

# VERWERKERSOVEREENKOMST

## R.P.O. AUTOMATISERING B.V.

### Verwerkersovereenkomst

#### Partijen

Verwerkingsverantwoordelijke en Verwerker hierna gezamenlijk ook aan te duiden als "Partijen";

#### IN AANMERKING NEMENDE:

- dat Verwerkingsverantwoordelijke beschikt over persoonsgegevens van diverse Betrokkenen;
- dat Verwerkingsverantwoordelijke bepaalde, in de Onderliggende Overeenkomst omschreven vormen van Verwerking laat verrichten of wil laten verrichten door Verwerker;
- dat Verwerker hiertoe bereid is en tevens bereid is verplichtingen omtrent beveiliging en andere aspecten van de Wetgeving op zich te nemen;
- Partijen, mede gelet op de vereisten uit artikel 28 van de Algemene Verordening Gegevensbescherming, hun rechten en plichten schriftelijk in deze Verwerkersovereenkomst wensen vast te leggen.

In tweevoud getekend op .....

te .....

R.P.O. Automatisering B.V.  
Namens deze: R.P.O. Beheer B.V.  
Namens deze: J. Roozen (directeur)

<<Bedrijfsnaam >>  
<<Contactpersoon >>

## KOMEN HET VOLGENDE OVEREEN:

# 1 Definitiebepalingen

De in deze Verwerkersovereenkomst gebruikte en met een hoofdletter geschreven woorden of formuleringen hebben de volgende betekenis:

- **Betrokkene:** een geïdentificeerde of identificeerbare natuurlijke persoon;
- **Onderliggende Overeenkomst:** de overeenkomst waarbij Verwerkingsverantwoordelijke aan Verwerker opdracht heeft gegeven om Verwerkingen te verrichten;
- **Verwerkersovereenkomst:** deze overeenkomst;
- **FG:** Functionaris Gegevensbescherming als bedoeld in de artikelen 37-39 van de Algemene Verordening Gegevensbescherming;
- **Persoonsgegevens(s):** elk gegeven betreffende een of meerdere Betrokkenen die Verwerker op grond van de Onderliggende Overeenkomst verwerkt of dient te verwerken;
- **Bijzondere Persoonsgegevens:** Persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, het lidmaatschap van een vakvereniging, alsmede strafrechtelijke gegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag;
- **BSN:** het burgerservicenummer in de zin van artikel 1 aanhef en onder b van de Wet algemene bepalingen burgerservicenummer;
- **Subverwerker:** een natuurlijke of rechtspersoon die de Verwerking van Persoonsgegevens ten behoeve van de Onderliggende Overeenkomst in opdracht van Verwerker uitvoert;
- **Verwerken/Verwerking:** de verwerking als bedoeld in artikel 4, aanhef en onder 2 van de AVG;
- **Wetgeving:** de Algemene Verordening Gegevensbescherming ("AVG") en de daarop gebaseerde Nederlandse Uitvoeringswet Algemene Verordening Gegevensbescherming.

# 2 Onderwerp van de overeenkomst

- 2.1** Deze Verwerkersovereenkomst houdt verband met de Onderliggende Overeenkomst. Algemene voorwaarden van Verwerker die in de Onderliggende Overeenkomst van toepassing zijn verklaard zijn op de Verwerkersovereenkomst gelijkelijk van toepassing. De bepalingen van deze Verwerkersovereenkomst zijn van toepassing op iedere Verwerking van Persoonsgegevens door Verwerker in verband met de Onderliggende Overeenkomst.
- 2.2** Verwerker verbindt zich door ondertekening van deze Verwerkersovereenkomst om in opdracht van Verwerkingsverantwoordelijke Persoonsgegevens te verwerken in overeenstemming met de in deze Verwerkersovereenkomst gestelde voorwaarden. Het doel van de Verwerking is om de door Verwerker op basis van de Onderliggende Overeenkomst aan Verwerkingsverantwoordelijke ter beschikking gestelde software en/of hosting services zo goed mogelijk te laten functioneren, waartoe de Verwerking van Persoonsgegevens door Verwerker, ofwel structureel indien door Verwerker ook hosting

services worden verleend, ofwel incidenteel als Verwerker op afstand periodiek en incidenteel onderhoud verricht aan de aan Verwerkingsverantwoordelijke ter beschikking gestelde software, onontkoombaar is. De volgende soorten persoonsgegevens worden daarbij verwerkt:

- (Elektronische) Contactgegevens
- NAW-gegevens
- Factuurgegevens
- Medewerkergegevens van Verwerkersverantwoordelijke
- Financiële gegevens

### 2.3 Relatiegegevens

De Persoonsgegevens hebben betrekking op de volgende categorieën van Betrokkenen: (contactpersonen van) Klanten, (contactpersonen van) Leveranciers en medewerkers van Verwerkingsverantwoordelijke. Verwerker zal de Persoonsgegevens alleen Verwerken voor de in artikel 2.2 genoemde doeleinden. Verwerker zal de Persoonsgegevens niet voor enig ander doel Verwerken.

### 2.4 De Persoonsgegevens blijven eigendom van Verwerkingsverantwoordelijke. Zij behoudt daarover steeds de volledige zeggenschap.

## 3 Verplichtingen Verwerker

### 3.1 Verwerker verwerkt de Persoonsgegevens slechts op basis van de schriftelijke instructies van de Verwerkingsverantwoordelijke, onder meer met betrekking tot doorgiften van persoonsgegevens aan een derde land of internationale organisatie, tenzij Verwerker een Unierechtelijke of Nederlandse wettelijke bepaling Verwerker tot verwerking verplicht. In laatstbedoeld geval stelt de Verwerker de Verwerkingsverantwoordelijke, voorafgaand aan de Verwerking, in kennis van die wettelijke bepaling, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

### 3.2 Uitsluitend die personen die binnen de organisatie van Verwerker noodzakelijkerwijs toegang tot de Persoonsgegevens dienen te hebben voor de uitvoering van hun werkzaamheden zullen toegang krijgen tot de Persoonsgegevens. Personen die binnen de organisatie van Verwerker niet noodzakelijkerwijs toegang tot de Persoonsgegevens behoeven, zullen geen toegang krijgen tot de Persoonsgegevens. De personen binnen de organisatie van Verwerker die toegang hebben tot de Persoonsgegevens zijn op grond van de wet althans op grond van de arbeidsovereenkomst tot geheimhouding van de Persoonsgegevens verplicht.

### 3.3 Verwerker treft passende technische en organisatorische maatregelen om te zorgen voor een passend beveiligingsniveau. De exacte maatregelen die Verwerkingsverantwoordelijke tenminste van Verwerker verwacht en waartoe Verwerker zich door ondertekening van deze Overeenkomst verplicht zijn beschreven in **Bijlage 1**.

### 3.4 Verwerker verplicht zich om steeds op verzoek van Verwerkingsverantwoordelijke en tegen de gebruikelijke commerciële tarieven bijstand te verlenen aan Verwerkingsverantwoordelijke bij het vervullen van diens plicht om enerzijds verzoeken tot uitoefening van rechten van Betrokkenen te beantwoorden en anderzijds de verplichtingen uit hoofde van artikel 32 tot en met 36 van de AVG na te komen.

### 3.5 Tevens zal Verwerker Persoonsgegevens die haar in het kader van deze Verwerkingsovereenkomst ter beschikking zijn gesteld niet langer bewaren dan noodzakelijk is (i) voor de uitvoering van deze Overeenkomst; of (ii) om een op hem rustende wettelijke verplichting na te komen. Aangezien de dienstverlening van Verwerker voor Verwerkingsverantwoordelijke uitsluitend bestaat uit het bieden van

toegang tot door Verwerkingsverantwoordelijke in haar bedrijfsprocessen gebruikte software en het periodiek en incidenteel verrichten van onderhoud aan de software, is Verwerker niet actief betrokken bij de handhaving van de overeengekomen bewaartermijnen. De verplichting tot (het toezicht op) naleving van de overeengekomen bewaartermijnen rust daarom uitsluitend op Verwerkingsverantwoordelijke, die zal zorgdragen voor tijdige verwijdering van Persoonsgegevens waarvan de bewaartermijn is verstreken. Bij overschrijding van de bewaartermijnen zal geen enkele aansprakelijkheid jegens Verwerkingsverantwoordelijke op Verwerker rusten.

