

Data uitwisseling beleid

Privacy is voor Het Nieuwe Verzuim een belangrijk onderwerp. Doordat wij u als werkgever en medewerker ondersteunen bij verzuimbegeleiding, Risico Inventarisatie & Evaluatie, Periodiek Medische Onderzoeken, open spreekuur en/of (aanstellings)keuringen is het noodzakelijk om over de persoonsgegevens te beschikken. Indien het gaat over persoonsgegevens, komt al snel de Algemene Verordening Gegevensbescherming (AVG) om de hoek kijken. Conform de AVG is het versturen, opslaan, bewerken en gebruiken van persoonsgegevens aan strenge eisen verbonden.

De meest voorkomende vorm waarin afspraken over het werken met persoonsgegevens tussen twee organisaties wordt vastgelegd, is door middel van beleid rondom dataverwerking. Conform de AVG is het verplicht om tussen een verwerker en een verantwoordelijke een beleid te hebben rondom dataverwerking. Het Nieuwe Verzuim treedt echter in haar dienstverlening jegens haar klanten niet op als verwerker maar als een zelfstandig verantwoordelijke. Dit volgt uit de aard van de dienstverlening en uit de visie van de Autoriteit Persoonsgegevens (AP). Het Nieuwe Verzuim verricht binnen de grenzen van de opdracht zelfstandig haar werkzaamheden en verwerkt derhalve als verantwoordelijke de verstrekte persoonsgegevens.¹

U, als werkgever en/of medewerker, bent ook aan te wijzen als verantwoordelijke. Nu Het Nieuwe Verzuim niet aan te wijzen is als verwerker maar als verantwoordelijke en u als werkgever en/of medewerker ook, is een verwerkersovereenkomst in de zin van de AVG niet verplicht. Een verwerkersovereenkomst zou geen juridische waarde hebben.

Het Nieuwe Verzuim wil echter toch duidelijk zijn met wat wordt vastgelegd en hoe omgegaan wordt met de verstrekte persoonsgegevens. Dit doen wij door middel van dit beleid rond data-uitwisseling tussen twee verantwoordelijken.

Het Nieuwe Verzuim heeft in het kader van de AVG een verwerkingsovereenkomst gesloten met de leverancier van ons digitale verzuimsysteem.

In aanmerking nemende dat:

Het Nieuwe Verzuim en opdrachtgever informatie uitwisselen ten doel van de bedrijfsgezondheidszorg (preventie en verzuim);

De uit te wisselen informatie persoonsgegevens zoals bedoeld in de Algemene Verordening Gegevensbescherming (AVG), kán bevatten;

- Partijen volgens Artikel 26, lid 1 van de AVG beide zelfstandig Verwerkingsverantwoordelijk(e) zijn;
- Partijen, gelet op het bovenstaande, volgen volgens het beleid data uitwisseling van Het Nieuwe Verzuim.

Artikel 1 Algemeen

1.1 Het gestelde in de overwegingen maakt deel uit van deze overeenkomst.

1.2 Termen in dit beleid die verwijzen naar overeenkomstige termen uit de AVG, hebben in dit beleid de betekenis zoals omschreven in de AVG.

Artikel 2 Voorwerp beleid

2.1 Opdrachtgever verstrekt aan Het Nieuwe Verzuim, persoonsgegevens in de vorm van NAW, BSN-nummer (bij verzuim), Persnr, geslacht, geboortedatum, telnr, mailadres, dienstverband gegevens, afdeling, functie, uren per week en de standplaats die door Het Nieuwe Verzuim vervolgens verwerkt worden ten behoeve van de bedrijfsgezondheidszorg.

2.2 Op haar beurt verstrekt Het Nieuwe Verzuim, opdrachtgever re-integratie adviezen in de vorm van mogelijkheden en beperkingen ten aanzien van het werk dat door opdrachtgever verwerkt wordt ten behoeve van de re-integratie van verzuimende werknemers.

2.3 Voornoemde uitwisseling van gegevens vindt plaats binnen een adequaat beveiligde digitale omgeving.

2.4 Het Nieuwe Verzuim legt bijzondere persoonsgegevens van werknemers van opdrachtgever vast in het medische deel van haar digitale verzuimapplicatie.

