie haar gegevensverwerking uitbesteed aan een bewerker (in de AVG 'verwerker' genoemd)? Beoordeel dan of de overeengekomen maatregelen in bestaande contracten met de bewerkers nog steeds toereikend zijn. En of deze voldoen aan de eisen die de AVG aan verwerkersovereenkomsten stelt. Zo niet, breng dan tijdig noodzakelijke wijzigingen aan. Zie bijlage 8 voor een nadere toelichting.

Stap 9. Leidende toezichthouder

Heeft de organisatie vestigingen in meerdere EU-lidstaten? Of hebben de gegevensverwerkingen in meerdere lidstaten impact? Dan hoeft de organisatie onder de AVG nog maar met één privacy-toezichthouder zaken te doen. Bepaal dan onder welke privacy-toezichthouder de organisatie valt.

Stap 10. Toestemming

De gegevensverwerking kan gebaseerd zijn op toestemming van de betrokkenen. De AVG stelt strenge eisen aan toestemming. Evalueer daarom de manier waarop er toestemming wordt gevraagd, verkregen en geregistreerd wordt en pas dit zo nodig aan. De organisatie moet kunnen aantonen dat zij een geldige toestemming van mensen heeft gekregen om hun persoonsgegevens te verwerken. Het moet voor mensen net zo makkelijk zijn om hun toestemming in te trekken als om die te geven.

2. Verwerkersovereenkomsten en Register van verwerkingsactiviteiten voor arbodiensten en verzuim-/casemanagementbedrijven

2.1 Wie zijn zelfstandige verwerkersverantwoordelijken?

Onder zelfstandige verwerkersverantwoordelijken worden verstaan:

- Werkgever;
- Verzekeringsadviseur;
- Inkomensverzekeraar;
- Gevolmachtigd agent;
- Zelfstandig werkende casemanager;
- Zelfstandig werkende bedrijfsarts;
- Re-integratiebedrijf.

Een uitzondering hierop is de leverancier van digitale portalen (werkloket, verzuimvolgsysteem, etc.) die al dan niet door de inkomensverzekeraar, gevolmachtigd agent en/of re-integratiebedrijf beschikbaar zijn gesteld.

Als er sprake is van zelfstandige en/of gezamenlijke verwerkersverantwoordelijken, dan is er dus geen verwerkersovereenkomst noodzakelijk. Wel is aan te raden om goede afspraken te maken over de onderlinge gegevensuitwisseling, het doel en de middelen die worden gebruikt.

Een zelfstandig werkend casemanager heeft geen overeenkomst nodig met het UWV, omdat de uitwisseling van persoonlijke gegevens is gebaseerd op de uitvoering van de wet. Ter vergelijking heeft de salarisadministrateur ook geen verwerkingsovereenkomst nodig met de Belastingdienst.

Salarisadministrateurs, accountants, etc., die in opdracht van de werkgever persoonsgegevens verwerken, dienen wel een verwerkersovereenkomst te sluiten. Zo ook leveranciers van ICT-systemen (HR-portalen, verzuimvolgsystemen, etc.).

2.2 Register van verwerkingsactiviteiten

Als een organisatie de verwerkingsverantwoordelijke is, moet de volgende informatie in het register van verwerkingsactiviteiten opgenomen worden:

- De naam en contactgegevens van:
 - De organisatie of de vertegenwoordiger van de organisatie;
 - Eventuele andere organisaties met wie de organisatie gezamenlijk de doelen en middelen van de verwerking heeft vastgesteld;
 - De Functionaris voor de gegevensbescherming (FG), als de organisatie die heeft aangesteld;
 - Eventuele andere (internationale) organisaties waarmee de organisatie persoonsgegevens deelt;
- De doelen waarvoor de persoonsgegevens verwerkt worden;

- Een beschrijving van de categorieën van personen van wie de gegevens verwerkt worden, zoals bijvoorbeeld uitkeringsgerechtigden, klanten of patiënten;
- Een beschrijving van de categorieën van persoonsgegevens, zoals BSN, NAW-gegevens, telefoonnummers, camerabeelden of IP-adressen;
- De datum waarop de organisatie de gegevens moet kennen (als deze bekend is);
- De categorieën van ontvangers aan wie de organisatie de persoonsgegevens verstrekt;
- Of de organisatie de gegevens deelt met een land of internationale organisatie buiten de EU;
- Een algemene beschrijving van de technische en organisatorische maatregelen die de organisatie heeft genomen om persoonsgegevens die verwerkt worden te beveiligen.

2.3 Data protection impact assessment (DPIA)

Een DPIA is o.a. bij grootschalige gegevensverwerking een verplicht instrument om vooraf na te denken over de privacy-risico's van een bepaalde gegevensverwerking en deze risico's vervolgens te verkleinen door aanpassingen te doen.

De AVG geeft geen definitie van 'grootschalige gegevensverwerkingen/ het op grote schaal verwerken'. De guideline Working Party 29 adviseert om met de volgende criteria te bepalen of hiervan sprake is:

- De hoeveelheid mensen van wie gegevens worden verwerkt;
- De hoeveelheid gegevens en/of de verscheidenheid aan gegevens die worden verwerkt;
- De tijdsduur van de gegevensverwerking;
- De geografische reikwijdte van de gegevensverwerking.

De kern van de DPIA is:

- In kaart brengen van de verwerking: Welke gegevens worden met welk doel verwerkt? Zie tevens bijlage 9 voor een toelichting van de verwerkingsverplichtingen.
- In kaart brengen van de impact daarvan op de privacy: wat zijn de gevolgen voor de mensen van wie organisatie gegevens verwerkt?
- Bekijken of de organisatie maatregelen kan treffen om de privacy-impact te verkleinen.

Een DPIA is alleen verplicht als een gegevensverwerking waarschijnlijk een hoog privacy-risico oplevert voor de betrokkenen. Dat is in ieder geval zoals een organisatie:

- Systematisch en uitvoerig persoonlijke aspecten evalueert, waaronder profiling;
- Op grote schaal bijzondere persoonsgegevens verwerkt;
- Op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

Ook gekoppelde databases met informatie over kwetsbare groepen personen kunnen aanleiding zijn voor het doen van een DPIA. In bijlage 10 zijn de criteria opgenomen om te toetsen of uw organisatie een DPIA moet uitvoeren.

2.4 Heeft een organisatie een Functionaris Gegevensbescherming nodig?

Een Functionaris Gegevensbescherming (FG) houdt toezicht op de toepassing en naleving van de privacywetgeving. Vaak wordt ook de Engelse term gebruikt: Data Protection Officer (DPO).

Er zijn drie soorten organisaties die onder de AVG verplicht zijn een FG te hebben:

- Overheidsinstanties en publieke organisaties, zoals zorg- en onderwijsinstellingen;
- Organisaties die vanuit hun kernactiviteiten op grote schaal individuen volgen;
- Organisaties die vanuit hun kernactiviteiten op grote schaal bijzondere persoonsgegevens verwerken.

Om te weten of een organisatie op grote schaal persoonsgegevens verwerkt, kan naar de volgende criteria worden gekeken:

- 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.

Voorbeelden van verwerkingen die als grootschalig worden gezien, zijn:

- Een ziekenhuis dat patiëntgegevens verwerkt;
- Een vervoersmaatschappij die reisinformatie verwerkt van mensen die met het openbaar vervoer in een bepaalde stad reizen;
- Een verzekeringsmaatschappij of bank die klantgegevens verwerkt als onderdeel van de gebruikelijke werkzaamheden;
- Een zoekmachine die persoonsgegevens verwerkt om advertenties te kunnen tonen op basis van internetgedrag;
- Een telefoon- of internetprovider die gegevens verwerkt over het telefoon- en/of internetgedrag van klanten.

De Europese privacy-toezichthouders verwachten dat er op den duur een praktische standaard komt waarmee eenvoudiger kan worden bepaald of een organisatie volgens de AVG op grote schaal (bijzondere) persoonsgegevens verwerkt en dus een FG moet aanstellen en een DPIA moet uitvoeren.

2.4.1 Wat moet de FG doen?

De FG moet in de organisatie privacy-bewustzijn creëren. Hij/zij informeert en adviseert de organisatie over de verplichtingen op grond van de privacywetgeving en zorgt voor bewustmaking en opleiding van het betrokken personeel.

Ook is de FG actief betrokken bij de wijze waarop wordt omgegaan met gegevens. Hij/zij denkt bijvoorbeeld mee over het wel of niet uitvoeren van een DPIA, de wijze waarop de DPIA uitgevoerd moet worden en het beperken van risico's die kleven aan de gegevensverwerking. Daarnaast ziet hij/zij toe op de naleving van de privacywetgeving, het eigen interne privacy-beleid en is hij/zij het eerste aanspreekpunt voor AP.

2.4.2 Aan welke eisen moet een FG voldoen?

Een FG moet voldoende deskundig zijn - en over voldoende professionele kwaliteiten beschikken - om de hiervoor genoemde taken te kunnen uitvoeren. Hij/zij moet dus:

- Ervaring hebben met nationale en Europese privacywetgeving en -gebruiken, inclusief uitgebreide kennis van de AVG;
- Verstand hebben van de gegevensverwerkingen die de organisatie uitvoert;
- Verstand hebben van IT en beveiliging van gegevens;
- Kennis hebben van de desbetreffende sector en organisatie;
- In staat zijn om binnen de organisatie beveiliging van data te promoten;
- Betrouwbaar zijn (geheimhoudingsplicht).

2.5 Meldplicht datalekken

De meldplicht datalekken vervalt niet: de werkgever moet datalekken blijven melden bij AP en hoe dan ook alle datalekken documenteren. De meldplicht zoals uitgewerkt in artikel 31 (zie voor meer informatie bijlage 6) bepaalt dat datalekken niet hoeven worden gemeld als het onwaarschijnlijk is dat deze resulteren in een risico voor de rechten en vrijheden van individuen. Wanneer een datalek tot een hoog risico leidt voor de rechten en vrijheden van de betrokkene(n), dan moet(en) de betrokkene(n) ook worden geïnformeerd.

Bij het verzamelen persoonsgegevens moet de volgende informatie gegeven worden:

- Doel waarvoor de persoonsgegevens zijn bestemd;
- In voorkomend geval: Wie de ontvangers zijn van de persoonsgegevens;
- Hoelang de gegevens worden bewaard;
- Recht op inzage of wissing, recht op bezwaar, recht op overdraagbaarheid gegevens;
- Recht om toestemming altijd in te trekken;
- Recht op het indienen van een klacht;
- Of de verstrekking van de gegevens een wettelijke of contractuele verplichting is - of een noodzakelijke voorwaarde - om de overeenkomst te sluiten en wat de gevolgen zijn als de gegevens niet worden verstrekt.

Van belang is dat er niet méér persoonsgegevens worden verwerkt, dan strikt noodzakelijk voor het doel van de verwerking.

Houdt steeds in de gaten dat er niet méér persoonsgegevens verwerkt worden dan strikt noodzakelijk voor het doel van de verwerking.

3. Beleidsregels AP ‘De zieke werknemer’

3.1 Aanleiding

Begin 2016 presenteerde de Autoriteit Persoonsgegevens (AP) het document ‘De zieke werknemer’, met beleidsregels voor de verwerking van persoonsgegevens over de gezondheid van zieke werknemers. Kortweg: Beleidsregels zieke werknemer. Het doel was het voor een breder publiek meer toegankelijk maken van de bestaande spelregels van de Wet bescherming persoonsgegevens (Wbp). Dit document geeft duidelijkheid over welke gegevens bijvoorbeeld werkgevers, verzekeraars, UWV, bedrijfsartsen en re-integratiebedrijven over de gezondheid van (zieke) werknemers mogen verwerken. De normen in deze beleidsregels zijn het uitgangspunt voor de AP bij het toepassen van handhavende maatregelen en dus belangrijk om te kennen. Daarnaast nam de sanctiemogelijkheid van AP toe tot ruim € 800.000,-. Met de komst van de AVG heeft AP nog veel ruimere sanctiemogelijkheden (20 miljoen Euro of 4% van de wereldwijde jaaromzet als dat bedrag hoger is).

Het document ‘De beleidsregels zieke werknemer’ heeft tot heel wat commotie in verzuimland geleid. Het werd duidelijk dat *alle* gezondheidsgegevens onder de Wbp vallen en dat een werkgever/leidinggevende al snel in overtreding is als hij/zij vragen stelt aan de werknemer die zich ziek meldt (en vaak het hele ‘verhaal’ vertelt). Ook gegevens over de functionele beperkingen en mogelijkheden van een werknemer, zijn gezondheidsgegevens in de zin van artikel 16 Wbp.

Sinds de publicatie van de beleidsregels zijn er tal van reacties en stromingen de revue gepasseerd die zich vooral bezighouden met het ontkennen of ombuigen van de beleidsregels. Enerzijds omdat ze niet werkbaar zouden zijn of te ver doorslaan en anderzijds dat AP toch geen capaciteit heeft om te handhaven.

Vanuit onze werkgroep adviseren we om de AVG en de beleidsregels de zieke werknemer serieus te nemen en ervoor te zorgen dat het verzuimbeleid en werkwijze overeenkomt met de grondbeginselen van de AVG en de door AP opgestelde beleidsregels ‘De zieke werknemer’. Onderstaande uitleg over deze beleidsregels is dus ook interessant voor een werkgever of HR-afdeling.

3.2 Verwerking van persoonsgegevens op grond van de arbeidsovereenkomst

Een werkgever mag persoonsgegevens verwerken op basis van een in de wet (o.a. Arbowet) genoemde juridische grond of op basis van een overeenkomst of indien betrokkene toestemming heeft gegeven. Deze toestemming moet bestaan uit een ‘vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting’. In arbeidsovereenkomsten staat vaak iets als de volgende bepaling: *“De werknemer verleent de werkgever door ondertekening van de arbeidsovereenkomst ondubbelzinnig toestemming om zijn persoonsgegevens te verwerken in het kader van de arbeidsverhouding.”* Deze ondubbelzinnige toestemming staat onder druk, omdat er tussen werkgever en werknemer sprake is van een gezagsverhouding, waardoor de vrije wilsuiting al snel ter discussie staat.

3.3 Controleer de personeelsdossiers: leg geen aard en oorzaak van ziekte vast

Voor personeelsdossiers is de hoofdregel dat alleen informatie mag worden bijgehouden die noodzakelijk is voor het kunnen onderbouwen van arbeidsrechtelijke zaken, zoals functioneren, verzuim, promotie en ontslag. Gegevens over de aard en oorzaak van ziekte horen daar niet bij!

De AVG geeft aan werkgevers de volgende voorwaarden voor het aanleggen van personeelsdossiers:

- Werkgevers zijn verantwoordelijk voor de juistheid en nauwkeurigheid van de gegevens in het personeelsdossier;
- Werkgevers mogen niet meer gegevens in het personeelsdossier vastleggen dan nodig is en de gegevens moeten ter zake doen;
- Werkgevers moeten de werknemers informeren over waarom zij hun gegevens verzamelen;
- Werkgevers moeten de persoonsgegevens beveiligen, zodat ze niet verloren raken of in verkeerde handen terechtkomen;
- Werkgevers mogen de persoonsgegevens niet langer bewaren dan noodzakelijk is;
- Werkgevers moeten werknemers de mogelijkheid bieden hun gegevens in te zien - dit geldt in principe voor het gehele personeelsdossier - en eventueel te corrigeren.

3.4 Gezondheidsgegevens

Als uitgangspunt geldt een verbod op verwerking van gegevens over de gezondheid. Zie hierover ook de informatie in Hoofdstuk 1.4 'Persoonsgegevens'. Het is nooit nodig dat de werkgever beschikt over gegevens over de aard en oorzaak van de ziekte of over de mogelijkheden en beperkingen van de werknemer. Daar mag de werkgever dus ook niet naar vragen; dat is voorbehouden aan de bedrijfsarts. De werkgever mag dus geen gezondheidsgegevens bewaren in een personeelsdossier. Ze mogen zelfs niet bewaard worden in een voor de bedrijfsarts bedoeld verzuimsysteem, als dat systeem door de werkgever zelf beheerd wordt.

Er zijn enkele uitzonderlijke situaties denkbaar waarin de bedrijfsarts of zijn/haar taakgedelegeerde op grond van toestemming van de zieke werknemer gegevens over zijn gezondheid aan de werkgever kan verstrekken. Bijvoorbeeld als de werknemer zelf expliciet vraagt om de werkgever te laten weten dat hij epilepsie heeft en wat de werkgever moet doen in noodsituaties.

Let op: Schakelt de werkgever een derde partij in om persoonsgegevens te verwerken (bijvoorbeeld in een extern verzuimsysteem) dan blijft werkgever wel (eind-) verantwoordelijk voor de verwerking van de persoonsgegevens. Een verwerkersovereenkomst tussen werkgever en de verwerker vormt dan de grondslag van de gemaakte afspraken omtrent gegevensverwerking.

3.5 Noodzakelijke gegevens voor de loondoorbetalingsplicht en re-integratie

De werkgever is twee jaar (104 weken) verantwoordelijk voor de loondoorbetaling en re-integratie van zijn zieke en/of arbeidsongeschikte werknemers. Deze verplichting is vastgelegd in artikel 7:658a BW en artikel 25 WIA. Gedurende de periode van loondoorbetaling, maar ook daarna (artikel 29, 30 en 42 WIA), moeten de werkgever en de werknemer werken aan re-integratie.

Re-integratie is het actief verkorten van ziekteverzuim en arbeidsongeschiktheid met als doel een (versnelde) terugkeer in de eigen of een andere functie bij de huidige (eerste spoor) of een andere werkgever (tweede spoor).

De AVG bevat een verbod op de verwerking van gezondheidsgegevens, tenzij er sprake is van een ontheffing op dit verbod welke staat beschreven in de Uitvoeringswet Algemene Verordening Gegevensverwerking (art. 30 UAVG). Gegevens die nodig zijn voor de re-integratie van werknemers vallen onder een ontheffing. De werkgever mag dus in het kader van zijn loondoorbetalingsverplichting en voor de re-integratie een beperkt aantal noodzakelijke medische gegevens verwerken van zijn zieke werknemers.

4. Rechten en plichten in de Wet verbetering poortwachter (WVP) en de WIA

4.1 Rechten en plichten in de WVP

De WVP stelt regels aan werkgever en werknemer voor verzuimbegeleiding en re-integratie in de eerste twee jaren ziekteverzuim. Die regels zijn vastgelegd in verschillende wetten, in de Regeling procesgang eerste en tweede ziektejaar en in de Beleidsregels beoordelingskader poortwachter.

Van deze procesgang maken deel uit:

- Ziekmelding;
- Probleemanalyse en advies door de bedrijfsarts (en bijstellingen);
- Plan van Aanpak, gezamenlijk opgesteld door werkgever en werknemer (en bijstellingen);
- Ziekmelding aan het UWV na 42 weken;
- (Eerstejaars)evaluatie;
- Re-integratieverslag;
- WIA-aanvraag/beoordeling.

Gedurende het traject houdt de werkgever een re-integratiedossier bij. Bij de (bijstellingen) Probleemanalyse (het niet-medische deel!) gaat het vooral om het vaststellen wat de werknemer nog wel kan, waarna een Plan van Aanpak voor re-integratie kan worden opgesteld. In (de bijstellingen van) het Plan van Aanpak wordt een casemanager Wet verbetering poortwachter aangewezen, die verantwoordelijk is voor het coördineren van het traject en die de contacten onderhoudt tussen alle betrokken partijen. De werkgever kan ook zelf de rol van casemanager WVP vervullen.

Casemanager Wet verbetering poortwachter (en WIA)

Een casemanager Wet verbetering poortwachter is een procesbegeleider van een verzuimdossier. De werkgever en werknemer benoemen samen een interne of externe persoon als casemanager Wet verbetering poortwachter en leggen dit vast in het Plan van Aanpak. Deze persoon begeleidt de overeengekomen activiteiten en verzorgt het contact tussen werknemer, werkgever en arbodienst. De casemanager Wet verbetering poortwachter (en WIA) mag over dezelfde persoonsgegevens beschikken als de werkgever. De casemanager verwerkt in deze rol van procesbegeleider alleen proces- en administratieve gegevens.

Ook na de periode van loondoorbetaling (na de reikwijdte van de Wet verbetering poortwachter) kan de casemanager een rol in de begeleiding hebben. Het gaat dan om de periode waarin een ex-werknemer recht heeft op een Ziektewetuitkering als de werkgever daarvoor eigenrisicodragend is en/of de eerste 10 jaar dat de (ex-)werknemer recht heeft op een WGA-uitkering waarvoor zijn (ex-)werkgever het eigen risico draagt.

De re-integratieactiviteiten zijn gericht op herstel van het arbeidsvermogen en op hervatting van dezelfde of andere werkzaamheden bij dezelfde of een andere werkgever. Werkgever en werknemer moeten zich hierin laten bijstaan door een arbodienst/bedrijfsarts en eventueel een re-integratiebedrijf.

Indien noodzakelijk moet de werkgever het werk, de werkplek en/of de arbeidsmiddelen van de werknemer aanpassen. De verschillende poortwachterstappen zijn aan een strak tijdspad gebonden, dit tijdspad is opgenomen in bijlage 14.

4.2. Rechten en plichten in de WIA

Op grond van de WIA hebben de (eigenrisicodragende) werkgever en de werknemer diverse verplichtingen, gericht op behoud, herstel of bevordering van de mogelijkheden tot werken. De verplichtingen van de werkgever zijn omschreven in artikel 42 Wet WIA. De verplichtingen van de (ex-)werknemer met een WGA-uitkering zijn omschreven in artikel 27 t/m 30 Wet WIA.

Als de (ex-)werknemer zich niet aan de regels houdt, kan dat gevolgen hebben voor de WGA-uitkering: de eigenrisicodragende werkgever kan dan een sanctie opleggen. De hoogte en duur van de sanctie is afhankelijk van de zwaarte van de overtreding.

In de procesbeschrijving re-integratie WGA-gerechtigden van het Verbond van Verzekeraars, de Nederlandse Vereniging van Arbeidsdeskundigen en de brancheorganisatie OVAL worden praktische handvatten aangereikt om werkgevers, werknemers, en partijen die hen ondersteunen te helpen om de re-integratie tijdens de WGA-uitkering zo goed mogelijk te organiseren. De procesbeschrijving wordt op dit moment herschreven als gevolg van de AVG.

4.3 Werknemer ziek melden in verband met claim op de inkomensverzekering

De werkgever, haar (intern/extern) HR-adviseur, (intern/extern) casemanager Wet verbetering poortwachter/WIA mag categorie A-gegevens in verband met het ziek melden van de werknemer en een mogelijke claim op de inkomensverzekering, conform de instructies in de verzekeringsovereenkomst, doorgeven aan de claimbehandelaar van de inkomensverzekeraar of gevolmachtigd agent. In opdracht van de werkgever mag ook de arbodienst deze categorie A-gegevens aan de inkomensverzekeraar doorgeven. De melding mag niet via de assurantieadviseur plaatsvinden. Zie voor de verschillende categorieën gegevens in het kader van inkomensverzekeringen (paragraaf 5.2) en de handleiding privacy inkomensverzekering van het Verbond van Verzekeraars en brancheorganisatie OVAL. In november 2018 is een nieuwe handleiding gepubliceerd.

4.4 Wat mag de werkgever vragen en registreren bij een ziekmelding?

Een werkgever mag als een werknemer zich ziek meldt de volgende gegevens over zijn gezondheid vragen en registreren:

- telefoonnummer en (verpleeg)adres;
- vermoedelijke duur van het verzuim;
- lopende afspraken en werkzaamheden;
- of de werknemer onder één van de vangnetbepalingen van de Ziektewet valt (maar niet onder welke vangnetbepaling hij valt);
- of de ziekte verband houdt met een arbeidsongeval;
- of er sprake is van een verkeersongeval, waarbij een eventueel aansprakelijke derde betrokken is (regresmogelijkheid).

Dit is een limitatieve opsomming. De werkgever mag dus in principe geen andere gegevens over de gezondheid verwerken dan de gegevens uit de hier bovengenoemde lijst. Vraag dus niet wat de werknemer precies mankeert en waardoor dat komt. Dat is wettelijk niet toegestaan.

Alleen in uitzonderlijke gevallen mag de werkgever de door werknemer vrijwillig verstrekte gegevens over de aard en oorzaak van de ziekte in het personeelsdossier registreren. Bijvoorbeeld als een werknemer in ernstige mate last heeft van suikerziekte of epilepsie en hij dit zelf of via de bedrijfsarts heeft aangegeven bij de werkgever. Zo weten de directe collega's wat zij in geval van nood moeten doen.

Naast de gegevens van de ziekmelding, mag de werkgever gegevens verwerken die de bedrijfsarts en/of arbodienst verstrekt over:

- Werkzaamheden waartoe werknemer niet meer of nog wel in staat is (functionele beperkingen, restmogelijkheden en gevolgen voor het soort werk dat werknemer nog kan doen);
- Verwachte duur van het verzuim;
- Mate waarin werknemer arbeidsongeschikt is (gebaseerd op functionele beperkingen, restmogelijkheden en gevolgen voor het soort werk dat werknemer nog kan doen);
- Eventuele adviezen over aanpassingen, werkvoorzieningen of interventies die werkgever voor de re-integratie moet treffen.

4.4.1 Gegevens die een werknemer vrijwillig verstrekt

In een normale arbeidsverhouding zal een werknemer de werkgever gewoon informeren over wat er aan de hand is. Let er echter op dat wat hij of zij vertelt nergens wordt vastgelegd. De werkgever mag, met uitzondering van de hierboven genoemde gegevens, in principe geen andere gegevens over de gezondheid van de werknemer in de eigen administratie registreren en/of doorgeven aan de bedrijfsarts/arbodienst. Ook niet als de werknemer deze gegevens vrijwillig verstrekt of zelfs als hij of zij hiervoor toestemming geeft. Het standpunt van AP is dat een werknemer zich al snel verplicht kan voelen om toestemming te geven. Er is immers sprake van een gezagsverhouding tussen werkgever en werknemer. Van een 'vrije' wilsuiting zal volgens de AP meestal geen sprake zijn. In juli 2018 heeft het Ministerie Sociale Zaken en Werkgelegenheid namens (onbekende) stakeholders een publicatie uitgebracht waarin de gezamenlijke uitleg van de beleidsregels is weergegeven. De werknemer mag geenszins onder druk staan en iets te vertellen, maar wel geheel vrijblijvend uit zichzelf wat delen. De werkgever mag er niet naar vragen. Zie bijlage 3.

4.4.2 Vermoedelijke duur van het verzuim

De werkgever heeft er natuurlijk belang bij om te weten hoelang het verzuim naar verwachting gaat duren, zodat de organisatie hiermee rekening kan houden. Als de werknemer hier zelf nog geen idee over heeft, dan is het aan de bedrijfsarts om de werkgever hierover te informeren. Dat is immers bij uitstek degene die hierover een deskundig oordeel kan geven. Op basis van zijn inschatting kan de werkgever naar de lopende afspraken en werkzaamheden kijken en beslissen of het noodzakelijk is activiteiten door een collega of vervanger over te laten nemen.

4.4.3 Over te nemen werkzaamheden

De werkgever mag vragen of er werkzaamheden overgenomen moeten worden. Dat is iets anders dan de vraag welke werkzaamheden werknemer nog wel kan verrichten. Hierover is in het veld veel onduidelijkheid, omdat sommige opleiders hierover anders denken. AP heeft hier in een brief van december 2017 duidelijkheid over gegeven: “Het standpunt van AP is dat de werkgever niet zonder tussenkomst van de bedrijfsarts mag vragen welke taken de werknemer nog wel kan uitvoeren.” Een werkgever mag er niet zelf naar vragen, maar in een publicatie van het Ministerie van Sociale Zaken en Werkgelegenheid uit juli 2018 staat dat de werknemer wel vrijwillig, zonder dwang, uit zichzelf mag delen wat hij nog wel zou kunnen doen. Deze uitleg van de beleidsregels is weergegeven in bijlage 3. Overigens heeft de AP niet op dit document gereageerd.

4.4.4 Vangnetbepaling

Voor sommige werknemers heeft de werkgever een compensatie voor de loondoorbetalingsplicht bij ziekte via het zogenaamde Vangnet Ziektewet. Werkgevers ontvangen dan een Ziektewetuitkering van het UWV.

De vangnetregeling geldt voor:

- werknemers die ziek zijn door zwangerschap of bevalling;
- werknemers die ziek zijn door orgaandonatie;
- werknemers met een arbeidsongeschiktheidsverleden die binnen vijf jaar na indiensttreding opnieuw arbeidsongeschikt worden (no-riskpolis);
- werknemers die vallen onder de Compensatieregeling (oudere langdurig werklozen).

Het is dus voor een werkgever belangrijk te weten of een werknemer onder een vangnetbepaling valt. Dat mag de werkgever dan ook vragen, maar niet onder welke vangnetbepaling.

4.4.5 Functionele beperkingen

Het is belangrijk hoe zaken worden omschreven, want de aard en oorzaak van ziekte mogen niet worden benoemd. De vastlegging moet aangeven waarin de werknemer functioneel beperkt is, zoals:

- Bukken, torderen, langdurig staan, langdurig zitten;
- Tillen, grijpen, vastpakken, dragen;
- Knielen, hurken;
- Duwen en reiken;
- Knikken, linksom of rechtsom kijken;
- Concentreren en verdelen van de aandacht;
- Omgaan met conflicten.

Of: beperkingen hebben een frequent karakter.

4.5 Welke gegevens mag de bedrijfsarts/arbodienst met werkgever delen?

Nadat een werknemer zich heeft ziekgemeld treedt de Wet verbetering poortwachter in werking. Samen met de werknemer start de werkgever een traject om ervoor te zorgen dat de werknemer zo snel mogelijk weer aan de slag kan. Op grond van de Arbowet en het Arbobesluit is de werkgever verplicht zich hierbij te laten bijstaan door een geregistreerde bedrijfsarts of een gecertificeerde arbodienst. De bedrijfsarts/arbodienst adviseert de werkgever over de beperkingen en

mogelijkheden van de zieke werknemer en wat deze betekenen voor het soort werk dat de werknemer nog kan doen.

Arbodienst

Een gecertificeerd dienstverlener* gericht op preventie, verzuimbegeleiding en re-integratie. De arbodienst is gecertificeerd volgens de Certificeringregeling Arbodiensten. De regeling wordt beheerd door de [Stichting Beheer Certificatieregeling Arbodienst](#) (SBCA). Voor meer informatie: www.sbca.nl. Waar in dit document gesproken wordt over een arbodienst, wordt ook de sbca-gecertificeerde Arboarts bedoeld.

**bij cao kan een uitzondering worden gemaakt waardoor de dienstverlener valt onder de zogenaamde maatwerkregeling en certificering niet noodzakelijk is.*

Bedrijfsarts

Een in het BIG-register geregistreerde medisch specialist op het terrein van arbeid en gezondheid. De titel 'bedrijfsarts' is een wettelijk beschermde titel. De NVAB is de beroepsvereniging van de bedrijfsarts. De gedragscode voor bedrijfsartsen en het professioneel statuut treft u aan op www.nvab-online.nl

De bedrijfsarts kan taken laten verrichten door onder zijn verantwoordelijkheid werkende functionarissen in verzuimbegeleiding en re-integratie, als de (basis-)arts, de casemanager of de verzuimconsulent. Zij werken dan onder de verlengde-armconstructie. Aan deze constructie zijn strikte voorwaarden verbonden ten aanzien van competenties, scholing, toezicht, geheimhouding en overdracht.

Het is dus niet voldoende om iemand administratief onder de verlengde arm te plaatsen; ook inhoudelijk zal de functionaris moeten voldoen aan bepaalde kwalificaties, waaronder geheimhouding. De bedrijfsarts blijft de eindverantwoordelijke en is tuchtrechtelijk aan te spreken op de activiteiten van degenen die onder zijn verantwoordelijkheid werken.

In de wet is vastgelegd dat verzuimbegeleiding/re-integratie primair de verantwoordelijkheid is van de werkgever en de zieke werknemer. De werkgever heeft bijvoorbeeld de verplichting om samen met de werknemer een plan van aanpak op te stellen, een re-integratiedossier samen te stellen en een re-integratieverslag te maken. De bedrijfsarts/arbodienst heeft de wettelijke taak om de werkgever een oordeel over de re-integratiemogelijkheid te geven.

Bij de ziekteverzuimbegeleiding en re-integratie, alsmede het verzekeren van deze risico's, spelen verschillende partijen een rol. Iedere partij heeft eigen taken en verantwoordelijkheden en mag alleen de gegevens verwerken die noodzakelijk zijn voor de uitvoering van de eigen rol.

De bedrijfsarts/arbodienst verwerkt veel informatie over de gezondheid van zieke werknemers. Denk hierbij aan:

- diagnoses, naam ziekte, specifieke klachten of pijn aanduidingen;
- eigen waarnemingen over de gezondheidstoestand van de werknemer;
- informatie over therapieën;
- afspraken met artsen, therapeuten of begeleiders;
- problemen uit het verleden of in de privésfeer.

Deze gegevens vallen onder het medisch beroepsgeheim en mogen dus niet aan de werkgever worden verstrekt.

