



## VERWERKERSOVEREENKOMST

### DE ONDERGETEKENDEN:

**Opdrachtgever**, hierna te noemen 'Verwerkingsverantwoordelijke'

en

**Wesselman Accounting I Outsourcing, Opdrachtnemer**, hierna te noemen 'Verwerker'

Verwerkingsverantwoordelijke en Verwerker worden afzonderlijk tevens genoemd 'Partij' of gezamenlijk 'Partijen'.

### OVERWEGENDE DAT:

- a. Verwerker met Verwerkingsverantwoordelijke een overeenkomst of opdracht is aangegaan vanwege het verrichten van de volgende diensten door Verwerker: administratieve diensten, (salaris)administratie en/of belastingaangifte en/of bezwaar/beroep en/of advies en alle daaruit voortvloeiende activiteiten zoals het informeren over belangrijke en actuele onderwerpen middels nieuwsbrieven, het versturen van uitnodigingen voor bijeenkomsten en het doen van aanbiedingen, allen in de breedste zin van het woord (hierna: 'de Opdracht').
- b. Verwerkingsverantwoordelijke in het kader van de uitvoering van de Opdracht aan Verwerker direct of indirect gegevens zal verstrekken die privacygevoelig zijn, welke gegevens Verwerker in opdracht van Verwerkingsverantwoordelijke zal verwerken;
- c. De te verwerken gegevens van Verwerkingsverantwoordelijke onder meer Persoonsgegevens bevatten in de zin van Privacy Wet- en Regelgeving;
- d. Verwerkingsverantwoordelijke kwalificeert als Verwerkingsverantwoordelijke in de zin van de Privacy Wet- en Regelgeving, nu zij het doel en de middelen voor de verwerking van Persoonsgegevens vaststelt;
- e. Verwerker kwalificeert als een Verwerker in de zin van de Privacy Wet- en Regelgeving omdat Verwerker ten behoeve van Verwerkingsverantwoordelijke Persoonsgegevens verwerkt, zonder aan diens rechtstreeks gezag onderworpen te zijn en Verwerkingsverantwoordelijke het doel van en de middelen voor de verwerking van de Persoonsgegevens vaststelt;
- f. Privacy Wet- en Regelgeving aan Verwerkingsverantwoordelijke de plicht oplegt om ervoor zorg te dragen dat Verwerker voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten bewerkingen;
- g. Dat Verwerkingsverantwoordelijke en Verwerker groot belang hechten aan het beschermen van de Persoonsgegevens van Betrokkene;
- h. Verwerkingsverantwoordelijke en Verwerker in aanvulling op de reeds tussen partijen geldende afspraken op basis van de Opdracht zoals genoemd onder a. middels deze Overeenkomst een Verwerkersovereenkomst zoals bedoeld in artikel 28 lid 3 AVG wensen te sluiten.

## VERKLAREN TE ZIJN OVEREENGEKOMEN ALS VOLGT:

### Artikel 1 Definities

1.1 Partijen hanteren in deze Overeenkomst de onderstaande duidingen, afkortingen en definities (in alfabetische volgorde):

<u>AVG</u>	Verordening (EU) 2016/679 Van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de Verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming);
<u>Algemene Voorwaarden</u>	De van toepassing zijnde Algemene Voorwaarden van Wesselman Accounting I Outsourcing, waar deze Overeenkomst onderdeel van uit maakt;
<u>Betrokkene</u>	Degene op wie een Persoonsgegeven betrekking heeft;
<u>Datalek</u>	Iedere inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot de door Verwerker of door Verwerker ingeschakelde derden, zoals maar niet beperkt tot Sub-verwerkers, verwerkte Persoonsgegevens;
<u>EER</u>	Europese Economische Ruimte;
<u>Overeenkomst</u>	Onderhavige Verwerkersovereenkomst tussen Verwerkingsverantwoordelijke enerzijds en Verwerker anderzijds, inclusief bijlagen en documenten waarnaar wordt verwezen;
<u>Persoonsgegeven(s)</u>	Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;
<u>Privacy Wet- en Regelgeving</u>	Alle wetten en regelingen, inclusief de wetten en regelingen zoals afkomstig van (enig orgaan of institutie van) de Europese Unie, de Europese Economische Ruimte en hun lidstaten, zoals van toepassing op de verwerking van Persoonsgegevens onder de Opdracht, zoals, maar niet beperkt tot, de AVG;
<u>Sub-verwerker</u>	Degene die de Verwerker bijstaat in de verwerking van Persoonsgegevens;
<u>Verwerking</u>	Elke handeling of elk geheel van handelingen met betrekking tot Persoonsgegevens, al dan niet geautomatiseerd, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met

elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;

