

Handboek Algemene Verordening Gegevensbescherming

15 februari 2019

Inhoudsopgave

Hoofdstuk 1 De Algemene Verordening Gegevensbescherming

Hoofdstuk 2 Toestemming verwerken gegevens

Hoofdstuk 3 Datagebruik

Hoofdstuk 4 Personeel en nieuwe wetgeving

Hoofdstuk 5 Verwerken en bewaren gegevens

Hoofdstuk 6 Informeren doelgroepen

Hoofdstuk 7 Verstrekken gegevens aan derden

Hoofdstuk 8 Opbergen gegevens

Hoofdstuk 9 Datalek

Hoofdstuk 10 Informatie over AVG

Dit handboek is geschreven voor Hermans Suikermais B.V., Hermans Agricultural Services Holding Kessel B.V., Hermans Holding Kessel B.V., Hermans Agro Kessel B.V., Natuur Beheer Limburg, Herefords Slagerij B.V., Hermans Herefords Holding B.V. en Guillaume Hermans. Indien er over wij wordt gesproken, worden alle bovengenoemde bedrijven bedoeld.

Hoofdstuk 1 De Algemene Verordening Gegevensbescherming

M.i.v. 25-05-2018 is de Wet Bescherming Persoonsgegevens gewijzigd in de AVG (Algemene Verordening Gegevensbescherming). Dit betekent dat aantoonbaar moet zijn dat er op een veilige manier met persoonsgegevens wordt omgegaan. Persoonsgegevens zijn alle gegevens die aan een natuurlijk persoon gekoppeld kunnen worden. Verwerken is alles wat er met persoonsgegevens gedaan kan worden, inclusief het opslaan (bijvoorbeeld in een bestand met meerdere personen en zelfs wissen). De Autoriteit Persoonsgegevens (voorheen Cbp) verwacht dat wij aantoonbaar voldoen aan deze wet en de bewijslast ligt bij ons als bedrijf. Denk aan het kunnen verantwoorden welke persoonsgegevens worden verwerkt en welke (wettelijk geldige) redenen hieraan ten grondslag ligt, waar en door wie deze worden verwerkt en wie ze wel en niet in kan zien.

Indien op een verkeerde wijze wordt omgegaan met persoonsgegevens heeft de Autoriteit Persoonsgegevens de bevoegdheid om boetes op te leggen. Deze kunnen oplopen tot 4% van de omzet met een maximum van 20 miljoen euro.

In alle gevallen dat persoonsgegevens bewaard worden, zijn er 3 uitgangspunten.

1. Doelbinding

Er moet een duidelijk antwoord zijn op de vraag waarom gegevens verwerkt worden en het doel ervan moet vastliggen. Deze doelstellingen moet wij als bedrijf kunnen verantwoorden aan de hand van de wet wanneer de Autoriteit Persoonsgegevens daar om vraagt. Deze kent een aantal grondslagen/kapstokjes waaraan de verantwoording gehangen kan worden:

- De gegevens worden gebruikt voor het aangaan of uitvoeren van een overeenkomst. Een voorbeeld hiervan is een bestand met leveranciers of klanten.
- De gegevens worden verwerkt uit hoofde van een wettelijke verplichting.. Een voorbeeld hiervan is een kopie van het paspoort in het Personeelsdossier. In dat geval mag (moet) u bijvoorbeeld ook het BSN nummer van uw medewerker hebben. In andere gevallen dient het BSN nummer doorgehaald te worden.
- Er is een vitaal belang van een betrokkene of van een derde; het helpt de situatie te verbeteren. Een vitaal belang is een belang dat essentieel is voor iemands leven of gezondheid en u die persoon niet om toestemming kunt vragen. Stel dat iemand een bedrijfsongeval krijgt en bewusteloos is. U mag de hulpdiensten dan zijn persoonlijke gegevens geven, bijvoorbeeld dat u weet dat hij bepaalde medicijnen gebruikt.
- Als het in het gerechtvaardigd belang is van uw organisatie. Voorbeelden hiervan zijn reclame maken, een rekening innen etc.

Op basis van toestemming alleen als er geen andere grondslag te vinden is.

Men moet steeds aan kunnen tonen dat de gegevens echt nodig zijn voor het doel.

Toestemming

Niet alle gegevens mogen bewaard blijven; zaken als ras, gezondheidsgegevens, religieuze opvattingen, seksuele voorkeur, gezondheid, lidmaatschap vakbond, politieke opvattingen, genetische data, biometrische gegevens mogen niet verwerkt worden, tenzij daarvoor uitdrukkelijke toestemming is gegeven.

Aan toestemming zitten een aantal ingewikkeldheden; deze kan namelijk altijd worden ingetrokken en deze moet "vrij" zijn. Zo wordt een werknemer niet geacht "vrij" te zijn omdat er een gezagsverhouding tussen werkgever en werknemer bestaat. De AVG stelt extra eisen aan de toestemming: er moet altijd een verklaring zijn of een ondubbelzinnige actieve handeling. Het gebruik van aangekruiste vakjes geldt niet als toestemming.

Bovendien bestaat het recht van betrokkene om bezwaar te maken. Zelfs als de gegevens worden gebruikt voor direct bedrijfsbelang kan iemand vragen om vergeten te worden.

De geldigheid van bestaande toestemmingen vervalt als deze niet aan alle voorwaarden voldoet waaronder deze toestemming is verleend. Er moet dan opnieuw toestemming gevraagd worden. Er mogen nooit meer gegevens of langer gegevens verwerkt en bewaard worden dan nodig is.

