

Privacyreglement Bedrijfsgezondheidsdienst Noord West

1 Voorwoord

Onderhavig document vervangt het Privacyreglement van Bedrijfsgezondheidsdienst Noord West versie 2013-03. De reden hiervoor is gelegen in het feit dat per 25 mei 2018 de Algemene verordening Gegevensbescherming (AVG) van kracht is. De Algemene Verordening Gegevensbescherming (AVG) komt dus in plaats van de oude Wet bescherming persoonsgegevens (Wbp). In de AVG staan een aantal verplichte maatregelen genoemd waaraan wij als Arbodienst moeten voldoen onder meer omdat wij persoonsgegevens vastleggen in cliëntendossiers.

Het beleidskader geeft inzicht in de persoonsgegevens die verwerkt worden alsmede de grondslagen waarop de wet is gebaseerd. Het beleidskader is hiermee tevens op te vatten als het in de AVG genoemde **Verwerkingsregister**.

2 Beleidskader BGD NW in relatie tot de AVG

Bedrijfsgezondheidsdienst Noord-West conformeert zich nadrukkelijk aan de vigerende wet –en regelgeving. Te noemen in dit kader.

1. De Wet op de geneeskundige behandelingsovereenkomst (**WGBO**) (beschrijft de rechten en plichten van cliënten in de zorg);
2. De Wet op de Beroepen in de Individuele Gezondheidszorg (wet BIG);
3. De Wet op de Medische Keuringen (WMK);
4. De wet Algemene Bepalingen Burgerservicenummer;
5. De AVG;
6. De zieke werknemer en privacy (CBP, 2008) (digitale map);
7. Taken en verantwoordelijkheden van de bedrijfsarts in het kader van de verzuimbegeleiding en re-integratie (KNMG, aug 2009);
8. De KNMG-code "Gegevensverkeer en samenwerking bij arbeidsverzuim en re-integratie (2007);
9. KNMG-advies "Inrichting en overdracht van het bedrijfsgeneeskundig dossier" (april 2009);
10. Leidraad Bedrijfsarts en privacy (Boaborea en privacy);
11. KNMG-richtlijn inzake het "Omgaan met medische gegevens" (januari 2010)"
12. Beroepscode Arbeid hygiënist, Veiligheidskundigen, Arbeid -en Organisatiedeskundigen.

2.1 Doelstelling Privacy beleid:

Voldoen aan de AVG en het creëren van een gemeenschappelijk referentiekader over hoe Bedrijfsgezondheidsdienst Noord West om gaat met privacygevoelige medische informatie. In het bijzonder informatie die noodzakelijk is in verband met re-integratie van een arbeidsongeschikte werknemer. Uitgangspunt van het beleid is het bevorderen van re-integratie conform de criteria gesteld door middel van de Algemene Verordening Gegevensbescherming (AVG).

2.2 Het register van verwerkingsactiviteiten

Bedrijfsgezondheidsdienst Noord-West heeft vooraf vastgesteld, welke administraties er gevoerd worden. Dit zijn onder meer verzuimadministratie in VX, de personeel- en salarisadministratie van de eigen medewerkers (hiertoe is een afzonderlijk Verwerkingsregister opgesteld), debiteuren -en crediteurenadministratie (middels de applicatie Snelstart, contractadministratie (Excel registraties), en de administratie ten behoeve van uitgevoerde keuringen (fysieke documenten). Vervolgens is bepaald welke registraties er zijn. Te noemen in dit kader persoonlijke e-mail boxen, centrale e-mailboxen, telefoongegevens, back-ups en papieren archieven, laptops. Op basis van deze administraties en registraties is een zogenoemd Register van Verwerkingsactiviteiten opgesteld.

Het register van verwerkingsactiviteiten van de Bedrijfsgezondheidsdienst Noord West bevat informatie over de persoonsgegevens die de BGD NW vastlegt over werknemers van opdrachtgevers in het cliëntendossier (via de digitale webapplicatie VerzuimXpert). [Meer specifiek](#) Bedrijfsgezondheidsdienst Noord West legt uitsluitend gegevens vast van medewerkers met een zorgvraag. Dit zijn medewerkers die ziekgemeld worden of medewerkers die ziek geweest zijn en waar de bewaartermijn van het dossier nog niet is verstrekken. Bedrijfsgezondheidsdienst Noord-West onderscheidt navolgende categorieën gegevens:

- A. Primaire persoonsgegevens;
- B. Secundaire persoonsgegevens;
- C. Bijzondere persoonsgegevens;

3 Primaire persoonsgegevens

3.1 Identificatie

	Categorie A: Primaire persoonsgegevens
	Naam, adres, postcode, woonplaats van de werknemers/ cliënt(en)
	Geboortedatum van de werknemer/ cliënt(en)
	Telefoonnummer en e-mail van de werknemer/ cliënt(en)
	Gegevens ten aanzien van het lopend dienstverband (startdatum, functie, aantal werkuren)
	Leidinggevende (contactpersoon van de werkgever)