De bedrijfsarts/arbodienst mag alleen informatie verschaffen die nodig is om een beslissing te nemen over loondoorbetaling, verzuimbegeleiding en re-integratie:

- werkzaamheden waartoe werknemer niet meer of nog wel in staat is (functionele beperkingen, restmogelijkheden en gevolgen voor het soort werk dat werknemer nog kan doen);
- verwachte duur van het verzuim;
- mate van arbeidsongeschiktheid van werknemer;
- adviezen over aanpassingen, werkvoorzieningen of interventies die de werkgever voor de re-integratie moet regelen.

Zie hiervoor ook paragraaf 4.4: Wat mag de werkgever vragen en registreren bij een ziekmelding.

4.5.1. Werknemersbestanden

Het doorgeven van werknemersbestanden aan de Arbodienst is op aandringen van de Autoriteit Persoonsgegevens niet meer toegestaan. De arbodienst mag geen actieve werknemersadministratie voeren. Pas op het moment van de ziekmelding, of op het moment dat een werknemer vrijwillig een beroep doet op de arbodienstverlener, mogen er persoonsgegevens verwerkt worden. Arbodiensten en bedrijfsartsen verwerken nu alleen nog de persoonsgegevens van niet-zieke werknemers (actieven), wanneer zij een vrijwillig beroep doen op de dienstverlening. Arbodiensten en bedrijfsartsen verwerken dus uitsluitend de gegevens van de werknemers met wie zij een behandelrelatie hebben of gaan starten. Dit betreft:

- Werknemers die op eigen verzoek een arbeidsomstandighedensprekkuur raadplegen;
- Werknemers die op verzoek van de werkgever met instemming van de werknemer een arbeidsomstandighedensprekkuur bezoeken;
- Werknemers die een aanstellings- of beroepskeuring ondergaan;
- Werknemers die aan een (arbeids)medisch onderzoek meedoen, zoals bijvoorbeeld PAGO en PMO;
- Werknemers die een interventietraject ingaan.

Er zijn nog enkele openstaande punten. Zo kunnen arbodiensten/bedrijfsartsen, nadat de door de Autoriteit Persoonsgegevens verstrekte uitgangspunten zijn verwerkt, per 1 januari 2018 niet goed meer voldoen aan sommige verzoeken tot dienstverlening. Sinds 1 juli 2017 is bijvoorbeeld het preventieve spreekuur bij de bedrijfsarts weer een verplichting (in de arbeidsomstandighedenwet) voor de werkgever om aan te bieden aan alle werknemers. Deze spreekuren zijn vrijwillig en moet de werknemer zonder tussenkomst van de werkgever kunnen aanvragen bij de arbodienst of bedrijfsarts.

Omdat arbodiensten en bedrijfsartsen sinds 1 januari 2018 niet meer beschikken over de juiste persoonsgegevens gekoppeld aan specifieke werkgevers van alle werknemers, onderzoeken zij samen met branche-organisaties oplossingen voor dit probleem. Arbodiensten en bedrijfsartsen kunnen immers geen juiste verificatie doen of de aanvrager bij de werkgever werkt en kunnen ook geen correcte geanonimiseerde factuur verzorgen zoals werkgevers dat gewend waren.

OVAL heeft dit punt namens de aangesloten arbodiensten aangekaart bij het ministerie van SZW en VNO-NCW/MKB. Op het moment van verschijnen van deze werkwijzer was er nog geen uitspraak vanuit het ministerie van SZW en VNO-NCW/MKB.

Wanneer casemanagers onder taakdelegatie van de bedrijfsarts werken, mogen zij meer gegevens vragen en verwerken. De AP formuleert dit als volgt: 'Daarnaast mogen zij dezelfde gegevens vragen of gebruiken als de bedrijfsarts, onder voorwaarde dat:

- de organisatie een geregistreerde bedrijfsarts heeft die een contract sluit met de werkgever;
- de casemanager onder taakdelegatie werkt en deze taak persoonlijk gedelegeerd heeft gekregen van deze bedrijfsarts;
- de bedrijfsarts actief toezicht houdt op de taken van de casemanager;
- de casemanager alleen bij die gegevens kan die nodig zijn voor het uitoefenen van zijn/haar taak.'

BELANGRIJK!

Voor een verzuim- of casemanagementbureau niet werkend onder (beperkte) taakdelegatie geldt dat zij dezelfde gegevens mogen vragen of gebruiken als de werkgever. Dit betekent dat ze niet mogen informeren naar de aard en oorzaak van de ziekte of mogen informeren naar wat een werknemer nog wel kan.

4.6. Stroomlijnen verplichtingen WVP en de grondslagen van de AVG

De beleidsregels van de AP deden nogal wat stof opwaaien, omdat ze botsen met een actieve verzuimbegeleiding door de werkgever. In hoofdlijnen liggen de kaders vast. Wel zijn er veel vraagtekens over punten die in de praktijk voorkomen, maar niet passend zijn bij de grondbeginselen van de AVG. Dit hebben we voorgelegd aan de AP (zie bijlage 4). Hier hebben we echter geen antwoord op teruggekregen.

4.6.1 Hoofdlijnen

- Werknemer en werkgever mogen alleen over mogelijkheden, beperkingen en re-integratie praten op basis van een advies van de arbodienst of bedrijfsarts. Zonder het advies van de bedrijfsarts kan de werkgever dus niet met de werknemer in gesprek gaan over welke werkzaamheden hij nog wel kan uitvoeren, tenzij de werknemer dit geheel vrijwillig zelf spontaan vermeldt. Dan mogen daarover wel werkafspraken worden gemaakt.
- Ook verzuimpercentages moeten gebaseerd zijn op het advies van de arbodienst of bedrijfsarts. Er mogen geen herstel-, verzuim-, loonwaarde of inzetbaarheidspercentages in het door de werkgever gebruikte verzuimpercentage worden verwerkt, als dat niet gebaseerd is op een advies van de arbodienst of bedrijfsarts. Indien de werknemer volkomen uit zichzelf aangeeft wat werkzaamheden vanaf huis te kunnen doen, dan mag dit mits de werkgever hem maar onder geen beding onder druk heeft gezet of ernaar heeft gevraagd. Dit vloeit voort uit de gezamenlijke uitleg van de beleidsregels die het ministerie van SZW heeft uitgebracht (zie bijlage 3).
- De reden achter/oorzaak voor de no-riskpolis of vangnetregeling mag niet door werkgever worden geregistreerd. De werkgever mag wel vragen of de werknemer onder een

vangnetbepaling valt, maar niet onder welke. Dit is in de praktijk niet werkbaar, omdat UWV bij de aanvraag van het vangnet wel vraagt om aan te geven om welke reden dat is.

In hoofdlijnen moet er eerst een advies van de arbodienst of bedrijfsarts aanwezig zijn voordat er gewerkt kan worden aan re-integratie. Terwijl juist de Wet verbetering poortwachter werkgever en werknemer stimuleert om vanaf de eerste verzuimdag de focus te hebben op re-integratie. In de praktijk blijkt het daarom nog niet zo eenvoudig om te werken met de Beleidsregels de zieke werknemer en is de huidige verzuimbegeleidingspraktijk nog strijdig met de grondbeginselen van de AP.

4.6.2 Aandachtspunten

We benoemen eerst de aandachtspunten (deze zijn ook aan AP voorgelegd) en in de paragraaf daaropvolgend treft u een uitwerking hoe dit in de praktijk ondervangen kan worden.

Aandachtspunt 1: Interventieadvies

Als de bedrijfsarts een interventieadvies geeft, conform verplichtingen WVP, dan is voor de casemanager in veel gevallen de soort interventie en daarmee de aard van het verzuim af te leiden. Er wordt bijvoorbeeld een interventie voorgesteld bij Winnock. Winnock biedt programma's voor het omgaan met fysieke klachten, dus er zal een fysieke component in de klachten schuilen. Dit interventieadvies dient echter wel opgenomen te worden in het re-integratieverslag dat in het kader van de WVP moet worden aangelegd. Ook voortgangsmeldingen, tijd en duur van trajecten en eindmeldingen dienen in het verslag te worden opgenomen. Het re-integratieverslag heeft betrekking op een uniek individu, dus de aard van de interventie en de individu zijn te koppelen. We zien dat dit een logisch uitvloeisel is vanuit de WVP, dat zich dus niet goed verhoudt met de AVG.

Aandachtspunt 2: FML/IZP en Probleemanalyse

Uit de door de bedrijfsarts aangegeven beperkingen, valt voor de casemanager de aard van de klachten ook af te leiden. Terugkoppeling van beperkingen en daaruit voortvloeiende resterende mogelijkheden zijn essentieel voor het als goed werkgever uitvoeren van de WVP-verplichtingen.

Aandachtspunt 3: Factuur interventie in de administratie

Interventiedienstverleners sturen een factuur naar de werkgever. De werkwijze is dat de casemanager die de interventie coördineert, de interventiedienstverlener instrueert dat de naam van de persoon niet op de factuur mag komen en dat er ook geen verdere persoonlijke gegevens worden vermeld. De persoon mag niet aan interventie worden gekoppeld. Bij kleinere organisaties of deelfacturen per afdeling/businessunit is er echter indirect vaak wel af te leiden op wie de interventie betrekking heeft. De administratie kan bij kleinere organisaties redelijk eenvoudig afleiden op wie de nota betrekking heeft. Aan de naam van de dienstverlener is in veel gevallen het soort interventie af te lezen (HSK is bijvoorbeeld een psychologisch dienstverlener).

Aandachtspunt 4: Verwijzing naar interventiedienstverlener

De privacyregels belemmeren de vrije marktwerking als het gaat om verwijzing naar interventiedienstverleners. Doordat de bedrijfsarts niet aan de casemanager mag laten weten welk type interventie gewenst is, kunnen er niet meerdere offertes bij diverse aanbieders worden

opgevraagd. Dit werkt, zonder dat het de bedoeling van de wetgever is, “gedwongen winkelnering” in de hand met bijbehorende hogere kosten voor de werkgever.

4.6.3 Standpunt verzuimprofessionals

In sommige organisaties is de leidinggevende de casemanager. Dat maakt bovenstaande situatie discutabel. Als de casemanager neutraal en onafhankelijk als regievoerder (hierna te noemen casemanager WVP) voor de werkgever gepositioneerd wordt, waarborg je op basis van professionaliteit en kennis, de bescherming van de bijzondere persoonsgegevens beter. Wij pleiten voor de casemanager als kernprofessional in de Arboret, die neutraal en onafhankelijk gepositioneerd is. Dit kan zijn bij een arbodienstverlener of een externe casemanager die als adviseur en regievoerder optreedt in de maatwerkconstructie. Ook bij een intern werkende arbodienstverlener is dit mogelijk, mits de systemen volledig los staan van de overige processen en met ontslagbescherming en mandaat voor betalingen.

Ten aanzien van de betaling biedt dit ook de mogelijkheid om de nota te accorderen, zodat de factuur daarna volkomen anoniem naar de administratie van de werkgever wordt gezonden. Het kan niet zo zijn dat er een betalingsrisico is voor de casemanager. En als dit wel het geval is, dan zal hiervoor een marge berekend moeten worden. Hierdoor wordt de dienstverlening onnodig duur. Interventiedienstverleners zouden zelf nog kunnen overwegen om de tenaamstelling neutraler te maken of te gaan werken met een centrale facturatie-organisatie (Famed constructie).

De ontstane gedwongen winkelnering is naar onze mening niet gewenst. Wij pleiten ervoor dat de bedrijfsarts aan de casemanager het type interventie kan benoemen, waarna de casemanager voor meerdere offertes kan zorgen, en/of het initiatief kan nemen tot het opzetten van een uitgebreide providerboog voor de werkgever, waarmee ook Service Level Agreements worden gesloten (bijvoorbeeld afspraken over de doorlooptijden) en waar de bedrijfsarts uit kan kiezen.

4.6.4 Samenwerking met UWV

De beleidsregels ‘de zieke werknemer’ van AP komen niet overeen met hetgeen UWV als publieke uitvoerder van de werkgever vraagt. Bij UWV wordt nog altijd om het BSN gevraagd, terwijl de verzuimbegeleider dit niet mag weten.

Zo is het nog altijd nodig dat bij de vangnetaanvraag vermeld wordt of het vangnet betrekking heeft op zwangerschap, orgaandonatie of een no-risk. Maar de reden (zwangerschap of orgaandonatie) mag de werkgever niet weten.

Toegang tot het verzuimportal van UWV, het zogenaamde werkgeversportaal, is op dit moment niet met een tweewegauthenticatie (ook niet voor de gemachtigde). Eenmalig wordt een akkoord gevraagd aan de werkgever. Daardoor is het mogelijk dat ook een casemanagement- of verzuimbureau met meerdere casemanagers en allemaal hetzelfde wachtwoord werken voor alle werkgevers. Vanwege de gevoeligheid van de gegevens in het systeem van UWV is meerfactorauthenticatie verplicht, aldus de Autoriteit Persoonsgegevens. Die legde het UWV in het najaar 2018 een last onder dwangsom op om dit te realiseren. De overheidsinstantie krijgt tot 31

oktober 2019 de tijd om het beveiligingsniveau van het werkgeversportaal te verbeteren. Het UWV heeft december 2018 het werkgeversportaal van het inlogmiddel eHerkenning voorzien.

4.7. Onderscheid tussen verschillende soorten casemanagers

Er is een groot verschil in werkzaamheden tussen de casemanager die werkt voor of namens de werkgever en de casemanager die werkt onder auspiciën van de bedrijfsarts in taakdelegatie. Let ook op dat de casemanager taakdelegatie op één en hetzelfde dossier niet ook de casemanager verzuimbegeleiding kan zijn. Hierover heeft de AP een duidelijk standpunt ingenomen, zie brief in bijlage 1.

Een register-casemanager is een professional die een intensief, geaccrediteerd en voor de titel verplicht opleidingsprogramma op hbo- of postbachelorniveau heeft gevolgd, hiervoor is geslaagd en is ingeschreven bij het Register Specialistisch Casemanagement (RSC) of het Register Nederlandse Vereniging van Case- en Caremanagers (RNVC). Pas dan mag de register-casemanager de bij de gevolgde opleiding passende titel voeren. De titels worden achter de naam geplaatst en zijn ROV, RCM, RSZ, RCMC of CMTD bij het RSC en Crov of Rccm bij de RNVC.

4.7.1 Casemanagers voor of namens de werkgever

Een (register-)casemanager die voor of namens de werkgever werkt, voert vanuit de wettelijke kaders de regie over het verzuim- en re-integratietraject. Hij/zij zorgt ervoor dat op het juiste moment de juiste keuzes door de juiste functionarissen worden genomen, zodat de werknemer optimaal wordt begeleid.

Er zijn ook casemanagers die meer beleidsmatig werken op corporate niveau. Kenmerkend is dat de grenzen van de disciplines (operationeel of meer beleidsmatig) gedeeltelijk in elkaar kunnen overlopen. De casemanager beslecht de muren tussen afdelingen, in elk geval die tussen HR en Finance. Meestal zijn deze afdelingen elk verantwoordelijk voor een deel van de processen rondom ziekte en arbeidsongeschiktheid. Een goede samenwerking is daarom een voorwaarde om risico's tijdig te signaleren en kansen zoveel mogelijk te verzilveren. Een goed voorbeeld is de uitvoering van de no-riskpolis en het benutten van diverse subsidies zoals de loonkostenvoordelen.

4.7.2 De casemanager taakdelegatie onder auspiciën van de bedrijfsarts

Naast de casemanager die werkt voor of namens de werkgever, zijn er ook casemanagers taakdelegatie (CMTD). Een CMTD werkt onder auspiciën van een geregistreerde bedrijfsarts en valt ook onder het beroepsgeheim van de bedrijfsarts. Belangrijk daarbij is de absolute voorwaarde dat de CMTD wel medische informatie verzamelt, maar deze onder geen beding mag interpreteren. De

De [Nederlandse Vereniging van Arbeids- en bedrijfsgeneeskunde](#) (NVAB) heeft zich hier strikt over uit gelaten:

Het is niet toegestaan dat een leek (zoals een CMTD) verzamelde informatie gaat interpreteren. Het is de exclusieve taak van de bedrijfsarts om in het kader van de verzuimbegeleiding de medische kant van de re-integratie te bewaken en daarbij alle verkregen medische (en privacygevoelige) informatie te beheren. Een casemanager in taakdelegatie mag daarom nooit zelfstandig adviseren over de begeleiding omdat hij daarvoor sociaal-medische informatie zou moeten interpreteren.

Hij/zij mag ook absoluut geen medische adviezen geven. De CMTD creëert wel al vroeg in het verzuimtraject draagvlak en maakt re-integratie-afspraken (na afstemming met de bedrijfsarts). Ook kent hij/zij alle sociaal- en arbeidsrechtelijke kaders.

De AP is er duidelijk over dat het uitvragen en terugkoppelen van wat de werknemer bij ziekte/verzuim wel of niet kan, is voorbehouden aan de bedrijfsarts/arbodienst en niet aan de werkgever, de register-casemanager (behalve in taakdelegatie) en de leidinggevende.

Dat een CMTD meer mag dan een reguliere register-casemanager, is ook veel dienstverleners niet ontgaan. Het behalen van een diploma Taakdelegatie is echter niet voldoende. Aan werken in taakdelegatie zijn bijzondere voorwaarden verbonden, die organisatorische gevolgen hebben.

Voorwaarden voor werken in taakdelegatie

De AP legt in de beleidsregels de zieke werknemer in zeven punten uit hoe er onder taakdelegatie gewerkt dient te worden:

1. De gedelegeerde is voldoende opgeleid voor - en aantoonbaar bekwaam - in de uitoefening van de taak;
2. De bedrijfsarts heeft zich in de praktijk overtuigd van de kennis en vaardigheden van de gedelegeerde;
3. Er zijn functiegerichte protocollen, die duidelijk maken welke taken de gedelegeerde wel en niet kan uitvoeren, waarbij er altijd een mogelijkheid moet zijn om de bedrijfsarts te consulteren;
4. In individuele gevallen kunnen de grenzen van de delegatie worden vastgelegd in nadere werkafspraken tussen betrokkenen of in een werkplan voor de behandeling van een individueel geval;
5. Er is structureel persoonlijk overleg tussen gedelegeerde en bedrijfsarts;
6. Overleg, toetsing en overname van de gevalbehandeling door de bedrijfsarts is altijd mogelijk;
7. De werknemer is in begrijpelijke termen ingelicht over het delegeren van elementen van de begeleiding, de eindverantwoordelijkheid van de bedrijfsarts en de mogelijkheid om de bedrijfsarts te consulteren.

Verder geldt het volgende:

- De bedrijfsarts heeft de eindverantwoordelijkheid voor de arbeidsgeneeskundige advisering. Taken die door de wet aan de bedrijfsarts zijn toegekend, kunnen alleen door anderen worden uitgeoefend als zij hiertoe van de bedrijfsarts een opdracht hebben gekregen. *Belangrijk daarbij is de absolute voorwaarde dat de CMTD wel medische informatie verzamelt, maar deze onder geen beding mag interpreteren. Hij/zij mag ook absoluut geen medische adviezen geven. Ook de praktijkondersteuner bedrijfsarts (POB) niet mag interpreteren ook al hebben zij een BIG achtergrond!*
- Bij het overdragen van een deel van de taken van de bedrijfsarts aan de CMTD, krijgt deze geen volledige zelfstandige bevoegdheid. De CMTD voert een deel van de taken van de

bedrijfsarts uit, maar werkt onder instructie, begeleiding én verantwoordelijkheid van de bedrijfsarts.

- De CMTD mag alleen beschikken over die gegevens over de gezondheid van de zieke werknemers, die voor de uitoefening van zijn taken strikt noodzakelijk zijn. Tot welke delen van het medisch dossier de medewerker toegang heeft, hangt dus af van de taken die de CMTD vervult en van de bijbehorende competenties. De CMTD valt onder het afgeleide beroepsgeheim van de bedrijfsarts. Dit betekent dat ook de CMTD met de werkgever uitsluitend die informatie mag uitwisselen die de bedrijfsarts met de werkgever mag uitwisselen.

5. Informatiestromen en rollen inkomensverzekeraar en bij re-integratie

Let op: waar verzekeraar staat kan ook worden gelezen: gevolmachtigd agent. Waar staat re-integratiebedrijf kan ook worden gelezen re-integratieafdeling van de verzekeraar.

De AP geeft in haar publicatie 'De zieke werknemer en privacyregels voor verwerking van persoonsgegevens van zieke werknemers' uit 2008 vrij precies aan welke informatiestromen er zijn te onderscheiden. Er dient onderscheid te worden gemaakt in de informatiestromen bij de claimbeoordeling door de inkomensverzekeraar en die bij re-integratie. Dit is noodzakelijk omdat de werknemer bij de verzekeringsovereenkomst tussen werkgever en verzekeraar geen partij is, voor zover de verzekeringsovereenkomst betrekking heeft op het verzekeren van de loondoorbetalingplicht van de werkgever. In het geval van ziekteverzuim dient de verzekeraar (claimbeoordelaar) zich te baseren op het oordeel van de arbodienst/bedrijfsarts.

De handreiking is opgesteld in 2008, waarbij de inkomensverzekeraar hoofdzakelijk als verzekeraar van de loondoorbetalingplicht van de werkgever is gepositioneerd. De handreiking houdt echter niet altijd rekening met de rol die de inkomensverzekeraar (o.a. aanbieder verzuim- en WIA-verzekering producten en dienstverlening) inneemt in zijn hoedanigheid van re-integratieadviseur of -bedrijf.

De AP geeft in haar handreiking aan dat gezondheidsgegevens door een re-integratiebedrijf alleen via de werkgever aan de inkomensverzekeraar mogen worden doorgegeven. Achterliggende gedachte daarbij is dat de werkgever een overeenkomst heeft met het re-integratiebedrijf. Praktijk is evenwel dat re-integratie (en daarmee de inschakeling van een re-integratiebedrijf/afdeling) onderdeel is van de verzekeringsovereenkomst en daarmee de verzekeringsdekking.

Het is dus de verzekeraar of gevolmachtigd agent die de re-integratie in dit soort gevallen aanstuurt vanuit het verzekeringsproduct. Daarmee is het niet altijd noodzakelijk om de informatiestroom via de werkgever te laten lopen. Daar komt bij dat het in dit geval uitsluitend gaat om gegevens uit de categorie A (zie hiervoor hoofdstuk 5.2.1.). Deze zijn dus beperkter dan de gezondheidsgegevens waarover de handreiking spreekt.

Gaat het echter om verzekerde re-integratieactiviteiten, dan is de werknemer niet alleen belanghebbende bij een goede uitvoering, maar is hij - vanuit zijn wettelijke plicht om mee te werken aan re-integratie - ook partij. In dat geval kunnen ook meer gegevens uitgewisseld worden. In de volgende paragrafen is specifiek aangegeven wanneer welke soort gegevens mag worden verwerkt en door wie. De bron van deze informatie is afkomstig uit de handleiding privacy inkomensverzekeringen opgesteld door het verbond van verzekeraars en brancheorganisatie OVAL.

Grondslag van het mogen verwerken van gegevens over de gezondheid is belegd in artikel 30 sub 3 lid b van de UAVG. In dit artikel wordt gesproken over verzekeraars én financieel dienstverleners.

- 3 Gelet op artikel 9, tweede lid, onderdeel h, van de verordening, is het verbod om gegevens over gezondheid te verwerken niet van toepassing indien de verwerking geschiedt door:
- a. hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening, voor zover de verwerking noodzakelijk is met het oog op een goede behandeling of verzorging van de betrokkene dan wel het beheer van de betreffende instelling of beroepspraktijk; of
 - b. verzekeraars als bedoeld in artikel 1:1 van de Wet op het financieel toezicht of financiële dienstverleners die bemiddelen in verzekeringen als bedoeld in artikel 1:1 van die wet, voor zover de verwerking noodzakelijk is voor:
 - 1°. de beoordeling van het door de verzekeraar te verzekeren risico en de betrokkene geen bezwaar heeft gemaakt; of
 - 2°. de uitvoering van de overeenkomst van verzekering dan wel het assisteren bij het beheer en de uitvoering van de verzekering.

Verwerking is alleen toegestaan voor die gezondheidsgegevens die noodzakelijk zijn voor de beoordeling van het door de verzekeraar te verzekeren risico en voor zover de betrokkene geen bezwaar heeft gemaakt, of voor de uitvoering van de overeenkomst van verzekering, dan wel het assisteren bij het beheer en de uitvoering van de verzekering.

In de polisvoorwaarden als onderdeel van de verzekeringsovereenkomst is omschreven welke diensten er worden aangeboden binnen de verzekeringsovereenkomst en of er sprake is van een re-integratiebedrijf of -afdeling die werkgevers en haar zieke werknemers ondersteunt bij de preventie- en re-integratieadviezen. Met externe re-integratiebedrijven hebben verzekeraars schriftelijke afspraken gemaakt omtrent de te leveren dienstverlening aan verzekeringnemers en verzekerden. Van belang is dat de verzekeraar in samenwerking met de re-integratieafdeling of het re-integratiebedrijf op het moment van aanvang van preventie- of re-integratieadviezen waarbij persoonsgegevens worden uitgewisseld, de betrokkene informeert uit hoofde waarvan de uitwisseling van persoonsgegevens plaatsvindt.

Het re-integratiebedrijf heeft als zelfstandig verwerkersverantwoordelijke een informatieplicht jegens betrokkene. Dit geldt eveneens voor de verzekeraar/financiële instelling. Het in de polisvoorwaarden opnemen van een passage dat deze informatieplicht via de werkgever kenbaar moet worden gemaakt, is onvoldoende.

Noodzakelijkheidsvereiste

Wanneer zijn persoonsgegevens noodzakelijk voor het uitvoeren van de overeengekomen verzekeringsovereenkomst? Het noodzakelijkheidvereiste is nauwelijks uitgewerkt. De AP merkt in de notitie 'De zieke werknemer' op, dat zowel voor de ziekmelding en de daaraan gekoppelde

verzuimverzekering (inkomensverzekering), als voor de financiering van re-integratieactiviteiten, de verzekeraar voor haar beslissingen dient af te gaan op het (medisch) oordeel van de arbodienst/bedrijfsarts. De AP beschrijft dit voor de inkomensverzekeraar in de hoedanigheid van claimbeoordelaar.

De AP noemt nog als voorbeeld ‘wachtlijstbemiddeling’. Dat suggereert in ieder geval dat de verwerking van persoonsgegevens in het belang moet zijn van de zieke en/of arbeidsongeschikte werknemer en kan bijdragen aan versnelling van het herstel en dus de werkhervatting.

5.1 Diverse rollen en functionarissen rondom de zieke werknemer

Er zijn verschillende functionarissen in dienst van c.q. ingeschakeld door de werkgever en inkomensverzekeraar. Deze hebben een actieve rol bij het uitwisselen van (persoons)gegevens in het kader van inkomensverzekeringen. Te denken valt aan:

- Werkgeversadviseurs zoals de HR-adviseur, verzuim- of casemanagementbureau*;
- Inkomensadviseur/assurantietussenpersoon;
- Arbodienst/bedrijfsarts;
- Medewerker acceptatie en prolongatie inkomensverzekeraar;
- Claimbeoordelaar inkomensverzekeraar;
- Re-integratieadviseur van de re-integratieafdeling/-bedrijf inkomensverzekeraar (interventiebedrijf);
- Interventiepartij (arbeidsdeskundige, re-integratiecoach spoor 1, 2 of 3, jobcoach, medische interventie, etc.);
- Medisch adviseur (re-integratieafdeling/-bedrijf).

**niet zijnde de casemanagers onder taakdelegatie van de bedrijfsarts, maar de procesregisseur werkgever.*

5.2 Soorten (bijzondere) persoonsgegevens

Voor het uitvoeren van de verzekeringsovereenkomst heeft de verzekeraar bepaalde gegevens nodig om bijvoorbeeld een claim te beoordelen en een vergoeding uit te keren. Daarnaast dienen verzekeraars voor elk risico dat zich heeft geopenbaard voorzieningen aan te houden, waaruit de toekomstige uitkeringsverplichtingen gefinancierd kunnen worden. Om deze voorzieningen zo adequaat mogelijk te kunnen vaststellen, dienen verzekeraars wel over de daarvoor relevante informatie te beschikken.

Er is een onderscheid in categorieën van gegevens naar het doel waarvoor deze gegevens mogen worden verwerkt. Voor alle gegevens geldt dat deze alleen verwerkt mogen worden voor zover dit noodzakelijk is voor het doel waarvoor zij verkregen worden.

5.2.1 Categorie A-gegevens

Dit zijn de gegevens die een rol spelen bij de verzekeringsovereenkomst tussen de werkgever en de inkomensverzekeraar voor zover het gaat om de claimbeoordeling. Het zijn hoofdzakelijk proces- en administratieve gegevens en enkele gegevens over de gezondheid, die de werkgever, de

inkomensverzekeraar in de hoedanigheid van claimbeoordelaar, de casemanager Wet verbetering poortwachter en de arbodienst/bedrijfsarts mogen verwerken. Hiertoe behoren onder meer:

- Naam, adres, woonplaats gegevens van de (zieke en/of arbeidsongeschikte) werknemer;
- Loongegevens van de zieke en/of arbeidsongeschikte werknemer*;
- Datum einde dienstverband (indien deze eindigt voordat de 104 weken loondoorbetaling/WIA-wachttijd voorbij is);
- Burgerservicenummer**;
- Datum eerste verzuimdag;
- Datum van (gedeeltelijk) herstel;
- (Vermoedelijke) duur van het verzuim;
- Arbeidsongeschiktheidspercentage of het percentage loonwaarde;
- Aantal uren per dag of per week dat de werknemer eigen of passend werk kan verrichten, met vermelding van de aanvangsdatum (opbouwschema);
- Of er sprake is van enige vorm van schadeloosstelling, zoals vangnetsituatie of regres;
- Of er sprake is van loonopschorting of loonstopzetting;
- Of er sprake is van enige vorm van sanctionering op grond van de ZW of WIA, indien de werkgever hiervoor eigenrisicodrager is;
- De beschikkingen van het UWV;
- In geval van WGA-eigenrisicodragerschap, na verkregen machtiging van de werkgever, de administratieve gegevens uit de SUAG-levering door UWV;
- Of en wanneer een interventie is ingezet;
- De kosten van de interventie;
- Of er een Plan van Aanpak is opgesteld;
- Of de activiteiten uit het Plan van Aanpak (tijdig) zijn uitgevoerd.

Het eigenlijke Plan van Aanpak of onderdelen uit het re-integratiedossier behoren nadrukkelijk *niet* tot de in dit kader uit te wisselen documenten.

* Het opvragen van een loonstrook met meer informatie dan de noodzakelijke loongegevens benodigd voor de claimbeoordeling is niet toegestaan! Gegevens als vakbondslidmaatschap, lunchkosten, mogelijk een persoonlijke lening bij de werkgever, inkoop vakantiedagen, BSN (zie hieronder), burgerlijke staat, etc. zijn allemaal gegevens die je mogelijk gaat verwerken bij het opvragen van een loonstrook. De inkomensverzekeraar zal de verzekerde werkgever goed moeten instrueren welke loongegevens van de zieke en/of arbeidsongeschikte werknemer zij wenst te ontvangen die noodzakelijk zijn voor de claimbeoordeling.

** Artikel 73, derde lid SUWI zoals dat is komen te luiden na invoering van de Verzamelwet SZW 2016. Volgens artikel 24 lid 1 van de Wbp mag het BSN alleen gebruikt worden als daar een wettelijke basis voor is. Inkomensverzekeraars in de hoedanigheid van claimbeoordelaar hebben deze basis op grond van het bepaalde in artikel 73, lid 3, sub b (tot 1 januari 2014 lid 11, sub b) van de Wet SUWI. Hierin is geregeld dat verzekeraars het BSN mogen gebruiken bij de uitvoering van verzekeringsovereenkomsten met werkgevers voor het risico van loondoorbetaling bij ziekte en het eigenrisicodrager zijn voor de uitkering op grond van de Wet WIA.

Voor de claimbehandeling onder de verzuimverzekering is het BSN geen noodzakelijk persoonsgegeven. Anders kan dit zijn voor de WGA-eigenrisicoverzekering, waarbij UWV

communiceert met het BSN als kenmerk op haar correspondentie, in portals en in telefonisch contact.

5.2.2 Categorie B-gegevens

Dit zijn gezondheidsgegevens die noodzakelijk zijn voor een adequate verzuimbegeleiding en re-integratie van de zieke/arbeidsongeschikte werknemer. Deze gezondheidsgegevens, veelal afkomstig van de arbodienst/bedrijfsarts, kunnen door het re-integratiebedrijf verwerkt worden, zodra er sprake is van een concrete re-integratieopdracht of -interventie.

Deze concrete re-integratieopdracht kan opgenomen zijn in de polisvoorwaarden van de verzekering en kan ook het inschakelen van een re-integratiebedrijf voor ondersteuning bij het re-integratieproces omvatten, zonder dat (direct) sprake is van de inzet van interventies. Dat kan al beginnen vanaf de ziekmelding, ook wanneer er nog geen benutbare mogelijkheden zijn. Ook indien er naar het oordeel van de arbodienst/bedrijfsarts (op korte termijn) nog geen sprake is van belastbaarheid, kan deze informatie uitgewisseld worden.

De werknemer en werkgever kunnen in dat geval door het re-integratiebedrijf worden geïnformeerd en voorbereid op de periode waarop er wel re-integratiemogelijkheden zijn. Het re-integratiebedrijf zal dan pas met de concrete opdracht 'werkhervatting in eigen of ander werk' beginnen, zodra de arbodienst/bedrijfsarts de benutting van de belastbaarheid mogelijk acht.