## **Artikel 2 Doel Verwerking Persoonsgegevens**

- 2.1 Partijen erkennen en komen hierbij overeen dat voor de verwerking van Persoonsgegevens, Verwerker zal optreden als Verwerker en dat Verwerkingsverantwoordelijke zal optreden als Verwerkingsverantwoordelijke, een en ander in de zin van de AVG.
- 2.2 Het onderwerp, de aard en het doel van de verwerking zijn het vervullen van de verplichtingen die volgen uit de Opdracht zoals genoemd onder a. Kort samengevat komen die neer op het verwerken van persoonsgegevens onder andere in het kader van werkzaamheden met betrekking tot (salaris)administratie en in het kader daar van opgaven aan belastingdienst, pensioenuitvoerders, verzekeraars en/of UWV, het doen van belastingaangifte en de gegevens die noodzakelijk zijn voor het geven van een gedegen advies.
- 2.3 De te verwerken Persoonsgegevens zijn van het soort en behelzen de categorieën van Persoonsgegevens zoals genoemd in **bijlage 1** bij deze overeenkomst.
- 2.4 Verwerkingsverantwoordelijke zal de Persoonsgegevens verwerken in overeenstemming met de vereisten van de Privacy Wet- en Regelgeving. De instructies van Verwerkingsverantwoordelijke voor de verwerking van Persoonsgegevens zullen overeenkomen met de Privacy Wet- en Regelgeving. Verwerkingsverantwoordelijke draagt, met uitsluiting van ieder ander, de verantwoordelijkheid voor de juistheid, kwaliteit en rechtmatigheid van de verwerking van Persoonsgegevens en de middelen waarmee de Verwerkingsverantwoordelijke de Persoonsgegevens verzamelt en heeft verzameld.
- 2.5 Verwerker verwerkt de Persoonsgegevens slechts ten behoeve van Verwerkingsverantwoordelijke, overeenkomstig de instructies en onder de verantwoordelijkheid van Verwerkingsverantwoordelijke. Verwerker behandelt de Persoonsgegevens als confidentiële informatie. Verwerker heeft geen zeggenschap over het doel en de middelen voor de verwerking van de Persoonsgegevens. Verantwoordelijke instrueert Verwerker hierbij de Persoonsgegevens te verwerken voor de volgende doeleinden:
  - I. Verwerking zoals voortvloeit uit de Opdracht;
  - II. Verwerking om eventuele verdere redelijke instructies van de Verwerker na te komen als deze instructies consistent zijn met de bepalingen van de Opdracht.
- 2.6 Tenzij een wettelijke bepaling en/of tuchtrecht anders bepalen, is het Verwerker niet toegestaan Persoonsgegevens anders dan voor de in artikel 2.5 bepaalde doeleinden te gebruiken.
- 2.7 De Verwerker is bevoegd om beslissingen te nemen over welke middelen hij gebruikt voor de verwerking(en). Dit mag alleen als het gaat om praktische zaken die geen significante impact op de bescherming van de Persoonsgegevens hebben.
- 2.8 Als naar het oordeel van de Verwerker een instructie van de Verwerkingsverantwoordelijke in strijd is met deze Verwerkersovereenkomst of Privacy Wet- en Regelgeving is zij gehouden de Verwerkingsverantwoordelijke hierover te informeren.