3.2 Legitimatie

Dit zijn algemene gegevens van werkgever en werknemers. Deze gegevens spelen een rol bij de dienstverleningsovereenkomst die is afgesloten tussen de werkgever en Bedrijfsgezondheidsdienst Noord West. Het zijn hoofdzakelijk proces -en administratieve gegevens. Bedrijfsgezondheidsdienst Noord-West heeft geen overeenkomst gesloten met werknemer zelf, maar met de werkgever. De grondslag “*uitvoering van een overeenkomst*” is hiermee niet bruikbaar om persoonsgegevens te verwerken, echter verwerkt Bedrijfsgezondheidsdienst Noord West persoonsgegevens om te voldoen

aan haar wettelijke verplichtingen, onder andere in het kader van de arbeidsomstandighedenwetgeving en de Regeling procesgang eerste en tweede ziektejaar.

3.3 Secundaire persoonsgegevens

3.3.1 Identificatie

Indien dit in belang is van de begeleiding/behandeling, worden navolgende gegevens vastgelegd:
Conform beschreven verwerking worden navolgende gegevens vastgelegd:

Of sec de volgende gegevens worden vastgelegd.

	Datum eerste verzuimdag
	De werkzaamheden waartoe men niet of nog wel tot toe in staat is (beperkingen en of mogelijkheden), periode AT
	Vermoedelijke duur van het verzuim
	Aantal uren & beperkingen
	Of en wanneer een interventie is ingezet
	Gegevens behandelend huisarts, specialist

3.3.2 Legitimatie

Dit zijn gegevens over de gezondheid die de werkgever, en artsen moeten verwerken ten einde de werkgever te ondersteunen ten aanzien van de Wet Verbeterde Poortwachter. De gegevensverwerking is derhalve noodzakelijk voor het nakomen van een wettelijke verplichting.

3.3.3 Bijzondere persoonsgegevens

De heer Craanen is functionaris verwerking bijzondere persoonsgegevens van BGD NW (0229 820230).
Identificatie

	Burgerservicenummer
	Geslacht
	De (actuele) gezondheidstoestand (specialistische informatie) van de verzuimende

3.3.4 Legitimatie

Gegevens over levensovertuiging, gezondheid en zaken met betrekking tot de seksualiteit, of strafrechtelijke gegevens worden bijzondere gegevens genoemd. Het verwerken van bijzondere persoonsgegevens is in principe verboden. Behalve indien dit op grond van de AVG of op grond van een specifieke wettelijke regeling is toegestaan.

In het kader van een zorgvraag aan Bedrijfsgezondheidsdienst Noord West worden gegevens verwerkt in het kader van gezondheidszorg, medisch onderzoek, hulpverlening en of re-integratie. In het proces van ziekte en gebrek rondom verzuim is de verwerking voorbehouden aan de bedrijfsarts van Bedrijfsgezondheidsdienst Noord West. In het kader van verzuimomstandigheden door ziekte en of gebrek is het verwerken van medische gegevens eveneens voorbehouden aan de bedrijfsarts van Bedrijfsgezondheidsdienst Noord West. In laatstbenoemde notitie is verwerking toegestaan omdat deze verwerking wordt uitgevoerd door beroepsbeoefenaren met een beroepsgeheim (en andere personen die aan geheimhouding gebonden zijn). Deze uitzondering geldt dus op basis van de Wet op de geneeskundige behandelovereenkomst (WGBO).

De Wet op de geneeskundige behandelovereenkomst en de Wet op de Beroepen in de Individuele Gezondheidszorg (wet BIG) vormen de grondslag voor het medisch handelen van de bedrijfsarts binnen Bedrijfsgezondheidsdienst Noord West. Alle gegevens over de gezondheid van werknemers vallen onder het medisch beroepsgeheim. Dit betreffen onder andere:

1. specifieke klachten of pijn aanduidingen, diagnoses,
2. Objectieve en subjectieve waarnemingen van de bedrijfsarts, o.a. indien van toepassing de fysieke en mentale gesteldheid. zowel over geestelijke als lichamelijke gezondheidstoestand
3. Gegevens over therapieën, afspraken met artsen, fysiotherapeuten, psychologen, etc.

3.3.5 Taakdelegatie en geheimhouding

Bij Bedrijfsgezondheidsdienst Noord West kan de bedrijfsarts een deel van zijn (medische) taken in het kader van de verzuimbegeleiding delegeren aan de Arbo-artsen en doktersassistenten. Genoemde functionarissen vallen onder de zogenoemde verlengde armconditie van de bedrijfsarts. En mogen in dat geval in het kader van diens werkzaamheden beschikken over medische informatie die voor de uitoefening van zijn of haar taken strikt noodzakelijk is.