Verwerkingsverantwoordelijke zal Verwerker vrijwaren voor alle aanspraken van derden op Verwerker wegens vermeende overschrijding van de bewaartermijnen, met inbegrip van de juridische kosten die Verwerker zal moeten maken ter afwering van de betreffende aanspraak.

- 3.6** De Verwerker heeft geen FG. De Verwerker wordt door Verwerkingsverantwoordelijke geacht geen FG aan te stellen.
- 3.7** De Verwerker houdt een register bij van voor Verwerkingsverantwoordelijke verwerkte Persoonsgegevens. Daarin vermeldt Verwerker:
- diens naam en contactgegevens;
  - de contactgegevens van Verwerkingsverantwoordelijke;
  - de categorieën van verwerkingen die Verwerker voor Verwerkingsverantwoordelijke uitvoert;
  - indien van toepassing, de doorgiften van persoonsgegevens aan derde landen of internationale organisaties, welke derde landen of internationale organisaties dat betreft en indien van toepassing de documenten waarde de passende waarborgen die worden getroffen inzichtelijk zijn;
  - indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.
- 3.8** Verwerker stelt het in artikel 3.7 bedoelde register op verzoek ter beschikking aan de Autoriteit Persoonsgegevens en desgewenst aan Verwerkingsverantwoordelijke.
- 3.9** De Verwerker stelt aan de Verwerkingsverantwoordelijke alle informatie ter beschikking die nodig is om de nakoming van de in deze Verwerkersovereenkomst opgenomen verplichtingen aan te tonen en zal audits, waaronder inspecties, door de Verwerkingsverantwoordelijke of een haar gemachtigde controleur mogelijk maken en daaraan volledige medewerking verlenen. Verwerker stelt Verwerkingsverantwoordelijke onmiddellijk in kennis indien naar zijn mening een instructie van Verwerkingsverantwoordelijke aan Verwerker inbreuk oplevert op de Wetgeving.
- 3.10** Indien Verwerkingsverantwoordelijke door middel van de Onderliggende Overeenkomst of de Verwerkersovereenkomst aan Verwerker de verwerking van het BSN opdraagt (waaronder mede wordt begrepen de verwerking door Verwerkingsverantwoordelijke op door Verwerker aan haar ter beschikking gestelde systemen in het kader van hosting services), garandeert Verwerkingsverantwoordelijke dat die verwerking plaats vindt ter uitvoering van de Wet algemene bepalingen Burgerservicenummer dan wel voor doeleinden bij de wet bepaald. Verwerkingsverantwoordelijke vrijwaart Verwerker voor alle schade, waaronder mede begrepen opgelegde boetes en kosten van bezwaar en beroep (inclusief kosten rechtsbijstand) tegen opgelegde boetes, die Verwerker lijdt in het geval de verwerking van het BSN ondanks de in dit artikellid door Verwerkingsverantwoordelijke verstrekte garantie niet legitiem blijkt.

## 4 Inzet Subverwerkers

- 4.1 Verwerkingsverantwoordelijke staat Verwerker toe om de uitvoering van de Verwerkersovereenkomst geheel of gedeeltelijk uit te besteden aan de in de Onderliggende Overeenkomst genoemde Subverwerkers. Bij wijzigingen in de inzet van die Subverwerkers, bijvoorbeeld de beëindiging van de inzet van een Subverwerker of de inschakeling van een nieuwe Subverwerker, is Verwerker verplicht om Verwerkingsverantwoordelijke daarover schriftelijk te informeren.
- 4.2 Verwerker zal hoe dan ook aan Subverwerkers dezelfde of soortgelijke verplichtingen opleggen als voor zichzelf uit deze Verwerkersovereenkomst voortvloeien en toezien op de naleving daarvan door Subverwerker.