Gezondheidsgegevens zijn ook noodzakelijk bij de ondersteuning van de werkgever in zijn hoedanigheid als ZBO (Zelfstandig Bestuursorgaan) of in het kader van bezwaar- en beroepszaken tegen UWV en bij herbeoordelingsverzoeken.

Tot categorie B-gegevens behoren onder meer:

- Visie van de bedrijfsarts op de te re-integreren zieke en/of arbeidsongeschikte werknemer;
- Vertaling van de medische gegevens door de bedrijfsarts naar beperkingen en mogelijkheden van de zieke en/of arbeidsongeschikte werknemer;
- Poortwachterrapportages, zoals het Plan van Aanpak en de Probleemanalyse;
- Belastbaarheid: de werkzaamheden waartoe de zieke en/of arbeidsongeschikte werknemer nog wel of niet meer toe in staat is, de fysieke en mentale mogelijkheden en beperkingen;
- Rapportage van de arbeidsdeskundige, waarin de belastbaarheid wordt vertaald naar concrete mogelijkheden tot het verrichten van arbeid;
- Advies over eventuele aanpassingen of werkvoorzieningen die nodig zijn;
- Advies over een interventie gericht op het verhogen van de belastbaarheid;
- Planning traject van de re-integratie;
- De wens van de werknemer ten aanzien van soort werk, niveau, arbeidspatroon en scholing;
- Fase-indeling met betrekking tot de arbeidsmarkt;
- Advies over interventies die nodig zijn voor het wegnemen of verminderen van de beperkingen dan wel voor het vinden van arbeid of het aanpassen van de arbeid.

Arbeidsdeskundige

Arbeidsdeskundigen zijn specialisten in de relatie mens, werk en inkomen. Zij wegen belasting, belastbaarheid en beleving van mens en werk in zijn gehele context. Ook coachen zij op het behalen van reële doelen in werk en inkomen. De arbeidsdeskundige werkt in zijn onderzoek samen met een bedrijfsarts, verzekeringsarts of medisch adviseur (die de ziekte of het gebrek van de werkende vertaalt naar een belastbaarheidsprofiel). Arbeidsdeskundigen werken zowel bij UWV, verzekeraars, arbodiensten, re-integratiebedrijven of als zelfstandige.

5.2.3 Bijzonderheden WIA-verzekeringen

Hoewel de uitkeringen pas na afloop van de WIA-wachttijd (104 weken na de 1e ziektedag) verstrekt worden, vangt de uitvoering van de verzekeringsovereenkomst feitelijk al aan op het moment dat het verzekerde risico zich heeft geopenbaard: dus de dag waarop de wachttijd voor de WIA start.

Om tijdig te kunnen beoordelen of een risico dat zich inmiddels geopenbaard heeft tot een mogelijke uitkeringsplicht leidt, hanteren verzekeraars veelal een meldingstermijn van drie maanden na de eerste ziektedag. Hiermee wordt voorkomen dat kortdurende ziektegevallen, die in ieder geval niet tot een uitkeringsverplichting zullen leiden, toch gemeld moeten worden.

Tijdige melding stelt de verzekeraar in staat om te beoordelen of het risico onder de dekking van de verzekering valt (hiervoor volstaan categorie A-gegevens) en of de verzekeringnemer en de uitkeringsgerechtigde alles doen, respectievelijk nalaten om de belangen van de verzekeraar niet te schaden (hiervoor zijn ook categorie B-gegevens nodig verstrekt door de werkgever).

Ook de wetgever heeft deze noodzaak erkend door de tijdige melding en de plicht tot het voorkomen en beperken van de schade wettelijk te verankeren in artikel 7:941 BW en artikel 7:957 BW.

Met inachtneming van de privacyregels kunnen claimbeoordelaars van verzekeraars op grond van artikel 30 sub 2 lid b van de UAVG de beperkte gezondheidsgegevens uit categorie A al gedurende de WIA-wachttijd verwerken.

Voor het adequaat ondersteunen van de werkgever heeft het re-integratiebedrijf gedurende deze periode ook categorie B-gegevens nodig.

5.2.4 Categorie C-gegevens

Dit zijn de gegevens die in het kader van een medisch onderzoek of een medische behandeling door een arts worden verwerkt.

Gezondheidsgegevens

Tot de gezondheidsgegevens behoren alle gegevens omtrent iemands gezondheid, zijn ziekte, aandoening of beperking en de (te) ondergane medische behandelingen. Gezondheidsgegevens omvatten niet alleen de gegevens die in het kader van een medisch onderzoek of een medische behandeling door een arts worden verwerkt, maar alle gegevens die de geestelijke of lichamelijke gezondheid van een persoon betreffen. Zo is ook het enkele gegeven dat iemand ziek is, een gegeven betreffende iemands gezondheid, hoewel dat gegeven op zichzelf nog niets zegt over de aard van de aandoening.

In het proces rondom verzuim en arbeidsongeschiktheid is de verwerking van deze gegevens voorbehouden aan de arbodienst/bedrijfsarts of de medisch adviseur van het re-integratiebedrijf.

Medisch adviseur verzekeraar/gevolmachtigd agent

Een medisch adviseur is een in het BIG-register geregistreerde bedrijfs- of verzekeringsarts die verantwoordelijk is voor de advisering van de verzekeraar/gevolmachtigd agent. Het BIG-register (Beroepen in de Individuele Gezondheidszorg) is een Nederlandse databank waarin een aantal officieel erkende gezondheidswerkers is geregistreerd. In het BIG-register zijn artsen, apothekers, fysiotherapeuten, gezondheidszorgpsychologen, psychotherapeuten, tandartsen, verloskundigen en verpleegkundigen opgenomen. Alleen wie in het register is ingeschreven, is door de wet bevoegd deze beschermde titel te voeren. In het register zijn die personen opgenomen die een relevante door de overheid erkende beroepsopleiding gevolgd hebben.

De medisch adviseur adviseert de verzekeraar/gevolmachtigd agent in zijn hoedanigheid van re-integratiebedrijf/-afdeling uitsluitend ten behoeve van de re-integratie. De informatie die een medisch adviseur heeft mag alleen betrekking hebben op re-integratie en interventie. Deze informatie mag niet gebruikt worden om een oordeel te geven over het ((on)rechtmatige) verzuim van een werknemer. Daartoe dient de verzekeraar (claimbeoordelaar) zich te baseren op het oordeel van de arbodienst/bedrijfsarts.

De medisch adviseur dient zich dus te beperken tot informatie als eerste ziektedag, vermoedelijke duur, en wel of niet meewerken aan re-integratie. Dat laatste kan overigens wel leiden tot gevolgen voor de vergoeding van de loondoorbetaling, maar is dan gebaseerd op het niet nakomen van de re-integratieverplichtingen.

Daarnaast kan de medisch adviseur de WGA-eigenrisicodragerverzekeraar adviseren over de (on)mogelijkheden van herbeoordelingen in het kader van de WIA.

Casemanager verlengde arm (onder delegatie van de bedrijfsarts/medisch adviseur)

Deze in opdracht en onder delegatie van de bedrijfsarts/medisch adviseur aangewezen casemanager werkt onder de verantwoordelijkheid van de bedrijfsarts/medisch adviseur. Hij/zij begeleidt de werkgever en werknemer bij het proces rondom verzuim en re-integratie, waarbij wordt voldaan aan de strikte voorwaarden die bij delegatie gelden ten aanzien van competenties, scholing, toezicht, geheimhouding en overdracht.

Ook hier geldt dat de begeleiding zich niet beperkt tot de periode van loondoorbetaling door de werkgever, maar zich ook uitstrekt tot de Ziektewet en/of de eerste 10 jaar van de WGA-uitkering als de (ex-) werkgever daarvoor eigenrisicodragers is.

Uitgangspunt is dat categorie C-gegevens verwerkt mogen worden onder verantwoordelijkheid van een bedrijfsarts. Voor die verantwoordelijkheid worden verschillende termen gebruikt zoals: 'verlengde arm', 'delegatie', 'werken onder de verantwoordelijkheid van', 'direct betrokkene' of 'op gelijkgerichte wijze betrokken zijn bij behandeling en begeleiding'.

Niet alle termen hebben juridisch gezien exact dezelfde betekenis. Voor het doel van deze handleiding zijn deze gradaties niet van belang. Uitgangspunt is dat iemand die dezelfde gegevens mag verwerken en inzien als de bedrijfsarts, daartoe gerechtigd kan zijn vanuit inhoudelijke of procesmatige ondersteuning van deze bedrijfsarts.

Als het alleen gaat om processen, dan zullen aan het verwerken van de categorie C-gegevens niet veel inhoudelijke eisen worden gesteld, behalve een geheimhoudingsverklaring. Daar waar iemand inhoudelijke taken van de arts overneemt, zullen er meer eisen worden gesteld aan competenties, bekwaamheid, toezicht, geheimhouding en overdracht.

Voor overdracht van taken door de bedrijfsarts zijn die normen beschreven in: 'Taken, verantwoordelijkheden en bevoegdheden van de bedrijfsarts bij de verzuimbegeleiding (KNMG/NVAB 2009). In de KNMG-/NVAB-documenten wordt de term delegatie het meeste gebruikt. AP daarentegen hanteert vooral de term: 'op gelijkgerichte wijze'. Voor de rolbeschrijvingen inkomensverzekeringen is de gebruikte term niet van belang.

Hoewel de verwerking van categorie C-gegevens is voorbehouden aan de medisch adviseur/bedrijfsarts of de functionarissen (arbodienst) onder taakdelegatie c.q. het medisch secretariaat van de bedrijfsarts, is de inzet van deze functionarissen geen vrijbrief voor uitwisseling of verwerking van deze gegevens. Ook hier geldt dat de gegevens slechts verwerkt mogen worden voor een duidelijk omschreven doel en mits noodzakelijk en proportioneel en na verkregen toestemming van de zieke en/of arbeidsongeschikte werknemer. Dat geldt ook, in geval van delegatie, voor de medewerkers die in de verlengde arm constructie onder de verantwoordelijkheid van de bedrijfsarts of bij een re-integratiebedrijf/-afdeling van een verzekeraar onder de verantwoordelijkheid van de medisch adviseur werken.

Tot de categorie C-gegevens behoren onder meer:

- Diagnose en behandelgegevens;
- Oorzaak en aard van de ziekte/aandoening;
- Informatie waaruit de diagnose en/of de aard en oorzaak van de ziekte/aandoening is af te leiden;
- Inhoudelijke onderbouwing van interventies die nodig zijn voor het wegnemen of verminderen van de beperkingen, dan wel voor het vinden van arbeid of het aanpassen van de arbeid.

Voor een goede uitvoering van de re-integratie/interventie kan het soms noodzakelijk zijn om over gegevens uit de categorie C te beschikken. Een medisch adviseur van het re-integratiebedrijf mag deze gegevens bij de arbodienst/bedrijfsarts opvragen. De arbodienst/bedrijfsarts vergewist zich dan van de noodzaak van de voor dat doel te verstrekken gegevens en informeert de zieke en/of arbeidsongeschikte werknemer over de informatieverstrekking. Er hoeft op grond van de verzekeringsovereenkomst *geen toestemming van de werknemer* te worden gevraagd. Het is wel aan te raden de betrokkene te informeren. De arbodienst/bedrijfsarts informeert de werknemer in het eerstvolgende spreekuurcontact, waarna de informatieverstrekking aan de medisch adviseur plaatsvindt.

Als de WGA-eigenrisicodragerverzekeraar na de verkregen machtiging van de werkgever, namens hem een herbeoordeling in het kader van de WIA aanvraagt, of bezwaar of beroep aantekent tegen een door UWV ingenomen standpunt, kan de medisch adviseur uitsluitend categorie C-gegevens opvragen bij de arbodienst/bedrijfsarts als hij ook beschikt over een machtiging van de (ex)werknemer. Is er geen machtiging, dan kan er geen herbeoordeling plaatsvinden op medische (categorie C) gegevens. Dit is ook van toepassing voor de medisch adviseur van het re-integratiebedrijf of -afdeling van een verzekeraar.

Hetzelfde geldt ook, in geval van delegatie, voor de functionarissen die in de verlengde-armconstructie (taakdelegatie) onder de verantwoordelijkheid van de bedrijfsarts of bij een re-integratiebedrijf onder de verantwoordelijkheid van de medisch adviseur werken.

Bij een verzekeraar dienen de functies ‘advies’ en ‘uitvoering’ gescheiden te blijven (organisatorische, technische en bouwkundige maatregelen). Dat betekent dat werknemers, die onder verantwoordelijkheid van de medisch adviseur categorie C-gegevens verwerken (adviesfunctie), niet werkzaam mogen zijn op de afdeling of binnen het bedrijf die zich met re-integratie of claimbeoordeling (uitvoering) bezighoudt. Belangrijk is dat personen, die onder de verantwoordelijkheid van de medisch adviseur werken, niet tevens een besluitvormende rol mogen hebben in de uitvoering van de verzekeringsovereenkomst.

5.2.5 Categorie D-gegevens

Dit zijn algemene gegevens van de werkgever en werknemer. Hiertoe behoren onder meer:

- Naam, adres, woonplaats gegevens van de werkgever;
- Naam, adres, woonplaats gegevens van de werknemer;
- Offertes, opdrachtbevestigingen, contracten en overeenkomsten;
- Facturatiegegevens.

5.3 Schema verwerking categorie persoonsgegevens per rol

Wie?	Welke informatie?
Werkgever/HR-adviseur	Categorie A- en B-gegevens (zie ook *)
Verzekeringsadviseur inkomensverzekeringen	Geen persoonsgegevens
Acceptant inkomensverzekeraar	Geen persoonsgegevens
Claimbehandelaar	Categorie A-gegevens
Casemanager Wet verbetering poortwachter in dienst van de werkgever	Categorie A- en B-gegevens
Casemanager verlengde arm	Categorie A-, B- en C-gegevens
Bedrijfsarts / medewerker arbodienst in taakdelegatie of medisch secretariaat bedrijfsarts	Categorie A-, B- en C-gegevens
Re-integratieafdeling/-bedrijf van een inkomensverzekeraar of gevolmachtigd agent	Categorie A- en B-gegevens
Medisch adviseur re-integratiebedrijf/-afdeling van een inkomensverzekeraar of gevolmachtigd agent	Categorie A-, B- en C-gegevens
UWV (beslissing, herbeoordeling, bezwaar & beroep)	Categorie A-, B- en C-gegevens

5.4. Matrix onderlinge uitwisseling persoonsgegevens

	Werknemer	Werkgever/HR-adviseur	Verzekeringsadviseur inkomensverzekeringen	Acceptant inkomensverzekeraar	Claimbehandelaar inkomensverzekeraar	Casemanager Wet verbetering poortwachter in dienst van de werkgever	Casemanager Wet verbetering poortwachter verlengde arm	Arbodienst/bedrijfsarts	Re-integratieafdeling/-bedrijf van een inkomensverzekeraar of gevolmachtigd agent	Medisch adviseur re-integratiebedrijf/-afdeling van een inkomensverzekeraar of gevolmachtigd agent	UWV
Uitwisseling persoonsgegevens (gezondheidsgegevens)											
Werknemer		A+B	geen	geen	geen	A+B	A+B+C	A+B+C	A+B	A+B+C*	A+B+C
Werkgever/HR-adviseur	A+B		geen	geen	A	A+B	A+B	A+B	A+B	A+B	A+B
Verzekeringsadviseur inkomensverzekeringen	geen	geen		geen	geen	geen	geen	geen	geen	geen	geen
Acceptant inkomensverzekeraar	geen	geen	geen		geen	geen	geen	geen	geen	geen	geen
Claimbehandelaar inkomensverzekeraar	geen	A	geen	geen		A	A	A	A	A	A
Casemanager Wet verbetering poortwachter in dienst van de werkgever	A+B	A+B	geen	geen	A		A+B	A+B	A+B	A+B	A+B
Casemanager Wet verbetering poortwachter verlengde arm	A+B+C	A+B	geen	geen	A	A+B		A+B+C	A+B	A+B+C	A+B+C
Arbodienst/bedrijfsarts	A+B+C	A+B	geen	geen	A	A+B	A+B+C		A+B	A+B+C	A+B+C
Re-integratieafdeling/-bedrijf van een inkomensverzekeraar of gevolmachtigd agent	geen	A+B	geen	geen	A	A+B	A+B	A+B		A+B	A+B
Medisch adviseur re-integratiebedrijf/-afdeling van een inkomensverzekeraar of gevolmachtigd agent	A+B+C*	A+B	geen	geen	A	A+B	A+B+C	A+B	A+B		A+B+C
UWV beslissingen en herbeoordeling & beroep/bezwaar (opgevraagde informatie alleen met machtiging werkgever)	A+B+C	A+B	geen	geen	A	A+B	A+B+C	A+B+C	A+B	A+B+C	

*Voor een goede uitvoering van de re-integratie/interventie kan het soms noodzakelijk zijn om over gegevens uit de categorie C te beschikken. Een medisch adviseur van het re-integratiebedrijf of -afdeling vraagt deze gegevens veelal op bij de arbodienst/bedrijfsarts in plaats van bij de werknemer. Dit mag dus zonder een machtiging van de werknemer. In geval van een herbeoordeling UWV of bezwaar of beroep namens de werkgever, mogen categorie C-gegevens nooit zonder toestemming van de werknemer worden uitgewisseld!

5.5 Rol van de adviseur zorg- en inkomensverzekeringen

Een verzekeringsadviseur (ook wel assurantietussenpersoon of -adviseur genoemd) adviseert en begeleidt de werkgever bij de keuze voor een verzekering en bemiddelt eventueel bij de totstandkoming van de verzekeringsovereenkomst inkomensverzekeringen. Bij de advisering moet een inkomensadviseur rekening houden met regelgeving rondom inkomensverzekeringen. De inkomensverzekeraar dient de regels van de privacywetgeving te respecteren en de klantrelatie te informeren.

5.5.1 De inkomensverzekeraar

Hiermee wordt een verzekeraar bedoeld die ten minste een van de volgende producten op het gebied van het werkgeversrisico aanbiedt:

- Verzekering die voor de werkgever het risico van loondoorbetaling gedurende de eerste 104 ziekte weken van een werknemer dekt;
- Verzekering die voor de werkgever het risico van Ziekte wet (niet zijnde Ziekte wet vangnet) gedurende de eerste 104 ziekte weken van een ex-werknemer dekt;

- Verzekering die voor de werkgever die eigenrisicodrager is het risico van de WGA-uitkeringen dekt;
- Verzekering die voor de werknemer het risico van WIA-iaten dekt.

Functionarissen

Dit zijn functionarissen in dienst van c.q. ingeschakeld door de inkomensverzekeraar en die een actieve rol hebben bij het uitwisselen van (persoons)gegevens in het kader van inkomensverzekeringen. Onder andere:

- medewerker acceptatie en prolongatie inkomensverzekeringen;
- claimbeoordelaar;
- re-integratieadviseur (re-integratiebedrijf of -afdeling);
- medisch adviseur (re-integratiebedrijf of -afdeling).

5.5.2 Rolscheiding

Bij de uitwerking van de geldende wet- en regelgeving maken we een onderscheid in de gegevensuitwisseling voor de claimbeoordeling en voor de verzuimbegeleiding en re-integratie. De verzekeraar kan dus ook de functie van re-integratiebedrijf uitoefenen, mits dat bedrijf of die afdeling strikt gescheiden opereert van het verzekeringsbedrijf (of de afdeling claimbeoordeling). Dit houdt in dat er zowel een fysieke als een organisatorische scheiding dient te zijn tussen de afdeling claimbeoordeling en de re-integratieafdeling.

In het kader van de uitvoering van de verzekeringsovereenkomst collectieve inkomensverzekering verwerkt de inkomensverzekeraar zogenaamde categorie A-persoonsgegevens (zie hoofdstuk 3.3). De inkomensverzekeraar sluit de overeenkomst af met de werkgever.

De verzekeringsovereenkomst (polis, clausules en/of (bijzondere) voorwaarden) bevat bepalingen voor de met de werkgever overeengekomen dekking van het risico en de daarbij behorende claimbeoordeling, en de hulp bij de re-integratie van de zieke en/of arbeidsongeschikte werknemer en de daarvoor overeengekomen risicodekking en financiering.

5.5.3 Rol van de medewerker acceptatie en prolongatie inkomensverzekeringen

De medewerker acceptatie en prolongatie inkomensverzekeringen is verantwoordelijk voor de acceptatie, het beheer en onderhoud van collectieve inkomensverzekeringen. De werkzaamheden bestaan uit het behandelen, beoordelen en begeleiden van offerteverzoeken, het accepteren van verzekeringsaanvragen alsmede het beoordelen en begeleiden van polismutaties.

Voor het advies- en offertetraject kan een inkomensverzekeraar (bijzondere) persoonsgegevens nodig hebben, alleen mag nooit te herleiden zijn om wie het precies gaat. Meer concreet zijn een naam en BSN niet nodig, maar leeftijd (of geboortedatum), geslacht, inkomen en mate van arbeidsongeschiktheid wel. Feitelijk zijn de 'wat-gegevens' wel nodig, maar de 'wie-gegevens' niet in het advies en offertetraject.

De medewerker acceptatie mag alleen de categorie A-gegevens verwerken voor zover deze absoluut noodzakelijk zijn voor het opmaken van de inkomensverzekering na acceptatie van de offerte of muteren van de inkomensverzekering. Denk hierbij aan de persoonsgebonden inkomensverzekering zoals een WIA-excedentverzekering.

5.5.4 Rol van de claimbehandelaar inkomensverzekeringen

Deze persoon is werkzaam op de afdeling claimbeoordeling van de verzekeraar of gevolmachtigde agent en houdt zich onder meer bezig met het beoordelen en al dan niet toekennen van een vergoeding voor de verzekerde loondoorbetalingsplicht van de werkgever en/of de eerste 10 jaar van de WGA-uitkering waarvoor de verzekerde werkgever eigenrisicodragers is, respectievelijk de vergoeding van re-integratiekosten in de loondoorbetalingsperiode en/of de eerste 10 jaar van de WGA-uitkering als de werkgever daarvoor eigenrisicodragers is, alsmede de uitkeringsperiode gedurende het WIA-hiaat uit hoofde van de WIA-aanvullingsverzekering. De claimbehandelaar mag alleen de categorie A-gegevens verwerken.

Gedragscodes Verwerking Persoonsgegevens Verzekeraars

De Gedragscodes Verwerking Persoonsgegevens Verzekeraars behoort tot de zelfregulering van verzekeraars. De code biedt een op de verzekeringssector toegespitste uitwerking van de (U)AVG. De gehele Gedragscodes is van toepassing.

Verzekeraars zijn gehouden aan de naleving van deze bindende zelfregulering en dienen periodiek te evalueren of de Gedragscodes wordt nageleefd. De Gedragscodes bepaalt wanneer persoonsgegevens en gezondheidsgegevens door een medisch adviseur en degenen die onder zijn verantwoordelijkheid werken (medische dienst of medische staf) moeten worden verwerkt en wanneer dat niet het geval is. De Gedragscodes is een uitwerking van de wettelijke verplichtingen volgens de (U)AVG.

5.5.5 Rol van de gevolmachtigde agent

Een gevolmachtigde agent is een natuurlijke persoon dan wel rechtspersoon die in de uitoefening van een beroep of bedrijf als gevolmachtigde van een verzekeraar voor diens rekening en risico verzekeringen sluit met een klantrelatie. In dit kader betekent het een gevolmachtigd agent collectieve inkomensverzekeringen.

De gevolmachtigde agent is, als het gaat om het verzamelen en verwerken van persoonsgegevens, te vergelijken met de positie van de verzekeraar, in geval van verzuimverzekeringen, Ziektewet-eigenrisicoverzekeringen en/of WIA-verzekeringen (WGA eigenrisico- en WIA-aanvullingsverzekeringen).

De privacywet- en regelgeving, zoals die geldt voor inkomensverzekeraars, dient ook door de inkomensverzekeraar gevolmachtigde agent te worden nageleefd bij de uitvoering van de door hem aan werkgevers aangeboden verzuimverzekeringen. Een gevolmachtigde agent kan dan ook niet als casemanager onder taakdelegatie van de bedrijfsarts optreden, maar zal in zijn/haar rol activiteiten van de primaire arbodienstverlener monitoren en de werkgever/werknemer adviseren vanuit de afgescheiden re-integratieafdeling/-bedrijf.

Indien de gevolmachtigde agent naast claimbeoordelaar ook optreedt als re-integratiebedrijf of -adviseur, dan dient er een strikte scheiding in informatiebeheer te zijn tussen de claimbeoordeling en de re-integratie-activiteiten. Bovendien moet worden geborgd dat (digitaal) vastgelegde gegevens alleen toegankelijk zijn voor degenen die daartoe bevoegd zijn. Er moeten dus organisatorische, technische en bouwkundige maatregelen zijn getroffen. Rolmix van functionarissen moet worden voorkomen.

Het is de taak van de verzekeraar (risicodragers) om als hij werkt met gevolmachtigde agenten, te borgen dat ook gevolmachtigde agenten de privacywet- en regelgeving naleven. Afspraken hierover zijn veelal vastgelegd in de volmachtovereenkomst.

5.5.6 Rol van het re-integratiebedrijf en de re-integratieadviseur

We spreken hier over een natuurlijk dan wel rechtspersoon, die in het kader van de uitoefening van zijn beroep of bedrijf de inschakeling van personen in de arbeid bevordert. Dit kan ook een bedrijf of afdeling van een verzekeraar zijn die het risico van loondoorbetaling (verzuimverzekeringen), Ziektewet-en/of WGA-eigenrisicodragerschap of WIA-aanvullingen verzekert.

Een van de verantwoordelijkheden van het re-integratiebedrijf betreft het optreden als gemachtigde bij herbeoordelingen en bezwaar- en beroepszaken in het kader van de WIA. Het re-integratiebedrijf of -afdeling van een WGA-eigenrisicodragerverzekeraar kan de werkgever bijstaan en/of optreden als gemachtigde bij herbeoordelingen en bezwaar- en beroepszaken in het kader van de WIA (mits hiertoe gemachtigd door de werkgever).

Inzet van de re-integratie-afdeling of -bedrijf is, als onderdeel van de verzekeringsovereenkomst, met de werkgever overeengekomen. Er wordt ook wel gesproken over een interventiebedrijf.

Bezwaar en beroep

Tegen officiële beslissingen van het UWV (zoals een loonsanctie of het arbeidsongeschiktheidspercentage) kan een werkgever bezwaar aantekenen. Wordt dat bezwaar niet gehonoreerd door het UWV, dan kan men in beroep gaan bij de rechtbank. De werkgever kan voor het behartigen van zijn belangen een advocaat of arts machtigen.

Ook kan het UWV toestemming geven iemand anders, bijvoorbeeld vanuit het re-integratiebedrijf, te machtigen. De gemachtigde heeft het recht om, conform art. 105 WIA, stukken die medische gegevens bevatten in te zien.

Inkomensverzekeraars hebben in hun polisvoorwaarden opgenomen de werkgever en werknemer te begeleiden bij de re-integratie en de werkgever, na verkregen machtiging, bij te staan in zijn hoedanigheid van Zelfstandig Bestuursorgaan (ZBO) bij het behandelen van bewaar- en beroepszaken in relatie tot de werknemer. De werknemer heeft de mogelijkheid bezwaar en beroep aan te tekenen tegen de eigenrisicodragers in diens positie als ZBO.

In bezwaar- en beroepsprocedures verstrekt het UWV onder voorwaarden (medische) gegevens aan de gemachtigde werknemer (jurist) van de verzekeraar.

5.5.7 Rol van de werkgever (en haar intern/extern HR-adviseur)

Een werkgever (en in het verlengde hiervan de door haar ingeschakelde intern-/externe HR-adviseur) is de partij die op basis van een arbeidsovereenkomst de bevoegdheid krijgt om de arbeidskracht van de werknemer gedurende de overeengekomen periode en tegen de overeengekomen

arbeidsvoorwaarden aan te wenden in de onderneming. Welke gegevens de werkgever mag vragen en registreren bij een ziekmelding is in hoofdstuk 2.6 benoemd.

5.5.8 Rol verzekeringsadviseur en bewustwording klantrelatie (werkgever) van AVG

De verzekeringsadviseur (financieel bemiddelaar op grond van de Wet op het Financieel toezicht ofwel Wft) heeft vanuit haar zorgplicht (Wft) de rol haar klantrelaties (werkgevers) te informeren over de gevolgen van de AVG in relatie tot het uitwisselen van (bijzondere) persoonsgegevens voor (inkomens)verzekeringen en de specifieke voorwaarden binnen de verzekeringsovereenkomst (acceptatie, prolongatie, na-verrekening, claimbehandeling, dekking re-integratie-ondersteuning).

5.5.9 Advies-, offerte- en aanvraagtraject

Voor een advies en offerte kan een inkomensverzekeraar/gevolmachtigd agent (bijzondere) persoonsgegevens nodig hebben; alleen mag nooit te herleiden zijn om wie het precies gaat. Meer concreet zijn een naam en BSN niet nodig, maar leeftijd (of geboortedatum), geslacht, inkomen en mate van arbeidsongeschiktheid wel. Feitelijk zijn de 'wat-gegevens' wel nodig, maar de 'wie-gegevens' niet.

Gegevens op organisatieniveau (bijvoorbeeld verzuimpercentages van de afgelopen 3 jaar in combinatie met het aantal werknemers, sector, totale loonsom, verhouding man/vrouw, gemiddelde leeftijd) en andere niet-persoonsgebonden gegevens zijn, in aanvulling op bovenstaande, voor de verzekeraar/gevolmachtigd agent voldoende om te komen tot een prijsopgave.

Het is niet toegestaan om werknemersbestanden te verwerken met (bijzondere) persoonsgegevens, die meer gegevens bevatten dan voor het tot stand komen van het advies, de offerte en de verzekeringsovereenkomst nodig zijn.

De inkomensverzekeraar/gevolmachtigd agent mag alleen de categorie A-gegevens verwerken voor zover deze absoluut noodzakelijk zijn voor het opmaken van de inkomensverzekering na acceptatie van de offerte of mutatie van de inkomensverzekering. Denk hierbij aan de persoonsgebonden inkomensverzekeringen zoals WIA-aanvullingsverzekeringen, het verzoek om een validiteitsverklaring en opgave van het strafrechtelijke verleden van de eigenaar/bestuurder.

Validiteitsverklaring

Validiteitsverklaringen, opgenomen in het aanvraagformulier inkomensverzekeringen, kennen specifieke voorwaarden. Er mag wel gevraagd worden naar de naam van de zieke werknemer(s), eerste ziekte dag en percentage arbeidsongeschiktheid, maar er mag niet meer informatie worden opgevraagd dan strikt noodzakelijk voor het doel van validiteit. De medewerker acceptatie inkomensverzekeringen mag bijvoorbeeld niet navragen wat de reden van de arbeidsongeschiktheid is en of iemand de bedrijfsarts regelmatig bezoekt, etc. Er mag wel worden gevraagd of er sprake is van een vangnetsituatie, maar niet welke vangnet. Het gaat vaak mis bij de no-riskpolis en als de vijf jaren zijn verstreken.

De verklaring mag op grond van artikel 30 sub 3 lid b van de UAVG worden verzonden, zolang maar duidelijk is gemaakt in de dienstverleningsovereenkomst dat de tussenpersoon de offerte-aanvraag naar de verzekeraar namens de werkgever begeleidt. Er moet sprake zijn van een noodzakelijkheidsvereiste. Niet meer dan de strikt noodzakelijke persoonsgegevens benodigd voor het offertetraject mogen worden uitgewisseld tussen werkgever, verzekeringsadviseur en verzekeraar. Dit geldt tevens voor het verzekeringsbeheer en de uitvoering van de overeenkomst. Denk hierbij aan begeleiding bij de schadeafwikkeling door de financieel dienstverlener en verzekeraar.

- 3 Gelet op artikel 9, tweede lid, onderdeel h, van de verordening, is het verbod om gegevens over gezondheid te verwerken niet van toepassing indien de verwerking geschiedt door:
- a. hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening, voor zover de verwerking noodzakelijk is met het oog op een goede behandeling of verzorging van de betrokkene dan wel het beheer van de betreffende instelling of beroepspraktijk; of
 - b. verzekeraars als bedoeld in artikel 1:1 van de Wet op het financieel toezicht of financiële dienstverleners die bemiddelen in verzekeringen als bedoeld in artikel 1:1 van die wet, voor zover de verwerking noodzakelijk is voor:
 - 1°. de beoordeling van het door de verzekeraar te verzekeren risico en de betrokkene geen bezwaar heeft gemaakt; of
 - 2°. de uitvoering van de overeenkomst van verzekering dan wel het assisteren bij het beheer en de uitvoering van de verzekering.

Specifieke WIA-aanvullingsverzekeringen

Specifieke persoonsgegevens zijn wel noodzakelijk voor de WIA-excedentverzekeringen of WGA-aanvullingsverzekeringen. In het offertetraject zijn de 'wie-vragen' nog niet nodig. Dit speelt pas bij de aanvraag/acceptatie. Immers, zolang er nog geen overeenkomst is, bestaat er geen grondslag voor het verwerken van specifieke persoonsgegevens.