### **Artikel 3 Medewerkingsplicht**

- 3.1 Verwerker zal de naar redelijkheid gevraagde medewerking verlenen aan Verwerkingsverantwoordelijke bij, door of namens Verwerkingsverantwoordelijke uit te voeren Privacy Impact Assessment voorgeschreven door de wet, alsmede bij een klacht, onderzoek, controle of inzageverzoek vanuit een Betrokkene of Verwerkingsverantwoordelijke.
- 3.2 Indien en voor zover Verwerkingsverantwoordelijke, in de uitvoering van de Opdracht, niet de mogelijkheid heeft tot inzage, rectificatie, het wissen van gegevens, beperking van de verwerking of overdracht van Persoonsgegevens, zoals vereist op basis van de Privacy Wet- en Regelgeving, zal Verwerker rekening houdend met de bepalingen inzake de toegang tot persoonsgegevens en de verzoeken hiertoe in de toepasselijke Privacy Wet- en Regelgeving en gelimiteerd tot de kosten zoals in deze bepalingen bepaald, conformeren aan redelijke verzoeken van Verwerkingsverantwoordelijke om dergelijke toegang te faciliteren.
- 3.3 Verwerker zal, voor zover wettelijk toegestaan, Verwerkingsverantwoordelijke prompt op de hoogte stellen indien Verwerker een verzoek van een Betrokkene ontvangt in verband met de inzage, rectificatie, het wissen van gegevens, beperking van de verwerking of overdracht van Persoonsgegevens van deze Betrokkene. Verwerker zal aan Verwerkingsverantwoordelijke alle redelijke medewerking en bijstand verlenen in verband met de afhandeling van verzoeken van Betrokkene in verband met de toegang tot Persoonsgegevens, voor zover wettelijk toegestaan en voor zover Verwerkingsverantwoordelijke geen toegang tot de Persoonsgegevens heeft.
- 3.4 Indien en voor zover hiertoe een wettelijke verplichting bestaat, en eerst nadat Verwerkingsverantwoordelijke hierover prompt althans op het eerste wettelijk of van overheidswege toegestane moment is geïnformeerd, werkt Verwerker mee aan een onderzoek audit of beslaglegging door de Autoriteit Persoonsgegevens of een andere toezichthouder. Verwerker waarborgt hierbij de veiligheid en vertrouwelijkheid van de Persoonsgegevens en verzekert dat niet meer Persoonsgegevens worden geopenbaard dan strikt noodzakelijk. Waar mogelijk worden Persoonsgegevens geanonimiseerd.
- 3.5 Kosten voortvloeiend uit inzageverzoeken, onderzoeken of controles (op instigatie) van Betrokkene of Verwerkingsverantwoordelijke, onderzoeken, audits of beslagleggingen door de Autoriteit Persoonsgegevens of een andere toezichthouder met betrekking tot Persoonsgegevens, zullen worden gedragen door Verwerkingsverantwoordelijke. Onder deze kosten wordt mede verstaan, doch deze zijn niet beperkt tot kosten voor het treffen van (aanvullende) technische en organisatorische beveiligingsmaatregelen in overeenstemming met artikel 3 en rekening houdend met eventuele aanwijzingen van de Autoriteit Persoonsgegevens.

### **Artikel 4 Personeel van Verwerker**

- 4.1 Verwerker verzekert hierbij dat zijn personeel, betrokken bij de verwerking van Persoonsgegevens, is geïnformeerd over de confidentiële aard van de Persoonsgegevens.
- 4.2 Verwerker onderneemt, in commercieel opzicht redelijke, stappen om de betrouwbaarheid van elk personeelslid van Verwerker die betrokken is bij de verwerking van Persoonsgegevens te verzekeren.
- 4.3 Verwerker verzekert hierbij dat de toegang van Verwerker tot de Persoonsgegevens beperkt is tot personeel wiens toegang noodzakelijk is voor de uitvoering van de Opdracht.