## 5 Doorgifte van Persoonsgegevens

- 5.1 Verwerker zal de Persoonsgegevens niet buiten de Europese Unie verwerken of doen verwerken zonder voorafgaande schriftelijke toestemming van de Verwerkingsverantwoordelijke.
- 5.2 Verwerker zal geen Persoonsgegevens aan derden ter beschikking stellen, tenzij op grond van een uitdrukkelijke schriftelijk verzoek van Verwerkingsverantwoordelijke of op een bevoegd gegeven bevel van een gerechtelijke of bestuurlijke instantie, op voorwaarde dat Verwerker in dat geval Verwerkingsverantwoordelijke binnen 24 uur na ontvangst van een dergelijk bevel daarvan in kennis stelt om Verwerkingsverantwoordelijke zodoende in staat te stellen daartegen tijdig een rechtsmiddel in te stellen.
- 5.3 Oordeelt Verwerker dat zij op grond van de Wetgeving verplicht is om Persoonsgegevens ter beschikking te stellen aan een daartoe bevoegde instantie zal zij daar niet toe overgaan, dan na overleg met en instemming van Verwerkingsverantwoordelijke. Zij zal Verwerkingsverantwoordelijke zo spoedig mogelijk schriftelijk in kennis stellen van de wettelijke verplichting en daarbij alle relevante informatie verstrekken die Verwerkingsverantwoordelijke redelijkerwijs nodig heeft om de benodigde maatregelen te treffen, om te bepalen of verstrekking kan plaatsvinden en, zo ja, onder welke voorwaarden. Daarnaast zal Verwerker de verstrekking beperken tot hetgeen wettelijk verplicht is en zal zij Verwerkingsverantwoordelijke in staat stellen om haar rechten en de rechten van Betrokkenen uit te oefenen en de belangen van Verwerkingsverantwoordelijke en Betrokkenen te verdedigen.

## 6 Datalek

- 6.1 Verwerker stelt Verwerkingsverantwoordelijke onverwijld en niet later dan 24 uur nadat Verwerker er kennis van heeft gekregen, in kennis van iedere inbreuk op de beveiliging van Persoonsgegevens. Verwerker doet deze melding aan een door Verwerkingsverantwoordelijke aan te wijzen persoon of personen. Indien een FG is aangesteld, wordt een kopie van de melding verzonden aan de FG van Verwerkingsverantwoordelijke.
- 6.2 De Verwerker meldt bij of zo snel mogelijk na de in lid 1 bedoelde melding aan Verwerkingsverantwoordelijke (1) wat de (vermoedelijke) oorzaak is van de inbreuk, (2)

wat het (vooralsnog bekende en/of te verwachten) gevolg is van de inbreuk en (3) wat de voorgestelde oplossing is. De onmogelijkheid om antwoord te geven op de in dit artikellid genoemde vragen laat de verplichting tot het doen van de in lid 1 bedoelde melding onverlet.

- 6.3 Wanneer zich een inbreuk voordoet bij Verwerkingsverantwoordelijke, meldt Verwerkingsverantwoordelijke de inbreuk onverwijld aan een door Verwerker aan te wijzen persoon of personen onder opgave van de antwoorden, voor zoveel mogelijk, op de in lid 2 van dit artikel genoemde vragen. Tevens stelt Verwerkingsverantwoordelijke aan Verwerker maatregelen voor die Verwerker kan treffen om de gevolgen te verhelpen of te matigen.
- 6.4 Nadere afspraken ten aanzien van de naleving van de meldplicht in verband met inbreuken op de beveiliging van Persoonsgegevens zijn weergegeven in **Bijlage 2**.

## 7 Verzoeken van Betrokkenen

- 7.1 Verwerker stelt Verwerkingsverantwoordelijke in kennis van alle bij haar binnen gekomen verzoeken van Betrokkenen tot inzage in, correctie en/of verwijdering van de Persoonsgegevens. Verwerker geeft aan een dergelijk verzoek uitsluitend gevolg indien Verwerkingsverantwoordelijke Verwerker daartoe schriftelijk toestemming heeft gegeven. Inzage wordt alleen via Verwerkingsverantwoordelijke verschaft.
- 7.2 Verwerker handelt alle verzoeken om inlichtingen van Verwerkingsverantwoordelijke met betrekking tot de verwerking van de Persoonsgegevens zo snel mogelijk af.