Wanneer de offerte wordt geaccepteerd dient in het aanvraagtraject een aantal persoonsgegevens wel te worden opgegeven. Het gaat dan om NAW-gegevens, geboortedatum, geslacht, salaris, eventuele parttime-percentages en in het kader van de validiteitsverklaring de naam, eerste ziektedag en eventuele mate van arbeidsongeschiktheid en de opgave van het strafrechtelijke verleden van de eigenaar/bestuurder.

Ook voor deze gegevens geldt dat deze rechtstreeks tussen de acceptatieafdeling van de inkomensverzekeraar en de werkgever moeten worden uitgewisseld. De informatie mag niet via de verzekeringsadviseur worden verzonden.

Strafrechtelijke gegevens

Het verwerken van strafrechtelijke gegevens in de slotvragen door een inkomensverzekeraar is toegestaan. Er is een juridische grondslag om toepasselijke navraag te doen naar het strafrechtelijk verleden 8 jaar voorafgaande aan de verzekeringsaanvraag om de aanvraag te kunnen beoordelen. Deze gegevens mogen slechts verwerkt worden als deze uitsluitend worden verstrekt aan functionarissen die de gegevens voor hun functie nodig hebben. Strafrechtelijke gegevens verdienen een bovengemiddeld beschermingsniveau en worden rechtstreeks tussen de acceptatieafdeling van de inkomensverzekeraar en de werkgever uitgewisseld.

Verzekeraars zouden er overigens verstandig aan doen om hun offertesystemen te reviewen en na te gaan of er niet meer gegevens worden gevraagd aan werkgevers/adviseurs dan noodzakelijk. De informatie mag niet via de verzekeringsadviseur worden verzonden.

5.5.10 Naverrekeningstraject

Naverrekeningsbestanden die persoonsgegevens bevatten en dus meer informatie uitwisselen dan noodzakelijk is voor de uitvoering van de verzekeringsovereenkomst, zijn niet toegestaan. Evenmin is het ontvangen en verwerken van werknemersbestanden, salarisstroken en verzamelloonstaten met persoonsgegevens door de verzekeringsadviseur toegestaan.

5.5.11 Schadetraject

De verzekeringsadviseur heeft geen rol bij de verzuimbegeleiding van zieke werknemers en mag dus niets daarover weten. Het namens de werkgever ziekmelden van een werknemer in het systeem van arbodienst, verzekeraar of gevolmachtigde agent is niet toegestaan. Het namens de werkgever beoordelen van de uitkeringenspecificatie inkomensverzekeringen, voorzien van categorie A (en B+C) persoonsgegevens is eveneens niet toegestaan (zie hoofdstuk 3.3)

Het namens de werkgever indienen bij de inkomensverzekeraar van facturen van (preventieve) interventies voor medefinanciering door de inkomensverzekeraar is niet toegestaan.

Persoonsgegevens noodzakelijk voor de claimbeoordeling

De claimbeoordelaar mag alleen gegevens verwerken voor de beoordeling van het recht op vergoeding van de loondoorbetaling. Deze dient daarbij uit te gaan van het oordeel van de arbodienst/bedrijfsarts of UWV bij WIA-dekkingen (inkomensverzekeraars zijn UWV volgend). De arbodienst/bedrijfsarts zal de claimbeoordelaar van de inkomensverzekeraar/gevolmachtigd agent alleen kunnen informeren over de voortgang (of het ontbreken van) een Plan van Aanpak, indien deze daarnaar vraagt bij de arbodienst/bedrijfsarts. De arbodienst/bedrijfsarts moet de werkgever daar wel actief over informeren. De werkgever heeft naar de claimbeoordelaar van de inkomensverzekeraar/gevolmachtigd agent een informatieplicht.

Voor de controle op de juistheid van de informatie, die de claimbeoordelaar van de werkgever ontvangt, kan de procesinformatie worden getoetst bij de arbodienst/bedrijfsarts.

Voor de claimbeoordeling is het opvragen van een loonstrook met meer informatie dan de noodzakelijke loongegevens niet toegestaan! Gegevens als vakbondslidmaatschap, lunchkosten, mogelijk een persoonlijke lening bij de werkgever, inkoop vakantiedagen, BSN, burgerlijke staat, etc., zijn allemaal gegevens die mogelijk verwerkt kunnen worden bij het opvragen van een loonstrook. De inkomensverzekeraar/gevolmachtigd agent zal de verzekerde werkgever goed moeten instrueren welke loongegevens van de zieke en/of arbeidsongeschikte werknemer zij wenst te ontvangen die noodzakelijk zijn voor de claimbeoordeling. Het is dus van belang dat het niet om het soort document gaat, maar om de gegevens die erop staan. Hoofdreel is dat alleen die gegevens moeten worden opgevraagd, die noodzakelijk zijn om de controle te doen.

Probleem hierbij is dat een verzekeraar niet gauw een zelf geknutseld bestandje voor waar zal aannemen. Wat is de praktische uitvoerbaarheid van weggelakte gegevens? En wat te doen als de verzekeraar zelf moet gaan lakken? Er is behoefte aan een nieuw format om de juistheid van salarisgegevens en dienstverbanden te kunnen vaststellen.

Met inachtneming van de privacyregels kunnen claimbeoordelaars WIA-verzekeringen op grond van artikel 30 sub 3 lid b van de UAVG de beperkte gezondheidsgegevens uit categorie A al gedurende de WIA-wachttijd verwerken. Voor het adequaat ondersteunen van de werkgever heeft het re-integratiebedrijf/de re-integratieafdeling van de verzekeraar gedurende deze periode ook categorie B-gegevens nodig.

Verzuimloket

Verzekeraars (en hun gevolmachtigde agenten) en brancheorganisaties bieden de werkgever vaak een zogenoemd verzuimloket, waarin de verzuimregistraties en -begeleiding al dan niet geautomatiseerd worden verwerkt. Het gaat hier uitsluitend om de verwerking van gegevens categorie A en dus geen gegevens uit de categorieën B en C.

Er mag tussen het loket en de inkomensverzekeraar geen andere informatie worden uitgewisseld dan die tussen de werkgever en inkomensverzekeraar.

5.5.12 Overeenkomst inkomensverzekeraar en arbodienst/bedrijfsarts

Kwaliteits- en privacy-borging door middel van een overeenkomst tussen een inkomensverzekeraar/gevolmachtigd agent en arbodienst/bedrijfsarts is noodzakelijk. In deze overeenkomst dient het volgende te zijn geregeld:

- a) Een verklaring dat medewerkers van het re-integratiebedrijf of de medisch adviseur van een verzekeraar, zodra zij daar komen werken, een geheimhoudingsverklaring ondertekenen voor de omgang met bijzondere persoonsgegevens (interventieadvies bedrijfsarts). In deze geheimhoudingsverklaring is ook opgenomen dat deze medewerkers een instructie krijgen over omgang met bijzondere persoonsgegevens;
- b) Een procesbeschrijving van re-integratiebedrijf en medisch adviseur van een verzekeraar voor de verwerking van de persoonsgegevens van het interventieadvies inclusief communicatie met de provider en factuur.

De verzekeraar/gevolmachtigd agent verplicht zich, als een arbodienst dit wenst, een gecombineerde verklaring van de competenties van een medewerker en de geheimhoudingsverklaring van een medewerker aan de desbetreffende arbodienst te sturen.

Op het moment dat er sprake is van een medisch adviseur van een re-integratiebedrijf of -afdeling van een verzekeraar/gevolmachtigd agent, ontvangt de arbodienst:

- De naam en het BIG-registratienummer van de medisch adviseur;
- De namen van de medewerkers die onder verantwoordelijkheid van de medisch adviseur het interventieadvies en nadere correspondentie verwerken.

Rolscheiding

Binnen de eenheid re-integratiebedrijf of -afdeling van een verzekeraar/gevolmachtigd agent dient een strikte scheiding te zijn tussen enerzijds de medische advisering en beoordeling door de medisch adviseur/medische staf en de beslissing door medewerkers van het re-integratiebedrijf of -afdeling bijvoorbeeld over het al dan niet inzetten van een interventie. De scheiding tussen beide bedrijven/afdelingen is essentieel en vastgelegd in artikel 6.1 van de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen.

In het re-integratiebedrijf of -afdeling is een scheiding van functies dus noodzakelijk vanwege het voorbehouden gebruik van categorie C-gegevens aan een bedrijfsarts of medisch adviseur. De casemanager Wet verbetering poortwachter, in dienst van het re-integratiebedrijf of -afdeling, werkt in opdracht van de werkgever. Op advies van en/of in overleg met de bedrijfsarts zet de casemanager Wet verbetering poortwachter namens de werkgever een interventie in. De interventie mag echter niet leiden tot herkenning van aard of oorzaak van de ziekte. Denk hierbij aan inzet van een arbeidsdeskundige of een spoor 2-traject.

5.5.13 Ongevraagd informatie ontvangen die men in zijn rol niet mag hebben

Als er geen grondslag is voor de verwerking van gegevens en er geen expliciete, ondubbelzinnige aantoonbare toestemming aanwezig is van werkgever, moet de afzender gewezen worden op de gegevensverwerking waarvoor geen grondslag is. Praat met de afzender en leg uit welke gegevens wel noodzakelijk zijn. Ook de afzender moet aan de AVG-vereisten voldoen.

Op deze situatie kan worden geanticipeerd door met de andere partijen rondom de zieke werknemer in contracten/standaardformulieren en dergelijke aan te geven welke informatie ontvangen moet worden. De onterecht ontvangen informatie moet vernietigd worden of zo mogelijk worden teruggestuurd. Het is verstandig om contact met de afzender op te nemen en te melden dat betreffende ongewenste gegevens niet ontvangen mogen worden.

5.5.14 Samenwerking/contact met UWV in de keten inkomensverzekeringen

In de contacten met UWV over zieke werknemers met een (toekomstig) uitkeringsrecht Ziektewet, WIA of een beroep op de no-riskpolis worden persoonsgegevens uitgewisseld. In het bijzonder wordt het BSN gebruikt in communicatie met UWV. In Nederland geldt dat alle overheidsorganisaties gebruik mogen maken van het BSN als dat nodig is. Toegestane verwerking van het BSN is vastgelegd in artikel 46 van de UAVG:

De wettekst luidt als volgt:

Artikel 46. Verwerking nationaal identificatienummer

1. Een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, wordt bij de verwerking van persoonsgegevens slechts gebruikt ter uitvoering van de desbetreffende wet dan wel voor doeleinden bij de wet bepaald.
2. Bij algemene maatregel van bestuur kunnen andere dan in het eerste lid bedoelde gevallen worden aangewezen waarin een daarbij aan te wijzen nummer als bedoeld in het eerste lid,

kan worden gebruikt. Daarbij kunnen nadere regels worden gegeven over het gebruik van een zodanig nummer.

De werkgever moet het BSN vastleggen in de salarisadministratie op grond van artikel 28 van de Wet op de loonbelasting 1964. Dit geldt ook voor de kopie van het identiteitsbewijs waar het BSN ook op staat.

UWV heeft het BSN nodig om hun taak uit te kunnen voeren. UWV communiceert altijd met het kenmerk BSN richting werknemer en werkgever. Het verwerken van het BSN is binnen de arbo/verzuimsystemen waarvan de werkgever (en haar eventuele externe adviseurs) veelal gebruik maken, echter pas toegestaan als er sprake is van een noodzakelijkheidsvereiste.

Bij wet is bepaald (artikel 30 sub 3 lid b van de UAVG) dat het BSN ook door inkomensverzekeraars en financieel bemiddelaars vallend onder de Wet op het financieel toezicht mag worden gebruikt, mits er sprake is van het noodzakelijkheidsvereiste. Denk bij voorbeeld aan de claimbehandeling van WGA-uitkeringen onder de WGA-eigenrisicodragerverzekering aan de hand van de WIA-beslissingen en uitkeringenspecificaties van het UWV. Op de genoemde documenten is het BSN van de werknemer opgenomen.

Standpunt BSN bij de meldingen aan het UWV

Wat betreft de Ziektewetvangnetmelding krijgen we veel vragen hoe dat dan moet als het BSN niet meer in het arbosysteem mag staan. Het UWV is van mening dat voor elke situatie de werknemer dan toestemming geeft om met het doel van de aanvraag Ziektewet zijn of haar BSN te gebruiken.

6. Mogelijkheden inzet interventie en de facturering

De komende jaren zal er nog veel overleg gevoerd gaan worden over de mogelijkheden voor de inzet van interventies en de facturering. Ook binnen de werkgroep is er uitgebreid over gesproken. De werkgever geeft namelijk toestemming om bepaalde dienstverlening in te zetten, en daarmee dat de werkgever dit ook (deels) financiert.

De essentiële vraag is of actieve toestemming van de werknemer geldt als grondslag om wel de interventies bij werkgevers neer te leggen. Want de interventie zegt in veel gevallen iets over de aard van de beperking.

Het document 'handleiding privacy en inkomensverzekeringen' van november 2018 gaat ten aanzien van het inzetten van de interventie wel uit van actieve toestemming, vrijwillig gegeven door de werknemer.

De juristen binnen de werkgroep zijn ook van mening dat toestemming wel een grondslag is, want het is in het voordeel van de werknemer als de werkgever zijn interventie betaalt en hij daardoor sneller de juiste hulpverlening krijgt.

Anderen in de werkgroep benoemen juist dat de AP erg kritisch kijkt naar toestemming door de werknemer. Vrijwillig gegeven informatie door werknemer aan de werkgever wordt in twijfel getrokken, gezien de gezagsverhouding tussen werkgever en werknemer.

De meest veilige oplossing vindt de werkgroep dat het organiseren van de interventies gaat lopen via de casemanagers taakdelegatie die onder auspiciën van de bedrijfsarts werken. Daar gaat ook de terugkoppeling van de dienstverleners heen. Maar dan is er nog het vraagstuk van de financiering van de interventies, want de facturering gebeurt veelal wel rechtstreeks aan de werkgever.

Kortom, hier is het laatste woord nog niet over gezegd en we benadrukken dat hoe de werkwijze ook wordt ingericht, er zal aangetoond moeten worden dat het maximale is gedaan om de privacy van de werknemer te borgen.

Onderstaand een uitwerking hoe er met de facturen van interventies omgegaan kan worden.

Let op: overal waar staat re-integratiebedrijf kan ook worden gelezen: re-integratie-afdeling van een verzekeraar/gevolmachtigd agent. Bij medisch adviseur gaat het om de medisch adviseur van een re-integratiebedrijf of -afdeling van een verzekeraar/gevolmachtigd agent.

Nota's en facturen omvatten vaak meer informatie dan alleen de 'kosten van de interventie', waardoor er direct of indirect een relatie te leggen is tussen het soort interventie en de werknemer.

Onderstaand zijn er drie mogelijkheden uitgewerkt:

1. a: De bedrijfsarts stelt een interventieadvies op en verstuurt dit advies;
 b: Het re-integratiebedrijf maakt op basis van het advies beperkingen en mogelijkheden van de bedrijfsarts een voorstel voor een interventie;
2. De uitvoerder van de interventie stuurt proces- of medische informatie op;
3. De uitvoerder van de interventie stuurt de factuur.

Mogelijkheid 1a: De bedrijfsarts stelt een interventie-advies op en verstuurt dit advies

De bedrijfsarts overlegt met de werknemer en zorgt voor een goede uitleg aan de werknemer waarvoor het interventieadvies dient. De werknemer kan in vrijheid beslissen of hij/zij akkoord is of het interventieadvies wordt verzonden aan de werkgever en het re-integratiebedrijf of medisch adviseur. Als de werknemer akkoord gaat, stuurt de bedrijfsarts het advies (niet inhoudelijk in verband met afgeleide naar aard of oorzaak) naar de werkgever en het re-integratiebedrijf.

Of

Mogelijkheid 1b: Het re-integratiebedrijf maakt op basis van het advies over beperkingen en mogelijkheden van de bedrijfsarts een voorstel voor een interventie

De bedrijfsarts geeft inzicht in beperkingen en mogelijkheden van de zieke en/of arbeidsongeschikte werknemer aan het re-integratiebedrijf. Het re-integratiebedrijf maakt op basis van dit inzicht een voorstel voor de in te zetten interventie. Na afstemming met de bedrijfsarts stemt het re-integratiebedrijf het voorstel (niet inhoudelijk in verband met afgeleide naar aard of oorzaak) af met de werknemer en werkgever.

In de situatie dat de bedrijfsarts het advies van het re-integratiebedrijf of -afdeling nog niet heeft besproken met de werknemer, informeert de bedrijfsarts de werknemer.

Het re-integratiebedrijf/de medisch adviseur beoordeelt het interventieadvies in relatie tot de polis van de werkgever en besluit vervolgens of 0%, deel% of 100% vergoeding mogelijk is.

- Bij 100% vergoeding informeert het re-integratiebedrijf/de medisch adviseur de werkgever (niet inhoudelijk in verband met afgeleide naar aard of oorzaak) en zet de interventie in;
- Bij een deel%-vergoeding informeert het re-integratiebedrijf of de medisch adviseur de werkgever. Als de werkgever akkoord is met de deelvergoeding, dan informeert het re-integratiebedrijf/de medisch adviseur de betreffende dienstverlener dat de interventie kan starten;
- Bij 0% informeert het re-integratiebedrijf /de medisch adviseur de werkgever en zet eventueel na akkoord interventie in.

Mogelijkheid 2: De uitvoerder van de interventie stuurt proces- of medische informatie op

Als de uitvoerder van de interventie tussentijdse en eindrapportages oplevert (niet inhoudelijk in verband met afgeleide naar aard of oorzaak), stuurt de uitvoerder van de interventie, verdeeld naar categorie gegevens, deze rapportages naar:

- Categorie B-gegevens:
 - Naar de werknemer en werkgever;
 - Naar de arbodienst/bedrijfsarts;
 - Naar het re-integratiebedrijf of de medisch adviseur.
- Categorie C-gegevens:
 - Naar de bedrijfsarts.

De verschillende betrokken partijen verwerken deze gegevens in hun eigen dossier.

Mogelijkheid 3: De uitvoerder van de interventie stuurt de factuur

Uitgangspunten zijn:

- De claimafdeling mag *geen combinatie ontvangen van factuur met inhoudelijke gegevens van de interventie en persoonlijke gegevens ofwel een naam van de interventiepartij/behandelaar waaruit de medische behandeling af te leiden is*. Een persoon en soort interventie moeten en mogen niet met elkaar kunnen worden gekoppeld. De factuur wordt direct ontvangen en gecontroleerd door de medisch adviseur. De betaling vindt plaats op basis van een bericht van het re-integratiebedrijf aan de claim- of betalingsafdeling.
- De claim- of betalingsafdeling ontvangt een bericht met de naam van de betrokken werknemer, de hoogte van het bedrag van de interventie en het betalingskenmerk voor de financiële afhandeling van de factuur. *Als de naam van de interventiepartij/behandelaar kan leiden tot inzicht in de soort medische behandeling, ontstaat er een probleem wat met een betaling naar een derdenrekening kan worden opgelost*. Op deze wijze kan wel budgetbewaking plaatsvinden, maar is de soort interventie niet herleidbaar. Voorkomen moet worden dat buiten de medisch adviseur een factuur met niet toegestane bijzondere gezondheidsgegevens verwerkt wordt. Uit de factuur en de persoonsgegevens zijn immers bijzondere gezondheidsgegevens af te leiden.

7. Eisen omtrent verzuimsystemen

Bij de ziekteverzuimbegeleiding en re-integratie verwerken veel werkgevers en arbodienstverleners gegevens over de gezondheid van zieke werknemers in digitale verzuimsystemen. Een verzuimsysteem dient minstens te voldoen aan de volgende concrete beveiligingsvereisten die voortvloeien uit artikel 32 AVG en artikel 34 AVG (passende organisatorische en/of technische maatregelen):

- Als het systeem via internet toegankelijk is voor bevoegde medewerkers, dan moet er sprake zijn van een meerfactorauthenticatie. Inloggen met alleen gebruikersnaam en wachtwoord is onvoldoende;
- De beveiligingsrisico's dienen periodiek in kaart te worden gebracht, bijvoorbeeld door penetratietesten en/of securityscans.

Daarnaast moeten passende organisatorische en/of technische maatregelen genomen worden om beveiligingsrisico's te beperken of te voorkomen:

- Het moet voor personen, die bepaalde medische gegevens niet mogen verwerken, onmogelijk zijn deze gegevens toch te kunnen inzien;
- De beheerder van de systemen mag de persoonsgegevens hierin niet gebruiken voor ontwikkeling en testen. Dit betekent dat de beheerder hiervoor geanonimiseerde of dummygegevens moet gebruiken;
- De werkgever mag bij de ziekmelding alleen die gegevens vragen (en opnemen in het verzuimsysteem) die noodzakelijk zijn voor de begeleiding van de zieke werknemer. Er mogen geen (meerkeuze)mogelijkheden in het systeem zitten, die hiermee in strijd zijn;
- Bij voorkeur staan er geen open invulvelden in het systeem. Zijn die er wel, dan moet duidelijk worden aangegeven dat hier geen medische gegevens ingevuld mogen worden;
- Het moet voor de werkgever onmogelijk zijn om rapportages uit te draaien waarin medische persoonsgegevens staan die hij niet mag verwerken;
- Als een (zelfstandige) bedrijfsarts in opdracht van een werkgever de verzuimbegeleiding uitvoert, mag de module waarin de arts de (medische) gegevens registreert op geen enkele manier toegankelijk zijn voor de werkgever. Dus ook niet voor de systeembeheerder die in dienst is bij de werkgever;
- De werkgever mag niet zelf inlogcodes uitgeven voor de toegang tot gegevens die hij niet mag verwerken. Dit moet de externe beheerder van het systeem of de arbodienst doen.

De applicatiebeheerder van de systeemleverancier kan de re-integratiedossiers verwijderen. Een applicatiebeheerder kan niet de inhoud van de dossiers zien, dat kan alleen de gebruiker. Door de functiescheiding is geborgd dat er geen oneigenlijk gebruik is van persoonsgegevens.

8. Bewaartermijnen ziekteverzuimgegevens

Voor de administratieve verzuimgegevens (zoals de datum van ziekmelding, de verwachte duur van het verzuim en de datum van herstel) is er geen wettelijke bewaartermijn. De gegevens moeten verwijderd worden, zodra ze niet meer noodzakelijk zijn. Een redelijke bewaartermijn is maximaal twee jaar na uitdiensttreding. De gegevens van een zieke ex-werknemer kunnen eventueel langer worden bewaard als er sprake is van een arbeidsconflict of een geschil over de toekenning van een arbeidsongeschiktheidsuitkering.

Re-integratiedossier

Er bestaat geen wettelijke termijn voor het bewaren van een re-integratiedossier. Volgens AP is het redelijk om een re-integratiedossier in beginsel niet langer dan twee jaar na afronding van de re-integratie te bewaren. Als een re-integratiedossier blijvende afspraken bevat, zoals blijvende aanpassingen in het gebruik van hulpmiddelen of in de taakhoud, is het uiteraard wel noodzakelijk dat deze afspraken langer bewaard blijven. Deze afspraken kan de werkgever dan opnemen in het personeelsdossier van de betreffende werknemer.

Omdat het re-integratiedossier vaak een onderdeel is van het medisch dossier en daarvoor een langere bewaarplicht geldt, mag niet zonder meer het re-integratiedossier worden verwijderd. Het re-integratiedossier wordt dan net zo lang bewaard als het medisch dossier.

Ziektewet-dossier

Wettelijk is bepaald dat, wanneer de werkgever eigenrisicodragend is voor de Ziektewet, het medisch dossier van een werknemer vijftien jaar bewaard moet worden en de overige gegevens vijf jaar. Het medisch dossier is uiteraard in handen van de bedrijfsarts. Voor de werkgever betekent dit dus een bewaartermijn van vijf jaar.

WIA-dossier

Is de werkgever eigenrisicodragend voor de WGA, en krijgt een werknemer recht op een WGA-uitkering, dan moet de werkgever deze uitkering de eerste tien jaar zelf betalen. Voor de benodigde gegevens geldt een bewaartermijn van tien jaar.

Indien een werknemer bij de WIA-keuring is geweest en < 35% arbeidsongeschikt is verklaard, dan is het mogelijk dat deze werknemer alsnog binnen vijf jaar met dezelfde oorzaak toenemend arbeidsongeschikt raakt en zonder wachttijd recht heeft op een WIA-uitkering. Dit is geregeld in artikel 55 WIA. In deze situaties is het redelijk dat ook de bewaartermijn voor dat dossier 5 jaar is. Aangezien in het publieke bestel bij de toerekening van de WGA-schadelast de rekening altijd twee kalenderjaren later volgt (gezien de T-2 toerekening), is het redelijk om dus 7 jaar het dossier te bewaren. Onderstaand treft u de uitwerking van de redelijke bewaartermijnen, rekening houdend met deze T-2.

8.1 Richtlijnen

Als richtlijn kan het volgende worden aangehouden:

- 2 jaar is gebruikelijk voor bijvoorbeeld het re-integratiedossier, uitdiensttreding, etc.;
- 5 jaar is goed te verdedigen voor een adviesdossier (op basis van art. 32A BGfo Wft);

- 7 jaar, indien noodzakelijk vanuit fiscale overweging;
- 20 jaar, waarbij wel aanvullende argumentatie nodig is om deze termijn te verdedigen;
- Onbeperkt bewaren van gegevens (ook in papieren dossiers) is vanuit privacywetgeving niet te verdedigen. Ook is het onbeperkt bewaren van gegevens van klanten of prospects op grond van AVG in het algemeen niet toegestaan.

Praktisch komt het op het volgende neer:

- Het re-integratiedossier* van een werknemer die binnen de wachttijd van 104 weken is hersteld: opschonen maximaal 2 kalenderjaren na de hersteldmelding;
- Dossiervorming: bij frequent verzuim (meer dan 3 meldingen per jaar), en ten behoeve van bijvoorbeeld de procedure om op basis van frequent verzuim een einde dienstverband overeen te komen, moet de documentatie over een langere periode worden bewaard. Te denken valt aan bijvoorbeeld 5 jaar of het moment dat er sprake was van frequent verzuim.
- Bij een werknemer die na de WIA-keuring < 35% arbeidsongeschikt wordt beoordeeld (artikel 55 WIA) is het noodzakelijk om tot maximaal 7 kalenderjaren de gegevens te bewaren i.v.m. T-2 bij UWV;
- Bij een werknemer met een WIA-uitkering is de bewaartermijn langer. Bij WGA geldt hiervoor 12 jaar (10 jaar verantwoordelijk plus 2 jaar). Dit geldt ook bij toekenning IVA, omdat er omzetting kan komen naar WGA;
- Bij de uitdiensttreding van een zieke werknemer is vernietiging van de gegevens 2 jaar na de hersteldmelding binnen de wachttijd aan de orde. Afhankelijk van de WIA-uitkomst zijn de bewaartermijnen langer;
- Het bewijs agh /sfb – inventarisatie blijft bestaan zolang het dienstverband loopt en er een onbeperkte no-risk van toepassing is (zoals bij Wajong of doelgroepverklaring banenafspraken);
- Is er geen sprake van een onbeperkte no-risk, dan geldt een bewaartermijn van 7 jaar na de indiensttreding. Indien er sprake is van een lopende no-risksituatie van iemand die binnen de no-riskperiode ziek is geworden, is er een bewaartermijn 12 jaar van toepassing, omdat de werking van de no-risk zich over een 12-jarige periode uitstrekt (2 jaar verzuim en 10 jaar WGA);
- In het geval van een dossier t.a.v. de nawerking ZW heeft de werkgever zelf geen dossier gevormd. Het personeelsdossier en de verzuimhistorie mag niet worden opgeschoond zolang de ZW- en/of WGA-uitkering toegerekend wordt;
- Een medisch dossier van de bedrijfsarts dient 15 jaar bewaard te worden conform richtlijnen KNMG.

**Omdat het re-integratiedossier vaak een onderdeel is van het medisch dossier en daarvoor een langere bewaarplicht geldt, mag niet zonder meer het re-integratiedossier worden verwijderd. Het re-integratiedossier wordt dan net zo lang bewaard als het medisch dossier.*

Schematisch overzicht van de bewaartermijnen:

Soort dossier	Beheerder	Bewaartermijn
Preventief niet-medisch dossier	Arbodienst	2 jaar
Preventief medisch dossier	Bedrijfsarts	15 jaar
Re-integratiedossier	Arbodienst	15 jaar
Medisch dossier bij ziekte	Bedrijfsarts	15 jaar
Medisch dossier bij ziekte (verlengde bewaarperiode bv kankerverwekkende stoffen)	Bedrijfsarts	?
Aanstellingskeuring	Bedrijfsarts	½ jaar
Beroepsziekte medisch dossier	Bedrijfsarts	15 jaar
Beroepsziekte niet medisch dossier	Bedrijfsarts	2 jaar
Verplichte medische keuring	Bedrijfsarts	2 jaar
PMO uitslagen	Bedrijfsarts	2 jaar
Blootstellingsgegevens	Bedrijfsarts	?

- De werkgever mag administratieve verzuimgegevens tot maximaal twee jaar na afloop van de arbeidsrelatie bewaren (hoofdstuk 8.1.1.), tenzij de werkgever eigenrisicodrager Ziektewet is. Dan moet de werkgever de gegevens over de ziekmelding vijf jaar bewaren en moet de bedrijfsarts deze tien jaar bewaren. Voor eigenrisicodragerschap WGA mogen de gegevens voor de duur van het WGA-traject bewaard blijven (tien jaar).
- De bedrijfsarts mag aanstellingskeuringsdossiers maximaal zes maanden bewaren (hoofdstuk 8.1.2).
- De bedrijfsarts mag medische dossiers maximaal vijftien jaar bewaren, tenzij er sprake is van een beroepsziekte. Dan mag de arts de gegevens langer bewaren. Voor niet-medische dossiers geldt een bewaartermijn van maximaal twee jaar (hoofdstuk 8.1.2).
- Re-integratie dossiers mogen maximaal vijftien jaar worden bewaard door de hulpverlener die rechtstreeks onder de WGBA valt en twee jaar door andere hulpverleners (hoofdstuk 8.1.3).

In de onderstaande paragrafen worden achtereenvolgens de bewaartermijnen voor de werkgever, bedrijfsarts, arbodienstverleners en re-integratiebedrijven behandeld.

8.1.1. Bewaartermijnen werkgever

Als een werknemer slechts een korte periode ziek is geweest, heeft de werkgever weinig persoonsgegevens over het ziekteverzuim verzameld. Het gaat dan vooral om administratieve gegevens voor de loondoorbetalingsverplichting, zoals de datum van de ziekmelding, de duur van het verzuim en de datum van herstel. Deze gegevens mag de werkgever bewaren zolang dat nodig is voor de doeleinden waarvoor ze verzameld zijn. Een redelijke bewaartermijn voor de administratieve verzuimgegevens betreft maximaal twee jaar nadat de arbeidsrelatie is afgelopen. De werkgever kan de gegevens van een zieke ex-werknemer zo nodig langer bewaren als er sprake is van een arbeidsconflict of een geschil over de toekenning van een arbeidsongeschiktheidsuitkering.

Bij langdurige ziekte zijn er meer persoonsgegevens van de zieke werknemer verwerkt en heeft de werkgever een re-integratiedossier opgebouwd. Er bestaat geen wettelijke termijn voor het bewaren van een re-integratiedossier. Het is echter redelijk om een re-integratiedossier in beginsel niet langer dan twee jaar na afronding van de re-integratie te bewaren. Als een re-integratiedossier blijvende afspraken bevat, zoals blijvende aanpassingen in het gebruik van hulpmiddelen of in de taakhoud, is het uiteraard wel noodzakelijk dat deze afspraken langer bewaard blijven. Deze afspraken kan de werkgever dan opnemen in het personeelsdossier van de betreffende werknemer.

Bewaartermijn voor eigenrisicodragers Ziektewet en WGA

Wettelijk is bepaald dat wanneer de werkgever eigen risico draagt voor de Ziektewet, het medisch dossier van een werknemer tien jaar bewaard moet worden en de overige gegevens vijf jaar. Dit betekent dat een werkgever de gegevens die hij verzamelt voor het eigen risico dragen vijf jaar moet bewaren. Aangezien de werkgever zelf geen medisch dossier mag aanleggen, is de bewaartermijn van tien jaar alleen van toepassing op het medisch dossier dat de bedrijfsarts over de werknemer voor het eigen risico dragen heeft aangelegd.

Bij eigen risico dragen WGA kiest een werkgever ervoor zelf het risico te dragen voor de WGA-uitkering van zijn (ex-)werknemers. Als een werknemer recht krijgt op een WGA-uitkering, moet de werkgever deze uitkering de eerste tien jaar zelf betalen. Omdat het hier gegevens van een medische keuring betreft die worden vastgelegd met een specifiek doel, geldt voor dergelijke gegevens een beperkte bewaartermijn, namelijk zolang als voor het doel noodzakelijk is. In dit geval voor de duur van het WGA-traject, namelijk tien jaar.

8.1.2. Bewaartermijnen bedrijfsarts/arbodienstverleners

Aanstellingskeuringsdossiers

De bedrijfsarts mag aanstellingskeuringsdossiers van sollicitanten, ongeacht of ze worden aangenomen of niet, maximaal zes maanden bewaren. Deze termijn geldt omdat een sollicitant tot uiterlijk zes maanden nadat de keuring heeft plaatsgevonden een klacht kan indienen bij de Commissie Klachtenbehandeling Aanstellingskeuringen.