3.3.6 De kwestie Case managers

Bedrijfsgezondheidsdienst Noord-West heeft geen casemanagers in dienst. Volledigheidshalve dient gesteld te worden dat indien een externe casemanager enkel het casemanagement van de werkgever verzorgt, er beslist geen sprake is van delegatie van taken van de bedrijfsarts aan de casemanager. In dit geval mag de externe casemanager dan net als de werkgever niet vragen naar gegevens over aard en oorzaak van de ziekte en die gegevens ook niet opslaan, ook als die spontaan, vrijwillig door de werknemer worden verstrekt.

3.3.7 Het Burger Service Nummer (BSN)

Het Burgerservicenummer (BSN) is een persoonsnummer dat in de eerste plaats bedoeld is voor het contact tussen burgers en de overheid. Organisaties buiten de overheid mogen het BSN alleen gebruiken als dat wettelijk is bepaald. Het BSN is een uniek en tot de persoon herleidbaar nummer. Daarom is het een zogeheten “*bijzonder*” persoonsgegeven. Voor het gebruik van bijzondere persoonsgegevens gelden extra strenge regels. Een nummer dat bij wet is voorgeschreven om een persoon te identificeren, mag alleen worden gebruikt voor de uitvoering van die wet of voor doeleinden die in de wet staan. Dat staat in artikel 24 van de Wet bescherming

persoonsgegevens. Het BSN is zo’n identificatienummer. Organisaties kunnen het verbod om het BSN te gebruiken niet doorbreken door toestemming aan mensen te vragen voor het gebruik van hun BSN.

Bedrijfsgezondheidsdienst Noord-West is echter een zorgverlener in haar hoedanigheid als Arbodienst. Om werkzaamheden uit te kunnen voeren voor de re-integratie alsmede in de communicatie heeft Bedrijfsgezondheidsdienst Noord West het BSN van een (verzuimende medewerker) nodig. Bedrijfsgezondheidsdienst Noord-West heeft het BSN van cliënt nodig om in zijn of haar zorgvraag te kunnen voorzien.

De werkgever is verplicht om alle noodzakelijke informatie aan de arbodienst door te geven zodat Bedrijfsgezondheidsdienst Noord West adequaat in haar dienstverlening kan voorzien. Indien er geen zorgvraag is ten gevolge van ziekte en of gebrek (een werknemer staat niet ziek) dan noodzaak/noodzaak/ grondslag tot kennisneming van het BSN. Kort samengevat mag Bedrijfsgezondheidsdienst Noord West in haar hoedanigheid als gecertificeerde Arbodienst op grond van artikel 14 lid 6 van de Arbeidsomstandighedenwet het BSN verwerken in het kader van verzuimomstandigheden op medische gronden.

4 Doelbinding

Persoonsgegevens worden door de Bedrijfsgezondheidsdienst Noord West uitsluitend verwerkt voor een welbepaald uitdrukkelijk en gerechtvaardigd doel. In onderhavig onderzoek wordt deze doelbinding nader omschreven.

4.1 Doeleinden van de persoonsgegevens die worden verwerkt.

Bedrijfsgezondheidsdienst Noord-West verwerkt persoonsgegevens ten behoeve van:

1. De zorg voor arbeidsomstandigheden in bedrijven en instellingen welke een overeenkomst hebben gesloten met Bedrijfsgezondheidsdienst Noord West;
2. De sociaal medische verzuimbegeleiding van werknemers van bedrijven en instellingen die een overeenkomst hebben met Bedrijfsgezondheidsdienst Noord West;
3. De re-integratie van werknemers van bedrijven en instellingen die een overeenkomst hebben met Bedrijfsgezondheidsdienst Noord West.
4. Het verzorgen (uitvoeren en archiveren) van medische keuringen van bedrijven en instellingen;
5. Het verzorgen van medische keuringen ten behoeve van rijvaardigheidsbewijzen;
6. Het signaleren, registreren en melden van beroepsziekten;

4.2 Voorwaarden voor de verwerking

Bedrijfsgezondheidsdienst Noord-West zal niet meer gegevens in de registratie opslaan of bewaren dan voor het doel van de persoonsregistratie nodig is (zie 3.1). Persoonsgegevens worden alleen verwerkt door medewerkers van Bedrijfsgezondheidsdienst Noord West die uit hoofde van ambt, beroep of wettelijk voorschrift, dan wel krachtens een overeenkomst tot geheimhouding zijn verplicht. Van belang is om aan te geven dat eenieder die handelt onder het gezag van Bedrijfsgezondheidsdienst Noord West verplicht is tot geheimhouding van de persoonsgegevens waarvan hij of zij kennisneemt, behoudens voor zover enig wettelijk voorschrift hem tot mededeling verplicht of uit zijn taak voortvloeit.

Het Burgerservicenummer (BSN) dat ter identificatie van een persoon bij wet is voorgeschreven, wordt bij de verwerking van persoonsgegevens slechts gebruikt ter uitvoering van de betreffende wet dan wel voor doeleinden bij de wet bepaald.