## Artikel 5 Beveiligingsmaatregelen

- 5.1 Verwerker zal alle passende technische en organisatorische maatregelen nemen om de Persoonsgegevens te beveiligen tegen verlies, of enige vorm van onrechtmatige verwerking. De betreffende maatregelen zijn nader omschreven in **bijlage 2** bij deze Overeenkomst. Verwerker zal zich daartoe houden aan het binnen Verwerker geldende (standaard) niveau van beveiliging. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.
- 5.2 Verwerker stelt Verwerkingsverantwoordelijke in de gelegenheid te controleren dat de verwerking van Persoonsgegevens plaatsvindt zoals overeengekomen in deze Overeenkomst en de beveiligingsprotocollen van Verwerker.
- 5.3 Partijen erkennen dat regelmatige aanpassing van de beveiligingsmaatregelen nodig is om te voldoen aan de Privacy Wet- en Regelgeving. Verwerker zal de maatregelen regelmatig evalueren en deze waar nodig aanvullen en verbeteren om aan de Privacy Wet- en Regelgeving te voldoen.
- 5.4 De Verwerker zal Verwerkingsverantwoordelijke tijdig informeren over de uitkomst van iedere evaluatie en waar nodig aanvullingen en verbeteringen voorstellen. De Verwerker zal Verwerkingsverantwoordelijke voldoende tijd geven om te reageren op de voorgestelde aanvullingen en verbeteringen.
- 5.5 Indien Verwerker relevante, door derden verstrekte, certificaten, audit-rapporten of beoordelingen heeft ontvangen in verband met de beveiliging van data, zal Verwerker deze certificaten, audit-rapporten of beoordelingen op eerste verzoek van Verwerkingsverantwoordelijke aan Verwerkingsverantwoordelijke verstrekken. Op verzoek van Verwerkingsverantwoordelijke, zoals met redelijke tussenpozen gedaan, zal Verwerker een kopie van de meest recente certificaten, audit-rapporten of beoordelingen aan Verwerkingsverantwoordelijke verstrekken, indien van toepassing, dan wel indien verzocht een samenvatting van het voorgaande, welke Verwerkingsverantwoordelijke ter beschikking zou kunnen stellen van haar klanten.

## Artikel 6 Datalekken

- 6.1 Verwerker verplicht zich hierbij tot een passend beleid ten aanzien van incidenten en Datalekken, zoals maar niet beperkt tot protocollen die conformeren met Privacy Wet- en Regelgeving.
- 6.2 Verwerker stelt de Verwerkingsverantwoordelijke onverwijld, maar in ieder geval binnen achtenveertig uur na ontdekking hiervan, in kennis van een Datalek of een inbreuk op de beveiliging, zoals bedoeld in artikel 5.1, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van Persoonsgegevens en verleent Verwerkingsverantwoordelijke voorts alle medewerking in de afhandeling van een dergelijke inbreuk, waaronder mede verstaan, doch niet beperkt tot de (medewerking aan) de tijdige melding van een inbreuk bij de Autoriteit Persoonsgegevens en (voor zover vereist) het tijdig inlichten van de Betrokkene.
- 6.3 Indien een situatie als bedoeld in artikel 6.2 zich voordoet, verplicht Verwerker zich hierbij tot geheimhouding van ieder gegeven in verband met het Datalek of de inbreuk op de beveiliging. Verwerker zal in geen enkele omstandigheid informatie naar buiten brengen over dit Datalek of

de inbreuk op de beveiliging zonder de voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke.

- 6.4 De melding die Verwerker aan Verwerkingsverantwoordelijke doet zoals bepaald in artikel 6.2, omvat in ieder geval:
- I. De mogelijke oorzaak en de mogelijke gevolgen van het Datalek of het incident;
  - II. De (categorieën van) de betrokken Persoonsgegevens;
  - III. Een weergave van de mogelijke gevolgen voor de Betrokkene;
  - IV. Een opgave van de mogelijke (ongeautoriseerde) ontvangers van Persoonsgegevens;
  - V. De door Verwerker aanbevolen maatregelen ter beperking van de schade, voor zover relevant;
- 6.5 Indien de melding zoals bepaald in artikel 6.2 plaatsvindt, houdt Verwerker zich beschikbaar en bereikbaar voor overleg met Verwerkingsverantwoordelijke.
- 6.6 Verwerker zal de melding aan Verwerkingsverantwoordelijke via e-mail en telefoon uitvoeren, verzekert zich ervan dat de melding de Verwerkingsverantwoordelijke tijdig bereikt.
- 6.7 Verwerkingsverantwoordelijke, uitsluitende de Verwerker, is verantwoordelijk voor enige melding aan de Autoriteit Persoonsgegevens of Betrokkene. Verwerker zal nimmer zelfstandig overgaan tot enige melding aan de Autoriteit Persoonsgegevens of Betrokkene.