2.5 Partijen verwerken slechts de hierboven genoemde persoonsgegevens voor zover dit doelmatig is.

Artikel 3 Geheimhouding

3.1 Partijen zullen de informatie uitsluitend gebruiken voor het doel waarvoor deze gegeven is.

3.2 Partijen zullen de verspreiding van de informatie binnen de organisatie beperken tot werknemers die deze informatie beroepsmatig nodig hebben en deze informatie vertrouwelijk behandelen.

3.3 Partijen zullen de informatie, voor zover het persoonsgegevens betreft, behandelen overeenkomstig de geldende wet- en regelgeving inzake omgang met en bescherming van persoonsgegevens.

Artikel 4 Gezamenlijke verplichtingen

4.1 Partijen informeren de betrokkenen zelfstandig over de doeleinden waarvoor persoonsgegevens worden verwerkt in hun eigen privacyverklaring en verwerken de persoonsgegevens niet anders dan waarvoor zij zelf een wettelijke grondslag hebben.

4.2 Partijen staan in voor de rechtmatige verwerking van de verkregen persoonsgegevens en zijn zelfstandig verantwoordelijk voor de naleving van alle wettelijke verplichtingen met betrekking tot het verwerken van persoonsgegevens.

4.3 De verplichtingen die voortvloeien uit dit beleid, gelden ook voor degenen die onder het gezag van Partijen persoonsgegevens verwerken, zoals maar niet beperkt tot werknemers.

4.4 Partijen zijn gehouden tijdens verzending en verwerking voldoende technische en organisatorische maatregelen te nemen om de persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking (zoals onbevoegde kennisname, aantasting, wijziging of verstrekking van de persoonsgegevens), en op zijn minst op een niveau dat gelet op de stand van de techniek en de gevoeligheid van de persoonsgegevens redelijk is.

4.5 Partijen zijn en blijven ieder zelfstandig verantwoordelijk voor het melden (binnen 24 uur) van een inbreuk in verband met de beveiliging van persoonsgegevens (datalek) aan de Autoriteit Persoonsgegevens en/of betrokkenen. Indien het datalek ziet op een situatie waarin Partijen als medeverantwoordelijke zijn aan te merken, treden Partijen in overleg met als doel een zorgvuldige en adequate afhandeling van het datalek te realiseren.

Artikel 5 Rechten van betrokkenen

Iedere aansprakelijkheid van opdrachtgever wegens toerekenbare tekortkoming in de nakoming van dit beleid of anderszins is beperkt tot vergoeding van directe schade tot maximaal het bedrag van de voor die overeenkomst bedongen prijs per maand (excl. Btw). Iedere aansprakelijkheid zal in geen geval meer bedragen dan €5.000 (zegge: vijfduizend EURO).

Artikel 6 Rechten van betrokkenen

6.1 In het geval dat een betrokkene een verzoek tot uitoefening van zijn rechten zoals bedoeld in de AVG, richt aan een van de Partijen, zal de Partij het verzoek zelfstandig afhandelen indien het verzoek verband houdt met een verwerking waarvoor de betreffende Partij zelfstandig verantwoordelijke is.

6.2 Indien het verzoek (zoals omschreven in lid 1) verband houdt met een verwerking waarvoor Partijen gezamenlijk verantwoordelijk zijn treden Partijen zo spoedig mogelijk in overleg om vast te stellen welk der Partijen het verzoek af zal handelen.

6.3 Partijen zullen over en weer de noodzakelijke inlichtingen verstrekken en

medewerking verlenen, om de andere Partij in staat te stellen het verzoek (zoals omschreven in lid 1) af te handelen.

6.4 Het Nieuwe Verzuim garandeert dat Opdrachtgever en de betreffende werknemer minimaal 15 jaar kunnen beschikken over het aangelegde dossier. Na deze termijn wordt het dossier verwijderd.