2. Transparantie

Het dient altijd helder te zijn wat er met de gegevens gedaan wordt. Als duidelijk is waar de gegevens voor gebruikt worden (bijvoorbeeld om een factuur te kunnen sturen), hoeven er geen verdere stappen gezet te worden. In alle andere gevallen moet erop het moment dat de gegevens rechtstreeks van de betrokkene verkregen worden, de verstrekker direct geïnformeerd worden. Als de gegevens van een ander verkregen worden, moet de betrokkene binnen 1 maand geïnformeerd worden. Hierbij dient ook aangegeven te worden hoe lang de gegevens bewaart worden en voor welk doel. Als er een nieuw doel is voor de verwerking van de gegevens moet de betrokkende opnieuw geïnformeerd worden, dan wel om toestemming gevraagd worden.

Ook moet er inzage gegeven worden aan de betrokkene als gevraagd wordt welke gegevens bewaard worden. De betrokkene heeft altijd het recht om een klacht in te dienen bij Autoriteit Persoonsgegevens.

3. Zorgvuldigheid

Men moet zorgvuldig met persoonsgegevens omgaan. Voorbeelden hiervan zijn:

Persoonsgegevens dienen afgeschermd te zijn en niet in handen kunnen vallen van mensen die die niet zouden mogen hebben. Denk hierbij aan mensen binnen uw organisatie die toegang hebben tot de bestanden (zowel "in de kast" als op de computer). Maar ook aan mensen buiten de organisatie. Men dient deugdelijk beschermd te zijn tegen bijvoorbeeld hackers en inbrekers.

Indien gegevens versterkt worden aan een ander (bijvoorbeeld een salarisverwerker) dient men zich er van te vergewissen dat de ander een betrouwbare partij is. Het is verstandig dat er een overeenkomst met de verwerker gesloten worden rond gegevensverwerking en dat er niet meer gegevens gedeeld worden dan strikt noodzakelijk is.

Als een bedrijf meer dan 250 werknemers heeft, dient er bijgehouden worden wat er met gegevens gedaan wordt. Dat zal in de land- en tuinbouw niet vaak voorkomen. Onder de 250 medewerkers moet dit alleen bijgehouden worden als de verwerking niet incidenteel is, of als er bijzondere persoonsgegevens verwerkt worden. Overigens is bijvoorbeeld de verwerking van gegevens van medewerkers NIET incidenteel en daarvan moet dus bijgehouden worden wat er mee gedaan wordt. Als de autoriteit persoonsgegevens komt controleren moet het bedrijf kunnen laten zien welke gegevens er zijn en wat er mee gedaan is/wordt. Dit is vormvrij.

Iedereen heeft een meldplicht indien er een stevig datalek heeft plaatsgevonden. Een voorbeeld van een datalek is een verloren of gestolen computer, een kwijtgeraakt USB stick, een hack, een verkeerd verzonden e-mail etc. Dergelijk lekken dient binnen 72 uur gemeld te worden aan de Autoriteit Persoonsgegevens. Daarnaast dient er een register bijgehouden te worden van incidenten die hier mogelijkwijs onder zouden kunnen vallen en daar beleid op hebben. Hiervoor kan een protocol worden gemaakt waarin omschreven staat wat een datalek is en wat het personeel in voorkomende gevallen zou moeten doen.

Hoofdstuk 2 Toestemming verwerken gegevens

Wij verwerken persoonsgegevens van mensen met wie wij direct of indirect een relatie hebben, willen krijgen of hebben gehad. Wij hechten veel waarde aan de bescherming van deze gegevens. Hierbij houden wij ons aan de toepasselijke wet- en regelgeving, waaronder de Algemene Verordening Gegevensbescherming (AVG).

Persoonsgegevens die wij verwerken zijn van:

- Klanten en hun vertegenwoordigers.
- Mensen die interesse tonen in onze producten en diensten.
- Mensen die aan een bedrijf of organisatie verbonden zijn waar wij een relatie mee hebben, willen krijgen of hebben gehad.

Als een bedrijf of organisatie persoonsgegevens van medewerkers aan ons doorgeeft, zijn wij verplicht om de medewerkers hierover te informeren. De betreffende medewerkers kunnen dan zien hoe wij met hun persoonsgegevens omgaan.

a. Om een relatie met u te kunnen aangaan

Als u klant bij ons wilt worden of wanneer u een product bij ons afneemt wilt afnemen, hebben wij persoonsgegevens nodig. Zo moeten wij bijvoorbeeld een onderzoek doen om te beoordelen of wij u als klant kunnen accepteren en onder welke voorwaarden wij aan een klant willen leveren. Hierbij valt ook te denken aan de kredietverzekering. Alvorens wij in zee gaan met een bedrijf willen wij graag weten hoe het zit met de kredietwaardigheid van het bedrijf. Hiervoor heeft de kredietverzekeringsmaatschappij gegevens nodig die wij verstrekken.

b. Om de relatie met u te onderhouden en opdrachten uit te voeren

Als u klant bij ons bent, willen wij u goed van dienst zijn. Hiervoor verwerken wij persoonsgegevens. Wij gebruiken uw naam en adresgegevens bijvoorbeeld om contact met u te onderhouden. Tevens hebben wij uw bankgegevens nodig voor het betalen van facturen.

c. Voor onze bedrijfsvoering

Als commercieel bedrijf is het belangrijk en noodzakelijk dat wij een goed overzicht hebben van onze klantrelaties. Daar hoort ook bij dat wij weten of u samenwerkt met andere partijen die een risico kunnen opleveren. Om dit overzicht te krijgen en vervolgens maatregelen te kunnen nemen, verwerken wij persoonsgegevens.

d. Voor archiefdoeleinden

Wij verzamelen niet meer persoonsgegevens dan noodzakelijk in het kader van de bovengenoemde doeleinden. Als wij de gegevens niet bewaren voor die doeleinden kunnen wij de gegevens toch nog bewaren voor archiefdoeleinden. Dat wil zeggen dat de gegevens alleen nog maar bij juridische procedures of voor historische, statistische of wetenschappelijke doeleinden worden gebruikt. De bewaarplicht is 7 jaar. Voor onroerend goed geldt een bewaarplicht van 10 jaar. Lease-,

hypotheekcontracten, bankpapieren, huurovereenkomsten, telerscontracten en subsidieregelingen moeten gedurende de gehele looptijd bewaard blijven. Gezondheidsgegevens van personeelsleden mogen niet bij ons bewaard blijven tenzij de instanties dit eisen.