#### **Artikel 7 Sub-verwerkers**

- 7.1 Zonder de voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke, zal Verwerker geen Sub-verwerker aanstellen voor de verwerking van Persoonsgegevens. Indien en voor zover Verwerkingsverantwoordelijke heeft ingestemd met het gebruik van een Sub-verwerker, zal Verwerker een schriftelijke overeenkomst met deze Sub-verwerker aangaan, welke de Sub-verwerker minimaal de dezelfde verplichtingen uit deze Overeenkomst oplegt als die waaraan de Verwerker uit hoofde van deze Overeenkomst dient te voldoen.

#### **Artikel 8 Doorgifte Persoonsgegevens**

- 8.1 Zonder de voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke is Verwerker niet gerechtigd om Persoonsgegevens uit de EER te transporteren, noch is Verwerker gerechtigd Persoonsgegevens naar Sub-verwerkers buiten de EER te transporteren of anderszins buiten de EER te verwerken. Voor de interpretatie van dit artikel wordt onder 'verwerken' tevens uitdrukkelijk verstaan de opslag en kennisname van Persoonsgegevens dan wel het gebruik van middelen voor verwerken anders dan louter voor de doorvoer van Persoonsgegevens.
- 8.2 In het geval Verwerkingsverantwoordelijke heeft toegestemd in het transport van Persoonsgegevens door Verwerker naar een Sub-verwerker die buiten de EER bevindt, zal Verwerker slechts Persoonsgegevens naar deze Sub-verwerker transporteren indien deze Sub-verwerker zich bevindt binnen een land of gebied alwaar een passend beschermingsniveau in de zin van de Privacy Wet- en Regelgeving wordt geboden.

## **Artikel 9 Geheimhouding**

- 9.1 De Verwerker garandeert dat zij alle Persoonsgegevens vertrouwelijk zal behandelen.
- 9.2 De Verwerker zal haar werknemers, adviseurs en onderaannemers die zich bezighouden met de verwerking van Persoonsgegevens op de hoogte stellen van de vertrouwelijke aard van die Persoonsgegevens en de overige gegevens. Daarnaast garandeert de Verwerker dat deze werknemers, adviseurs en onderaannemers tegenover de Verwerker gebonden zijn aan dezelfde geheimhoudingsverplichtingen als de Verwerker volgens deze Verwerkersovereenkomst en dat de Persoonsgegevens uitsluitend aan deze personen en partijen worden verstrekt voor zover dit noodzakelijk is uit hoofde van de Opdracht.
- 9.3 De Verwerker mag de Persoonsgegevens alleen openbaar maken, verstrekken of op een andere manier beschikbaar stellen aan Derden, met voorafgaande en specifieke schriftelijke toestemming van de Verwerkingsverantwoordelijke of indien een wettelijke of tuchtrechtelijke regel zulks toestaat.
- 9.4 Verwerker implementeert procedures en protocollen om aan haar verplichtingen uit hoofde van dit artikel te voldoen en verstrekt Verwerkingsverantwoordelijke hiervan op eerste verzoek een kopie.

## **Artikel 10 Aansprakelijkheid**

- 10.1 De totale aansprakelijkheid van Verwerker voor alle (financiële) schade, boetes en kosten die Verwerkingsverantwoordelijke heeft en die rechtstreeks of indirect voortvloeien uit een tekortkoming door de Verwerker of derden in de nakoming van verplichtingen onder deze Verwerkersovereenkomst is beperkt tot de aansprakelijkheidsbeperking van Wesselman, zoals beschreven is in de Algemene Voorwaarden en/of de Opdracht.
- 10.2 Verwerker is niet aansprakelijk voor de door de Autoriteit Persoonsgegevens aan Verwerkingsverantwoordelijke opgelegde boetes, dwangsommen en kosten.