4.3 Rechtmatige grondslag van de verwerking

De vastlegging van (medische) persoonsgegevens in verband met medische keuringen, ziekteverzuim en re-integratie zijn gebaseerd op de Wet op de geneeskundige behandelovereenkomst (WGBO), de Wet op de Beroepen in de Individuele Gezondheidszorg (wet BIG), Wet Algemene Bepalingen Burgerservicenummer, de Wet op de Medische Keuringen (WMK), de KNMG-code "Gegevensverkeer en samenwerking bij arbeidsverzuim en re-integratie (2007)",

KNMG-advies voor "Inrichting en overdracht van het bedrijfsgeneeskundig dossier (april 2009),

KNMG-richtlijn inzake het "Omgaan met medische gegevens (januari 2010)", en beroepscode van de kerndeskundigen.

4.4 Dossierplicht

Op grond van de Wet op de geneeskundige behandelingsovereenkomst (WGBO) is de BGD NW als zorgverlener verplicht een medisch dossier bij te houden.

4.5 Bewaartermijn en opschonen dossiers

De hoofdregel voor het bewaren van medische dossiers staat in de WGBO. Dat is 15 jaar, gerekend vanaf de datum van vastlegging van ieder afzonderlijk gegeven. De termijn kan langer zijn indien dit noodzakelijk is met het oog op de behandeling (bijvoorbeeld indien iemand een chronische ziekte heeft). Uitzonderingen op de hoofdregel:

1. Aanstellingskeuringsdossiers worden maximaal 6 maanden bewaard;
2. Medische dossiers worden maximaal 15 jaar bewaard tenzij er sprake is van een beroepsziekte. In dit geval moete het dossier langer bewaard worden dan nodig. Inschatting van deze termijn wordt gedaan door de (meldend) bedrijfsarts.
3. Asbestdossiers kennen een bewaartermijn van 40 jaar.
4. Keuringen in het kader van rijvaardigheidsbewijzen worden bewaard conform de duur van het rijbewijs.

Door de leverancier van VerzuimXpert is de signaalfunctie op bewaartermijnen geautomatiseerd. Bedrijfsgezondheidsdienst Noord-West heeft bovengenoemde bewaartermijnen ingesteld per type dossier. Maandelijks wordt er een rapport vanuit VerzuimXpert gegenereerd die aankondigt dat over 30 dagen de volgende gegevens opgeschoond gaan worden. Vervolgens wordt automatisch geschoond "bij niet ingrijpen" vanuit Bedrijfsgezondheidsdienst Noord West

4.6 Dataminimalisatie, noodzakelijkheid, proportionaliteit en subsidiariteit

Bedrijfsgezondheidsdienst Noord-West is zich bewust van het feit dat de verwerking van persoonsgegevens uitsluitend geschiedt in overeenstemming met de privacywetgeving waarbij niet meer gegevens worden verwerkt dan noodzakelijk. Maandelijks wordt er een interne audit op naleving van privacyaspecten uitgevoerd, waarin dataminimalisatie een belangrijk item is.

Het beginsel van proportionaliteit betekent dat de inbreuk op de privacy van een betrokkene evenredig moet zijn aan het doel dat wordt beoogd met de verwerking. Deze belangenafweging is bij het opstellen van het register van verwerkingsactiviteiten genomen.

Het subsidiariteitsbeginsel houdt in dat het doel waarvoor de persoonsgegevens worden verwerkt redelijkerwijze niet op een andere, voor betrokkene minder nadelige wijze, kan worden bereikt.

5 Informatievoorziening

5.1 Algemeen kader (privacyverklaring)

Bedrijfsgezondheidsdienst Noord-West dient, vanuit haar rol als verwerkingsverantwoordelijke, de personen van wie zij persoonsgegevens verwerkt, te informeren. Onder meer over de over de werkwijze van de Arbodienst (rechten en plichten van medewerkers), de dossierplicht (bewaartermijnen), verplichtingen als gevolg van de WGBO, beroepscode, etc.

Bedrijfsgezondheidsdienst Noord-West heeft als Arbodienst geen overeenkomst met de werknemer zelf, maar alleen met de werkgever. De grondslag voor de verwerking van persoonsgegevens is hiermee niet het uitvoeren van een overeenkomst, maar het uitvoeren van een wettelijke verplichting.

Bedrijfsgezondheidsdienst Noord-West heeft onderhavig privacy beleid op de website geplaatst zodat deze voor eenieder na te lezen is. Conform Artikel 13 van de AVG zijn navolgende aspecten opgenomen in het privacy beleid van Bedrijfsgezondheidsdienst Noord West:

1. De identiteit en contactgegevens van Bedrijfsgezondheidsdienst Noord West;
2. De naam en contactgegevens van de Functionaris voor de Gegevensbescherming;
3. Een overzicht van de categorieën van persoonsgegevens die door de BGD NW verwerkt worden;
4. De verschillende doeleinden waarvoor de gegevens worden verwerkt;
5. De grondslagen op basis waarvan de gegevens worden verwerkt;
6. Een overzicht van intern en externe toegang tot de persoonsgegevens;
7. Een overzicht van de bewaartermijnen;
8. De rechten van betrokkene waaronder de klachtenmogelijkheid bij de Autoriteit Persoonsgegevens.