Gegevens mogen niet langer dan de bewaarplicht bewaard blijven. Het archief wordt regelmatig opgeschoond en gegevens worden vernietigd. Bij uitdiensttreding van personeelsleden worden evt. visitekaartjes vernietigd.

Personen zijn ten alle tijden bevoegd om hun persoonsgegevens op te vragen bij ons. Indien iemand vindt dat deze gegevens onjuist of onvolledig zijn verwerkt, dan kan er contact opgenomen worden met Marijke Smedts, managementassistente.

Het privacy statement kan van tijd tot tijd wijzigen. Als er nieuwe gegevensverwerkingen zijn, dan passen wij het privacy statement daarop aan. En als deze wijzigingen ook voor u van belang zijn, dan attenderen wij u daarop of maken wij de wijzigingen op een opvallende manier aan u kenbaar.

Hoofdstuk 3 Datagebruik

Wanneer men zich aanmeldt voor één van onze diensten wordt er gevraagd om persoonsgegevens te verstrekken. Het gaat dan om gegevens zoals initialen, naam, adres, telefoonnummers, e-mailadres, geboortedatum, identificatie, betaalgegevens en overige gegevens. Deze gegevens worden gebruikt om de dienst uit te kunnen voeren. De gegevens worden opgeslagen op eigen beveiligde servers of die van een derde partij. Deze gegevens worden niet gecombineerd met andere persoonlijke gegevens waarover wij beschikken. De persoonlijke gegevens zullen niet langer bewaard worden dan noodzakelijk is voor de doeleinden waarvoor de gegevens worden verwerkt, tenzij anders vereist door de wet.

Wij verzamelen gegevens voor onderzoek om zo een beter inzicht te krijgen in onze klanten, zodat wij onze diensten hierop kunnen afstemmen.

De websites maken gebruik van 'cookies' (tekstbestandjes die op de computer worden geplaatst) om de websites te helpen analyseren hoe gebruikers de sites gebruiken. De door het cookie gegenereerde informatie over het gebruik van de websites kan worden overgebracht naar eigen beveiligde servers van ons of die van een derde partij. Deze informatie wordt gebruikt om bij te houden hoe de websites gebruikt worden, om rapporten over de website-activiteiten op te stellen en om andere diensten aan te bieden met betrekking tot website-activiteiten en internetgebruik.

De website kan verwijzingen bevatten naar andere site die betrekking hebben op een specifiek aspect van deze website. Dit betekent niet dat Hermans Suikermis B.V. verbonden is aan deze andere sites of de eigenaren hiervan. Hermans Suikermis B.V. is dan ook niet verantwoordelijk voor de naleving van de privacywetgeving door deze derden.

De website kan verwijzingen bevatten naar andere sites die betrekking hebben op een specifiek aspect van deze website. Dit betekent niet dat wij verbonden zijn aan deze andere sites of de eigenaren hiervan. Wij zijn dan ook niet verantwoordelijk voor de naleving van de privacywetgeving voor deze derden.

Hoofdstuk 4 Personeel en nieuwe wetgeving

Wij hechten veel waarde aan de bescherming van persoonsgegevens. Wij respecteren de privacy en verwerken de persoonsgegevens alleen voor het doel waarvoor ze verstrekt zijn. Bij de verwerking van persoonsgegevens houden wij ons aan de toepasselijke wet- en regelgeving, waaronder de Algemene Verordening Gegevensbescherming (AVG).

Voor ingang van de nieuwe wet is het personeel in een gezamenlijke bijeenkomst op de hoogte gebracht van de inhoud van de wet. Deze bijeenkomst is zowel in het Nederlands als in het Pools gegeven.

In de beleidsverklaring mensenrechten is een paraaf toegevoegd die betrekking heeft op het privacybeleid. Alle medewerkers hebben deze verklaring eind 2018-begin 2019 opnieuw getekend.

Nieuwe medewerkers tekenen deze verklaring bij aanvang van de werkzaamheden. De beleidsverklaring is zowel in het Nederlands als in het Pools opgemaakt.

Er zijn duidelijke afspraken gemaakt over de zorgvuldigheid van de gegevens. Onze medewerkers zijn verplicht om te allen tijde de privacy te respecteren.

Mochten er klachten zijn dan kunnen deze ingediend worden bij de bevoegde instanties (in Nederland is dit de Autoriteit Persoonsgegevens).

Bij vragen over het onderwerp kan men zich melden bij M. Smedts, management assistente.

Hoofdstuk 5 Verwerken en bewaren gegevens

Persoonsgegevens worden opgevraagd om de gevraagde dienst uit te kunnen voeren. Wij erkennen onze verantwoordelijkheid om de gegevens te beschermen die ons toevertrouwt zijn.

Bij crediteuren en debiteuren hebben wij naam, adres, woonplaats, e-mailadres, bankgegevens en telefoonnummer nodig. Deze gegevens dienen vanuit de wet 7 jaar bewaard te worden.

Wij dragen zorg voor passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies en tegen enige vorm van onrechtmatige verwerking.

De websites worden gehost door Solutior vanuit Nederland. Solutior verwerkt de (persoons)gegevens zorgvuldig door, onder andere, voldoende veiligheidsmaatregelen te implementeren en de gegevens alleen volgens onze instructie te verwerken.