Gegevens van zieke werknemers

Voor medische dossiers bij een behandelingsovereenkomst geldt een wettelijk bewaartermijn van vijftien jaar of zoveel langer als redelijkerwijs uit de zorg van een goed hulpverlener voortvloeit. Voor de situatie dat er geen sprake is van een behandelingsovereenkomst (dit geldt voor het merendeel van de handelingen van de bedrijfsarts) mag het medisch dossier bewaard worden zolang dat noodzakelijk is voor het doel van het onderzoek.

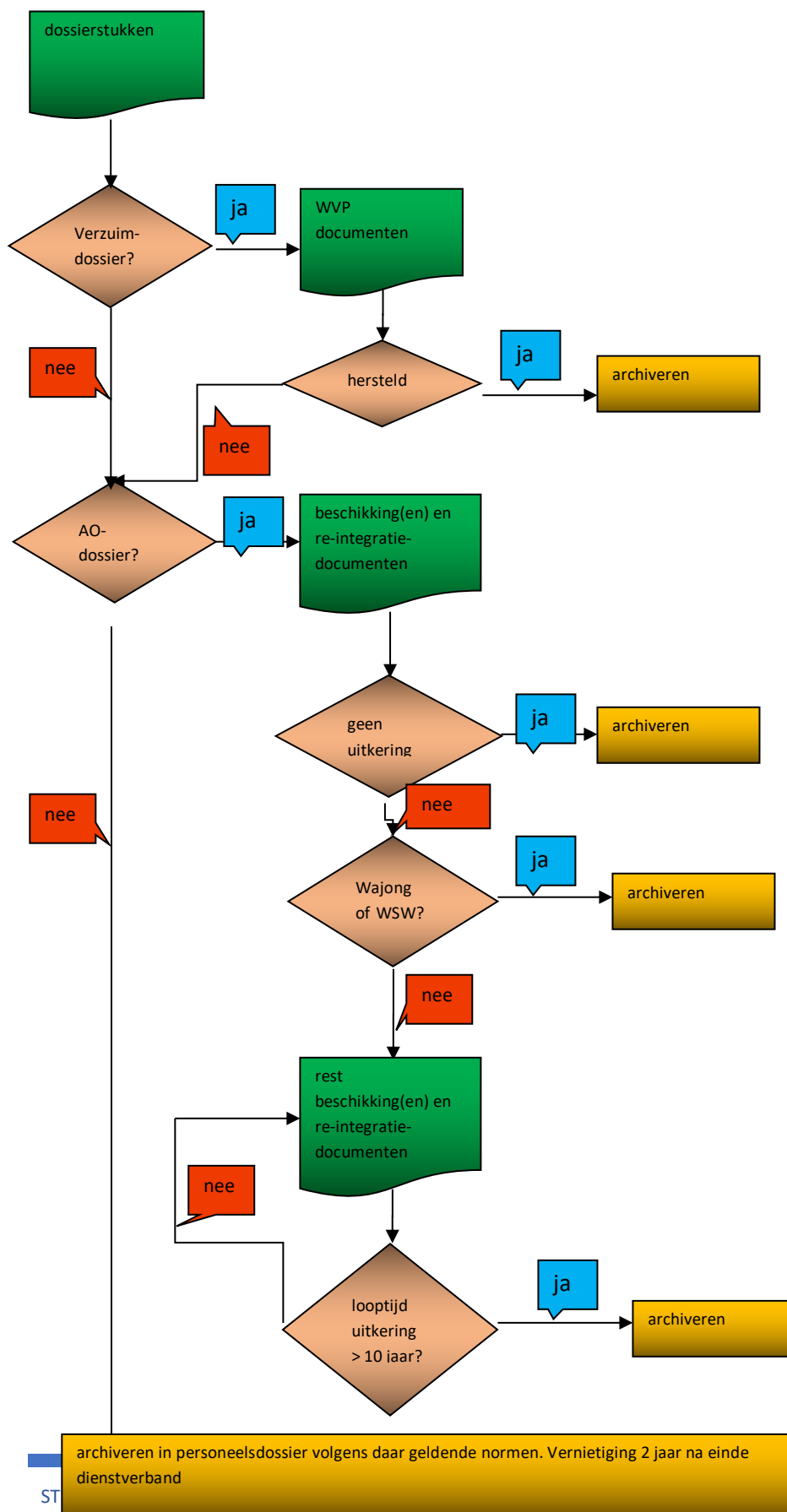
Medische dossiers die voor de controle en verzuimbegeleiding zijn aangelegd, moeten naar analogie van artikel 7:454, derde lid, BW, tot vijftien jaar vanaf het moment van opmaak van de betreffende stukken worden bewaard. Er zijn beroepsgebonden aandoeningen die zich na verloop van (nog langere) tijd kunnen openbaren. Wanneer dit risico aanwezig is moeten medische gegevens voor dit doeleinde langer worden bewaard.

Voor de overige gegevens over zieke werknemers die arbodienstverleners registreren bestaat geen wettelijke bewaartermijn. Het is echter redelijk deze niet langer te bewaren dan twee jaar na afronding van de verzuimbegeleiding en/of het re-integratietraject.

8.1.3. Bewaartermijnen voor re-integratiebedrijven

Aangezien het medisch deel van een re-integratiedossier in het bezit is van een hulpverlener die onder de werking van de Wet inzake de geneeskundige behandelingsovereenkomst (WGBO) valt, geldt hiervoor een bewaartermijn van vijftien jaar. Er bestaat geen wettelijke termijn voor het bewaren van het niet-medisch deel van een re-integratiedossier. Het is echter redelijk om dit in beginsel niet langer dan twee jaar na afronding van de re-integratie te bewaren.

Bewaartermijnen niet medische verzuim- en AO dossierstukken



bewaartermijn

Max. **2 kalenderjaren** na datum hersteld melding. Indien er sprake is van frequent verzuim is noodzakelijkheidvereiste van toepassing en mogen de WVP documenten **4 kalenderjaren** bewaard worden.

5 jaar na datum einde uitkering kan er nog sprake zijn van herleving van de uitkeringsrechten, welke obv T-2 tot uiting kunnen komen. Hierdoor noodzakelijk om dossierstukken tot max. **7 kalenderjaren** na beschikkingsdatum te bewaren.

Beschikkingen Wajong of WSW blijven bewaard in het dossier zolang zij vigerend zijn. Voor overige documenten gelden de bewaartermijnen in dit schema.

Max. **2 kalenderjaren** na de datum waarop de uitkering 10 jaar heeft geduurd, vervalt de noodzaak tot archivering van de stukken die betrekking hebben op de uitkering (T-2).

Bijlage 1 brief AP – geen combifunctie werkgever casemanager en cmt**AUTORITEIT PERSOONSgegevens**

Datum

Ons kenmerk

Toelichting Beleidsregels zieke Werknemer'

Geachte heer Klompsma,

In bovengenoemde brief heeft u de Autoriteit persoonsgegevens (AP) verzocht te reageren op uw conclusie dat de AP, zoals volgens u blijkt uit de Beleidsregels 'de zieke werknemer' (beleidsregels), het onwenselijk vindt dat een casemanager die optreedt als faciliterend en coördinerend casemanager voor de werkgever eveneens optreedt als casemanager die gedelegeerde taken uitvoert onder eindverantwoordelijkheid van een bedrijfsarts.

In de beleidsregels heeft de AP uitgelegd dat een medewerker in opdracht van een bedrijfsarts alleen die gegevens mag verwerken die strikt noodzakelijk zijn voor de uitoefening van haar/zijn gedelegeerde taken. De medewerker valt onder het afgeleide beroepsgeheim van de bedrijfsarts. Dit betekent dat ook de medewerker met de werkgever uitsluitend die informatie mag uitwisselen die de bedrijfsarts met de werkgever mag uitwisselen.

In de beleidsregels is tevens aangegeven dat een medewerker, waarvan de taak bestaat uit faciliterende en coördinerende werkzaamheden tijdens het ziekteverzuimproces, is aan te merken als procesbewaker voor de werkgever. Deze medewerker mag alleen beschikken over de informatie die noodzakelijk is voor de vervulling van deze taken. Dit betekent dat de medewerker niet meer gegevens mag verwerken dan de gegevens die voor de werkgever noodzakelijk voor de re-integratie/ begeleiding van werknemers vanwege ziekte of arbeidsongeschiktheid

In praktijk wordt vaak gesproken over een 'casemanager',

Z2015-00.T74 Beleidsregels voor de verwerking van persoonsgegevens over de gezondheid van zieke werknemers p. 25.

Z2015-00774 Beleidsregels voor de verwerking van persoonsgegevens over de gezondheid van zieke werknemers p. 2'.

Door (een deel van) de taken van zowel de bedrijfsarts als de werkgever in één persoon te verenigen verwerkt de betreffende medewerker bij de uitvoering van de taken voor de werkgever meer gegevens dan de gegevens die hiervoor noodzakelijk zijn. Namelijk de gegevens die worden verwerkt in het kader van de uitvoering van de taken voor de bedrijfsarts, wat onder andere gegevens over aard en oorzaak van de ziekte kunnen zijn. Omgekeerd verwerkt deze persoon bij de uitvoering van de taken voor de bedrijfsarts ook meer informatie dan noodzakelijk is voor de uitvoering van deze taken, Deze wijze van werken is derhalve niet in overeenstemming met de wet.

De Autoriteit Persoonsgegevens vertrouwt erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,

Bijlage 2 : brief AP – een werkgever mag niet vragen naar de taken



AUTORITEIT PERSOONSgegevens

Uw brief van 22 november 2017
Uw kenmerk
Vraag over de lopende afspraken en
Werzaamheden

Op 22 november 2017 heeft u de Autoriteit Persoonsgegevens (hierna: AP) een brief gestuurd. Daarin schrijft u dat u zich strikt houdt aan het wettelijk kader zoals de AP die aangeeft in de 'Beleidsregels zieke werknemer (2016)'.

Uit deze beleidsregels blijkt onder meer dat de werkgever met een zieke werknemer mag praten over zijn functionele beperkingen en mogelijkheden onder de voorwaarde dat een bedrijfsarts in kaart heeft gebracht wat de functionele beperkingen en mogelijkheden van de werknemer zijn.

Via uw werkgever volgt u een opleiding bij het opleidingsbedrijf Z. Dit bedrijf stelt nu dat de werkgever zonder tussenkomst van de bedrijfsarts (of casemanager Taakdelegatie) wel mag vragen welke taken uit de eigen functie een werknemer nog wel zou kunnen uitvoeren. Het opleidingsbedrijf baseert dit op de in bovengenoemde beleidsregels benoemde 'lopende afspraken en werkzaamheden'.

U wilt graag weten of een werkgever inderdaad zonder tussenkomst van de bedrijfsarts mag vragen naar welke taken de werknemer nog kan uitvoeren onder het mom dat 'de werkgever mag vragen naar de lopende afspraken en werkzaamheden'.

Reactie AP op uw vraag

Het standpunt van de AP is dat de werkgever niet zonder tussenkomst van de bedrijfsarts mag vragen welke taken de werknemer nog wel kan uitvoeren. De achterliggende gedachte is dat een werknemer al binnen de grenzen van de wet verplicht is om volledig mee te werken aan zijn re-integratie. Van de werknemer mag niet ook nog worden verwacht dat hij aangeeft welke (deel)taken, (deel)functies of werkzaamheden hij zou kunnen verrichten. Zou dit wel het geval zijn, dan wordt de werknemer - die financieel afhankelijk is van de werkgever - geforceerd worden om zijn eigen beperkingen en mogelijkheden vast te stellen en de uitkomst daarvan aan de werkgever te communiceren. Dat laatste is niet de taak van een werknemer en kan enkel onafhankelijk worden vastgesteld door tussenkomst van een bedrijfsarts. De AP vertrouwt erop u hiermee voldoende te hebben geïnformeerd.

Autoriteit Persoonsgegevens

Bijlage 3: Publicatie met gezamenlijke uitleg beleidsregels door ministerie Sociale Zaken en Werkgelegenheid met (onbekende) stakeholders

De onderstaande tekst heeft betrekking op de periode van de ziekmelding tot het eerste advies van de bedrijfsarts.

Verwerken van gegevens bij ziekmelding

Werkgevers mogen volgens de Algemene verordening gegevensbescherming (AVG) slechts beperkt gegevens vragen en verwerken van een werknemer in het kader van een ziekmelding of re-integratieproces. In de beleidsregels ‘De zieke werknemer’ (1) heeft de Autoriteit Persoonsgegevens beschreven welke gegevens dat zijn: de gegevens die noodzakelijk zijn voor de uitvoering van de arbeidsovereenkomst, de bedrijfsvoering of om een wettelijke verplichting – zoals re-integratie – na te komen. In dat kader mag de werkgever (2) de werknemer niet vragen naar een diagnose of behandeling door een arts en ook niet naar de functionele mogelijkheden en beperkingen (3) van de werknemer.

Het is in het belang van de werknemer om zijn werkgever bij de ziekmelding te melden dat hij door ongeschiktheid ten gevolge van ziekte niet in staat is om zijn normale werkzaamheden (4) te verrichten. De werkgever mag bij de ziekmelding vragen naar de vermoedelijke duur van het verzuim.

1) De zieke werknemer, Beleidsregels voor de verwerking van persoonsgegevens over de gezondheid van zieke werknemers, Autoriteit Persoonsgegevens, z2015-00774 – 23 februari 2016

2) En aan de werkgever gelijk te stellen functionarissen zoals casemanagers.

3) Bijvoorbeeld: ‘hoeveel kun je nog tillen’; ‘kun je op je knieën zitten’; ‘hoe lang kun je geconcentreerd werken’; ‘is hectiek op de afdeling een probleem’; ‘kun je in een groep werken’.

4) Hiermee wordt bedoeld “de bedongen arbeid”: in arbeidsrechtelijke zin de overeengekomen arbeidsduur en de overeengekomen inhoudelijke werkzaamheden die de werknemer verricht op grond van de arbeidsovereenkomst.

5) Artikel 7:611 BW

Terugkeer naar werk

De werkgever en de werknemer kunnen het gesprek aangaan over de manier waarop de terugkeer naar werk invulling kan krijgen. Daarbij kan de werknemer zelf aangeven of hij bepaalde (deel)taken, (deel)functies of werkzaamheden nog wel kan verrichten. Goed werknemerschap (5) brengt immers ook met zich mee dat een werknemer zelf mede verantwoordelijkheid draagt voor zijn herstel en de terugkeer naar werk. De werkgever mag hier echter geen druk op uitoefenen en hier niet naar vragen. Zo nodig kan hij de bedrijfsarts vragen welke (deel)taken, (deel)functies of werkzaamheden de werknemer nog wel kan verrichten.

Werkafspraken

Van het gesprek tussen werkgever en werknemer mag worden vastgelegd welke werkafspraken zijn gemaakt in de zin van uit te voeren taken of werkzaamheden. Als er op initiatief van de werknemer eventueel gesproken is over functionele mogelijkheden en beperkingen of een diagnose of behandeling, dan worden die gegevens niet geregistreerd door de werkgever. De werkgever kan de functionele mogelijkheden en beperkingen die door de bedrijfsarts zijn vastgesteld en gedeeld met werknemer en werkgever wel registreren.

Als de omstandigheden daar aanleiding toe geven, kan zowel de werkgever als de werknemer de bedrijfsarts inschakelen in een eerder stadium dan de wettelijke voorgeschreven termijn van maximaal zes weken na de ziekmelding.

Juli 2018

Deze gezamenlijke uitleg is tot stand gekomen in afstemming met stakeholders.

– Einde publicatie–

Bijlage 4 : vragenbrief van werkgroep Gegevensverwerking verzuim aan AP

Autoriteit Persoonsgegevens
Postbus 93374
2509 AJ DEN HAAG

Gorinchem, 20 april 2018

Betreft: vraagstellingen verzuimbegeleiding van de zieke werknemer

Geachte heer of mevrouw,

Namens de Werkgroep Gegevensverwerking rondom de (zieke) werknemer verzoeken wij de Autoriteit Persoonsgegevens te reageren op de vragen/standpunt opgenomen in de bijlage behorende bij deze brief.

De Werkgroep Gegevensverwerking rondom de (zieke) werknemer bestaat uit een afvaardiging van professionals uit het gehele werkveld van arbeid en gezondheid. Deze professionals zijn werkzaam bij of als: arbodienstverlener, zelfstandig bedrijfsarts, re-integratiebedrijf, ICT-leverancier van HR-, Arbo- en verzuimsystemen, arbeidsjurist, opleider casemanagers procesbewaking en taakdelegatie, arbeidsdeskundige, register casemanager, functionaris gegevensverwerking, HR-adviseur en inkomensverzekeraar. Daarnaast is het merendeel van deze professionals werkgever dan wel werknemer.

Voor veel werknemers, werkgevers en betrokken partijen die gegevens over de gezondheid van (zieke) werknemers verwerken, is nog te vaak onduidelijk hoe zij gezamenlijk actief aan verzuimbegeleiding en re-integratie kunnen werken conform de aangescherpte privacyregels. Ook voor bedrijfsartsen zijn er uitdagingen om de gewenste of noodzakelijke ondersteuning te geven, terwijl hun agenda al onder druk staat.

In de praktijk botsen de beleidsregels 'de zieke werknemer' met een actieve verzuimbegeleiding door de werkgever en het doel van de Wet verbetering poortwachter. Voor een aantal vraagstukken is het niet duidelijk hoe deze zijn in te passen in de grondbeginselen van de AVG.

De Werkgroep Gegevensverwerking rondom de (zieke) werknemer geeft een aantal van deze knelpunten in de bijlage weer, met een vraag dan wel standpunt hoe dit praktisch zou kunnen werken. Wij verzoeken u om deze standpunten en vragen te toetsen en hierop schriftelijk te reageren. Uw terugkoppeling zien we graag tegemoet, indien mogelijk voor 1 mei 2018.

Met vriendelijke groet,

Werkgroep Gegevensverwerking rondom de (zieke) werknemer

Vertegenwoordigd door o.a.

Brenda Damkat, Eureka Advies

Monique van de Graaf, Van de Graaf Juridisch Advies, arbeids- en sociaal verzekeringsjurist

Stefan Königs, directeur Regio HR

Marjol Nikkels, directeur CS Opleidingen

Carmen Schermer, directeur RiskSZ

Bijlage: Vragen en standpunt Werkgroep Gegevensverwerking rondom de (zieke) werknemer

Aanleiding

In het Burgerlijk Wetboek is vastgelegd dat verzuimbegeleiding/re-integratie primair de verantwoordelijkheid is van de werkgever en de zieke werknemer (Artikel 7:658a BW).

Bij een ziekmelding mag de werkgever een beperkt aantal vragen stellen aan de zieke werknemer, omdat hij wettelijk verplicht is de voortgang van de ziekte van de werknemer bij te houden. Uit de Wet bescherming persoonsgegevens (Wbp) volgt dat de werkgever zich bij de ziekmelding moet beperken tot de gegevens die noodzakelijk zijn, bijvoorbeeld voor de uitvoering van de arbeidsovereenkomst, om een wettelijke verplichting na te komen, dan wel voor de bedrijfsvoering. De werkgever mag bij de ziekmelding niet vragen naar de aard en/of de oorzaak van de ziekte van de werknemer (Kamerstukken II 1997/98, 25 892, nr.3, p. 113 en 114). Ook mag de werkgever niet zelf vragen naar de beperkingen en mogelijkheden van de werknemer (toelichting op artikel 2 Regeling procesgang eerste en tweede ziektejaar; Rechtbank Rotterdam, 4 februari 2014, ECLI:NL:RBAMS:2014:564, r.o.v. 7).

Zoals ook door de Autoriteit Persoonsgegevens is vastgelegd in de beleidsregels de zieke werknemer mag de werkgever bij de ziekmelding van de werknemer alleen de volgende gegevens over de gezondheid van de zieke werknemer vragen en registreren:

- 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 (maar niet onder welke vangnetbepaling hij valt);
- of de ziekte verband houdt met een arbeidsongeval;
- of er sprake is van een verkeersongeval waarbij een eventueel aansprakelijke derde betrokken is (regresmogelijkheid).

De werkgever mag, met uitzondering van bovenstaande gegevens, in principe geen andere gegevens over de gezondheid van de werknemer in zijn eigen administratie registreren en/of doorgeven aan de bedrijfsarts/arbodienst. Ook niet als deze gegevens vrijwillig door de werknemer zijn verstrekt. Het noodzakelijkheidsvereiste geldt namelijk ook wanneer gegevens over de gezondheid vrijwillig aan de werkgever zijn verstrekt (Afdeling bestuursrechtspraak Raad van State, 5 februari 2014, (ECLI:NL:RVS:2014:308).

In een enkel geval kan het echter wel noodzakelijk zijn om vrijwillig verstrekte gegevens over de gezondheid in de administratie op te nemen, bijvoorbeeld als een werknemer in ernstige mate last heeft van suikerziekte of epilepsie en dit zelf of via de bedrijfsarts heeft aangegeven bij de werkgever. Het kan dan noodzakelijk zijn dat de directe collega's van de zieke werknemer op de hoogte zijn van de ziekte en wat zij in geval van nood moeten doen.

1. Hoe omgaan met situatie waarbij werknemer zelf aangeeft wat hij of zij kan doen?

De werkgever heeft er belang bij te weten wat de vermoedelijke duur van het verzuim is, zodat hij hiermee rekening kan houden binnen zijn organisatie. Heeft de werknemer hier zelf nog geen idee over, dan **kan** de werkgever zich laten informeren door de bedrijfsarts. Afhankelijk van de concrete omstandigheden van het geval, zoals de vermoedelijke door de werknemer ingeschatte duur van het verzuim, kan het voor de werkgever noodzakelijk zijn sommige werkzaamheden door collega's van de zieke werknemer voort te laten zetten. De werkgever kijkt dan naar de lopende afspraken en werkzaamheden om te kunnen beslissen welke werkzaamheden en afspraken kunnen wachten totdat de zieke werknemer is hersteld en welke activiteiten een vervanger kan overnemen.

Bij de ziekmelding mag niet meer door werkgever gevraagd worden wat de werknemer nog wel kan doen (toelichting op artikel 2 Regeling procesgang eerste en tweede ziektejaar; Rechtbank Rotterdam, 4 februari 2014, ECLI:NL:RBAMS:2014:564, r.o.v. 7.), zonder tussenkomst van de bedrijfsarts.

Ca. 80% van alle verzuimmeldingen zijn echter gekoppeld aan kort verzuim (< 8 dagen) waarbij de bedrijfsarts of een taakgedelegeerde nog niet wordt ingezet. Ook bij kort verzuim kan het zijn dat werknemers nog benutbare mogelijkheden hebben en dat zij ook graag deels aan het werk willen blijven. Veel werknemers hebben in de praktijk een prima beeld van wat zij zelf nog aan taken kunnen uitvoeren. Bijvoorbeeld in de situatie dat een zieke werknemer een tijdelijke reisbeperking heeft, maar mogelijkheden ziet om een deel van de taken vanuit huis te organiseren. Door hier niet over in gesprek te mogen, worden re-integratiekansen gemist. Dit doet afbreuk aan de gezamenlijke verantwoordelijkheid voor verzuimbegeleiding en re-integratie van werkgever en werknemer zoals die verankerd is in de Wet verbetering poortwachter.

Overleg in het verleden tussen de Nederlands Vereniging voor Arbeids- en Bedrijfsgeneeskunde en de Autoriteit Persoonsgegevens leek tot nuancering te leiden. Werkgevers en werknemers zouden wel zelfstandig over taken mogen praten. Dit standpunt is nooit door de Autoriteit Persoonsgegevens bevestigd en dit geeft verwarring en discussie in de markt. Vandaar vraag 1.

Vraag 1

Indien de werknemer geheel vrijwillig uit zichzelf aangeeft dat hij of zij nog een deel van zijn taken kan doen al dan niet met ondersteuning van de werkgever (al dan niet via de casemanager werkgeversregievoerder/procesbewaker), bijvoorbeeld met tijdelijke hulpmiddelen, mag een werkgever deze werkherstattingsmogelijkheden dan vernemen om in samenspraak met de werknemer tot uitvoer van deze werkzaamheden (taken) te komen?

2. Hoe om te gaan met voorinformatie richting bedrijfsarts?

In een normale verstandhouding tussen werkgever en werknemer is het gebruikelijk dat de werknemer deelt wat er speelt. De richtlijnen zijn dermate strikt opgesteld dat werkgevers het idee hebben dat alle menselijke maat ontbreekt bij de ziekteverzuimbegeleiding/re-integratie.

Als de werkgever de vrijwillig verstrekte informatie heeft gehoord, dan heeft de werkgever (al dan niet via de casemanager werkgeversregievoerder/procesbewaker) behoefte om dit in voorkomende situaties aan de bedrijfsarts door te geven. De werkgever mag, met uitzondering van de eerdergenoemde gegevens, in principe geen andere gegevens over de gezondheid van de werknemer in zijn eigen administratie registreren en/of doorgeven aan de bedrijfsarts/arbodienst. Ook niet als deze gegevens vrijwillig door de werknemer zijn verstrekt. Het noodzakelijkheidsvereiste geldt namelijk ook wanneer gegevens over de gezondheid vrijwillig aan de werkgever zijn verstrekt (Afdeling bestuursrechtspraak Raad van State 5 februari 2014 ECLI:NL:RVS:2014:308)

De werkgever mag (al dan niet via de casemanager werkgeversregievoerder/procesbewaker) aan de bedrijfsarts wel informatie doorgeven over de aard van de functie en het functioneren. Ook mag de werkgever de bedrijfsarts vragen stellen over veiligheid, welzijn en beschikbaarheid voor passende arbeid.

De praktijk laat zien dat de bedrijfsarts graag meer informatie wil ontvangen van de werkgever (al dan niet via de casemanager werkgeversregievoerder/procesbewaker) voordat de bedrijfsarts het gesprek met werknemer aangaat. Overdracht van informatie draagt bij tot het voorbereiden en efficiënter laten verlopen van het spreekuur in tijden van beperkte en teruglopende bedrijfsartsencapaciteit.

Vraag 2a

Er mag door werkgevers niet gevraagd worden naar meer informatie dan eerdergenoemd, maar werknemers willen graag een luisterend oor en 'hun ei' kwijt kunnen. Hoe moeten werkgevers (al dan niet via de casemanager werkgeversregievoerder/procesbewaker) omgaan met alles wat vrijwillig door de werknemer wordt verteld?

Vraag 2b

Hoe kan de werkgever tegemoetkomen aan de wens van de bedrijfsarts om hetgeen hij vrijwillig heeft vernomen van de werknemer (al dan niet via de casemanager werkgeversregievoerder/procesbewaker) door te geven aan de bedrijfsarts als de werknemer daarmee heeft ingestemd?

3. Hoe om te gaan met de private uitvoerder Ziektewet die voor de werkgever het eigenrisicodragerschap Ziektewet uitvoert?

Indien de werknemer ziek uit dienst gaat en daarmee recht krijgt op de Ziektewetuitkering, kan dit lopen via het UWV (publieke uitvoerder) of via de private uitvoerder (indien werkgever eigenrisicodrager voor de Ziektewet is). Het re-integratieverslag (RIV) opgesteld tijdens het dienstverband conform de regeling procesgang eerste en tweede ziektejaar tot overgang naar de Ziektewet moet normaliter naar het UWV gestuurd worden bij de publieke uitvoering.

Het standpunt wat wij gerechtvaardigd vinden, is dat de private uitvoerder Ziektewet in de uitvoering van de re-integratieverplichtingen gelijk behandeld wordt als de publieke uitvoerder (UWV). Dit betekent dat werkgever het RIV kan overdragen aan de private uitvoerder zonder toestemming van

de werknemer. Voor het medisch dossier zal dit gevoeliger liggen. In de praktijk geeft de bedrijfsarts bij een werknemer die ziek uit dienst gaat, het medisch deel geeft aan de werknemer en de medewerker overhandigt dit aan de verzekeringsarts bij het UWV of aan de bedrijfsarts van de private uitvoerder.

Vraag 3a

Kan bij de private uitvoering het RIV opgesteld tijdens het dienstverband conform de regeling procesgang eerste en tweede ziektejaar tot overgang naar de Ziektewet over worden gedragen naar de private uitvoerder Ziektewet? Of is hier toestemming van de werknemer voor nodig?

Vraag 3b:

Mag de bedrijfsarts die de zieke werknemer begeleidde tijdens het dienstverband het medisch dossier overdragen aan de bedrijfsarts van de private uitvoerder Ziektewet of is hiervoor ook toestemming van de werknemer nodig (bijv. de situatie dat de werknemer het medisch dossier overhandigt aan de bedrijfsarts van de private uitvoerder)?

Vraag 3c

Als er voor overdracht aan de bedrijfsarts van de private uitvoerder Ziektewet toestemming van de werknemer nodig is, kan dit dan aan de werknemer worden gevraagd bij het laatste bezoek aan de bedrijfsarts binnen het dienstverband, waarin ook het actueel oordeel wordt opgesteld?

4. Hoe om te gaan met interventieadvies en terugkoppeling van beperkingen?

Interventieadvies

Als de bedrijfsarts een interventieadvies geeft, conform de verplichtingen als neergelegd in de Wet verbetering poortwachter, is voor de casemanager werkgeversregievoerder/procesbewaker in veel gevallen de soort interventie (behandeling) en daarmee de aard van het verzuim af te leiden. Er wordt bijvoorbeeld een interventie voorgesteld bij HSK. HSK is een landelijk opererende organisatie voor psychische zorg en is gespecialiseerd in werknemerszorg.

Het interventieadvies dient opgenomen te worden in het RIV dat in het kader van de Wet verbetering poortwachter moet worden aangelegd. Ook voortgangsmeldingen, tijd en duur van de trajecten en eindmeldingen dienen in het verslag te worden opgenomen. Het RIV heeft betrekking op een uniek individu, dus de aard van de interventie en het individu zijn te koppelen. We zien dat dit een logisch uitvloeisel is vanuit de Wet verbetering poortwachter en zich dus niet goed verhoudt met de AVG.

Nota interventie

Interventiedienstverleners sturen vervolgens een factuur naar de werkgever. De werkwijze is dat de casemanager werkgeversregievoerder/procesbewaker die de interventie coördineert, de interventiedienstverlener instrueert dat de naam van de persoon niet op de factuur mag komen en ook geen verdere persoonlijke gegevens worden vermeld. De persoon mag niet aan de interventie worden gekoppeld. Bij kleinere organisaties of deelfacturen per afdeling/businessunit is er echter

indirect vaak wel af te leiden op wie de interventie betrekking heeft. Aan de naam van de dienstverlener is in veel gevallen de aard van de ingezette interventie af te lezen.

Functionele Mogelijkheden Lijst (FML), Inzetbaarheidsprofiel (IZP), probleemanalyse

Uit de aangegeven beperkingen in de door de bedrijfsarts opgestelde FML, IZP en probleemanalyse valt voor de casemanager werkgeversregievoerder/procesbewaker de aard van de klachten ook af te leiden.

Terugkoppeling van beperkingen en daaruit voortvloeiende resterende mogelijkheden zijn essentieel voor het goed uitvoeren van de verzuimbegeleiding en re-integratieverplichtingen conform de Wet verbetering poortwachter. Ook hier botst de AVG met de uitvoeringskant van de Wet verbetering poortwachter. In de praktijk is dit niet te voorkomen, omdat de bedrijfsarts wel mag communiceren in termen van beperkingen.

Vraag 4

Toetsing van onderstaand standpunt door de Autoriteit Persoonsgegevens:

Vanuit het gerechtvaardigd belang van de Wet verbetering poortwachter is het een gegeven dat bij kleinere bedrijven de interventienota wat kan zeggen over de aard en oorzaak van het verzuim van de betrokkene. Ook het interventieadvies dat de bedrijfsarts geeft en de beperkingen die de bedrijfsarts duidt, kunnen indirect wat zeggen over de aard en oorzaak van het verzuim. Dat valt in de praktijk niet te voorkomen.

Bijlage 5: Toelichting op artikel 30 UAVG : verwerken van gezondheidsgegevens

Bij de WBP kenden we artikel 21 waarin geregeld was dat verzekeraars in bepaalde situaties wel gezondheidsgegevens mogen verwerken. Deze situaties liggen heel complex want ook binnen de AVG moet altijd eerst bekeken worden of de verwerking van het gezondheidsgegeven niet in strijd is met het medisch beroepsgeheim. Als dat niet zo is, dan volgt pas de toetsing van artikel 30 UAVG die vijf specifieke uitzonderingsgronden geeft wanneer de verwerking wel mogelijk is.

“het verbod om gezondheidsgegevens te verwerken is niet van toepassing op verzekeraars en financiële dienstverleners die bemiddelen in verzekeringen (definities art 1:1 Wft) voor zover de verwerking noodzakelijk is voor de beoordeling van het door de verzekeraar te verzekeren risico en de betrokkene geen bezwaar heeft gemaakt (sub 1); of de uitvoering van verzekeringsovereenkomst dan wel het assisteren bij het beheer en de uitvoering van de verzekering (sub 2).”

Uit de verwijzingen naar artikel 1:1 Wft volgt dat het in dit onderdeel uitsluitend gaat om herverzekeringen, levensverzekeringen, natura-uitvaartverzekeringen en schadeverzekeringen. Onderdeel b is ook op financiële dienstverleners van toepassing, die bemiddelen in verzekeringen als bedoeld in artikel 1:1 Wft (tussenpersonen). Onder ‘bemiddelen’ wordt in de Wft mede verstaan: het assisteren bij het beheer en de uitvoering van een verzekering.