## 8 Opsporingsverzoek

- 8.1 Indien Verwerker een verzoek of een bevel van een Nederlandse of buitenlandse toezichthouder op het gebied van de bescherming van persoonsgegevens, overheidsinstantie of een opsporings-, strafvorderings- of nationale veiligheidsinstantie ontvangt om (inzage in) Persoonsgegevens te verschaffen, dan zal Verwerker de Verwerkingsverantwoordelijke onverwijld informeren. Bij de behandeling van het verzoek of bevel zal Verwerker alle instructies van Verwerkingsverantwoordelijke in acht nemen (waaronder de instructie om de behandeling van het verzoek of bevel geheel of gedeeltelijk aan Verwerkingsverantwoordelijke over te laten) en alle redelijkerwijs benodigde medewerking verlenen.
- 8.2 Indien het Verwerker op grond van het verzoek of bevel is verboden om te voldoen aan zijn verplichtingen op grond van het eerste lid, dan zal Verwerker de redelijke belangen van Verwerkingsverantwoordelijke zo goed mogelijk behartigen. Verwerker zal daartoe in ieder geval:
- zich juridisch laten adviseren over de verplichting om aan het bevel te voldoen en het verbod om Verwerkingsverantwoordelijke te informeren;
  - uitsluitend aan het bevel meewerken in het geval van een daadwerkelijke wettelijke verplichting en waar mogelijk (in rechte) bezwaar maken tegen het bevel en/of het verbod om Verwerkingsverantwoordelijke daarover te informeren.
  - Niet meer Persoonsgegevens verstrekken dan strikt noodzakelijk om aan het verzoek of bevel te voldoen;

- d. Indien sprake is van doorgifte naar een land buiten de EER of naar een internationale organisatie zal Verwerker steeds zoveel mogelijk de voorschriften van artikel 44 tot en met 50 AVG opvolgen en zich waar nodig daarover juridisch laten adviseren;
- e. Verwerkingsverantwoordelijke onverwijld informeren zodra dit is toegestaan.

## 9 Geheimhouding en vertrouwelijkheid

- 9.1 Verwerker verplicht zich tot geheimhouding van alle Persoonsgegevens die Verwerker van Verwerkingsverantwoordelijke ontvangt en/of zelf verzamelt in het kader van deze Verwerkersovereenkomst. Verwerker zal deze Persoonsgegevens niet aan derden ter beschikking stellen, tenzij met uitdrukkelijke voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke, indien het verstrekken van de Persoonsgegevens noodzakelijk is ter uitvoering van deze overeenkomst of de Onderliggende Overeenkomst, of indien Verwerker op grond van de wet verplicht is om Persoonsgegevens aan derden te verstrekken. Deze geheimhoudingsverplichting is bestemd om voort te duren ook nadat deze Overeenkomst zal zijn geëindigd.
- 9.2 Onder derden in de zin van deze bepaling wordt ook begrepen de medewerkers en/of opdrachtnemers van Verwerker voor zover het niet noodzakelijk is dat zij bij de Opdracht en/of deze overeenkomst kennis hoeven te nemen van de Persoonsgegevens.
- 9.3 Verwerker zorgt dat zijn personeel en opdrachtnemers gebonden zijn aan de in dit artikel opgenomen geheimhoudingsplicht en dat Verwerker van die gebondenheid schriftelijk bewijs bezit. Op eerste verzoek van Verwerkingsverantwoordelijke verstrekt Verwerker dat bewijs aan Verwerkingsverantwoordelijke.