De Europese privacy wetgeving geeft een aantal rechten:

Recht op inzage: als de persoon hierom vraagt, delen wij de verzamelde persoonsgegevens

Recht op identificatie: als de persoon hierom vraagt, passen wij foute of ondertussen gewijzigde persoonsgegevens aan

Recht op overdracht: als de persoon hierom vraagt, kunnen persoonsgegevens overgedragen worden aan een andere partij

Recht op het stoppen van het gebruik van gegevens:

als de persoon hierom vraagt, zullen de persoonsgegevens die wij verzameld hebben conform het verzoek niet meer gebruikt en/of niet meer bijgehouden worden. Conform de wetten kunnen wij genoodzaakt zijn de gegevens nog enige tijd te gebruiken/bewaren.

Er kan gebruik gemaakt worden van de rechten door een aanvraag in te dienen via info@mielies.nl of info@herefords.nl. Binnen een redelijke termijn (max. 4 weken) zullen wij het verzoek behandelen.

Mogelijk zijn kosten verbonden aan dit verzoek, wij zullen u dan in kennis stellen van deze kosten en deze overeenkomstig de wettelijke bepalingen doorbelasten.

Hoofdstuk 6 Informeren doelgroepen

Mensen worden geïnformeerd middels een privacyverklaring op de websites. Hierin staat o.a. vermeld welke gegevens worden opgevraagd, hoe deze worden gebruikt en hoe deze worden beveiligd. Deze gegevens kunnen door ons worden gebruikt voor diverse doeleinden, zoals het beantwoorden van vragen. Wij gebruiken de gegevens niet om u per mail te benaderen met nieuws over onze bedrijven. Verder zullen wij ook niet aan de hand van de persoonsgegevens personen per post benaderen. Personen worden alleen telefonisch benaderd indien de gestelde vraag onduidelijk is. Deze site/gegevens is alleen toegankelijk voor een selecte groep medewerkers. Voor al onze medewerkers geldt geheimhoudingsplicht.

Hoofdstuk 7 Opbergen gegevens

Personeelsgegevens worden digitaal opgeslagen in beveiligde mappen die slechts voor een beperkte groep toegankelijk zijn. Gegevens van personeel op papier wordt bewaard in een afsluitbare kast op het kantoor van A. Wolters. De sleutel van deze kast is in het bezit van G. Hermans en A. Wolters.

Alle computers zijn voorzien van een eigen wachtwoord. De toegang tot mappen wordt beheerd door A. Wolters en G. Hermans. Zij geven aan of 2WCF een medewerker toegang mag geven tot bepaalde mappen in het systeem.

De gegevens van de medewerkers van de uitzendbureaus worden bewaard in de kast op het kantoor van J. van Dommelen.

Hoofdstuk 8 Verstrekken gegevens aan derden

Persoonsgegevens worden zorgvuldig bewaard en niet langer dan noodzakelijk is voor het doel waarvoor zij zijn verwerkt. Binnen onze bedrijven worden persoonsgegevens alleen gebruikt door medewerkers die hier gelet op hun functie toegang tot moeten hebben. Onze medewerkers hebben een geheimhoudingsplicht.

Persoonsgegevens worden nooit verkocht of verhuurd.

Voor het verwerken van bedrijfsgegevens en mailadressen voor de facturering hebben wij toestemming nodig. Hiervoor hebben wij naar alle debiteuren een brief gestuurd met hierin onze afspraken met het verzoek deze getekend te retourneren.

Soms zijn wij genoodzaakt om gegevens te delen met derden. Deze derden kunnen alleen toegang krijgen als aantoonbaar wordt gemaakt dat er passende beveiligingsmaatregelen zijn en geheimhouding wordt gegarandeerd. Er zijn overeenkomsten gesloten met iedereen die persoonsgegevens namens ons verwerken. In deze overeenkomsten zijn strikte afspraken gemaakt over het beveiligen en bewaren van persoonsgegevens.

Bedrijven die toegang hebben tot persoonsgegevens:

- Smits Van den Broek
Zij zorgen voor de salarisadministratie.
Zij beschikken over persoonsgegevens van ons personeel (naam, adres, woonplaats, geboortedatum, bankgegevens, salarisgegevens)
- ARBO
Zij zorgen voor de administratie van het ziekteverzuim en beschikken over persoonsgegevens van ons personeel (naam, adres, woonplaats, geboortedatum, salarisgegevens)
- Ziekteverzuimverzekering
Zij zorgen samen met de ARBO voor de administratie van het ziekteverzuim en beschikken over persoonsgegevens van ons personeel (naam, adres, woonplaats, geboortedatum, salarisgegevens)
- SVB
Dit loopt via Smits Van den Broek i.v.m. de loonadministratie.
- Solutior
Het beheer van de websites.
- UWV
Dit is van toepassing bij ontslag of langdurig ziekte (vanaf 1 jaar). Zij ontvangen gegevens van de ARBO.
- Belastingdienst
Dit loopt via Smits Van den Broek i.v.m. de loonadministratie

- 2WCF
Zij zorgen voor het beheer van de computers en hebben dus toegang tot onze systemen. Hier ligt een contract aan ten grondslag.
- Contrain
Dit betreft een uitzendbureau voor onze Poolse medewerkers. Er ligt een contract aan ten grondslag.
- Lancyr + Visschers Assurantiën B.V.
Zij beheren alle verzekeringen van Hermans Suikermais B.V..
- Accountants en Advieskantoor GBV
Accountant van Hermans Suikermais B.V.. Er ligt een contract aan ten grondslag.
- Mobiele telefoons
Mail via telefoon door G. Hermans, J. van Dommelen en J. Schell

Hoofdstuk 9 Datalek

Onder een datalek wordt o.a. verstaan een verloren of gestolen computer, laptop of mobiele telefoon, een kwijtgeraakte USB stick, een hack of een verkeerd gezonden mail. Deze lekken worden binnen 72 uur gemeld aan de Autoriteit Persoonsgegevens. Deze contacten zullen lopen via M. Smedts, management assistente of bij haar afwezigheid door A. Wolters, hoofd administratie.