Aan eigen medewerkers van Bedrijfsgezondheidsdienst Noord West wordt voorlichting en instructie gegeven op het gebied van privacy. Aan medewerkers wordt verzocht een verklaring te tekenen waarin zij zich conformeren aan het beleid dat de Bedrijfsgezondheidsdienst Noord West voert in het kader van privacy.

Naast het recht op informatie, hebben betrokkenen het recht op inzage, het recht op correctie, het recht op gegevenswissing en het recht op gegevensoverdracht. Daarnaast kunnen betrokkenen bezwaar maken tegen de verwerking van hun persoonsgegevens wegens bijzondere persoonlijke omstandigheden.

5.1.1 Recht op inzage

Op grond van artikel 15 AVG heeft een betrokkene het recht om inzage te vragen in de persoonsgegevens die van hem of haar worden verwerkt. Bedrijfsgezondheidsdienst Noord-West zal binnen één maand na dit verzoek een overzicht verstrekken met de gegevens die geregistreerd worden. Feitelijk betreft het hier een overzicht van de drie categorieën persoonsgegevens zoals/ zoals eerder beschreven in hoofdstuk 2.

Aan betrokkene kunnen op verzoek kopieën worden verstrekt van gegevens die van hem of haar verwerkt worden. Het doel van het recht op inzage is dat een betrokkene zich een beeld kan vormen over wat er met zijn of haar persoonsgegevens gebeurt en kan controleren of deze juist zijn en of de juiste waarborgen zijn getroffen door de verwerkingsverantwoordelijke.

5.1.2 Recht op rectificatie en aanvulling

Als persoonsgegevens niet kloppen en of onvolledig zijn (bijvoorbeeld een onjuist adres), dan kan betrokkene op grond van artikel 16 AVG een verzoek doen op rectificatie en aanvulling. In dit geval zal Bedrijfsgezondheidsdienst Noord West er zorg voor dragen dat onjuiste persoonsgegevens worden aangepast. Let wel het betreft hier “onjuiste” persoonsgegevens. Indien betrokkene het niet eens is met de inhoud, kan hij of zij niet met een beroep op rectificatie een wijziging van een rapportage eisen.

5.1.3 Recht op gegevenswissing

Nieuw in de AVG is dat betrokkene het recht hebben om vergeten te worden (artikel 17 AVG). Het betreft hier het recht om persoonsgegevens te laten wissen die bijvoorbeeld niet meer relevant zijn of onrechtmatig verwerkt zijn. Ook kan een beroep worden gedaan op het wissen van persoonsgegevens na het intrekken van een toestemming voor de verwerking. Ook heeft een betrokkene op grond van artikel 18 AVG het recht om te vragen dat er **minder** gegevens worden verwerkt. Echter de wettelijke bewaartermijnen gaan boven dit recht.

5.1.4 Recht op dataprotaliteit

Een betrokkene heeft het recht om zijn of haar persoonsgegevens die digitaal zijn verwerkt “in een gangbare en machinaal leesbare vorm” te verkrijgen en over te dragen aan een andere dienstverlener.

5.1.5 Toegang tot de Persoonsgegevens.

Bedrijfsgezondheidsdienst Noord-West maakt onderscheidt tussen zogenoemde “interne toegang”, dit zijn de medewerkers van de eigen organisatie en medewerkers van externe organisaties (externe toegang).

Bij de inrichting van de digitale verzuimapplicatie VerzuimXpert is een classificatie gemaakt van bevoegdheden. Navolgende rollen en toegankelijkheden worden hierin onderscheiden.

5.1.6 Legenda:

	Volledige toegang
	Geen toegang
	Toegang op basis van de verlengde armconstructie (onder auspiciën bedrijfsarts)

De artsen van Bedrijfsgezondheidsdienst Noord West hebben toegang tot persoonsgegevens categorie 3. Hier is het medisch beroepsgeheim op van toepassing. De doktersassistenten (medewerkers van de verzuimadministratie) hebben eveneens toegang tot de persoonsgegevens categorie 3. Dit is geregeld via de zogenoemde verlengde arm constructie van de bedrijfsarts. In arbeidsovereenkomst met betrokkene medewerkers, is de kwestie geheimhouding expliciet vastgelegd.

Bedrijfsgezondheidsdienst Noord-West is een “opleidingsarbodienst”. Dit is de reden dat er met collega’s, of in intervisiegroepen casuïstiek uit de praktijk wordt besproken. Uitgangspunt is dat dit altijd anoniem en onherkenbaar plaats vindt. Regelmatig wordt er in het kader van opleidingsomstandigheden of intervisie geanonimiseerd niet herleidbare casuïstiek geëvalueerd.