- Sub 1 regelt de situatie waarin iemand een aanvraag invult voor het verkrijgen van een bepaalde verzekering en in dat kader gegevens omtrent gezondheid verstrekt. Deze gegevens zijn nodig ter beoordeling van het door de verzekeraar te verzekeren risico. De aspirant-verzekerde dient voorafgaand aan de afsluiting van de overeenkomst de gelegenheid te worden geboden om tegen een zodanige verwerking bezwaar te maken. Het aantekenen van bezwaar kan uiteraard tot gevolg hebben dat de verzekeraar afziet van het sluiten van de overeenkomst, indien naar zijn opvatting onvoldoende gegevens beschikbaar zijn om het risico adequaat te beoordelen.
- Sub 2 gaat over situaties die zich kunnen voordoen bij de uitvoering van de verzekeringsovereenkomst, waarbij verzekeraars gezondheidsgegevens verwerken. *Daarvoor regelt deze bepaling dat de verwerking van gegevens over gezondheid geoorloofd is, voor zover dat met het oog op dat doel noodzakelijk is.* Deze norm zal toepassing kunnen vinden gedurende de periode dat de overeenkomst wordt uitgevoerd. In sub 2 is ten opzichte van artikel 21 van de Wbp een redactionele verheldering toegevoegd, waardoor tot uitdrukking komt dat verwerking van gegevens betreffende de gezondheid ook noodzakelijk kan zijn bij het assisteren bij het beheer en de uitvoering van de verzekering (bemiddelen tussenpersoon Wft).

Alle verwerkingen van gezondheidsgegevens die plaatsvinden op basis van de uitzonderingen in de Uitvoeringswet, zijn gehouden aan een geheimhoudingsplicht. Ook waar dit niet voortvloeit uit andere wetten, waaraan de dienstverlener onderworpen is (lid 4) (thans artikel 21, tweede lid, van de Wbp).

Het zesde lid bepaalt dat omtrent de toepassing van het eerste lid en het derde lid, aanhef en onderdeel b, bij amvb nadere regels kunnen worden gesteld. De mogelijkheid hiertoe dient om te kunnen komen tot een precisering van de noodzakelijkheidseis met het oog op de verwerking van gezondheidsgegevens in de sociale zekerheid en verzekeringen.

Bijlage 6: Datalekken nader uitgeschreven

Beveiliging en Datalekken

Beveiliging art 32

De verantwoordelijke en verwerker moeten passende beveiligingsmaatregelen nemen. Er moet geanalyseerd worden of verwerking gepaard gaat met een hoog of laag risico. De Verordening kent een expliciete bepaling over het in werking hebben van een autorisatiestructuur, waarbij medewerkers alleen toegang mogen hebben tot de gegevens die zij in verband met hun functie daadwerkelijk nodig hebben.

Er moeten passende technische en organisatorische maatregelen worden genomen passend bij het risico die waar passend onder meer het volgende omvatten:

- Pseudonimisering en versleuteling van persoonlijke gegevens;
- De mogelijkheid om de integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- De mogelijkheid om beschikbaarheid van en toegang tot persoonsgegevens tijdig te herstellen;
- Een proces voor het regelmatig testen, beoordelen en evalueren van de doeltreffendheid van maatregelen ter beveiliging.

Hierbij kan een goedgekeurde gedragscode of goedgekeurd certificeringsmechanisme worden gebruikt om aan te tonen dat aan de vereisten van beveiliging wordt voldaan.

Concreet

- Er zal dus altijd gekeken worden naar wie wel/niet redelijkerwijs toegang dient te hebben;
- Processen zullen op orde moeten zijn en regelmatig geëvalueerd dienen te worden.

Datalekken art 33 en 34 AVG en 42 UAVG

De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde. De AVG stelt wel strengere eisen aan de registratie van de datalekken die zich hebben voorgedaan. Alle datalekken moeten gedocumenteerd worden. Met deze documentatie moet AP kunnen controleren of een organisatie aan de meldplicht heeft voldaan. Dit gaat verder dan de protocolplicht uit de Wet bescherming persoonsgegevens, die alleen betrekking heeft op de gemelde datalekken.

Niet alle datalekken hoeven gemeld te worden aan AP

Alle daadwerkelijke inbreuken in verband met persoonsgegevens moeten binnen 72 uur, nadat de verantwoordelijke zich hiervan bewust is geworden, worden gemeld aan de toezichthouder. Dit tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Dit gaat verder dan huidige meldingsplicht waarbij enkel ernstige inbreuken gemeld hoeven worden.

Van het 'er zich bewust van is geworden' is volgens WP 29 sprake als de verantwoordelijke een redelijke mate van zekerheid heeft dat een securitylek tot het aantasten van persoonsgegevens heeft geleid. Wanneer dat 'bewust worden' zich voordoet hangt af van de situatie. Er zal in ieder geval

prompt actie ondernomen moeten worden als er met redelijke mate van zekerheid sprake is van een lek. Als voorbeeld wordt genoemd het verlies van een cd met niet-geencrypte data. De wettelijke verplichting van de verwerker om de verantwoordelijke zonder vertraging in te lichten is dan ook bedoeld om ervoor te zorgen dat de verantwoordelijke aan zijn eventuele meldingsverplichtingen kan voldoen. Nadat verantwoordelijke met een potentiële personal data breach/datalek bekend is geworden, mag hij kort de tijd nemen om e.e.a. te onderzoeken: dit wordt nog niet aangemerkt als 'zich ervan bewust zijn geworden'. Dit zal over het algemeen wel snel afgehandeld moeten zijn. Een verantwoordelijke moet daarom ook een proces gereed hebben dat het mogelijk maakt een lek te ontdekken en te adresseren, waaronder het ook het in orde hebben van rapportagelijnen.

Als de verantwoordelijke een verwerker gebruikt, betekent dat ook dat zodra de verwerker met een redelijke mate van zekerheid bewust is van een personal data breach/datalek de verantwoordelijke geacht wordt ook met redelijke mate van zekerheid bewust te zijn van dit personal data breach/datalek. De verantwoordelijke blijft echter verantwoordelijk voor de melding. In het contract zal in ieder geval iets moeten worden opgenomen over de verplichtingen van de verwerker.

Drie types van lekken volgens WP 29

1. Vertrouwelijkheidslek: dit betekent dat er een ongeautoriseerde toegang of een niet bedoelde ontsluiting of toegang tot persoonsgegevens is;
2. Beschikbaarheidslek: het per ongeluk of ongeautoriseerd verliezen van de toegang tot of vernietiging van de persoonsgegevens;
3. Integriteitslek: dit betekent dat er ongeautoriseerde toegang is of per ongeluk persoonsgegevens worden gewijzigd.

Er kan sprake zijn van een combinatie van voornoemde lekken.

Datalek melding: Wat moet in de melding worden opgenomen?

- Aard van de inbreuk en waar mogelijk categorieën van betrokkenen en persoonsgegevensregisters en het aantal betrokkenen;
- Naam van de contactgegevens van de FG of een andere contactpersoon waar meer informatie kan worden verkregen;
- De waarschijnlijke gevolgen van de inbreuk;
- De maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk i.v.m. persoonsgegevens aan te pakken, waaronder de maatregelen om de nadelige gevolgen in te beperken.

Als niet alle informatie direct verstrekt kan worden, kan dat in stappen (dit evenwel zonder onredelijke vertraging).

Alle inbreuken, dus ook de niet-meldingsplichtige, moeten worden geadministreerd.

Als de inbreuk een *hoog risico* inhoudt voor de rechten en vrijheden van natuurlijke personen moet *de betrokkene onverwijld* geïnformeerd worden.

Categorieën van betrokkenen en persoonsgegevensregisters

De AVG/GDPR maakt niet duidelijk wat categorieën van betrokkenen en categorieën van persoonsgegevensregisters zijn:

- Categorieën van betrokkenen: Bij deze categorieën moet volgens WG 29 gedacht worden aan onder meer: klanten, medewerkers, kinderen, minder-validen, etc. Het gaat volgens WG 29 aldus om de type betrokkenen wiens data geraakt is;
- Categorieën van persoonsgegevensregisters: bij deze categorieën dient dan weer gedacht te worden aan de soorten van verwerkingen c.q. welke verwerkingen bij persoonsgegevens in geval van data breach/datalek betrokken zijn, zoals gezondheidsgegevens, opleidingen, financiële gegevens, bankgegevens, paspoortnummers, etc.

Doel van de datalek melding

Het doel is het beperken van schade voor individuen. Voornoemde categorieën van betrokkenen en categorieën van persoonsregisters geven een indicatie voor het risico op schade, zoals fraude, financieel verlies, etc. Dit is ook gelinkt aan de andere verplichting om te beschrijven wat de waarschijnlijke gevolgen van de data breach/datalek zijn.

Het aantal betrokkenen moet ook gemeld worden. Als dat onduidelijk is moet er toch tijdig gemeld worden. Er mogen volgens AVG/GDPR ook schattingen worden gemaakt over het aantal betrokkenen en ook over het aantal en de categorieën van persoonsgegevensregisters die betrokken zijn bij de personal data breach/datalek. Het adresseren van de negatieve consequenties is belangrijker dan de exacte getallen aldus de WP29. Dus als er een personal data breach/datalek is vastgesteld, dan is een melding belangrijker en kan desnoods de melding met nadere informatie worden aangevuld zodra er meer helderheid is over bijvoorbeeld de aantallen. Dat is de veilige manier om aan de verplichtingen te voldoen.

Let op: Artikel 34 – melding aan de betrokkene - van de verordening is niet van toepassing op financiële ondernemingen als bedoeld in de Wet op het financieel toezicht (Wft).

Aan betrokkene moet gemeld /verstrekkt worden:

- Omschrijving van de aard van de inbreuk (in heldere taal);
- Dezelfde gegevens die ook aan de toezichthouder gemeld zijn betreffende:
 - Naam van de FG of ander contactpersoon;
 - De waarschijnlijke gevolgen van de inbreuk;
 - De voorgestelde of genomen maatregelen om de inbreuk i.v.m. persoonsgegevens aan te pakken, waaronder de maatregelen die nodig zijn om de nadelige gevolgen in te beperken.

Melding kan achterwege blijven als:

- De verantwoordelijke beschermingsmaatregelen heeft genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk betrekking heeft, met name daar waar de gegevens onbegrijpelijk zijn voor onbevoegden bijvoorbeeld door versleuteling;
- De verantwoordelijke achteraf maatregelen heeft genomen om ervoor te zorgen dat de hoge risico's zich waarschijnlijk niet voordoen;

- De melding onevenredige inspanningen vergt van de verantwoordelijke. In dat geval kan een openbare mededeling of andere doeltreffende melding volstaan

Als de verantwoordelijke volgens de toezichthouder ten onrechte niet aan betrokkenen heeft gemeld, dan kan zij de verantwoordelijke hiertoe verplichten of beslissen dat een uitzonderingsgrond zich daadwerkelijk heeft voorgedaan.

Concreet

- Zorg voor een procedure waarbij alle inbreuken in verband met persoonsgegevens gemeld en geadministreerd worden;
- Beoordeel of er sprake is van een meldingsplichtige inbreuk en meld dat binnen 72 uur na de inbreuk aan de toezichthouder;
- Als er vertraging is in de melding, dus na 72 uur, dient er gemotiveerd te worden waarom er sprake is van een vertraging;
- Zorg voor volledige melding aan toezichthouder;
- Draag er zorg voor dat ook bewerkers zich aan de meldplicht houden en de verantwoordelijke tijdig informeren, zodat er gemeld kan worden. En leg dat vast in de overeenkomsten;
- Meld zo nodig aan de betrokkene en neem hierin dezelfde gegevens mee die ook aan de toezichthouder zijn gemeld betreffende:
 - Naam van de FG of ander contactpersoon;
 - De waarschijnlijke gevolgen van de inbreuk;
 - De voorgestelde of genomen maatregelen om de inbreuk i.v.m. persoonsgegevens aan te pakken, waaronder de maatregelen die nodig zijn om de nadelige gevolgen in te beperken.
- Omschrijving van de aard van de inbreuk (in heldere taal)

Bijlage 7: Rechten van betrokkene – artikelnummers AVG

Inzagerecht, correctie en gegevenswissing art 15, 16,17

De organisatie moet regelingen treffen, zodat de betrokkene hieronder genoemde rechten eenvoudig en gratis (m.u.v. het verstrekken van meerdere kopieën van het overzicht van persoonsgegevens ex art 15, want daar kan een redelijke vergoeding worden gevraagd), maar ook elektronisch kan uitoefenen. Er moet binnen een maand gereageerd worden en een weigering wordt met redenen omkleed. Daarnaast moet de identiteit van de betrokkene worden vastgesteld. De eisen van artikel 12 zijn van toepassing op communicatie met betrokkenen in dit verband. In rec. 59 wordt benadrukt dat "modaliteiten moeten worden geboden om de uitoefening van deze rechten van de betrokkene te vergemakkelijken" en dat de voor de verwerking verantwoordelijke "ook middelen moet bieden voor verzoeken om elektronisch te worden gedaan, met name wanneer persoonsgegevens elektronisch worden verwerkt".

Recht van inzage Artikel 15

Dit inzageverzoek is vergelijkbaar met de verzoeken op grond van artikel 35 Wbp. Voor deze inzageverzoeken is binnen de organisatie een procedure die beschreven staat in de werkinstructie inzageverzoeken. Op grond van artikel 15 zal daarnaast nog moeten voldaan aan de onderstaande punten:

- Onder schriftelijk wordt eveneens verstaan elektronisch. Als het gaat om een elektronisch verzoek, dan wordt deze in elektronische vorm door de organisatie verstrekt, tenzij de betrokken anders verzoekt;
- Als de organisatie een grote hoeveelheid gegevens van de betrokkene verwerkt, mag gevraagd worden het verzoek te preciseren of op welke verwerkingsactiviteit dit verzoek betrekking heeft. Als de organisatie slechts weinig gegevens heeft (bijvoorbeeld alleen NAW-gegevens) dan mag dat niet;
- Indien mogelijk moet de organisatie toegang geven tot een beveiligd systeem, waarop de betrokkene zijn persoonsgegevens kan inzien;
- De organisatie moet ervoor zorgen dat binnen 1 maand na ontvangst van het inzageverzoek de betrokkene de gevraagde inzage heeft gekregen. Let op: Bij afwijzing van een verzoek om inzage zal binnen een maand na het verzoek geantwoord moeten worden, met daarbij de mededeling dat een klacht ingediend mag worden bij de toezichthouder en beroep bij de rechter ingesteld kan worden;
- De betrokkene moet het volgende ontvangen:
 - Een overzicht van de persoonsgegevens;
 - De verwerkingsdoeleinden;
 - De betrokken categorieën van persoonsgegevens;
 - De ontvangers die de persoonsgegevens zullen ontvangen. Dit geldt met name als er sprake is van doorgifte aan ontvangers in derde landen of internationale organisaties (als sprake is van een doorgifte aan derde landen of internationale organisaties dan moeten ook de passende waarborgen ex artikel 46 gemeld worden);

- De periode gedurende welke de persoonsgegevens zullen worden opgeslagen (hiervoor kan aangesloten worden bij het beleid inzake bewaartermijnen van de organisatie);
- Het recht van bezwaar/rectificatie/wissen/beperken van de gegevensverwerking van de betrokkene (zie ook hieronder);
- Het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens.

En eventueel (indien van toepassing):

- De bron van de gegevens (wanneer deze gegevens niet bij de organisatie zijn verzameld);
- Het bestaan van geautomatiseerde besluitvorming (ook m.b.t. profilering, zie hierna, artikel 22) inclusief informatie over de onderliggende logica, het belang en de gevolgen voor betrokkene. Denk daarbij bijvoorbeeld aan de aanvraagstraten of Kameda (online gezondheidsverklaring).

In rec. 63 staat dat de verwerkingsverantwoordelijke, indien mogelijk, op afstand toegang kan geven tot een beveiligd systeem, waarop de betrokkene direct zijn persoonsgegevens kan inzien. Dit kan bijvoorbeeld via een klantportaal. Dat zal tevens leiden tot minder inzageverzoeken.

Recht op rectificatie Artikel 16

De betrokkene kan aanpassing van onjuiste gegevens vragen. Aan dit verzoek moet direct worden voldaan. Ook kan hij verzoeken de persoonsgegevens aan te vullen door middel van een aanvullende verklaring. Uiteraard alleen voor zover nodig in verband met de doeleinden van de verwerking. Dit artikel heeft impact voor heel de organisatie voor wat betreft alle systemen waarin persoonsgegevens worden verwerkt.

Recht op vergetelheid (gegevenswissing) Artikel 17

Een organisatie moet op verzoek van de betrokkene zo spoedig mogelijk de persoonsgegevens wissen, mits:

- De gegevens niet langer nodig zijn voor de doeleinden waarvoor ze zijn verkregen;
- De betrokkene zijn eerder gegeven toestemming om de (bijzondere) persoonsgegevens te verwerken intrekt en er geen andere grond is waarvoor de gegevens nodig zijn;
- De betrokkene bezwaar maakt tegen de verwerking op grond van artikel 21 en er geen dwingende gerechtvaardigde grond is waarop die gegevens worden verwerkt;
- De gegevens onrechtmatig worden verwerkt;
- De gegevens moeten worden gewist op grond van een wettelijk plicht;
- De gegevens zijn verzameld in verband met een aanbod van de informatiemaatschappij (dit geldt alleen voor kinderen die van een dergelijk aanbod gebruik hebben gemaakt).

Als het gaat om gegevens die openbaar zijn gemaakt, moet deze verantwoordelijke redelijke maatregelen nemen om ook andere verwerkers van het wissen in kennis te stellen.

Het wissen hoeft niet indien de gegevens nodig zijn voor:

- Het uitoefenen van het recht op vrijheid van meningsuiting en informatie;
- Nakoming van een wettelijke plicht of het vervullen van een taak van algemeen belang of het uitoefenen van openbaar gezag;

- Algemeen belang op het gebied van volksgezondheid (waarbij wordt verwezen naar artikel 9, lid 2 onder h en i en lid 3;
- Archivering, wetenschappelijk, historisch onderzoek of statistisch doeleinden (met een verwijzing naar artikel 89 lid 1) en het wissen dat onmogelijk maakt;
- Het instellen, uitoefenen of onderbouwen van een rechtsvordering.

Recht op beperking van de verwerking Artikel 18

Onder omstandigheden kan de betrokkene de wens uiten de verwerking van zijn of haar persoonsgegevens te beperken. Er kunnen dan wel persoonsgegevens worden verwerkt, maar niet op de integrale wijze die de verantwoordelijke voor ogen staat. Dit recht bestaat in een aantal limitatief in de verordening aangeduide situaties. Na bijvoorbeeld een inzageverzoek kan de betrokkene de mening toegedaan zijn dat de persoonlijke data niet correct zijn. Het is dan aan de verantwoordelijke om gedurende een redelijke termijn te controleren of de persoonsgegevens inderdaad niet correct zijn. Ook kan een betrokkene constateren dat op onrechtmatige wijze gegevens zijn verwerkt. In beginsel dienen dergelijke gegevens verwijderd te worden, maar de betrokkene kan ook aangeven dat deze niet gewist worden, maar uitsluitend voor een specifiek gebruik kunnen worden toegepast.

Een verantwoordelijke dient de persoonsgegevens niet langer te bewaren dan noodzakelijk is. Het kan daarom voorkomen dat gegevens niet meer gebruikt worden en de verantwoordelijke deze voornemens is te verwijderen. De betrokkene heeft dan het recht de data toch bewaard te laten. Deze kunnen dan gebruikt worden voor de instelling, onderbouwing of uitoefening van een rechtsvordering. Ook in de situatie dat een betrokkene bezwaar heeft gemaakt tegen de verwerking van zijn persoonsgegevens, maar de verantwoordelijke meent een zwaarder wegend belang te hebben bij verwerking dan de betrokkene heeft bij verwijdering. Het gebruik van persoonlijke data dient in een dergelijke situatie wel te worden beperkt.

Wanneer een van bovenstaande situaties zich voordoet is het gebruik van persoonlijke data dus aan banden gelegd. Het bewaren van de persoonsgegevens vindt plaats zonder verdere complicaties, maar de verdere verwerking kan alleen plaatsvinden indien de betrokkene daar expliciet mee akkoord gaat. Een uitzondering daarop is de situatie waarin het algemeen belang van de Unie of de lidstaat, of de situatie waarin sprake is van een rechtsvordering of de bescherming van de rechten van een andere natuurlijk persoon of rechtspersoon. Hierbij wordt niet aangeduid door wie die rechtsvordering kan worden uitgeoefend en hoe breed de kring van derden is waarvan de rechten worden beschermd.

Een beperking zoals verwoord in dit artikel hoeft niet onbeperkt van kracht te blijven. Het kan zijn dat deze aan een termijn wordt verbonden. Ook kan de beperking aflopen in geval een ingesteld onderzoek door de verantwoordelijke is afgerond. In dat geval wordt de voorwaarde gesteld dat de betrokkene alvorens de beperking wordt opgeheven wordt geïnformeerd.

Nog even in het kort: een organisatie moet het gebruik van data bevriezen wanneer:

- De juistheid van de gegevens worden betwist door de betrokkene voor de duur dat de juistheid wordt gecontroleerd;

- De verwerking onrechtmatig is en de betrokkene zich tegen wissen verzet;
- De organisatie de gegevens niet meer nodig heeft maar betrokkene wel de gegevens nodig heeft om bijvoorbeeld een rechtsvordering te kunnen onderbouwen;
- Betrokkene bezwaar maakt en in afwachting is van de onderbouwing van de organisatie of hun belangen zwaarder wegen.

Concreet:

- Let op: Ga na of de bedrijfsvoering dit kan;
- Let op: Houd er rekening mee dat iedere andere ontvanger, aan wie persoonsgegevens zijn verstrekt, in kennis gesteld moet worden van de rectificatie, wissing van gegevens of beperking van de verwerking.

In artikel 19 wordt bepaald dat de verantwoordelijke verplicht is om elke ontvanger van persoonsgegevens in kennis te stellen van elke rectificatie, het wissen of de beperking van de betreffende gegevensverwerking. De betrokkene kan de verwerker vragen om welke ontvangers van persoonsgegevens het gaat. Wanneer het verstrekken van de gewenste informatie niet meer mogelijk is of onevenredig veel inspanning kost, dan hoeft dit niet te worden gedaan.

Recht om data door te geven Artikel 20

Dit artikel gaat over het recht op dataportabiliteit, het recht van een betrokkene om de persoonsgegevens, die ze aan de verantwoordelijke hebben verstrekt, in een gestructureerd, gangbaar en machineleesbaar formaat te kunnen ontvangen, zodat deze aan een andere verantwoordelijke kunnen worden overgedragen. Een betrokkene krijgt hiermee het recht om een subset van zijn persoonsgegevens te verkrijgen. Hierdoor kan een betrokkene indien gewenst, zijn of haar gegevens eenvoudig van de ene naar de andere IT-omgeving verplaatsen, kopiëren of doorsturen. Ook kan een betrokkene verzoeken de gegevens rechtstreeks door te sturen naar de andere verantwoordelijke. Het wisselen van dienstverlener wordt hierdoor gemakkelijker en een betrokkene kan de gegevens zo ook bewaren voor later gebruik. Te denken valt aan een profiel op social media, een afspeellijst van een streamingdienst, een overzicht van bestellingen of een klantaccount bij een dienstverlener.

Het invoeren van dit recht kan als aan onderstaande voorwaarden wordt voldaan.

1. Het moet allereerst gaan om persoonsgegevens van de betrokkene zelf. Het betreft data die met de grondslag 'consent van betrokkene' digitaal is verwerkt of in het kader van de uitvoering van de overeenkomst. Deze data zijn door betrokkene zelf verstrekt. Het begrip verstrekken moet daarbij ruim worden uitgelegd. Ook gegevens die uit de activiteiten van een betrokkene kunnen worden opgesteld, worden beschouwd als verstrekt door de betrokkene zelf.
2. Bij de uitoefening van het recht op dataportabiliteit ten behoeve van betrokkene mogen de rechten van derden niet worden aangetast. Wanneer door het uitoefenen van het recht op directe doorzending de rechten van derden in het gedrang dreigen te komen, dan dienen deze te prevaleren boven de rechten van de betrokkene. Gegevens van derden mogen door een ontvangende verantwoordelijke ook niet gebruikt worden voor eigen doeleinden. Zo is

het niet toegelaten de gegevens te gebruiken voor marketingactiviteiten of het aanvullen van een reeds aanwezig profiel van de derde.

Bedacht moet worden dat deze voorwaarden niet gelden indien de gegevens zijn verkregen in het kader van het algemeen belang of de uitoefening van het openbaar gezag. Het is dan aan de verantwoordelijke zelf te bepalen op welke wijze invulling aan het verzoek wordt gegeven. Indien de betrokkene tegemoet wordt gekomen in een dergelijk verzoek, vindt dat onverplicht plaats.

In geval van een verzoek tot overdracht van data is de overdragende partij verantwoordelijk voor het eigen handelen, maar niet voor de wijze waarop deze data door de ontvangende partij verder wordt verwerkt. Deze partij draagt op haar beurt de verantwoordelijkheid dat de ontvangen data en de verwerking daarvan niet bovenmatig is en plaats vindt binnen de reikwijdte van het bepaalde in de AVG. Het inwilligen van een verzoek om data over te dragen betekent niet dat de overdragende partij ook tot verwijdering van de data uit de eigen systemen over dient te gaan.

Een betrokkene kan onder omstandigheden eisen stellen aan de wijze waarop de data aan hem wordt aangeleverd. De verantwoordelijke kan er niet mee volstaan een pak papier te overhandigen. De gegevens zullen op geordende wijze worden aangeleverd en het uitgangspunt is dat deze digitaal worden verstrekt. Dit kan op elektronische wijze plaatsvinden, maar denkbaar is ook dat de data wordt opgeslagen op een elektronische gegevensdrager, zoals bijvoorbeeld een USB-stick, en zo aan de betrokkene ter hand wordt gesteld. De data moeten bovendien gestructureerd worden aangeleverd zodat deze door betrokkene makkelijk doorzoekbaar is en op redelijk eenvoudige wijze kan worden getoetst of de informatie compleet is.

Deze vereisten gaan echter niet onder alle omstandigheden op. In het kort zijn de vormvereisten van toepassing voor verwerking van persoonsgegevens waarvoor expliciet instemming is verleend. Bovendien gaat het dan om data die op geautomatiseerde wijze zijn verwerkt. Het is als verantwoordelijke aan te raden een mogelijkheid te construeren waarmee een betrokkene op eenvoudige wijze persoonlijke data kan downloaden teneinde deze data naar een andere digitale omgeving over te zetten. Een andere mogelijkheid is om dergelijke data op te slaan in een beveiligde omgeving waar de betrokkene deze data vervolgens op kan halen. De partij die de data als nieuwe verantwoordelijke ontvangt, zal op haar beurt moeten nagaan in hoeverre de ontvangen gegevens relevant en niet buitensporig zijn. De gegevens die niet aan dit criterium voldoen mogen niet bewaard worden.

Een betrokkene waarvan gegevens zijn verwerkt kan deze ook direct door laten sturen van de ene verantwoordelijke naar de andere verantwoordelijke. Dit moet wel technisch mogelijk zijn. Dus wanneer bepaalde systemen niet op elkaar aansluiten kan dit verzoek afgewezen worden. In dat geval zal de betrokkene zelf voor de overdracht zorg moeten dragen. Een overstap van Facebook naar Instagram zou zo vergemakkelijkt moeten worden.

Het is denkbaar dat een overstap van de ene naar de andere verzekeraar op restricties stuit nu systemen verschillend zijn opgebouwd en daardoor niet op elkaar aansluiten. Van verantwoordelijken wordt echter wel verwacht dat zij de data in een interoperabel formaat

verzenden, zodat de kans wordt gemaximaliseerd dat deze ook door de ontvangende verantwoordelijke kunnen worden verwerkt. Het gegevensformaat moet gestructureerd, gangbaar en machineleesbaar zijn. Daarbij geldt nog dat aandacht moet worden besteed aan de beveiliging van de gegevens. De verantwoordelijke dient maatregelen te nemen om te zorgen voor een veilige overdracht van de data, bijvoorbeeld door codering van de gegevens.

Een verantwoordelijke heeft de verplichting om betrokken op het recht op dataportabiliteit te attenderen. Informatie moet in beknopte en begrijpelijke vorm worden aangeboden. Deze verplichting zit niet alleen op de verantwoordelijke die de gegevens heeft verwerkt, maar ook op een eventuele ontvangende verantwoordelijke.

Door een betrokkene moet op zo kort mogelijke termijn en in ieder geval binnen een maand aan het verzoek tot dataportabiliteit worden voldaan. In complexe gevallen kan deze termijn echter tot drie maanden worden opgerekt. Daarbij wordt wel van de verantwoordelijke verwacht dat deze de betrokkene informeert over de termijn waarop aan het verzoek gehoor wordt gegeven. In de situatie dat het verzoek niet wordt ingewilligd, zal de betrokkene daar binnen een termijn van een maand bericht over moeten ontvangen. Deze afwijzing moet door de verantwoordelijke onderbouwd worden en de betrokkene wordt daarbij geïnformeerd over de mogelijkheid een klacht bij de toezichthouder in te dienen of een gerechtelijke procedure te starten.

Concreet:

- Onderzoeken in hoeverre dataportabiliteit kan worden afgedwongen en of hier een format voor moet worden ontwikkeld.

Recht van bezwaar Artikel 21

Er zijn 3 rechten op bezwaar voor betrokkenen bij verwerking :

- Direct marketing;
- Wetenschappelijke, historische en statistische doeleinden;
- Verwerking is nodig ter vervulling van een taak van algemeen belang of in het kader van de uitoefening van het openbaar gezag dat aan de organisatie is verleend; of op grond van gerechtvaardigd belang van de organisatie of een derde; ook indien profilering daarop gestoeld is.

De organisatie moet stoppen met de verwerking, tenzij de organisatie dwingende gerechtvaardigde gronden kan aanvoeren die zwaarder wegen dan de belangen van klanten zoals t.b.v. fraudebestrijding of die verband houden met een eventuele rechtsvordering. Dus de organisatie moet dit nu aantonen, daar waar in de Wbp de betrokkene dit moest doen.

Direct marketing

Dit is een absoluut recht en mag altijd en kosteloos. De organisatie toont op het moment van het eerste contact met de betrokkene het recht om bezwaar te maken. Dit moet uitdrukkelijk onder de aandacht worden gebracht, duidelijk en gescheiden van enig andere informatie. Dit kan via de website.

Indien de betrokkene bezwaar maakt t.b.v. direct marketing/profilering, dan stopt de organisatie met deze verwerking (geen reclame/aanbiedingen meer sturen).

Let op: Direct Marketing kent geen definitie. De grondslag is een gerechtvaardigd belang, die overigens wel aan betrokkenen medegedeeld moet worden met het recht van verzet. Het gaat dan wel over de normale bedrijfsvoering, proportioneel en ter zake dienend.

Let op: Voor e-marketing zijn er strengere regels bij e-mail en sms, cookies.

Wetenschappelijke, historische en statistische doeleinden

Betrokkene moet bezwaar kunnen maken tegen verwerking die betrekking heeft op zijn specifieke situatie.

Algemeen belang

Bezwaar hoeft de organisatie niet te respecteren indien de verwerking noodzakelijk is voor de uitvoering van een taak van algemeen belang.

Bijlage 8: Toelichting derden – bewerkers/verwerkers

Derden- partijen

Bewerkers art 3 (1), 28-30, 30-33, 44

De Verordening is met bepaalde verplichtingen DIRECT van toepassing op verwerkers (processors)! Dit is anders dan de Wbp. Het is raadzaam om alleen samen te werken met bewerkers die voldoende garanties bieden m.b.t. technische en organisatorische maatregelen, om te kunnen voldoen aan de AVG.

Een verwerker mag geen subverwerker nemen, anders dan alleen met specifieke of algemene schriftelijke toestemming van de verantwoordelijke (verzekeraar/gevolmachtigd agent). Algemene toestemming kan, indien de verwerker de verantwoordelijke inlicht over veranderingen en dat de verantwoordelijke de mogelijkheid heeft bezwaar te maken. De verwerker zet dezelfde schriftelijke bepalingen door en zorgt ervoor dat deze andere verwerker voldoende garanties in maatregelen biedt om de gegevens te beschermen. Als de andere verwerker hier niet aan voldoet, is de verwerker volledig aansprakelijk voor het niet nakomen van de andere verwerker.

Indien de verwerker zelf doeleinden en middelen van verwerking bepaalt, wordt deze verwerker beschouwd als verantwoordelijke!

De verantwoordelijke organisatie moet de verwerkers registreren.

T.a.v. aansprakelijkheid verantwoordelijke en bewerk:

- Een klant/betrokkene kan zowel de verzekeraar als een verwerker aansprakelijk stellen;
- De verzekeraar/gevolmachtigd agent is aansprakelijk voor schade als gevolg van een inbreuk op de verordening;
- Een verwerker is aansprakelijk voor schade die door de verwerking is veroorzaakt, wanneer niet is voldaan aan de bepalingen uit de AVG die op verwerkers zijn gericht én wanneer is strijd is gehandeld met de instructies van de verantwoordelijke;
- Verwerkers kunnen ook direct boetes opgelegd krijgen indien de specifieke bepalingen art 28 AVG niet worden nageleefd (denk aan: geen subprocessor zonder toestemming);
- Verantwoordelijke en verwerker zijn niet aansprakelijk, indien aangetoond kan worden dat zij niet verantwoordelijk zijn voor het schadeveroorzakende feit;
- Betrokkene moet alle schade vergoed krijgen; partijen kunnen op elkaar verhalen.