Er is een formulier waarop incidenten worden genoteerd met daarbij vermeld de datum, medewerker en genomen actie.

In de personeelsbijeenkomst over dit onderwerp is uitgelegd hoe te handelen in het geval van een datalek. Hierin staat ook duidelijk vermeld wat het personeel in voorkomende gevallen moet doen.

Hoofdstuk 10 Informatie over AVG

Informeer uzelf goed over dit onderwerp en vraag indien nodig bedrijfsspecifiek advies aan een specifiek adviesbureau. Lees meer achtergrondinformatie over de wetgeving en uitleg van de verschillende begrippen in dit [achtergrondartikel over de AVG](#).

Voorbeeld brief voor klanten/debiteuren:

Op 25 mei 2018 zal de nieuwe Algemene Verordening Gegevensbescherming wettelijk van kracht worden. Als bedrijf dat persoonlijke gegevens met betrekking tot uw bedrijf bewaart, zijn wij wettelijk verplicht u te informeren over welke gegevens we voor u bewaren en hoe we deze zullen / zullen gebruiken.

Wij verzoeken u de informatie in deze brief te lezen en schriftelijk aan ons te bevestigen dat u ermee instemt dat wij uw gegevens gebruiken en opslaan zoals hieronder uiteengezet. De informatie die we opslaan en gebruiken, is om ons in staat te stellen met u te handelen. Om te bevestigen dat u hiermee akkoord gaat, vult u het formulier bijvoegsels in en scant en e-mailt u het ondertekende formulier naar ons of retourneert u dit per post.

We houden uw informatie binnen onze eigen beveiligde systemen.

Informatie over uw bedrijf wordt geback-up't en off-site opgeslagen voor veiligheid en verliespreventie.

Wij gebruiken gegevens die betrekking hebben op uw bedrijf om de handel met u en uw bedrijf en voor algemene correspondentie met uw personeel op regelmatige basis mogelijk te maken. LFP zal deze informatie nooit doorgeven of verkopen zonder uw toestemming.

Wij namens

autoriseren en accepteren dat alle gegevens die ons bedrijf of ik aan Hermans Suikermis B.V. verstrekt voor handelsdoeleinden kan en zal worden gebruikt zoals hierboven beschreven.

Voorbeeld overeenkomst derden

Verwerkersovereenkomst tussen Opdrachtgever en

De besloten vennootschap met beperkte aansprakelijkheid **IT&Care B.V.**, statutair gevestigd te Eindhoven en kantoorhoudende te 5692 ED Son, aan het adres Science Park 5127 hierbij rechtsgeldig vertegenwoordigd door mevrouw C.I. Joling, in haar hoedanigheid van algemeen directeur, hierna ook te noemen: '**IT&Care**' of '**Verwerker**',

hierna afzonderlijk ook aangeduid als '**Partij**' en gezamenlijk als '**Partijen**'.

in overweging nemende dat:

- Opdrachtgever in het kader van goed werkgeverschap de gezondheid, competenties en motivatie van haar werknemers wenst te bewaken en te bevorderen teneinde werknemers duurzaam inzetbaar te houden gedurende hun dienstverband bij Opdrachtgever;
- Opdrachtgever hierbij ondersteuning krijgt van ArboNed B.V., een gecertificeerde dienstverlener en zorgaanbieder die zich richt op de duurzame inzetbaarheid van werknemers gedurende hun werkzame leven (hierna '**ArboNed**');;
- Opdrachtgever en ArboNed voor de uitvoering van eerdergenoemde diensten een overeenkomst met elkaar hebben gesloten (hierna '**ArboNed Overeenkomst**') en hierbij gebruikmaken van de ICT infrastructuur van IT&Care, een partij die integrale webbased softwareapplicaties ontwikkelt en levert aan werkgevers, werknemers en zorgaanbieders waarbij de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens optimaal gewaarborgd is;
- Meer specifiek, Opdrachtgever gebruik maakt van het enkel voor haar toegankelijke werkgeverportaal (hierna: '**Werkgeverportaal**') waarin gegevens van werknemers van Opdrachtgever worden verwerkt, waaronder persoonsgegevens van die werknemers (hierna: '**Persoonsgegevens Werknemers**');;
- IT&Care ten behoeve van Opdrachtgever optreedt als verwerker van de Persoonsgegevens Werknemers die via het Werkgeverportaal worden verwerkt;
- IT&Care in opdracht van Opdrachtgever zorg draagt voor de verstrekking van de voor de uitvoering van de ArboNed Overeenkomst noodzakelijke Persoonsgegevens Werknemers aan ArboNed;
- Partijen gehouden zijn uitvoering te geven aan het bepaalde in de AVG, in het bijzonder artikel 28 en 32 AVG, en in dit kader deze verwerkersovereenkomst sluiten om hierin de door hen gemaakte afspraken over de verwerking van Persoonsgegevens Werknemers vast te leggen (hierna: '**Verwerkersovereenkomst**').

komen het volgende overeen:

Artikel 1. Definities

1.1 De begrippen 'Persoonsgegevens', 'Verwerking', 'Verwerkingsverantwoordelijke', 'Verwerker', 'Betrokkene' en 'Derde' zoals opgenomen in artikel 4 van de Algemene Verordening Gegevensbescherming (hierna: '**AVG**') hebben de betekenis die daaraan in de AVG is gegeven. Deze worden in de Verwerkersovereenkomst met een hoofdletter geschreven. Overige, met een hoofdletter geschreven begrippen hebben de betekenis zoals opgenomen in de Verwerkersovereenkomst.