5.2 Externe toegang

Bedrijfsgezondheidsdienst Noord-West is binnen haar gebruikelijke werkzaamheden altijd een verwerkingsverantwoordelijke. Medewerkers van Bedrijfsgezondheidsdienst Noord West verwerken namelijk gegevens waar de werkgever geen toegang toe heeft. Bovendien heeft Bedrijfsgezondheidsdienst Noord West deze verwerking ook zelf ingericht. Te denken hierbij aan het verwerken van gegevens van artsen, medische gegevens en persoonlijke omstandigheden van zieke werknemers. De reguliere werkzaamheden bestaan uit sociaal medische verzuimbegeleiding, periodiek arbeidsdeskundig onderzoek, medische keuringen en verzuimanalyses. De gegevensverwerking die met deze activiteiten gepaard gaan, maken dat Bedrijfsgezondheidsdienst Noord West verwerkingsverantwoordelijke is.

Bovengenoemde is dan ook de reden dat Bedrijfsgezondheidsdienst Noord West heeft vastgelegd welke externe personen of bedrijven (= de groep verwerkers) toegang hebben tot bepaalde persoonsgegevens en of met welke externe partijen(n) persoonsgegevens worden gedeeld. Met deze externe personen of bedrijven die tot de groep verwerkers behoren, sluit Bedrijfsgezondheidsdienst een verwerkersovereenkomst.

	Categorie 1 Gegevens werkgever (NAW)	Categorie 1 Primaire Persoonsgegevens (NAW)	Categorie 2 Secundaire persoonsgegevens Verzuimhistorie Poortwachter documenten	Categorie 3 Bijzondere persoonsgegevens Medische gegevens BSN
Directie				
Kwaliteitsmanager				
Bedrijfsarts				
Arts, AIO				
Verzuimadministratie				
Kerndeskundigen anders dan bedrijfsarts				
financiële administratie				
Arbeidsdeskundige				
Externe deskundigen				
Relatiebeheerder				

Voor de volledigheid dient opgemerkt te worden dat het zo kan zijn dat Bedrijfsgezondheidsdienst Noord West (t.o.v. opdrachtgever) naast verwerkingsverantwoordelijke ook verwerker is. Dit is het geval indien Bedrijfsgezondheidsdienst Noord West, naast de reguliere kerntaken als arbodienst, ook specifiek gegevens ten behoeve van de opdrachtgever verwerkt. In dat geval verwerkt Bedrijfsgezondheidsdienst Noord West persoonsgegevens ten behoeve van de verwerkingsverantwoordelijke. In dit geval mag de Bedrijfsgezondheidsdienst Noord West geen enkele zeggenschap hebben over de wijze van verwerking van de gegevens. De regel is dat: “zodra de

gegevens naar eigen inzicht worden ingericht (of gebruikt)", Bedrijfsgezondheidsdienst Noord West verwerkingsverantwoordelijke is.

5.3 Verwerkersovereenkomst

Er zijn situaties waarin er externe leveranciers zijn die de persoonsgegevens uit het cliëntendossier *zouden kunnen* inzien. Met deze leveranciers heeft Bedrijfsgezondheidsdienst Noord West een zogenoemde verwerkersovereenkomst afgesloten. Bedrijfsgezondheidsdienst Noord-West is van mening dat dit niet wenselijk is en heeft getracht om dit zoveel mogelijk te beperken. Op dit moment hebben toegang tot de gegevens van Bedrijfsgezondheidsdienst Noord West:

1. Otherside at Work als de leveranciers van het programma VerzuimXpert waarin de digitale cliëntendossiers zijn opgenomen.
2. De Smeth & Kok te Hoorn (inclusief Ziggo, internet toegang)
3. Administratiekantoor Winkelaar (uitsluitend financiële gegevens)

5.4 UWV

Aan het UWV mag voor zover wettelijke verplichtingen (artikel 54 lid 1 en 3 sub c SUWI) daartoe rechtvaardigen, informatie worden verschaft. In de overige situatie mag dat uitsluitend met uitdrukkelijke en gerichte toestemming van de werknemer.

6 Beveiliging van de persoonsgegevens

Bedrijfsgezondheidsdienst Noord-West heeft technische en organisatorische maatregelen genomen om het verlies van persoonsgegevens of onrechtmatige verwerking tegen te gaan. Bewust is beknopt in het navolgende een uiteenzetting gegeven van maatregelen.

6.1 Technische maatregelen vanuit de BGD NW

Ten behoeve van de technische infrastructuur van Bedrijfsgezondheidsdienst Noord West is een contract gesloten met een externe deskundige ICT-organisatie, namelijk De Smeth & Kok te Hoorn.