## 10 Aansprakelijkheid

- 10.1 Verwerker is niet aansprakelijk voor schade die Verwerkingsverantwoordelijke lijdt die voortvloeit uit of verband houdt met tekortkomingen in de nakoming van de op Verwerker rustende verplichtingen uit hoofde van deze Verwerkersovereenkomst en/of de Wetgeving, tenzij de schade het gevolg is van opzet of bewuste roekeloosheid van de zijde van Verwerker.
- 10.2 In alle gevallen is de aansprakelijkheid van Verwerker beperkt tot het bedrag dat in voorkomende gevallen wordt uitgekeerd op basis van de aansprakelijkheidsverzekering van Verwerker.

## 11 Duur en beëindiging

- 11.1 Deze Verwerkersovereenkomst wordt aangegaan voor onbepaalde tijd, althans voor de duur van de Onderliggende Overeenkomst.
- 11.2 Tenzij anders overeengekomen zal Verwerker in geval van beëindiging van de onderliggende Overeenkomst onverwijld alle aan haar ter beschikking gestelde en door haar bij uitvoering van deze overeenkomst verzamelde Persoonsgegevens aan Verwerkingsverantwoordelijke retourneren en alle digitale kopieën van Persoonsgegevens vernietigen en aan Verwerkingsverantwoordelijke bevestigen dat zij dit heeft uitgevoerd, behoudens en voor zover Verwerker op basis van de op haar van toepassing zijnde wettelijke bepalingen tot het bewaren van Persoonsgegevens verplicht is. Daarnaast zal

de Verwerker een kopie van het bijgehouden register van verwerkingen aan Verwerkingsverantwoordelijke ter beschikking stellen.

## 12 Overdracht rechten en verplichtingen

De rechten en verplichtingen uit deze Verwerkersovereenkomst kunnen door Verwerker niet aan een andere partij worden overgedragen zonder de voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke.

## 13 Intellectuele eigendomsrechten

- 13.1** Alle (aanspraken op) intellectuele eigendomsrechten - waaronder auteursrechten, databankrechten en alle overige rechten van intellectuele eigendom - op de verzameling van Persoonsgegevens, kopieën of bewerkingen daarvan, berusten te allen tijde bij en/of komen toe aan Verwerkingsverantwoordelijke. Verwerker erkent de (aanspraken op) intellectuele eigendomsrechten van Verwerkingsverantwoordelijke en verbindt zich ertoe het bestaan daarvan niet te betwisten. Indien en voor zover overdracht van enig intellectueel eigendomsrecht ten aanzien van de Persoonsgegevens noodzakelijk is om deze rechten bij Verwerkingsverantwoordelijke te laten belanden, dan verplicht Verwerker zich door ondertekening van deze Verwerkingsovereenkomst tot medewerking aan elke noodzakelijke handeling om die overdracht te bewerkstelligen.
- 13.2** Alle intellectuele eigendomsrechten - waaronder auteursrechten, databankrechten en alle overige rechten van intellectuele eigendom - op de producten en dienstverlening van Verwerker, berusten te allen tijde bij Verwerker. Verwerkingsverantwoordelijke erkent de intellectuele eigendomsrechten van Verwerker en verbindt zich ertoe het bestaan daarvan niet te betwisten.

## 14 Toepasselijk recht en geschillen

- 14.1** Uitsluitend Nederlands recht is van toepassing op deze Verwerkersovereenkomst.
- 14.2** Eventuele geschillen in verband met deze Verwerkersovereenkomst zullen uitsluitend worden behandeld door de bevoegde rechtbank in de plaats van vestiging van Verwerker.
- 14.3** Deze Verwerkersovereenkomst kan slechts worden gewijzigd door middel van een schriftelijk stuk waarin uitdrukkelijk staat vermeld dat het stuk bedoelt een dergelijke wijziging aan te brengen en dat door ter zake bevoegde vertegenwoordigers van Partijen is ondertekend.



## Bijlage 1

# BESCHRIJVING VAN DE TECHNISCHE EN ORGANISATORISCHE BEVEILIGINGSMAATREGELEN

### **Verantwoordelijkheid Verwerker**

Op onderstaande gebieden zijn er meerdere maatregelen binnen de organisatie en infrastructuur geïmplementeerd.

### **Beveiligingsbeleid**

Verwerker heeft een privacybeleid. Dit beleid is leidend voor alle Verwerkers bedrijfsonderdelen, medewerkers en alle beveiligingsinspanningen.