1.2 Onder Persoonsgegevens Werknemers wordt verstaan: alle informatie over een geïdentificeerde of identificeerbare werknemer, zoals bedoeld in artikel 4 sub 1 AVG, die Opdrachtgever verwerkt in het Werkgeverportaal.

Artikel 2. Doel en noodzakelijkheid van de Verwerking

2.1 Via het Werkgeverportaal voert Opdrachtgever een volledige en up-to-date werknemer administratie die haar in staat stelt om uitvoering te geven aan haar wettelijke verplichtingen ten aanzien van re-

integratie, verzuim, duurzame inzetbaarheid en gezondheidsmanagement. Deze wettelijke verplichtingen vloeien onder meer voort uit de Arbeidsomstandighedenwet en de Wet verbetering poortwachter. Het Werkgeverportaal stelt Opdrachtgever tevens in staat om de juiste en noodzakelijke Persoonsgegevens Werknemers te verstrekken aan:

- ArboNed voor de uitvoering van ArboNed Overeenkomst conform toepasselijke wet- en regelgeving;
- Verzuimverzekeraar voor de uitvoering van de overeenkomst conform de gemaakte wet- en regelgeving.

2.2 IT&Care verwerkt Persoonsgegevens Werknemers alleen voor het doel zoals omschreven in artikel 2.1 en alleen voor zover de verwerking noodzakelijk is om te voldoen aan dit doel.

2.3 Partijen erkennen dat op de Verwerking van Persoonsgegevens Werknemers via het Werkgeverportaal de AVG van toepassing is en dat zij beide op de hoogte zijn van de verplichtingen die in de AVG zijn neergelegd. Partijen zijn ieder afzonderlijk en zelfstandig verplicht om ervoor zorg te dragen dat aan voornoemde verplichtingen wordt voldaan.

2.4 Partijen verstrekken elkaar over en weer tijdig alle benodigde medewerking om een goede naleving van de AVG, alsmede de overige geldende privacy wet- en regelgeving, mogelijk te maken.

Artikel 3. Verwerking van Persoonsgegevens Werknemers door IT&Care

3.1 Zoals gedefinieerd in de AVG is IT&Care aan te merken als 'Verwerker' en Opdrachtgever als 'Verwerkingsverantwoordelijke'.

3.2 IT&Care verwerkt Persoonsgegevens Werknemers slechts in opdracht van Opdrachtgever, overeenkomstig diens instructies en onder diens verantwoordelijkheid en met inachtneming van de bepalingen uit de gebruiksrechtovereenkomst die Opdrachtgever als onderdeel van de ArboNed Overeenkomst met ArboNed sluit voor het gebruik van het Werkgeverportaal. IT&Care heeft geen zeggenschap over het doel van en de middelen voor de verwerking van de Persoonsgegevens.

3.3 De Persoonsgegevens Werknemers worden uitsluitend opgeslagen en verwerkt binnen Nederland.

3.4 De Verwerking van Persoonsgegevens Werknemers door IT&Care is nader uitgewerkt in het privacyreglement van IT&Care, te raadplegen via de website www.itandcare.nl.

Artikel 4. Categorieën van Persoonsgegevens en Betrokkenen

4.1 IT&Care kan de volgende categorieën van Persoonsgegevens Werknemers voor Opdrachtgever verwerken:

- Persoonsgegevens, waaronder:

- a. NAW gegevens;
- b. E-mailadres;
- c. Telefoonnummer;
- d. Geboortedatum;
- e. Geslacht;
- f. Verpleegadres van de zieke werknemer;
- g. Werknemer ID¹;

- Bijzondere persoonsgegevens, waaronder:

- a. Gezondheidsgegevens, zoals de datum van ziekmelding werknemer, datum van herstelmelding, duur van het verzuim, of sprake is van één van de vangnetbepalingen uit de Ziektewet, , of een zieke werknemer betrokken is geweest bij een ongeval met regresmogelijkheid.
- b. Uniek identificerend persoonsgegeven.

¹ Hiermee wordt bedoeld het Werknemer ID, dan wel een andere specifiek bij een werknemer behorende codering die het Burger Service Nummer vervangt als sleutelwaarde, zoals omschreven in de Nationale Verzuimstandaard ('NVS') 2017. Deze standaard wordt onderschreven door arbodiensten aangesloten bij brancheorganisatie OVAL en beheerd door de Stichting Sivi.

4.2 De Betrokkenen waarop de Persoonsgegevens Werknemers betrekking hebben zijn in ieder geval:

- a. Werknemers
- b. Ex-werknemers

Artikel 5. Verstrekking Persoonsgegevens Werknemers uit het Werkgeverportaal aan ArboNed

5.1 Ten behoeve van de uitvoering van de ArboNed Overeenkomst verstrekt IT&Care op verzoek van Opdrachtgever Persoonsgegevens Werknemers aan ArboNed voor zover dat noodzakelijk is en indien daarvoor een wettelijke grondslag bestaat.

5.2 ArboNed verleent als zorgaanbieder - afhankelijk van de overeengekomen dienstverlening in de ArboNed Overeenkomst - arbeidsgezondheidskundige zorg aan werknemers van Opdrachtgever ten einde hen duurzaam inzetbaar te houden gedurende hun werkzame leven. In het kader van de medische begeleiding van werknemers legt ArboNed dossiers aan van die werknemers waaraan zij zorg verleent. Om aan deze wettelijke dossierplicht te kunnen voldoen, krijgt ArboNed via het Werkgeverportaal de beschikking over de noodzakelijke Persoonsgegevens Werknemers op het moment dat zij zorg verleent c.q. gaat verlenen aan werknemers van Opdrachtgever.