Let wel: AP heeft de bevoegdheid tot het doen van onderzoek, ook bij verwerkers (art 58) en kan toegang krijgen tot ruimtes en persoonsgegevens én kan ook de bewerk waarschuwen bij inbreuk op de bepalingen van de AVG, kan berispen, gelasten de verwerkingen compliant te brengen met de AVG, verwerkingsbeperking ofwel verbod opleggen, boete opleggen conform art 83.

Een verwerker moet voldoen aan (art 30):

- Registratie bijhouden van alle verwerkingen die zij ten behoeve van een verantwoordelijke doet;
- Meewerken met toezichthouder;
- Voldoende passende technische en organisatorische beveiligingsmaatregelen treffen;
- Direct de organisatie informeren indien er een datalek is;
- De regels van cross-border doorgiftes.

Verwerkersovereenkomst

Verantwoordelijke organisaties hebben een schriftelijke overeenkomst nodig. Daarin moet ten minste staan dat verwerker:

- Alleen op instructies en in opdracht van de verantwoordelijke data verwerkt;
- De geheimhouding waarborgt van zijn medewerkers;
- De noodzakelijke beveiligingsmaatregelen neemt;
- Alleen een subverwerker met toestemming mag nemen;
- Assisteert bij het compliant kunnen zijn aan de wet.

Zo ook bij rechten klanten:

- Alle informatie ter beschikking stelt die nodig is om aan te kunnen tonen dat de verantwoordelijke voldoet aan de verplichtingen en audits mogelijk maakt en eraan bijdraagt;
- De verantwoordelijke onmiddellijk in kennis stelt indien een instructie inbreuk van de wet oplevert.

Co-controllers

Als er zaken worden gedaan met een co-controller, dan moeten daar ook afspraken mee worden gemaakt.

Concreet

- Bekijk of er sprake is van een co-controller situatie, en zo ja sluit daar een contract mee af;
- Inventariseer alle bewerkersovereenkomsten en ga na of ze voldoen aan de verordening;
- Registreer alle verwerkers.

Bijlage 9: Verwerkingsverplichtingen

Verwerkingsverplichtingen

Iedere verwerking van persoonsgegevens moet een grondslag hebben. Dit is niet anders dan onder de Wbp. Maar de voorwaarden zijn zwaarder geworden.

Hieronder de verplichtingen.

De grondslagen zijn (6(1)(a-f):

- a) Uitvoering van een (voorgenomen) overeenkomst;
- b) Te voldoen aan een wettelijke plicht die op de organisatie rust;
- c) Bescherming vitale belang individu;
- d) Vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van een openbaar gezag dat aan de organisatie is opgedragen;
- e) De behartiging van de gerechtvaardigde belangen van de organisatie of van een derde, behalve wanneer de belangen of grondrechten van de betrokkenen die tot bescherming van de persoonsgegevens nopen, zwaarder wegen dan die belangen;
- f) Toestemming betrokkenen voor de verwerking voor een specifiek doeleinde.

Ad c: Dit hoeft niet een expliciete wettelijke plicht te zijn, maar kan ook een zorgplicht zijn.

Ad e: Gerechtvaardigd belang: dit kan, mits de belangen van de persoon niet zwaarder wegen én rekening gehouden wordt met de redelijke verwachtingen van de persoon. Die verwachting moet er zijn bij het aangaan van de dienst en verzameling van gegevens. De balanstoets moet gedaan worden.

Fraudevoorkoming is een gerechtvaardigd belang en conservatieve direct marketing ook. Evengoed het doorzenden van gegevens binnen een concern voor interne administratieve doeleinden waaronder van klanten en werknemers. De derdenland-regels blijven wel gelden.

Verenigbaar gebruik (art 6 lid 4; beginsel van doelbinding):

De persoonsgegevens mogen alleen voor een ander doel dan het oorspronkelijke doel gebruikt worden als het verenigbaar gebruik is. De organisatie moet dan bij het bepalen of er sprake is van verenigbaar gebruik rekening houden met:

- Het verband tussen de doeleinden;
- Het kader waarin de gegevens zijn verzameld en de verhouding tussen betrokkenen en de organisatie;
- De aard van de gegevens, met name bijzondere gegevens;
- De gevolgen van de verdere verwerking en het bestaan van passende maatregelen waaronder versleuteling en pseudonimisering.

Als er sprake is van verenigbaar gebruik, dan behoeft er geen afzonderlijke rechtsgrond gevonden te worden dan die op grond waarvan de verzameling werd toegestaan. Dit kan sowieso niet indien toestemming is gegeven voor het oorspronkelijke doel. Dan is opnieuw toestemming nodig.

Archivering voor wetenschappelijke en historisch onderzoek en statistische doeleinden horen hierbij.

Is de verdere verwerking NIET verenigbaar, dan moet toestemming gevraagd worden. De toestemming moet wel expliciet en vrijelijk gegeven zijn. Dus verwerking kan dan wel plaatsvinden. Let op: Het kan ook gaan om verstrekking aan een andere verantwoordelijke, die uiteraard wel een grondslag moet hebben voor de verwerking.

Verwerkingsprincipes art 5:

Organisaties moeten hier aantoonbaar aan voldoen en persoonsgegevens moeten:

- Rechtmatig, behoorlijk en transparant verwerkt worden;
- Doelbinding: Voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en mogen niet verder verwerkt worden op een met die doeleinden onverenigbare wijze worden verwerkt;
- Minimale gegevensverwerking: Toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden;
- Juistheid: Juist zijn en zo nodig geactualiseerd. Maatregelen moeten getroffen worden om gegevens die onjuist zijn onverwijld te wissen of te rectificeren;
- Opslagbeperking: Bewaren in een vorm die mogelijk maakt personen niet langer te identificeren zijn, dan voor de doeleinden waarvoor de gegevens worden verwerkt noodzakelijk is;
- Integriteit en vertrouwelijkheid: Passende technische en organisatorische maatregelen, zodat een passende beveiliging gewaarborgd is en dat zij tegen ongeoorloofde of onrechtmatige verwerking beschermd zijn en tegen onopzettelijk verlies, vernietiging of beschadiging.

Deze beginselen zijn complementair.

Verdere verwerking

Het beginsel van doelbinding is niet absoluut. Persoonsgegevens mogen gebruikt worden voor een ander doel, mits dat gebeurt op een wijze die niet onverenigbaar is met de doeleinden waarvoor de gegevens oorspronkelijk zijn verzameld. Zie hierboven.

Transparantie is op zich nieuw ten opzichte van de Wbp en komt tot uitdrukking bij de rechten van betrokkenen en bij de informatieverplichtingen.

Toestemming inrichten en intrekking ervan (art 7 en 8, ro 42. 43, 50):

Een van de grondslagen voor de verwerking van persoonsgegevens is gegeven toestemming door de betrokkene. De verwerkingsverantwoordelijke dient aan te kunnen tonen dat een betrokkene die instemming heeft verleend. Het is daarbij van belang dat de toestemming op de juiste wijze wordt verkregen. De betrokkene dient zich bewust te zijn van hetgeen waarvoor toestemming wordt verleend en de toestemming moet uitdrukkelijk worden gegeven. Ook moet de instemming worden verleend, voordat aangevangen wordt met de verwerking van de persoonlijke data.

Aangezien toestemming expliciet moet worden gegeven, wordt een actieve handeling van de betrokkene gevraagd. Impliciete toestemming kan niet worden aangenomen. Op een later moment zal de verwerkingsverantwoordelijke ook moeten kunnen reproduceren dat daadwerkelijk is ingestemd met de verwerking van de persoonsgegevens. Dit maakt dat een

verwerkingsverantwoordelijke dient te borgen dat het archief zodanig is ingericht dat een gegeven toestemming wordt bewaard en op ieder gewenst moment getoond kan worden. Ook moet dan blijken waarvoor de toestemming is gegeven.

Van belang is voorts dat instemming vrij wordt gegeven en er geen schijn bestaat dat betrokkene zich op enigerlei wijze gedwongen heeft gevoeld om akkoord te gaan met de verwerking van zijn of haar gegevens. Een akkoord dat niet vrij is verkregen, kan niet als een daadwerkelijke instemming worden aangemerkt.

Toestemming kan op diverse manier worden verkregen. Zo kan gevraagd worden om een 'natte handtekening', maar ook kan worden gekozen voor het zetten van een vinkje of het vragen van een mondelinge bevestiging. Bij het verkrijgen van de toestemming is het noodzakelijk dat de betrokkene begrijpt en beseft waarvoor instemming wordt verleend. Er zal duidelijk moeten worden aangegeven waarvoor betrokkene nu daadwerkelijk toestemming verleend. Een instemming die verkregen wordt via het accepteren van algemene voorwaarden voldoet niet aan de vereisten en wordt niet gekwalificeerd als een geïnformeerde en vrijelijk verkregen instemming. Ook voldoet niet de situatie waarin instemming alleen voor een 'volledig pakket' moet worden verstrekt, terwijl het ook mogelijk is om voor verschillende doelen afzonderlijk instemming te verzoeken. Ook zal opnieuw om een akkoord verzocht moeten worden als de verantwoordelijke reeds verkregen data voor een nieuw doel wenst te gebruiken.

Een eis wordt gesteld aan duidelijk taalgebruik. Naast de begrijpelijkheid is de laagdrempeligheid een vereiste. Gezien de verdergaande digitalisering van processen ligt het vooral voor de hand dat instemming digitaal wordt verkregen. De persoon kan, indien hij instemt met gegevensverwerking, een vinkje plaatsen. De vraag is dan hoe ver de informatieplicht van de verwerker reikt. Kan worden volstaan met een vraag waarbij de toelichting achter een icoontje wordt geplaatst? Voor de gemiddelde computergebruiker zal dit als voldoende toegankelijk worden beschouwd. Een aantal elementen moeten voorts gebruikt worden, zodat betrokkene voldoende informatie heeft om een afgewogen beslissing te nemen. Denk daarbij aan de identiteit van de verantwoordelijke, het doel van de verwerking, welke data wordt verwerkt, de mogelijkheid instemming in te trekken en informatie in hoeverre de data wordt gebruikt voor automatische verwerking.

Op een even eenvoudige manier waarop instemming kan worden gegeven, kan de betrokkene deze instemming ook weer intrekken. Aan het intrekken van instemming mogen geen kosten verbonden zijn en er mogen geen negatieve consequenties aan verbonden worden. Hierbij is het niet noodzakelijk dat de intrekking via exact dezelfde procedure plaatsvindt als de verstrekking van de toestemming. Een digitaal verkregen instemming kan ook op telefonische, schriftelijke, etc. wijze worden ingetrokken. Uitgangspunt is dat dit voor de persoon laagdrempelig is.

Indien instemming digitaal is verkregen, ligt het wel voor de hand dat betrokkene deze ook weer digitaal kan intrekken, omdat anders onnodige inspanning van betrokkene wordt geleverd. Indien de toestemming wordt ingetrokken, is de data die na de verstrekte instemming is verkregen wel rechtmatig verkregen, maar zal het verwerken van de data direct gestopt moeten worden. Zodra het

houden van de data niet meer noodzakelijk is, doordat er geen enkele grondslag voor verwerking meer is, zal de verantwoordelijke deze alsnog moeten verwijderen.

Voor zover het gaat om het uitvoeren van een overeenkomst is geen afzonderlijke toestemming van de betrokkene vereist om zijn of haar gegevens te verwerken. Wanneer echter werkzaamheden worden verricht buiten de reikwijdte van de overeenkomst, en hiervoor gegevens worden verwerkt, is het wel noodzakelijk om toestemming van de betrokkene te verkrijgen, tenzij er een gerechtvaardigd belang is of een wettelijke plicht. Het is daarom zaak alert te zijn welke activiteiten in het kader van een met een betrokkene gesloten overeenkomst noodzakelijk zijn. Hiervoor is immers geen instemming vereist. Bij het verwerken van gegevens buiten de overeenkomst, waarvoor dus instemming moet worden verkregen, is het van belang de persoon in kwestie duidelijk te informeren, zodat begrepen wordt waarvoor instemming wordt gevraagd. Ook zal bij de informatie van het doel aangegeven moeten worden hoe de toestemming weer ingetrokken kan worden.

Concreet:

- Iedere verwerking van persoonsgegevens moet een geldige grondslag hebben: Breng per verwerking in kaart wat de grondslag is en leg dit vast in het register van verwerkingen. Leg ook vast of er sprake is van verenigbaar gebruik. Indien er geen grondslag is, moet overwogen worden of toestemming gevraagd kan worden, dan wel dat de verwerking stopgezet moet worden (NB. toestemming kan ook ingetrokken worden, waardoor de verwerkingsgrondslag weer verdwijnt. Toestemming als enige grondslag is niet echt een stabiele basis);
- Bekijk bij iedere verwerking of de gegevens verwerkt worden conform:
 - Rechtmatigheid, behoorlijkheid en transparantie;
 - Doelbinding;
 - Minimale gegevensverwerking;
 - Juistheid;
 - Opslagbeperking;
 - Passende beveiligingsmaatregelen;
 - Review procedures toestemming en intrekking;
 - Bewaartermijn bepalen en implementeren;
 - Passende beveiligingsmaatregelen: ga na of er ergens aanpassingen moeten worden gedaan.

Bijlage 10. Criteria of uw organisatie een DPIA moet uitvoeren

Als vuistregel om een DPIA uit te voeren kan worden aangehouden dat de verwerking aan twee of meer van de onderstaande criteria voldoet:

1. Het beoordelen van mensen op basis van persoonskenmerken

Het gaat hierbij onder meer om profiling en het maken van prognoses, met name op basis van kenmerken als iemands beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen. Bijvoorbeeld een bank die de kredietwaardigheid van klanten beoordeelt of een bedrijf dat bezoekers van zijn website volgt en op basis daarvan profielen van deze mensen opstelt.

2. Geautomatiseerde beslissingen

Het gaat hierbij om beslissingen die voor de betrokkene rechtsgevolgen of vergelijkbare wezenlijke gevolgen hebben. Zo'n gegevensverwerking kan er bijvoorbeeld toe leiden dat mensen worden uitgesloten of gediscrimineerd. Gegevensverwerkingen met geringe of geen gevolgen voor mensen, vallen niet onder dit criterium. Er komen nog guidelines met meer uitleg.

3. Stelselmatige en grootschalige monitoring

Het gaat hierbij om monitoring van openbaar toegankelijke ruimtes, bijvoorbeeld met cameratoezicht. Hierbij kunnen persoonsgegevens worden verzameld, zonder dat de betrokkenen weten wie hun gegevens verzamelt en wat daar vervolgens mee gebeurt.

4. Gevoelige gegevens

Het gaat hierbij om bijzondere categorieën van persoonsgegevens (zie artikel 9 van de AVG), zoals informatie over iemands politieke voorkeuren of strafrechtelijke gegevens. Ook gaat het om gegevens die over het algemeen als privacygevoelig worden beschouwd, zoals gegevens over elektronische communicatie, locatiegegevens en financiële gegevens.

5. Grootschalige gegevensverwerkingen

De AVG geeft geen definitie van 'grootschalige gegevensverwerkingen'. De guideline WP29 adviseert om met de volgende criteria te bepalen of hiervan sprake is:

- De hoeveelheid mensen van wie gegevens worden verwerkt;
- De hoeveelheid gegevens en/of de verscheidenheid aan gegevens die worden verwerkt;
- De tijdsduur van de gegevensverwerking;
- De geografische reikwijdte van de gegevensverwerking.

Naar verwachting zal er op den duur een praktische standaard komen om te bepalen of er op grote schaal (bijzondere) persoonsgegevens verwerkt.

6. Gekoppelde databases

Het gaat hierbij om gegevensverzamelingen die aan elkaar gekoppeld of met elkaar gecombineerd zijn. Bijvoorbeeld databases die voortkomen uit twee of meer verschillende

gegevensverwerkingen met verschillende doelen en/of uitgevoerd door verschillende verantwoordelijken, op een manier die betrokkenen niet redelijkerwijs kunnen verwachten.

7. Gegevens over kwetsbare personen

Bij het verwerken van dit type gegevens kan een DPIA nodig zijn, omdat er sprake is van een ongelijke machtsverhouding tussen de betrokkene en de verantwoordelijke. Dit heeft als gevolg dat betrokkenen niet in vrijheid toestemming kunnen geven of weigeren voor het verwerken van hun gegevens. Het kan hierbij om bijvoorbeeld werknemers, kinderen en patiënten gaan.

8. Gebruik van nieuwe technologieën

De AVG is er duidelijk over dat een DPIA nodig kan zijn bij het gebruik van een nieuwe technologie. Er kan dan sprake zijn van nieuwe manieren om gegevens te verzamelen en gebruiken, met mogelijk grote privacy-risico's. Een DPIA helpt de verantwoordelijke dan om de risico's te begrijpen en te verhelpen.

9. Blokking van een recht, dienst of contract

Het gaat hierbij om gegevensverwerkingen die tot gevolg hebben dat betrokkenen:

- Een recht niet kunnen uitoefenen of;
- Een dienst niet kunnen gebruiken of;
- Een contract niet kunnen afsluiten.

Bijvoorbeeld een bank die persoonsgegevens verwerkt om te bepalen of zij een lening aan iemand willen verstrekken.

Bijlage 11: Beveiligingsbeleid

Beveiligingsbeleid

Beveiliging van informatie is een belangrijke vereiste van de privacywetgeving. Naast de juiste organisatorische maatregelen, zullen ook de nodige passende maatregelen genomen moeten worden in de ICT-voorziening. Wat passend is, hangt af van de data die vastgelegd wordt en de risico's die een betrokkene loopt indien gegevens verloren gaan.

Beveiligingsmaatregelen

Om de bepalen welke beveiligingsmaatregelen genomen moeten worden, is het verstandig om een risico-inventarisatie te maken. Het gaat hierbij niet alleen om technische maatregelen, zoals firewall, Multi Factor Authenticatie en encryptie, maar ook om organisatorische maatregelen, zoals toegangsbeveiliging, beleid m.b.t. externe opslag (memory sticks, notebooks, tablets) en clean desk policy.

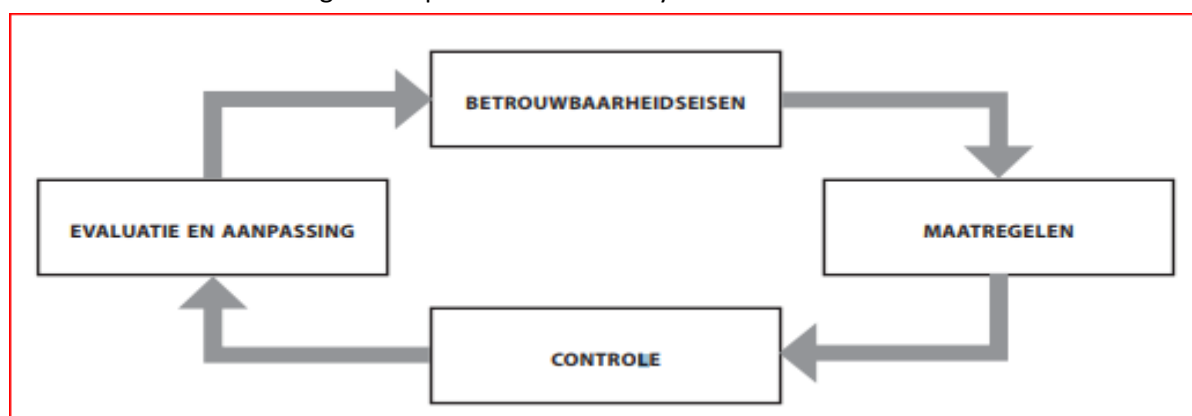
De soft- of hardwarematige beveiligingsmaatregelen die genomen kunnen worden zijn sterk afhankelijk van de 'stand van de techniek'. Regelmatig worden er beveiligingslekken ontdekt in software die dagelijks worden gebruikt, zoals Windows of Browsers. Deze kunnen vanzelfsprekend niet zelf opgelost worden en organisaties zijn hierin dus afhankelijk van derden. De organisatie heeft echter wel een eigen verantwoordelijkheid om te zorgen dat alles up to date is. Dit betekent dat een actief updatebeleid gevoerd moet worden van alle hard- en software en dat een organisatie moet beschikken over de actuele versies. De wet schrijft in artikel 32 het volgende voor:

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:
 - a) De pseudonimisering en versleuteling van persoonsgegevens;
 - b) Het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
 - c) Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
 - d) Een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.
2. Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

Daarnaast heeft de AP in de richtsnoeren beveiliging van persoonsgegevens aangegeven dat het beveiligingsbeleid ingebed moet worden via de zogeheten plan-do-check-act cyclus:

- Beoordeel de risico's die de gegevens en de aard van de verwerking met zich meebrengen voor de betrokkenen en bepaal op basis daarvan het gewenste beveiligingsniveau. Inventariseer vervolgens de dreigingen die kunnen leiden tot een beveiligingsincident, de gevolgen die het beveiligingsincident kan hebben en de kans dat deze gevolgen zich voor zullen doen. Tref op basis daarvan gericht beveiligingsmaatregelen die het gewenste beveiligingsniveau kunnen waarborgen.
- Maak gebruik van algemeen geaccepteerde beveiligingsstandaarden. Het vakgebied informatiebeveiliging kent vele beveiligingsmethoden, -standaarden en -maatregelen die zijn gebaseerd op ervaringen uit de dagelijkse beveiligingspraktijk. Gebruik bij het nemen van beveiligingsmaatregelen de richtsnoeren in samenhang met de beschikbare beveiligingsstandaarden. Deze standaarden geven houvast bij het daadwerkelijk treffen van passende maatregelen om de beveiligingsrisico's af te dekken.
- Controleer en evalueer met een zekere regelmaat of de beveiligingsmaatregelen daadwerkelijk zijn getroffen en worden nageleefd. Beoordeel periodiek of het beveiligingsniveau nog steeds past bij de risico's die de verwerking en de aard van de te verwerken gegevens met zich meebrengen en of de beveiligingsmaatregelen nog steeds voldoen. Betrek daarbij ook de stand van de techniek en de nieuwste inzichten binnen het vakgebied informatiebeveiliging. Pas waar nodig de beveiligingsmaatregelen aan.

Het onderstaande schema geeft de plan-do-check-act cyclus weer:



Privacy Impact Assessment (PIA)

Het uitvoeren van een privacy impact assessment (PIA) helpt de verantwoordelijke om de risico's te beoordelen die een verwerking van persoonsgegevens met zich meebrengt voor de rechten en vrijheden van de betrokkenen en om maatregelen te treffen die deze risico's beperken. Een PIA wordt als regel uitgevoerd in het eerste ontwerpstadium van een verwerking. De uitkomsten van de PIA kunnen van invloed zijn op de beveiliging van de persoonsgegevens die worden verwerkt, maar kunnen bijvoorbeeld ook leiden tot de keuze om minder persoonsgegevens te verzamelen dan in eerste instantie was voorzien of tot het uitbreiden van de mogelijkheden voor de betrokkenen om zeggenschap uit te oefenen over het gebruik van hun gegevens. De PIA valt buiten de reikwijdte van artikel 13 Wet bescherming persoonsgegevens (Wbp) en van deze richtsnoeren. Wel geeft het uitvoeren van een PIA een totaalbeeld van de risico's voor de betrokkenen en helpt het de verantwoordelijke om beveiligingsmaatregelen te treffen als onderdeel van een samenhangend

geheel aan maatregelen waarmee hij de risico's voor de betrokkenen afdekt en voldoet aan de Wbp. Een model van een PIA kunt u vinden op <https://www.rijksoverheid.nl/documenten>

Data Protection Impact Assessment (DPIA)

De DPIA is een instrument om vooraf de privacy-risico's van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Organisaties hoeven, zodra de AVG geldt, niet voor elke gegevensverwerking een DPIA uit te voeren. Een DPIA is alleen verplicht als een gegevensverwerking waarschijnlijk een hoog privacy-risico oplevert voor de betrokkenen (de mensen van wie de organisatie gegevens verwerkt). De Europese privacy-toezichthouders hebben criteria opgesteld om het risico te bepalen. U kunt deze richtlijnen vinden op de website van de Autoriteit Persoonsgegevens.

Organisaties dienen zich te realiseren dat een DPIA geen eenmalige actie is. Er zal moeten blijven gemonitord of de gegevensverwerkingen gewijzigd zijn en dus of een nieuwe DPIA moet worden uitgevoerd of moet worden bijgesteld.

Privacy by design en Privacy by default

Privacy by design houdt in dat een organisatie al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) ten eerste aandacht besteedt aan privacy-verhogende maatregelen, ook wel Privacy Enhancing Technologies (PET) genoemd. PET is de verzamelnaam voor een aantal technieken die de verantwoordelijke kan toepassen om bij het verwerken van persoonsgegevens de risico's voor de betrokkenen te beperken. Een centraal principe van PET is het verminderen van de herleidbaarheid: de mate waarin persoonsgegevens kunnen worden herleid tot de betrokkenen. De zwaarste vorm van PET is anonimisering van de verwerkte persoonsgegevens.

Daarnaast helpt het natuurlijk om de toegang tot gegevens te beperken, al dan niet met een goede rol-afscherming. Er moet dus worden gezorgd dat uitsluitend bevoegde medewerkers of derden toegang hebben tot bepaalde data. Voor iedere rol kan dat weer verschillend zijn en kan er dus een andere relevantie zijn van de gegevens. Alles hangt hierbij dus weer af van het doel van de verwerking van de betreffende medewerker of derden. Hiervoor zal een autorisatiebeleid moeten worden opgesteld.

Verder geldt natuurlijk ook dat hoe meer personen toegang hebben tot de data, hoe groter de kans is op een beveiligingsincident. Hierbij is het ook vooral van belang om actief user-management toe te passen. Denk hierbij aan vertrekkende medewerkers of derden met wie de samenwerking beëindigd wordt. Het is verstandig om met enige regelmaat de loggegevens te controleren van degene die toegang hebben verkregen tot privacygevoelige data, om vast te stellen of er onrechtmatig toegang is verkregen met het mogelijke risico dat er onrechtmatig gebruik is gemaakt van persoonsgegevens.

Privacy by default heeft als belangrijk uitgangspunt om niet meer te verzamelen aan privacygevoelige informatie dan nodig is: dataminimalisatie. Een organisatie mag alleen gegevens verzamelen die noodzakelijk zijn voor het doel van de verwerking. Hoe minder privacy gevoelige data, hoe kleiner de impact bij een datalek. Indien een organisatie bijvoorbeeld het BSN-nummer niet nodig heeft voor

bepaalde verwerkingen, zoals bijvoorbeeld het kunnen factureren van een dienst/product, dan moeten die gegevens ook niet worden gevraagd en opgenomen.

Bronnen:

- Richtsnoeren beveiliging persoonsgegevens van februari 2013 door College Bescherming Persoonsgegevens:
https://www.autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf
- Autoriteit Persoonsgegevens: <https://autoriteitpersoonsgegevens.nl>
- Stappenplan Privacy voor Dienstverleners van 9 februari 2018 door Blik op Werk, Noloc en Oval.

Bijlage 12: Vragen werknemers en werkgevers en antwoorden AP

Bron: website AP

Onderstaand zijn er allerlei vragen die op het vakgebied van verzuim , ziekmelding, preventie etc. gesteld zijn aan het AP met de antwoorden die het AP daarop zelf heeft gegeven.

Preventie

1. Mag mijn werkgever vragen naar mijn fitheid, bewegingspatroon, gewicht en/of stressgevoeligheid?

Om ziekteverzuim te voorkomen, wil uw werkgever misschien weten hoe fit u bent, hoeveel u beweegt etc. Maar uw werkgever mag deze informatie niet hebben. Dus mag uw werkgever hier ook niet naar vragen. Of op een andere manier informatie over verzamelen (zoals via een smartwatch die u draagt).

2. Mag mijn werkgever van mij eisen dat ik een wearable draag en de gegevens deel?

Nee, dat mag niet. Uw werkgever mag u een wearable (zoals een smartwatch) cadeau doen, zodat u zelf aan de slag kunt om uw fitheid te verbeteren. Maar uw werkgever mag niet van u eisen dat u de verzamelde gegevens - zoals uw aantal stappen, hartslag, verbrande calorieën, slaappatroon - met hem en/of uw collega's deelt. Uw werkgever mag geen inzicht krijgen in de informatie uit uw wearable. Het gaat namelijk om gegevens over uw gezondheid. Uw werkgever mag deze gegevens niet verwerken.

3. Mag mijn werkgever een bedrijf inhuren om informatie uit mijn wearable voor mij te analyseren?

Uw werkgever mag u deze service bieden. Maar u bent niet verplicht om hieraan mee te doen. Het bedrijf mag alleen informatie uit uw wearable voor u analyseren als u hiervoor toestemming heeft gegeven. Wilt u niet dat het bedrijf uw gegevens verwerkt, dan mag het dus niet. Uw werkgever kan u niet dwingen.

4. Mag ik als werkgever informatie ontvangen uit wearables van mijn werknemers?

Nee, dat mag niet. Gegevens uit een wearable - zoals over iemands fitheid, bewegingspatroon, gewicht en stressgevoeligheid - zijn namelijk gezondheidsgegevens. Als werkgever mag u die niet verwerken. Zelfs niet als een werknemer hiervoor toestemming zou geven.

Ziekmelding

5. Welke gegevens mag mijn werkgever aan mij vragen als ik me ziek meld?

Uw werkgever mag een aantal gegevens van u vragen. Bijvoorbeeld om te kunnen beoordelen hoe het verder moet met uw werkzaamheden. Of om te kunnen (laten) controleren of u wel echt ziek bent. Maar uw werkgever moet hierbij wel rekening houden met uw privacy. Uw werkgever mag daarom alleen gegevens vragen die noodzakelijk zijn. Uw werkgever mag naar de volgende gegevens vragen:

- *Het telefoonnummer waarop u te bereiken bent en uw (verpleeg)adres;*
- *Hoe lang uw ziekte vermoedelijk gaat duren;*
- *Uw lopende werkzaamheden en afspraken;*
- *Of u onder een van de vangnetbepalingen van de Ziektewet valt. Als u onder een vangnetbepaling valt, dan betaalt het UWV uw loon in plaats van uw werkgever. Maar uw werkgever mag niet vragen onder welke vangnetbepaling u valt;*
- *Zodra u 2 maanden of langer in dienst bent: of u onder de no-riskpolis valt;*
- *Of uw ziekte verband houdt met een arbeidsongeval. Maar uw werkgever mag niet vragen of uw verzuim werk gerelateerd is;*
- *Of er sprake is van een verkeersongeval met regresmogelijkheid. Dat houdt in dat uw werkgever de kosten van uw ziekteverzuim en re-integratie dan mogelijk kan verhalen op de veroorzaker van het ongeval.*

6. Mag mijn werkgever vragen of ik onder de no-riskpolis val als ik me ziek meld?

Bent u 2 maanden of langer in dienst? Dan mag uw werkgever bij uw ziekmelding vragen of u onder de no-riskpolis valt.

7. Mag mijn werkgever controleren of ik echt ziek ben als ik me heb ziek gemeld?

Ja, dat mag. Als u ziek bent, heeft u recht op doorbetaling van uw loon. Voor uw werkgever is het daarom belangrijk om te (laten) controleren of u echt ziek bent. En u dus daadwerkelijk recht heeft op uw salaris.

8. Ben ik na mijn ziekmelding verplicht om een vragenlijst in te vullen?

Heeft u zich ziek gemeld, dan kunt u een vragenlijst krijgen van de arbodienst of bedrijfsarts waarin om medische informatie wordt gevraagd. U bent verplicht deze vragenlijst in te vullen.

9. Mag mijn werkgever vragen of ik een ziekte of beperking heb?

Nee, dat mag niet. Uw werkgever mag als u langer dan 2 maanden in dienst bent alleen vragen of u in aanmerking komt voor de no-riskpolis van de Ziektewet. Komt u door een ziekte of beperking, uw leeftijd en/of uw uitkering(en) van nu of vroeger in aanmerking voor de no-riskpolis van de Ziektewet? Dan betaalt het UWV uw Ziektewetuitkering. Uw werkgever heeft daarom het recht om te weten of u hiervoor in aanmerking komt. Ook kan uw werkgever premiekortingen en subsidies voor u aanvragen. U moet de vraag van uw werkgever eerlijk beantwoorden. Maar u hoeft geen details te geven. Uw werkgever mag niet vragen welke ziekte of beperking u heeft (gehad) of welke uitkeringen u heeft (gehad).

10. Welke gegevens over mijn ziekte mag mijn werkgever vastleggen?

Uw werkgever mag gegevens over uw ziekteverzuim registreren, zoals hoe vaak en hoe lang u ziek bent. Dit is ten eerste nodig om uw loon te kunnen doorbetalen als u ziek bent. Ten tweede kan het voor uw werkgever van belang zijn om verzuimoverzichten te hebben. Bijvoorbeeld om te kijken of de oorzaak van veelvuldig of langdurig ziekteverzuim binnen de organisatie ligt.