4. De verzuimapplicatie die door Bedrijfsgezondheidsdienst Noord West wordt gebruikt, wordt ontsloten via internet. De toegang tot de applicatie is uitsluitend mogelijk met een zogenoemde meerfactorauthenticatie.);
5. Toegangscontroles, computers zijn voorzien van wachtwoorden. Iedere PC is voorzien van een schermbeveiliging;
6. Vastlegging van gebruik van systemen en applicaties is geregeld via inlogcodes;
7. Toepassing van Privacy Enhancing Technologies (PET);
8. Toepassen van een solitair netwerk, uitsluitend bereikbaar voor bevoegde medewerkers van Bedrijfsgezondheidsdienst Noord West;
9. Toepassing diverse beveiligingsschillen (firewall, up to date virusscanner, toepassing recente patches voor gebruikte software);
10. De gegevens binnen verzuimXpert worden gecrypt verstuurd;
11. De externe ICT-partner draagt er zorg voor dat regelmatig de laatste versie update van gebruikte software geïnstalleerd wordt.

6.2 Technische maatregelen in relatie tot de veruimapplicatie VerzuimXpert

Otherside at work (de leverancier en beheerder van VerzuimXpert) heeft een ISO-27001 certificaat. Hiermee is het managementsysteem waarmee Otherside at work de risico's rondom de beschikbaarheid en beveiliging van VerzuimXpert beheerd volgens de internationale standaard geauditeerd, gecertificeerd en geaccrediteerd. Jaarlijks worden bij Other side at work audits gehouden waarna een ISAE3402 type II verklaring wordt afgegeven.

Data wordt tegen vernietiging beschermd door middel van een back-up proces dat de afgelopen 7 dagen, 3 weken (voor die 7 dagen) en 11 maanden (voor die 2 weken) wordt uitgevoerd op klantbases (effectief dus tot maximaal 12 maanden terug). De Back-ups worden geencrypt en periodiek getoetst door middel van restores. Doordat er losse back-ups per klant zijn, is restoren per klant mogelijk. Otherside kan mede hierdoor eenvoudig garanderen dat, indien dit gewenst is, alle data van een specifieke klant gewist wordt.

Het Webverkeer is altijd beveiligd via SSL. De dataservers zijn niet rechtstreeks te benaderen en per klant van Other side at Work gescheiden. Opgeslagen data worden middels het TDE-mechanisme van SQL-servers geencrypt en er vindt daarnaast cell-level encryptie plaats voor medische gegevens die door de artsen worden ingevoerd. De cell-level encryptie vindt plaats via de applicatie met een klant- en applicatiesleutel.

6.3 Organisatorische maatregelen

Bedrijfsgezondheidsdienst Noord-West heeft een ISO 9001:2015 managementcertificaat hetgeen aangeeft dat de organisatie op een beheerste wijze omgaat met haar processen. Voor de specifieke kerntaken die voortvloeien uit de arbeidsomstandigheden wetgeving is Bedrijfsgezondheidsdienst Noord West geaudit ten aanzien van de Regeling dienstverlening Arbodiensten. Jaarlijks wordt Bedrijfsgezondheidsdienst Noord West geaudit door een externe certificerende instantie (Loyds) die onder meer beoordeelt of er voldaan wordt aan de eisen die voortvloeien uit de AVG. Naast een stringent bevoegdhedenbeleid (zie 5.1) waarin de toegang tot persoonsgegevens verbonden is aan rollen, heeft Bedrijfsgezondheidsdienst Noord West navolgende organisatorische maatregelen getroffen:

1. Volgens artikel 37 van de AVG geldt de verplichting tot het aanstellen van een Functionaris voor de Gegevensbescherming (FG) indien er (grootschalig) bijzondere persoonsgegevens worden verwerkt. Bedrijfsgezondheidsdienst Noord-West heeft meerdere artsen in dienst en op basis hiervan is geconsolideerd dat er een verplichting is tot het aanstellen van een FG.
2. Bedrijfsgezondheidsdienst Noord-West maakt gebruik van de webapplicatie VerzuimXpert.
3. De leverancier *other side at work* te Den Bosch beschikt over een BSI Certificaat (informatiebeveiligingssysteem ISO/IEC 27001:2005. Tijdens de jaarlijkse Leveranciersbeoordeling wordt nadrukkelijk op geaudit op de geldigheid van dit document.
4. De applicatie voldoet aantoonbaar aan de beveiligingseisen uit artikel 13 Wbp
5. Via een bevoegdheden matrix is vastgelegd welke functionaris van Bedrijfsgezondheidsdienst Noord West, welke bevoegdheden heeft in VerzuimXpert;
6. Voor keuringsdoeleinden wordt gewerkt met papieren cliëntdossiers. Deze worden in een afgesloten kast bewaard.
7. Er wordt volgens een vast stramien een back-up gedraaid van alle data van Bedrijfsgezondheidsdienst Noord West.

8. De papieren keuringsdossiers van de rijvaardigheidsbewijzen (CBR), worden in een afgesloten ruimte bewaard.
9. Medewerkers van Bedrijfsgezondheidsdienst Noord West die Ambulant werken, hebben een laptop die beveiligd is met een wachtwoord/ bit locker. De verzuimapplicatie is beveiligd middels de tweefactorauthenticatie en derhalve niet benaderbaar zonder een speciek mobiel telefoontoestel. Van de laptops worden dagelijks back-ups gemaakt.
10. Bedrijfsgezondheidsdienst Noord-West hanteert een streng "clean desk policy".