5.3 Vanaf het moment dat Persoonsgegevens Werknemers aan ArboNed ter beschikking zijn gesteld, geldt ArboNed als Verwerkingsverantwoordelijke ten aanzien van deze Persoonsgegevens Werknemers. De wijze waarop ArboNed de Persoonsgegevens Werknemers verwerkt is beschreven in het privacyreglement van ArboNed, op te vragen via de website www.arboned.nl.

Artikel 6. Geheimhouding

6.1 IT&Care is verplicht tot geheimhouding van de Persoonsgegevens Werknemers, behoudens voor zover:

- a. IT&Care de Persoonsgegevens Werknemers op grond van het bepaalde in de Verwerkersovereenkomst aan ArboNed mag verstrekken, of
 - b. een wettelijk voorschrift IT&Care tot mededelen verplicht, of
 - c. de gegevensverstrekking plaatsvindt in opdracht van Opdrachtgever;
 - d. het verstrekken van Persoonsgegevens Werknemers logischerwijs noodzakelijk is gezien de aard van de door IT&Care verrichte dienstverlening aan Opdrachtgever.
- 6.2 IT&Care zal aan haar medewerkers die werkzaamheden verrichten in het kader van de Verwerking van Persoonsgegevens Werknemers, dezelfde geheimhoudingsverplichting opleggen ten aanzien van het geheimhouden van Persoonsgegevens Werknemers als bedoeld in dit artikel.

6.3 De in dit artikel opgenomen geheimhoudingsplicht geldt onafhankelijk van de duur van deze Verwerkersovereenkomst zoals nader bepaald in artikel 13 en blijft ook na beëindiging van de Verwerkersovereenkomst voortduren. De geheimhoudingsplicht is niet van toepassing op Persoonsgegevens Werknemers die reeds publiekelijk bekend zijn geworden, anders dan ten gevolge van een schending van voormelde geheimhoudingsplicht.

Artikel 7. Beveiligingsmaatregelen

7.1 Partijen zijn conform artikel 28 AVG verantwoordelijk voor de bescherming van Persoonsgegevens en de persoonlijke levenssfeer van Betrokkene(n). IT&Care zal passende technische en organisatorische beveiligingsmaatregelen treffen om de vertrouwelijkheid, integriteit en beschikbaarheid van de Persoonsgegevens Werknemers veilig te stellen, alsmede de rechten van Betrokkene(n) te waarborgen. Bij de te treffen maatregelen zal IT&Care rekening houden met de stand van de techniek, de uitvoeringskosten, de aard, omvang, context en verwerkingsdoeleinden en de risico's voor de rechten en vrijheden van de Betrokken(n).

7.2 IT&Care is ISO 27001 en NEN 7510 gecertificeerd. De organisatorische en beveiligingsmaatregelen die zij treft om uitvoering te geven aan het bepaalde in artikel 7.1 zijn opgenomen in de Verklaring van Toepasselijkheid. Hieronder vallen onder meer de volgende maatregelen:

- a. Van Persoonsgegevens Werknemers wordt een real time back-up gemaakt zodat verlies van Persoonsgegevens Werknemers wordt tegengegaan;
- b. De onder sub a) genoemde back-ups worden op een fysiek gescheiden (brand)veilige locatie bewaard;
- c. Het Werkgeverportaal is geplaatst in een twin data center concept om een hoge beschikbaarheid te kunnen garanderen;
- d. IT&Care treft voorzieningen voor een adequate toegangsbeveiliging zodat de Persoonsgegevens Werknemers alleen toegankelijk zijn voor geautoriseerd personeel;
- e. IT&Care heeft een adequaat en actueel mechanisme in werking om kwaadaardige software, waaronder – maar niet beperkt tot – computervirussen, op te sporen en af te wenden;
- f. Door externe partijen worden regelmatig penetratietesten uitgevoerd om de systemen te toetsen op eventuele kwetsbaarheden;
- g. IT&Care maakt gebruik van beveiligde netwerkverbindingen.

Artikel 8. Samenwerking met sub-Verwerkers

8.1 IT&Care maakt gebruik van sub-Verwerkers, die in de **Bijlage** bij de Verwerkersovereenkomst zijn opgenomen. Opdrachtgever gaat akkoord met de inschakeling van deze sub-Verwerkers. Van andere sub-Verwerkers dan die genoemd in de Bijlage, mag door IT&Care slechts na voorafgaande toestemming van Opdrachtgever gebruik worden gemaakt.. IT&Care blijft als Verwerker van Opdrachtgever volledig verantwoordelijk voor de Verwerking van Persoonsgegevens Werknemers door sub-Verwerkers.

8.2 IT&Care sluit met door haar ingeschakelde sub-Verwerkers een sub-verwerkersovereenkomst waarin aan deze sub-Verwerkers dezelfde verantwoordelijkheden en verplichtingen inzake gegevenverwerking en -bescherming worden opgelegd als die in de Verwerkersovereenkomst zijn opgenomen.

Artikel 9. Procedure Datalek

9.1 Ondanks de genomen technische en organisatorische maatregelen aan de zijde van IT&Care, kan onverhoopt een inbreuk in verband met de Persoonsgegevens Werknemers ontstaan waarbij de Persoonsgegevens Werknemers daadwerkelijk zijn vernietigd of verloren zijn gegaan, zijn gewijzigd, verstrekt of toegankelijk zijn gemaakt op een manier die onrechtmatig is (hierna: 'Datalek').

9.2 Een Datalek zal door IT&Care zo spoedig mogelijk en in ieder geval binnen 24 uur na ontdekking daarvan schriftelijk worden gemeld aan Opdrachtgever.