## **Artikel 11 Duur en beëindiging**

- 11.1 De Overeenkomst wordt aangegaan voor de duur van de Opdracht. Deze Overeenkomst eindigt van rechtswege op het moment van beëindiging c.q. ontbinding van de Opdracht.
- 11.2 Artikel 3 (Medewerkingsplicht), Artikel 9 (Geheimhouding), en Artikel 12 (Toepasselijk recht en forumkeuze) zullen ook na de beëindiging of ontbinding van deze Overeenkomst voor onbepaalde tijd tussen partijen voortduren.
- 11.3 Voor zover Verwerker na de beëindiging van de Opdracht nog Persoonsgegevens zoals ontvangen van Verwerkingsverantwoordelijke in haar bezit heeft, zal zij deze Persoonsgegevens op zo kort mogelijke termijn aan Verwerkingsverantwoordelijke retourneren of – op uitdrukkelijk verzoek van de Verwerkingsverantwoordelijke- vernietigen, tenzij Verwerker op grond van geldende wet- of regelgeving gehouden is de Persoonsgegevens te bewaren en rekening houdend met de back-up cyclus van de systemen van Verwerker. Voor de interpretatie van dit artikel wordt onder het bezitten van Persoonsgegevens onder andere, maar niet slechts, verstaan de Persoonsgegevens die zich bevinden op gegevensdragers, door Verwerker ingehuurd of ingekochte serverruimte, waar dan ook ter wereld, in sandboxes, op memorysticks, SSD-kaarten of andere middelen gebruikt ter opslag of bewaring van Persoonsgegevens.



- 11.4 Als de Verwerker om technische redenen niet in staat is tot teruggave, vernietiging of verwijdering van de Persoonsgegevens, of als het toepasselijk recht langere opslag van de Persoonsgegevens voorschrijft, zal de Verwerker de Verwerkingsverantwoordelijke daarvan onmiddellijk op de hoogte stellen. In dat geval neemt de Verwerker alle noodzakelijke maatregelen om zo dicht mogelijk bij een volledige en blijvende teruggave, vernietiging of verwijdering van de Persoonsgegevens te komen, en de Persoonsgegevens ongeschikt te maken voor verdere verwerking.
- 11.5 Het risico dat de Persoonsgegevens niet worden teruggegeven, vernietigd of verwijderd blijft bij de Verwerker en de Verwerker blijft gebonden aan die artikelen die gezien hun aard bedoeld zijn om ook na afloop of beëindiging van deze Verwerkersovereenkomst te blijven gelden.
- 11.6 De Verwerker zal alle derden die betrokken zijn bij de verwerking van Persoonsgegevens op de hoogte stellen van de afloop of beëindiging van deze Verwerkersovereenkomst, en garandeert dat alle derden de Persoonsgegevens zullen vernietigen, verwijderen of teruggeven aan Verwerkingsverantwoordelijke op dezelfde wijze als de Verwerker.

## **Artikel 12 Toepasselijk recht en forumkeuze**

- 12.1 Op deze rechtsverhouding is Nederlands recht van toepassing.
- 12.2 Deze Overeenkomst vormt een onderdeel van c.q. een aanvulling op de Algemene Voorwaarden en de Opdracht. Bij strijdigheid tussen bepalingen uit deze Verwerkersovereenkomst en de Opdracht prevaleren de bepalingen uit deze Verwerkersovereenkomst.
- 12.3 Door deze Verwerkersovereenkomst komen alle eerder gemaakte afspraken in dit kader en/of de eventueel eerder(e) ondertekende Verwerkersovereenkomst(en) te vervallen.
- 12.4 Verwerker behoudt zich het recht voor om deze Overeenkomst en/of de bijbehorende bijlagen te wijzigen, te verduidelijken of aan te vullen.
- 12.5 Alle geschillen tussen partijen worden beslecht door de bevoegde rechter in het arrondissement Oost-Brabant.

**Bijlage 1: persoonsgegevens die verwerkt worden door Verwerker (niet limitatief)**

- E-mailadres
- Voornaam
- Achternaam
- Doopnamen
- Adres
- Postcode
- Woonplaats
- Telefoonnummer (zowel mobiel als vast)
- Geslacht
- Burgerlijke staat
- Geboorteplaats
- CV's/CV gegevens
- Kopie paspoort/paspoort gegevens
- Kopie rijbewijs/ rijbewijs gegevens
- Kopie loonstrook/loonstrook gegevens
- Sofinummer/BSN
- Bankrekeningnummer/IBAN
- Creditcardnummer
- Handelsregisternummer
- Overeenkomsten
- Verzekeringspolis
- Klantnummer
- Factuurnummer
- Relatienummer
- Loginnaam
- Wachtwoorden
- Gezondheid (voor zover nodig voor ziektekostenaftrek inkomstenbelasting)
- Lidmaatschapsgegevens
- Social media accounts
- Profiel foto
- Videobeelden
- Kentekens
- Telecomgegevens
- Verkeersgegevens
- Gegevens bedrijf/ bedrijfsnaam
- Gegevens simkaart
- Unieke apparaat nummers
- Serienummers software
- WWFT check/recherche check
- Cliënt groep (bijdrage aan de omzet)
- Financiële informatie (aangiftes/aanslagen)
- Niet geanonimiseerd bezwaar/beroep