Artikel 7 Beveiligingsafspraken

7.1 Organisatorische maatregelen

Concreet worden de volgende beveiligingsmaatregelen afgesproken (SLA) of toegepast door Het Nieuwe Verzuim:

1. een geïmplementeerd informatiebeveiligingsbeleid binnen de organisatie en het jaarlijks herzien en/of updaten en implementeren van het geüpdatete beveiligingsbeleid;
2. geïmplementeerde interne gedragscode binnen de organisatie;
3. persoonlijke toegangscontroles voor specifiek geselecteerde werknemers middels een autorisatieschema;
4. portabiliteit (de mogelijkheid om Persoonsgegevens over te zetten naar een nieuwe dienstverlener, aan te passen of in te zien, de mogelijkheid Persoonsgegevens permanent te wissen (inclusief back-ups) indien daartoe aanleiding is)
5. het uitvoeren van een geschikte training en regelmatige bijscholing van de werknemers en/of ingeschakelde derden ten aanzien van het informatiebeveiligingsbeleid en informatiebeveiligingsprocedures van provider.

Specifiek wordt aandacht besteed aan het werken met bijzondere Persoonsgegevens.

6. het uitvoeren van jaarlijkse interne en externe audits in het kader van het informatiebeveiliging en ISO 9001/arbodiensten;
7. het aanstellen van een Functionaris Gegevensbescherming.
8. het actief naleven van de beleidsregels 'De zieke werknemer' van de Autoriteit Persoonsgegevens².

7.2 Omschrijving Technische maatregelen (uitvoerder digitale verzuimapplicatie) Concreet worden de volgende beveiligingsmaatregelen afgesproken (SLA) of toegepast:

1. de data wordt opgeslagen bij een organisatie welke ISO 27001/ NEN 7510 gecertificeerd is;
2. opstellen SLA en verwerkingsovereenkomst met de leverancier van het digitale verzuimdossier.
3. veilige wijze voor het opslaan van gegevensbestanden;

4. toegang (logische) uitsluitend middels tweefactorauthenticatie.
5. fysieke bescherming van IT-voorzieningen en apparatuur tegen toegang door onbevoegden;
6. controleren van toegekende rechten aan werknemers van verwerker en verantwoordelijke;
7. logging en controle van toegang tot het systeem (waaronder begrepen het controleren op tekenen van onrechtmatige toegang tot de Persoonsgegevens);
8. encryptie van Persoonsgegevens tijdens elektrische overdracht naar externe partijen, mits een dergelijk overdracht wettelijk en/of contractueel is toegestaan;
9. uitvoeren van penetratietesten op de digitale verzuimapplicatie;
10. toegang tot besturingssysteem is tenminste beschermd door een gebruikersnaam en wachtwoord (minimaal 8 karakters, 1 hoofdletter en een speciaal teken).

7.3 Omschrijving Gedragmatige maatregelen

Concreet worden de volgende beveiligingsmaatregelen afgesproken (SLA) of toegepast:

- 1 geheimhoudingsverplichtingen in (arbeids-)overeenkomsten met interne en externe werknemers;
- 2 het is medewerkers verboden op welke wijze dan ook correspondentie, andere bescheiden, dan wel afschriften daarvan, die hij in verband met zijn werkzaamheden bij werkgever onder zich heeft gekregen, in zijn particuliere bezit te hebben of te houden, behoudens voor zover en voor zolang dit voor de uitoefening van zijn werkzaamheden voor de werkgever is vereist.
- 3 de medewerkers hebben geen bestanden van opdrachtgevers op de laptop of andere datadragers, zonder passende beveiliging. Correspondentie andere documentatie wordt teruggegeven aan de opdrachtgever of vernietigd.

Artikel 8 Slotbepalingen

8.1 Dit beleid is niet overdraagbaar.

Mocht u naar aanleiding van dit beleid nog vragen hebben, dan kunt u contact opnemen met onze Functionaris gegevensbescherming (FG).

¹ De Autoriteit Persoonsgegevens heeft in het rapport 'Onderzoek naar de verstrekking van medische gegevens van werknemers aan werkgevers door arbodienst Perspectief Group B.V.' uit 2013 bevonden dat een arbodienst een (verwerkings)verantwoordelijke is. Volgens de AP is een arbodienst de partij die het doel en middelen van de verwerking bepaalt en daarmee aan te merken als verantwoordelijke volgens de Wbp. Deze visie blijft onder de AVG gehandhaafd. Een Arbodienst is dus ook een verwerkingsverantwoordelijke.

² Raadpleegbaar via

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_de_zieke_werknemer.pdf