9.3 Opdrachtgever beoordeelt als Verwerkingsverantwoordelijke na voorafgaand overleg met IT&Care of het Datalek gemeld dient te worden bij de Autoriteit Persoonsgegevens en eventueel aan de Betrokkene(n). De verantwoordelijkheid voor de (correcte, tijdige en volledige) melding aan de Autoriteit Persoonsgegevens en eventueel aan de Betrokkene(n) binnen de daarvoor geldende wettelijke termijn ligt bij Opdrachtgever. Indien Opdrachtgever voornemens is een Datalek te melden bij de Autoriteit Persoonsgegevens en/of Betrokkene(n), stelt zij IT&Care daarvan op de hoogte.

9.4 IT&Care heeft na voorafgaand overleg met Opdrachtgever het recht om zelfstandig melding te maken van het Datalek bij de Autoriteit Persoonsgegevens en eventueel aan Betrokkene(n).

9.5 IT&Care verstrekt in ieder geval die informatie omtrent het Datalek die Opdrachtgever nodig heeft om aan voorgenoemde meldingsplicht(en) te kunnen voldoen, waaronder:

- a. De aard van de inbreuk, waar mogelijk onder vermelding van de categorieën van Betrokkenen en persoonsgegevensregisters en, bij benadering, het aantal Betrokkenen en persoonsgegevensregisters in kwestie;
- b. Indien voor IT&Care inzichtelijk, de waarschijnlijke gevolgen van het Datalek, zoals verlies van controle over de Persoonsgegevens Werknemers door Betrokkenen en het niet kunnen uitoefenen door Betrokkenen van hun rechten;

c. Maatregelen die door IT&Care zijn getroffen ter beperking van de eventuele nadelige gevolgen van het Datalek. 9.6 IT&Care zal Opdrachtgever op de hoogte houden van eventuele nieuwe ontwikkelingen omtrent het Datalek en van de maatregelen die IT&Care zal treffen om de gevolgen van het Datalek te beperken en herhaling te voorkomen.

Artikel 10. Audit

10.1 IT&Care is ISO 27001 en NEN 7510 gecertificeerd en wordt in dit kader jaarlijks geaudit. Indien Opdrachtgever desondanks de naleving van deze Verwerkersovereenkomst middels een audit wenst te laten controleren, is zij daartoe gerechtigd na overleg met IT&Care. Een audit zal uitsluitend worden uitgevoerd door een daartoe bevoegde onafhankelijke instantie.

10.2 Een audit vindt plaats nadat Opdrachtgever met IT&Care schriftelijk overeenstemming heeft bereikt over het tijdstip en de omvang van de audit, alsmede over de instantie die de audit zal uitvoeren. De kosten van de audit worden gedragen door Opdrachtgever.

10.3 Met inachtneming van het bepaalde in dit artikel zal IT&Care haar medewerking verlenen aan een audit en alle voor de audit relevante informatie tijdig ter beschikking stellen op de locatie waar de audit wordt verricht.

10.4 De bevoegde instantie die een audit uitvoert, conformeert zich aan de beveiligingsprocedures zoals die bij IT&Care van kracht zijn.

10.5 Een audit mag de bedrijfsactiviteiten van IT&Care niet onnodig verstoren.

Artikel 11. Verzoeken van Betrokkenen

11.1 IT&Care verleent Opdrachtgever alle redelijke medewerking om ervoor te zorgen dat Opdrachtgever binnen de wettelijke termijnen kan voldoen aan de verplichtingen op grond van Hoofdstuk III van de AVG. Indien IT&Care haar medewerking dient te verlenen aan verzoeken van betrokkenen die als buitensporig, dan wel kennelijk ongegrond kunnen worden aangemerkt in de zin van artikel 12 lid 5 AVG, heeft IT&Care het recht om haar medewerking aan dergelijke verzoeken te weigeren, dan wel een redelijke kostenvergoeding te vragen voor haar medewerking. Deze kostenvergoeding zal in overleg tussen IT&Care en Opdrachtgever worden vastgesteld.

Artikel 12. Aansprakelijkheid

12.1 Indien een Partij toerekenbaar tekortschiet in de nakoming van de op haar rustende verplichtingen uit hoofde van deze Verwerkersovereenkomst, de AVG en/of overige wet- en regelgeving op het gebied van de Verwerking van Persoonsgegevens, is deze Partij aansprakelijk voor de schade die de andere Partij dientengevolge lijdt.

12.2 De aansprakelijkheid van Partijen is beperkt tot directe schade en tot het maximale bedrag dat de verzekeraar van de aansprakelijkgestelde Partij uitkeert.

Artikel 13. Duur en einde Verwerkersovereenkomst

13.1 De Verwerkersovereenkomst zal van kracht zijn gedurende de looptijd van de ArboNed Overeenkomst. Indien laatstgenoemde ArboNed Overeenkomst eindigt, eindigt deze Verwerkersovereenkomst automatisch.

13.2 Geen van beide Partijen kan de Verwerkersovereenkomst tussentijds opzeggen.

13.3 Na beëindiging van de Verwerkersovereenkomst draagt IT&Care binnen een redelijke termijn, en in ieder geval binnen drie maanden na beëindiging van de Verwerkersovereenkomst, zorg voor verwijdering van Persoonsgegevens Werknemers in hun systemen, dan wel teruggave van de Persoonsgegevens Werknemers aan Opdrachtgever op een door Partijen overeen te komen wijze, tenzij voor IT&Care een wettelijke plicht bestaat om Persoonsgegevens Werknemers te bewaren.

Artikel 14. Toepasselijk recht en geschillen

14.1 Op deze Verwerkersovereenkomst is uitsluitend Nederlands recht van toepassing.

14.2 Alle geschillen (daaronder inbegrepen geschillen die slechts door één der Partijen als zodanig worden beschouwd) die naar aanleiding van de Verwerkersovereenkomst ontstaan, zullen aanhangig worden gemaakt bij de bevoegde rechter in het arrondissement Oost-Brabant.

Aldus overeengekomen en opgemaakt in tweevoud, op _____