7 Toezicht op naleving privacyaspecten

7.1 Preventief

De functionaris voor de Gegevensbescherming ziet erop toe dat Bedrijfsgezondheidsdienst Noord West de AVG naleeft conform afspraken zoals in de wet beschreven. In zijn rol informeert en adviseert de FG de organisatie en de medewerkers. De FG is verantwoordelijk voor de actualiteit van onderhavig privacy reglement en ziet toe op een periodieke voorlichting en instructie aan eigen medewerkers.

De geregistreerde bedrijfsarts heeft als belangrijke taak, naast zijn reguliere werkzaamheden, het toezicht houden op de naleving van de privacy door alle medewerkers (inclusief inhuur) van Bedrijfsgezondheidsdienst Noord West. Eens per maand wordt een steekproef gehouden waarbij de geregistreerde bedrijfsarts, samen met de kwaliteitsmanager (tevens FG), een aantal activiteiten beoordeeld op de naleving van privacy. Het betreft hier minimaal;

1. 3 verzuimintakes
2. 3 terugkoppelingen spreekuur bedrijfsarts
3. 3 probleemanalyses
4. 3 e-mails aan werkgevers, hoe doet BGD NW dit
5. 3 facturen
6. 1 PAGO/ PMO verslag (indien van toepassing)
7. 1 SMT verslag (indien van toepassing)

De activiteiten worden afzonderlijk beoordeeld op grond van navolgende criteria:

1. Worden diagnoses, naam ziekte, specifieke klachten en of pijn aanduidingen benoemd?
2. Bevat het te beoordelen document "persoonlijke" subjectieve waarnemingen van de arts,
3. zowel over geestelijke als lichamelijke gezondheidstoestand?
4. Wordt in het document verwezen naar specialisten en of gegevens over therapieën, afspraken met artsen, fysiotherapeuten, psychologen, etc?
5. Bevat het document verwijzingen naar situationele problemen zoals relatieproblemen, problemen uit het verleden, verhuizingen, overlijden partner, scheiding, etc). De resultaten van de rapportages worden besproken zowel in het kerndeskundigenoverleg als het artsenoverleg. Corrigerende en preventieve maatregelen worden vanuit het artsenoverleg geïnitieerd en waar nodig bewaakt.

Eens per jaar wordt een zogenoemde interne audit uitgevoerd. Onderdeel van de interne audit is de zogenoemde gegevensbeschermingseffectbeoordeling. In het Engels ook wel Data Protection Impact Assessment (DPIA) genoemd. Tijdens de audit worden navolgende onderwerpen beoordeeld:

1. De mate van pseudonimisering (of anonimisering) en versleuteling van persoonsgegevens
2. Evaluatie analyse zorgvuldigheidbeginsel anonimisering encryptie van Persoonsgegevens
3. De competentie om op permanente basis de vertrouwelijkheid, integriteit en beschikbaarheid van de digitale systemen te kunnen garanderen
4. De adequaatheid van handelen van Bedrijfsgezondheidsdienst Noord West om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen.
5. Beoordeling van de doeltreffendheid van de genomen technische en organisatorische maatregelen ten einde te voldoen aan de AVG

Naast de periodieke audits op de naleving van privacyaspecten wordt jaarlijks tijdens de externe audit door een externe instantie de gehele organisatie en omgang op dit aspect beoordeeld en waar nodig bijgesteld.

7.2 Correctief “Datalekken”

De meldplicht datalekken was al van kracht op 1 januari 2016. Deze meldplicht houdt in dat Bedrijfsgezondheidsdienst Noord West direct en uiterlijk binnen 72 uur na het datalek een melding moet doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek heeft vastgesteld.

Voorbeelden van datalekken zijn: een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak in een databestand door een hacker.

De stelregel van Bedrijfsgezondheidsdienst Noord West is, dat alle (veronderstelde) datalekken gemeld moeten worden aan de FG (Guus Craanen). Deze zal vanuit hoofde van zijn functie beoordelen of er een melding dient plaats te vinden aan de AP. Dit is in de regel het geval in navolgende situatie:

1. Een datalek leidt tot ernstige nadelige gevolgen voor de bescherming van persoonsgegevens;
2. Er een aanzienlijke kans bestaat dat dit gebeurt;
3. Er persoonsgegevens verloren zijn gegaan (niet meer terug te halen);
4. Er sprake is van onrechtmatige verwerking van persoonsgegevens (iemand heeft toegang (gehad) tot persoonsgegevens terwijl diegene daartoe niet bevoegd was en er is geen controle over wat diegene met de gegevens heeft gedaan of nog zal doen).

De FG zal tevens de betrokkene informeren indien het datalek ongunstige gevolgen heeft voor hun persoonlijke levenssfeer. Dat kan het geval zijn als er gegevens van gevoelige aard zijn gelekt (bijvoorbeeld gezondheidsgegevens). De FG houdt een register bij van meldingen.