**Betrokkenen (niet limitatief)**

- Werknemers
- Familierelaties/partners van werknemers
- Cliënten
- Familierelaties/partners van cliënten
- Zakelijke contacten, waaronder o.a. Belastingdienst-/UWV-/gerechtmedewerkers, medewerkers concullega's, externe advocaten en juristen, bankmedewerkers

## **BIJLAGE 2 – TECHNISCHE EN ORGANISATORISCHE BEVEILIGINGSMATREGELEN**

Verwerker verklaart de volgende technische en/of organisatorische maatregelen te hebben getroffen om te kunnen voldoen aan hetgeen is bepaald in artikel 5 van deze Overeenkomst.

### **1. Software partner AFAS en IT partner ArcusIT**

Wesselman maakt gebruik van de software van AFAS en heeft als IT partner ArcusIT.

Beide partijen beschikken over certificeringen die garant staan voor voldoende huidige beveiligingsmaatregelen op gebied van informatiebeveiliging.

ArcusIT en AFAS werken beide volgens de normenkaders van ISO/IEC 27001.

Dit is de meest bekende standaard voor requirements voor informatiebeveiliging.

En zijn daarmee passende maatregelen voor informatiebeveiliging conform de AVG. (ISO, sd) (ArcusIT, 2016)

AFAS heeft de ISAE 3402 norm voor beheersing van de kwaliteit en veiligheid van AFAS-online en de MJA-3 norm waarbij wordt getest of de systemen kwetsbaar zijn voor aanvallen.

### **2. Technische beveiliging van de cloud-omgeving Wesselman**

Toegang tot de cloud werkomgeving van Wesselman is afgeschermd middels Two-factor authenticatie.

De online omgeving van de gebruikte AFAS software is zo ingericht dat deze enkel te benaderen is vanuit de Wesselman cloud-omgeving. Binnen de Wesselman cloud-omgeving wordt middels single-sign-on ingelogd in de AFAS applicatie.

### **3. Interne maatregelen betreffende de organisatorische beveiligingsmaatregelen**

Binnen Wesselman wordt een streng lock-screen policy gehanteerd voor een goede afscherming van gevoelige data, wordt actief aandacht besteed aan een goede bewustwording voor wat betreft het omgaan met gevoelige data bij haar medewerkers en wordt een streng wachtwoordbeleid gehanteerd.

Tevens wordt de kring van functionarissen die toegang hebben tot bepaalde persoonsgegevens beperkt tot enkel de personen welke deze gegevens nodig hebben voor het uitoefenen van hun werkzaamheden. Daarnaast is er met de medewerkers een geheimhoudingsbeding opgesteld met daaraan gekoppelde boeteclausule.

Binnen Wesselman zijn er protocollen en procedures voor het tijdig en doeltreffend behandelen van informatiebeveiligingsincidenten en wordt er toezicht gehouden op de naleving van de protocollen en wet- en regelgeving.

### **4. Netwerk, internet beveiliging en login**

Wesselman werkt met een afgeschermd digitale omgeving, waarin al de netwerkactiviteiten middels login vastgelegd en gemonitord worden. Deze omgeving is beveiligd middels firewalls en de benodigde virusscanners om optimale veiligheid te realiseren.

### **5. Backup's**

Er worden dagelijks back-ups gemaakt ten behoeve van de continuïteit van de dienstverlening.

Hierbij wordt een retentie van 30 dagen gehanteerd. Deze back-ups worden vertrouwelijk behandeld en bewaard in een gesloten omgeving.

## **6. Fysieke beveiliging**

De locaties van Wesselman beschikken over een alarminstallatie waarbij zorggedragen is aan opvolging indien het alarm afgaat.

Tevens bevinden de bedrijfsservers zich in afsluitbare ruimtes op beide locaties, zowel Eindhoven als Helmond.