11. Wie heeft op mijn werk toegang tot de gegevens over mijn ziekteverzuim?

Uw werkgever mag gegevens over uw ziekteverzuim alleen doorgeven aan de direct betrokkenen. Dit zijn bijvoorbeeld uw leidinggevende en medewerkers van de personeelsadministratie.

12. Welke gegevens mag mijn werkgever doorgeven aan de verzekering?

Raakt u arbeidsongeschikt? Dan is uw werkgever verplicht uw loon 2 jaar lang door te betalen. Veel werkgevers hebben voor deze kosten een verzekering afgesloten. Uw werkgever (of de bedrijfsarts) mag alleen administratieve gegevens over uw ziekteverzuim doorgeven aan de verzekeraar. Hierbij gaat het om gegevens die nodig zijn om de claim te beoordelen. Bijvoorbeeld welke periode u ziek bent geweest. Alleen in uitzonderlijke gevallen, zoals bij wachtlijstbemiddeling, mag de bedrijfsarts uw medische gegevens aan de verzekeraar doorgeven. De bedrijfsarts moet daarvoor wel uw toestemming hebben.

13. Hoe lang mag mijn werkgever mijn ziekteverzuimgegevens bewaren?

Voor uw administratieve verzuimgegevens (zoals de datum van ziekmelding, de verwachte duur van het verzuim en de datum van herstel) is meestal geen wettelijke bewaartermijn. Uw werkgever moet deze gegevens verwijderen zodra ze niet meer noodzakelijk zijn. Een redelijke bewaartermijn is maximaal 2 jaar nadat u uit dienst bent. Let op: Uw werkgever kan zogeheten eigenrisicodrager zijn voor de Ziektewet. Dat houdt in dat hij zelf uw uitkering betaalt als u arbeidsongeschikt bent. In dat geval geldt dat hij de gegevens 5 jaar voor het UWV moet bewaren (artikel 3, tweede lid, Regeling werkzaamheden, administratieve voorschriften en kosten eigenrisicodragen ZW).

14. Mag ik als werkgever met een zieke werknemer praten over zijn functionele beperkingen en mogelijkheden?

Ja, dat mag, onder de voorwaarde dat een bedrijfsarts in kaart heeft gebracht wat de functionele beperkingen en mogelijkheden van uw medewerker zijn. Aan de hand hiervan kunt u met uw werknemer bespreken wat dit betekent voor zijn werk en hoe u samen zijn re-integratie verder vorm gaat geven.

15. Wat doe ik als werkgever wanneer ik mij afvraag hoe het met mijn (zieke) werknemer gaat?

Als goed werkgever moet u goed voor uw (zieke) werknemers zorgen. U mag daarom best gesprekken voeren met uw werknemers waarin u vraagt hoe het met hen gaat en of u nog wat voor hen kunt betekenen. Maar u mag bij zieke werknemers niet naar de aard en oorzaak van hun ziekte vragen. Vertelt een werknemer hier zelf iets over? Dan mag u deze informatie niet registreren. Ook mag u op basis hiervan geen oordeel geven over de inzetbaarheid van uw werknemer.

16. Wat doe ik als werkgever wanneer een werknemer over zijn ziekte wil praten?

Uw werknemer kan de behoefte hebben om met u over zijn ziekte te praten. Natuurlijk mag u dan een luisterend oor bieden. En vragen of u iets voor uw werknemer kunt doen. Maar u mag de informatie die uw werknemer geeft over zijn ziekte niet registreren. Ook mag u op basis hiervan geen oordeel geven over de inzetbaarheid van uw werknemer.

17. Welke gegevens van mij krijgt de arbodienst of bedrijfsarts?

Zodra u zich ziek meldt, geeft uw werkgever dit door aan de arbodienst of bedrijfsarts. Zelf moet u ook gegevens doorgeven aan de arbodienst of bedrijfsarts. Tot slot kan de arbodienst of bedrijfsarts gegevens opvragen bij uw behandelend arts.

18. Welke gegevens van mij geeft de arbodienst of bedrijfsarts door?

De arbodienst of bedrijfsarts geeft beperkte informatie aan uw werkgever. En is verplicht om bepaalde gegevens door te geven aan het UWV. Verder kan de arbodienst of bedrijfsarts, indien van toepassing, bepaalde gegevens doorgeven aan het Sociaal Medisch Team/Overleg en het Nederlands Centrum voor Beroepsziekten.

19. Wie heeft er binnen een arbodienst toegang tot mijn dossier?

Bij de arbodienst heeft niet iedereen toegang tot uw dossier. De toegang is beperkt tot de medewerkers die direct bij uw behandeling betrokken zijn. Dat zijn:

- *De bedrijfsarts;*
- *Verpleegkundigen;*
- *Doktersassistenten;*
- *Collega-vakgenoten die de bedrijfsarts om advies vraagt (als het niet lukt om dit anoniem te doen);*
- *De vervangende bedrijfsarts(en).*

20. Mag mijn oude arbodienst of bedrijfsarts mijn dossier overdragen aan een nieuwe?

Uw oude arbodienst of bedrijfsarts mag alleen het deel van uw dossier overdragen waar geen medisch beroepsgeheim op rust. De gegevens die wel onder het medisch beroepsgeheim vallen,

mag uw oude arbodienst of bedrijfsarts alleen overdragen als die gegevens noodzakelijk zijn voor uw verzuimbegeleiding. Gegevens zijn noodzakelijk voor uw verzuimbegeleiding als u bij de wisseling van arbodienst of bedrijfsarts ziek bent of binnen 4 weken na uw herstelmelding opnieuw uitvalt. De arbodienst/bedrijfsarts moet u hierbij van tevoren laten weten dat uw gegevens overgedragen worden. Ook moet u de kans krijgen om hiertegen bezwaar te maken. Tot slot mag de arbodienst of bedrijfsarts uw gegevens alleen overdragen aan een andere gecertificeerde arbodienst of bedrijfsarts.

21. Hoe lang mag de arbodienst of bedrijfsarts mijn medisch dossier bewaren?

Voor uw medisch dossier bij de arbodienst of de bedrijfsarts geldt een bewaartermijn van 15 jaar na het einde van uw dienstverband. Of na de beëindiging van de overeenkomst tussen uw werkgever en de arbodienst/bedrijfsarts.

22. Mag de arbodienst of bedrijfsarts de loonwaarde van een zieke werknemer aan de werkgever doorgeven?

Nee. De arbodienst of bedrijfsarts mag weliswaar de mate waarin een werknemer arbeidsongeschikt is aan de werkgever doorgeven, maar de loonwaarde valt hier niet onder.

23. Mag de arbodienst of bedrijfsarts een probleemanalyse naar de werkgever sturen?

Dat hangt ervan af om wat voor probleemanalyse het gaat. Is het een document waarin onder meer de aard en oorzaak van de klachten en de omstandigheden van de zieke werknemer staan? Dan mag de arbodienst of bedrijfsarts deze probleemanalyse niet naar de werkgever sturen. Let op: de werknemer zelf heeft het recht om over de totale probleemanalyse te beschikken, dus ook over het medische deel.

Re-integratie

24. Welke gegevens worden uitgewisseld tijdens mijn re-integratie?

Bij dreigend langdurig ziekteverzuim vinden vanaf ongeveer 6 weken na uw ziekmelding gegevensuitwisselingen plaats tussen onder meer u, uw werkgever, de arbodienst/bedrijfsarts en het UWV. Dit gebeurt in de vorm van een probleemanalyse en advies, plan van aanpak, re-integratiedossier en re-integratieverslag.

25. Hoe lang mag mijn werkgever mijn re-integratiedossier bewaren?

Er bestaat geen wettelijke termijn voor het bewaren van uw re-integratiedossier. Het is redelijk om het dossier in principe niet langer dan 2 jaar te bewaren nadat u uit dienst bent. Let op: uw werkgever kan zogeheten eigenrisicodragers zijn voor de Ziektewet. Dat houdt in dat hij zelf uw uitkering betaalt als u arbeidsongeschikt bent. In dat geval geldt dat hij de gegevens 5 jaar voor

het UWV moet bewaren (artikel 3, tweede lid, Regeling werkzaamheden, administratieve voorschriften en kosten eigenrisicodragers ZW).

26. Hoe lang mag het re-integratiebedrijf mijn gegevens bewaren?

Bent u langdurig ziek geweest en heeft uw werkgever een re-integratiebedrijf ingeschakeld? Dan geldt voor uw medische gegevens bij het re-integratiebedrijf een bewaartermijn van 15 jaar. Voor de overige (niet-medische) gegevens is de bewaartermijn 2 jaar.

Verzuimsystemen

27. Mag ik als bedrijfsarts of arbodienst medische dossiers opslaan in een verzuimsysteem van een werkgever zelf?

Nee, dat mag niet. Een werkgever (uw opdrachtgever) mag medische dossiers met gegevens over de gezondheid van zijn werknemers (aard en oorzaak van de ziekte e.d.) niet verwerken. En mag u dus ook niet vragen om deze gegevens op te slaan in een systeem dat hij zelf beheert. Een werkgever mag u wél vragen medische dossiers op te slaan in een verzuimsysteem dat hij zelf ook gebruikt als dit extern wordt beheerd.

28. Mag ik als bedrijfsarts of arbodienst medische dossiers opslaan in een verzuimsysteem dat een werkgever uitkiest?

Wil een werkgever (uw opdrachtgever) dat u de medische dossiers van zijn zieke werknemers opslaat in een door hem uitgekozen verzuimsysteem? Bijvoorbeeld het (extern beheerde) verzuimsysteem dat hij zelf ook gebruikt? Dat mag alleen onder bepaalde voorwaarden.

29. Mag ik als bedrijfsarts of arbodienst medische dossiers opslaan in een extern verzuimsysteem?

Dat mag alleen als u een bewerkersovereenkomst heeft afgesloten met de externe partij die het systeem beheert. Bij de begeleiding en re-integratie van zieke werknemers bent u de zogeheten verantwoordelijke voor de verwerking van gegevens over de gezondheid van deze werknemers in hun medische dossiers (zie: Beleidsregels zieke werknemer, p. 24). Verwerkt u deze gegevens in een extern verzuimsysteem (een systeem dat door een externe partij wordt beheerd)? Dan is deze externe partij een bewerker. Dat betekent dat u een verwerkersovereenkomst met deze partij moet afsluiten.

30. Wat moet er in de verwerkersovereenkomst staan tussen de bedrijfsarts/arbodienst en de beheerder van een verzuimsysteem?

Verwerkt u als bedrijfsarts of arbodienst medische gegevens van werknemers in een extern verzuimsysteem (een systeem dat door een externe partij wordt beheerd)? Dan moet u een verwerkersovereenkomst afsluiten met de beheerder van het systeem.

31. Mag ik als werkgever verzuimgegevens registreren in een extern verzuimsysteem?

Dat mag alleen als u een verwerkersovereenkomst heeft afgesloten met de externe partij die het systeem beheert. Bij de begeleiding en re-integratie van zieke werknemers bent u de zogeheten verantwoordelijke voor de verwerking van gegevens over de ziekmeldingen en de (door de bedrijfsarts vastgestelde) beperkingen en mogelijkheden van uw werknemers (zie: Beleidsregels zieke werknemer, p. 19 en 27). Verwerkt u deze verzuimgegevens in een extern verzuimsysteem (een systeem door een externe partij wordt beheerd)? Dan is deze externe partij een verwerker. Dat betekent dat u een verwerkersovereenkomst met deze partij moet afsluiten.

32. Hoe moet ik als organisatie de online toegang tot ziekteverzuimgegevens beveiligen?

Is het verzuimsysteem dat u als werkgever, arbodienst of re-integratiebedrijf gebruikt via internet toegankelijk voor bevoegde medewerkers? Dan mag toegang tot het systeem alleen via meerfactorauthenticatie verlopen. Meerfactorauthenticatie houdt in dat de identiteit van de persoon die wil inloggen op minstens twee manieren wordt gecontroleerd. Inloggen met alleen een gebruikersnaam en wachtwoord is dus niet genoeg. Gegevens over iemands ziekteverzuim kunnen iets zeggen over zijn gezondheid. Voor de beveiliging van gezondheidsgegevens gelden extra strenge eisen. Daarom moet iedereen die in het verzuimsysteem in kan loggen om ziekteverzuimgegevens te bekijken naast het 'gewone' inloggen ook op een andere manier zijn identiteit aantonen om toegang te krijgen. Bijvoorbeeld door een token te gebruiken.

33. Mag een bedrijfsarts of Arboarts het interne ICT-systeem gebruiken?

Een werkgever kan een eigen bedrijfsarts of Arboarts in dienst hebben. Deze arts mag niet zomaar hetzelfde ICT-systeem gebruiken als de rest van de organisatie. Dit mag alleen als verzekerd is dat uitsluitend deze arts toegang heeft tot de medische gegevens van de medewerkers. Anderen die het ICT-systeem gebruiken, zoals leidinggevenden of de systeembeheerder van het bedrijf, mogen geen toegang hebben tot deze gegevens.

Bijlage 13: veel voorkomende vragen uit de praktijk beantwoord door de werkgroep

Onderstaande vragen zijn vragen die we als werkgroep in de praktijk hebben gekregen waar de diverse professionals een antwoord hebben gezocht, oftewel dit is niet de bron van de AP zelf. Vervelende is dat ook diverse standpunten en vragen wel aan de AP zijn voorgelegd, maar dat hier nog geen antwoord op is gekomen. Dit document wordt uiteraard bijgewerkt indien deze antwoorden alsnog komen.

1. Wanneer moet de werknemer geïnformeerd worden over verwerking van zijn gegevens bij de arbodienst of de casemanager?

Het advies is om hier in het verzuimprotocol voorlichting over te geven, maar ook het twee-maanden-uitvraagmoment te nemen. Een werknemer die in dienst komt, krijgen na 2 maanden van de werkgever een informatiebrief met een uitvraag naar de vangnetsituaties no-risk conform artikel 38b Ziektewet. Bij deze brief wordt uitleg gegeven dat de werkgever in bepaalde situaties door het UWV gecompenseerd wordt voor de loondoorbetaling bij ziekte. Het advies is dat op dit moment bij de informatievoorlichting de werknemer ook informatie krijgt over hetgeen er gebeurt bij een ziekmelding en welke gegevens er naar de arbodienst gaat die de verzuimbegeleiding op zich neemt. De werknemer wordt pas in het verzuimsysteem opgenomen wanneer hij ziek is. Er is immers geen grondslag voor de verzuimregistratie (Artikel 6 lid 1 sub c AVG).

2. Wanneer mag je als zelfstandige bedrijfsarts of bedrijfsarts vanuit arbodienst werken in een verzuimsysteem van een klant? Het medisch deel is daarbij altijd afgesloten voor de klant zelf, maar in feite behoort het systeem aan de klant. Ligt dat eraan wie het beheer doet van het systeem (externe partij)? (Geen verschil arbodienst of zelfstandig).

Bedrijfsartsen werken veelal niet in het systeem van de werkgever zelf, maar dat kan wel. Het beheer van het medisch deel van het dossier ligt dan altijd bij de systeemleverancier. Deze verstrekt ook de autorisatiegegevens aan de bedrijfsarts. Dit kan nooit bij het functioneel beheer van de werkgever zelf liggen. Zie AP beleidsregels de zieke werknemer. Veelal werken de bedrijfsartsen in een eigen systeem en dat betekent dat ze per post of encrypted mails de spreekuurterugkoppelingen, PA of de FML moeten verstrekken. Of dat ze aan de casemanager in het systeem toegang geven in het re-integratiedossier, waarbij er sprake is van een tweefactorauthenticatie.

3. Er zijn casemanagers die de werknemer begeleiden in een juridische beroep- en bezwaarprocedure. Bijvoorbeeld om een 80-100% WGA om te zetten naar IVA. Hier is altijd een arts-gemachtigde voor nodig. Wat doe je als je als casemanager stukken krijgt die je niet mag ontvangen volgens de privacywetgeving, maar waarvan de werknemer wel wil dat je die ontvangt? Ook als het niet medische documenten betreft en werknemer graag wil dat je hem of haar in alles begeleidt. Zijn er dan grenzen aan de informatie die een casemanager mag

ontvangen als er een formele machtiging van de werknemer ligt met zijn vrijwillig gegeven handtekening en de werknemer wil dat jij representant van hem of haar bent?

Bij het toezenden van de stukken hoort het UWV aan de werknemer te vragen of deze toestemming geeft om de stukken ook te sturen naar de casemanager juridisch van de werkgever. Wil werknemer dit niet, dan kan de casemanager juridisch alleen de informatie krijgen die de werkgever heeft. Wel zal de casemanager juridisch er een arts-gemachtigde op zetten die wel toegang krijgt tot alle stukken. Ook een advocaat heeft toegang tot het volledige dossier.

Let op: Als een casemanager als niet-medisch gemachtigde optreedt naar de werkgever, worden er wel eens medische stukken toegestuurd als de werknemer daar toestemming voor heeft gegeven. Het UWV schakelt dan de casemanager juridisch gelijk aan de positie van een advocaat. Een advocaat mag wel kennis nemen van medische stukken maar niet interpreteren. Het UWV is hier niet eenduidig in en een casemanager dient zichzelf te beschermen in de rol van de werkgeverregievoerder om deze medische stukken niet te verwerken.

4. Uitwisseling tussen claimbehandelaar verzekeraar en werkgever ten aanzien van het loon?

In de praktijk werkt 'meldverzuim' niet meer indien het loonstrookje niet wordt geüpload. De claimbehandelaar bij de verzekeraar mag alleen de verzamelloonstaat en niet het loonstrookje ontvangen. Er zijn nog verzekeraars die aan de casemanager Wvp vragen om een loonstrook te verstrekken. De casemanager Wvp mag dit zelf niet weten. De werkgever wil graag dat de volledige regie wordt gevoerd door de casemanager Wvp. Indien de werkgever het loon niet verstrekt, betaalt verzekeraar niets uit.

5. Mag het RIV na uitdiensttreding zonder meer worden overgedragen aan de private uitvoerder ZW? Of is hier toestemming van de medewerker voor nodig? En hoe zit het met het medisch dossier? Mag dat worden overgedragen aan de bedrijfsarts van de private uitvoerder of is hier ook toestemming werkgever voor nodig?

Het standpunt ter toetsing door AP is dat de private uitvoerder ZW in de uitvoering van de re-integratieverplichtingen gelijk behandeld moet worden als de publieke uitvoerder (UWV). Dit betekent dat werkgever het RIV kan overdragen aan de private uitvoerder zonder toestemming van de werknemer. Voor het medisch dossier kan aan de werknemer gevraagd worden om dit mee te brengen bij het eerste bezoek, dit gaat echter in de praktijk niet goed.

Vraag aan AP is of het mogelijk is dat de werknemer bij het laatste bezoek aan de bedrijfsarts binnen het dienstverband, waarin ook het actueel oordeel wordt opgesteld, toestemming geeft voor overdracht aan de bedrijfsarts van de uitvoerder ZW?

6. Vraag omtrent de nota second opinion. Indien de werknemer niet wil dat zijn werkgever op de hoogte wordt gebracht dat hij een second opinion heeft aangevraagd, mag de bedrijfsarts dat niet communiceren. Maar als er een nota binnenkomt kan een kleine middelgrote werkgever wel herleiden op wie deze nota betrekking heeft. Dat is toch niet de bedoeling?

Bedrijfsarts werkt over het algemeen zeker aan de eerste second opinion mee. De nota van de second-opinion bedrijfsarts gaat wel rechtstreeks naar de werkgever. Indirect kan de kleine of middelgrote werkgever herleiden op wie de second opinion betrekking heeft, maar dit is een gegeven. Belangrijk is dat de nota van de second opinion in ieder geval wel anoniem is, dus de naam van de werknemer niet op de factuur staat.

7. Het mailen van medische stukken vindt momenteel nog op regelmatige basis plaats vanuit interventiebureaus naar bedrijfsarts, vanuit interventiebureaus naar werknemers zelf, vanuit bedrijfsarts naar medisch secretaresse voor verwerking. Soms gebeurt dat met versleuteling (bijvoorbeeld openen met een specifieke code, waarbij afgesproken is dat de code de geboortedatum is). Maar soms is het ook gewoon een Word-bijlage zonder versleuteling. Mag dat?

Nee, medische stukken kunnen per post (briefgeheim) of encrypted of via systeem met twofactorauthenticatie verstuurd worden.

8. Een werkgever krijgt vaak veel informatie van de werknemer over wat er aan de hand is. Mag de werkgever/casemanager deze informatie aan de bedrijfsarts doorgeven?

Dit mag niet. Werkgever en daarmee de casemanager Wvp ontvangt vrijwillig van de werknemer veel meer informatie dan hij/zij mag verwerken. Standpunt is dat wat niet verwerkt mag worden, ook niet aan de bedrijfsarts mag worden doorgegeven. Wel mag informatie worden doorgegeven over de aard van de functie en het functioneren. Ook mogen er door werkgever vragen worden gesteld over veiligheid, welzijn en beschikbaarheid voor passende arbeid.

9. Als de werkgever is geïnformeerd door naasten dat er bijvoorbeeld sprake is van langdurige opname in een zorginstelling, mag dit aan de bedrijfsarts worden doorgegeven. Ook geven naasten of de werknemer zelf veelal heel veel privacygevoelige informatie aan de casemanager. Hoe hiermee om te gaan?

Allereerst: de werkgever vraagt er niet op door, maar biedt alleen een luisterend oor en mag deze informatie echt niet weten en zeker niet opslaan. Een casemanager vanuit de werkgeversrol zit daarmee in een spagaat omdat enerzijds hij/zij betrokken is bij zijn klanten en de werkgever een goed werkgever wil zijn. Anderzijds mag hij/zij niets weten en niets met de informatie doen. Een casemanager/ werkgever wil juist deze informatie dan kwijt bij de bedrijfsarts, zodat die er wel gericht actie op kan ondernemen. Dit komt in de dagelijkse praktijk voor en kenmerkt de aard van de werkzaamheden van een casemanager. In een normale verstandhouding tussen werkgever en werknemer is het gebruikelijk dat werknemer deelt wat er speelt. De regels zijn dermate strikt opgesteld dat werkgevers het idee hebben dat alle menselijke maat ontbreekt. Het enige dat de werkgever kan doen is zorgen dat de werknemer snel bij de bedrijfsarts (of de casemanager taakdelegatie) terecht kan indien het noodzakelijk is dat de bedrijfsarts snel iemand zijn mogelijkheden in kaart brengt of indien het noodzakelijk is dat er snel de juiste dienstverlening wordt opgestart.

10. Hoe moet de werkgever omgaan met situatie waarbij werknemer zelf aangeeft wat hij of zij kan doen?

Alleen indien de werknemer dit volkomen vrijwillig uit zichzelf meldt zonder dat het hem of haar gevraagd is, mag de werkgever hier werkafspraken met de werknemer over maken volgens de gezamenlijke interpretatie van de beleidsregels de zieke werknemer die het ministerie van sociale zaken naar buiten heeft gebracht in juni 2018. Bij de ziekmelding mag niet meer door werkgever gevraagd worden wat de werknemer nog wel kan doen, zonder tussenkomst van de bedrijfsarts. Rond de 80% van alle verzuimmeldingen zijn gekoppeld aan kort verzuim. Ook bij deze meldingen kan het zijn dat mensen nog wel iets kunnen en ook graag deels aan het werk willen blijven. Veel werknemers hebben in de praktijk wel een prima beeld bij hetgeen ze kunnen doen, en daar mag de werknemer uit zichzelf ook mee komen, maar er mag niet naar gevraagd worden door de leidinggevende. Een logisch voorbeeld is dat indien iemand aangeeft alleen een reisbeperking te hebben, dat er vervolgens afspraken over het vervoer worden gemaakt of dat er gekeken wordt naar mogelijkheden om een deel van zijn taken vanaf huis te organiseren.

11. Mag een werkgever gezondheidsgegevens verwerken als hiervoor toestemming van de werknemer is gegeven?

Toestemming geldt niet en een werkgever mag geen gezondheidsgegevens verwerken, ook al heeft de werknemer hiervoor toestemming gegeven. De werknemer is namelijk afhankelijk van de werkgever en kan zich daardoor onder druk gezet voelen om toestemming te geven. In die situatie voldoet de toestemming niet aan de wettelijke eis dat de werknemer deze in vrijheid moet hebben gegeven. En kan de werkgever die toestemming dus niet gebruiken als uitzondering op het wettelijke verbod om gezondheidsgegevens van de werknemer te verwerken.

12. Als het verzuimsysteem wordt ontsloten via internet hoe is dit dan beveiligd?

Wordt het verzuimsysteem ontsloten via internet? Dan mag u alleen toegang tot het systeem krijgen met meerfactorauthenticatie. Het systeem moet ook voldoen aan alle andere beveiligingseisen uit artikel 13 Wbp (artikel 32 AVG)

13. Mag ik als werkgever verzuimgegevens registreren in een extern verzuimsysteem?

Dat mag alleen als u een verwerkersovereenkomst heeft afgesloten met de externe partij die het systeem beheert. Bij de begeleiding en re-integratie van zieke werknemers bent u de zogeheten verantwoordelijke voor de verwerking van gegevens over de ziekmeldingen en de (door de bedrijfsarts vastgestelde) beperkingen en mogelijkheden van uw werknemers (zie: Beleidsregels zieke werknemer, p. 19 en 27). Verwerkt u deze verzuimgegevens in een extern verzuimsysteem (een systeem door een externe partij wordt beheerd)? Dan is deze externe partij een verwerker. Dat betekent dat u een verwerkersovereenkomst met deze partij moet afsluiten.

14. Verzuimgegevens versus medische gegevens en welke mag ik als werkgever verwerken?

Let op: Als werkgever mag u verzuimgegevens van uw werknemers verwerken (en dus opslaan in een intern of extern systeem), maar geen medische gegevens. Dat betekent dat u dus ook niet aan de bedrijfsarts of arbodienst mag vragen om deze gegevens in uw eigen verzuimsysteem (dat u zelf beheert) op te slaan. U mag wél aan de bedrijfsarts vragen om medische gegevens op te slaan in een verzuimsysteem dat u zelf ook gebruikt als dit extern wordt beheerd en het medisch deel is afgeschermd met een aparte meerfactorauthenticatie en niet toegankelijk is voor de werkgever.

15. Hoe moet ik als organisatie de online toegang tot ziekteverzuimgegevens beveiligen?

Is het verzuimsysteem dat u als werkgever, arbodienst of re-integratiebedrijf gebruikt via internet toegankelijk voor bevoegde medewerkers? Dan mag toegang tot het systeem alleen via meerfactorauthenticatie verlopen. Meerfactorauthenticatie houdt in dat de identiteit van de persoon die wil inloggen op minstens twee manieren wordt gecontroleerd. Inloggen met alleen een gebruikersnaam en wachtwoord is dus niet genoeg. Gegevens over iemands ziekteverzuim kunnen iets zeggen over zijn gezondheid. Voor de beveiliging van gezondheidsgegevens gelden extra strenge eisen. Daarom moet iedereen die in het verzuimsysteem in kan loggen om ziekteverzuimgegevens te bekijken, naast het 'gewone' inloggen ook op een andere manier zijn identiteit aantonen om toegang te krijgen. Bijvoorbeeld door een token te gebruiken.

16. Mag een bedrijfsarts of arboarts het interne ICT-systeem gebruiken?

Een werkgever kan een eigen bedrijfsarts of arboarts in dienst hebben. Deze arts mag niet zomaar hetzelfde ICT-systeem gebruiken als de rest van de organisatie. Dit mag alleen als verzekerd is dat uitsluitend deze arts toegang heeft tot de medische gegevens van de medewerkers. Anderen die het ICT-systeem gebruiken, zoals leidinggevenden of de systeembeheerder van het bedrijf, mogen geen toegang hebben tot deze gegevens. Een arts heeft medisch beroepsgeheim en moet er daarom voor zorgen dat niemand anders de medische gegevens van de medewerkers kan inzien. De organisatie moet technische en organisatorische maatregelen treffen om te verzekeren dat uitsluitend de BIG geregistreerde bedrijfsarts, de arboarts (of een onder zijn verantwoordelijkheid werkende medewerker) bij de medische gegevens kan. Is dit in het ICT-systeem van de organisatie niet mogelijk? Dan mag de arts geen medische gegevens in het systeem opslaan.

Bijlage 14. Tijdslijn Wet verbetering poortwachter

Wanneer?	Wat?
<i>In het eerste jaar</i>	
Week 1 Binnen een week na de eerste ziekte dag	Melding bij arbodienst/bedrijfsarts Melding bij arbodienst/bedrijfsarts bij voorkeur de 4 ^{de} ziekte dag.
Week 6 Uiterlijk 6 weken na de eerste ziekte dag	Opstellen probleemanalyse De bedrijfsarts maakt een Probleemanalyse. Hierin staat onder meer welke mogelijkheden en beperkingen de werknemer heeft, of er geschiktheid is voor eigen of passend werk, of er interventies mogelijk zijn om het herstel of de re-integratie te bespoedigen, wat het einddoel van de re-integratie is en wat de gewenste contactmomenten zijn. Dit is de visie van de bedrijfsarts op de belastbaarheid en de nodige stappen in de begeleiding van de werknemer. De werkgever ontvangt uitdrukkelijk alleen het niet medische deel van de probleemanalyse.
Week 8 Uiterlijk 8 weken na de eerste ziekte dag	Opstellen Plan van Aanpak De werkgever stelt in overleg met de werknemer op basis van de Probleemanalyse van de bedrijfsarts een Plan van Aanpak op dat beschrijft wat beiden gaan doen om de werknemer te laten re-integreren. Het Plan van Aanpak maakt deel uit van het re-integratiedossier. Re-integratiedossier Bij dreigend langdurig verzuim moet de werkgever een re-integratiedossier bijhouden. Hierin staan het verloop van het verzuim en alle activiteiten die werkgever en werknemer hebben ondernomen voor de re-integratie.
Week 8 Uiterlijk in de 8e week	Benoemen casemanager Om ervoor te zorgen dat iedereen de afspraken nakomt, wijzen werkgever en werknemer samen iemand aan die de overeengekomen re-integratieactiviteiten begeleidt, bewaakt en het contact verzorgt tussen werknemer, werkgever en bedrijfsarts of arbodienst. Dit is de casemanager Wet verbetering poortwachter. De casemanager kan een medewerker van de arbodienst (niet zijnde de casemanager onder taakdelegatie c.q. de verlengde arm constructie) zijn, maar bijvoorbeeld ook een leidinggevende of een collega. Zowel werkgever als werknemer kunnen bij de casemanager terecht als zij vinden dat iets niet volgens afspraak verloopt. De re-integratieactiviteiten zijn vastgelegd in het plan van aanpak of de bijstellingen van het plan van aanpak.
Week 14 t/m 38 Elke 6 weken	Voortgangsgesprekken Iedere zes weken (of zoveel vaker of minder afhankelijk van de aard van het verzuim) moet de werkgever de voortgang met de werknemer bespreken en daarvan verslagleggen in het re-integratiedossier. Periodieke evaluatie bedrijfsarts Ook de bedrijfsarts maakt, afhankelijk van de situatie, globaal iedere 6 weken een evaluatie. Dit geldt voor het hele traject, dus niet alleen t/m 38 weken. Periodieke evaluatie Wanneer re-integratieactiviteiten wijzigen dient het Plan van Aanpak of latere afspraken te worden bijgesteld in een evaluatieformulier.
Week 42 In de 42 ^{ste} week	Melding UWV In de 42 ^{ste} week moet de werkgever de werknemer ziek melden bij het UWV.
Week 46 t/m 52	Eerstejaarsevaluatie Blijft de werknemer ziek, dan stellen werkgever en werknemer de eerstejaarsevaluatie vast. Hierin evalueren zij het afgelopen jaar en leggen vast welk re-integratieresultaat ze in het tweede ziektejaar willen behalen en hoe ze dat gaan doen. Dit wordt ook wel het 'opschudmoment' genoemd.
<i>Het tweede jaar</i>	
Week 84 Na 20 maanden	Opstellen re-integratieverslag

	Is de werknemer na 20 maanden nog niet (volledig) aan de slag, dan stelt de werkgever in overleg met de werknemer een re-integratieverslag op. Hierin staan alle afspraken en concrete resultaten van de geplande werkhervatting. Periodieke Evaluatie Aanpassingen op het Plan van Aanpak of latere afspraken worden vastgelegd in een evaluatieformulier. Opstellen actueel oordeel In deze week maakt ook de bedrijfsarts een actueel oordeel en medisch resumé.
Week 87 87 weken na de eerste ziekte dag	Ontvangst WIA-aanvraagformulier In week 87 ontvangt de werknemer van het UWV een WIA-aanvraagformulier.
Week 87 t/m 90 Tussen week 87 en week 90	Indienen WIA-aanvraagformulier De werknemer moet het WIA-aanvraagformulier binnen drie weken terugsturen naar het UWV. Beoordeling re-integratieverslag door UWV Het UWV beoordeelt het re-integratieverslag. WIA-keuring Het UWV voert de WIA-keuring uit als de re-integratie-inspanningen voldoende zijn en geeft de WIA-beslissing af.
Na 104 weken	Aanvang WIA-uitkering Als aan de wettelijke voorwaarden is voldaan en een WIA-uitkering is toegekend dan start de WIA-uitkering veelal na 104 weken verzuim. Uitzonderingen door verlenging van de loondoorbetalingsperiode (de zogenaamde sancties) daargelaten.