### **Beheer van bedrijfsmiddelen**

Alle bedrijfsmiddelen zijn geïnventariseerd en toegewezen aan individuele gebruikers. Klantgegevens worden beveiligd opgeslagen.

### **Beveiligingseisen van personeel**

Alle medewerkers, in loondienst of ingehuurd, tekenen bij indiensttreding een verklaring waarin zij zich verplichten tot geheimhouding inzake alles aangaande het bedrijf, processen, klanten en relaties. Alle medewerkers worden bij indiensttreding gewezen op de regels en procedures binnen de organisatie, in het bijzonder op de geldende beveiligings- en privacyregels en -procedures.

### **Cryptografie**

Ter bescherming van informatie worden er een aantal cryptografische beheersmaatregelen geïmplementeerd, zoals harddisk encryptie in alle Verwerker laptops en encryptie op externe gegevensdragers.

### **Fysieke beveiliging en beveiliging van de omgeving**

De diensten van Verwerker worden geleverd vanuit een behoorlijk beveiligde kantoor- en serverruimte. Het centrale platform is redundant uitgevoerd en verdeeld naar een behoorlijk beveiligde datacenterlocatie. De beveiligde zones, zoals hiervoor benoemd, zijn beschermd middels toegangsbeveiliging, zodat alleen geautoriseerd personeel toegang heeft. Er zijn tevens maatregelen getroffen om ongeautoriseerde toegang te detecteren.

### **Beheer van communicatie- en bedieningsprocessen**

De processen noodzakelijk voor het beheer van de dienst worden volgens vaste gedocumenteerde procedures afgehandeld. Dit betreft:

- incidentbeheer
- probleembeheer
- wijzigingsbeheer
- configuratiebeheer

Wanneer de applicatie lokaal (on premises) bij de klant staat, zal Verwerker via een behoorlijk beveiligde verbinding toegang verkrijgen tot het netwerk.

### **Toegangbeveiliging**

Autorisaties worden toegekend op basis van need-to-know principes. Dit wil zeggen dat een gebruiker in principe alleen die autorisaties krijgt voor het gebruiken van bedrijfsmiddelen en bedrijfsinformatie, die nodig zijn voor zijn of haar werkzaamheden. Er is een gedocumenteerde procedure van kracht voor aanvraag, registratie, beheer en wijziging van logische toegangsrechten en autorisaties. Periodiek wordt gecontroleerd of de autorisaties nog in overeenstemming zijn met het vastgelegde toegangsbeleid. Alle gebruikers hebben een unieke gebruikersidentificatie (user-id) voor strikt eigen gebruik om ervoor te zorgen dat activiteiten terug te voeren zijn tot de daarvoor verantwoordelijke persoon. Tweemaandelijks worden de wachtwoorden gewijzigd, volgens vastgestelde eisen.

### **Verwerving, ontwikkeling en onderhoud van informatiesystemen**

De Verwerkers applicaties zijn ontwikkeld op basis van erkende ontwikkelstandaarden, waarbij rekening wordt gehouden met security standaarden en niet functionele eisen.

### **Beheer van informatiebeveiligingsincidenten**

Er is een procedure voor de afhandeling van beveiligingsincidenten. Beveiligingsincidenten worden gerapporteerd aan en besproken met de Verwerker. Daarnaast beschikt Verwerker over relevante contacten met beveiligingsorganisaties. Deze organisaties informeren Verwerker over mogelijke bedreigingen die een potentieel risico voor de organisatie kunnen vormen, zodat hierop tijdig actie kan worden ondernomen.

### **Naleving**

Alle relevante eisen uit wet- en regelgeving en contractuele eisen van klanten zijn in kaart gebracht en er zijn passende maatregelen getroffen om te waarborgen dat hieraan wordt voldaan.

## Bijlage 2

# NADERE AFSPRAKEN TEN AANZIEN VAN DE NALEVING VAN DE MELDPLICHT DATALEKKEN

Verwerkingsverantwoordelijke en Verwerker onderkennen het belang van goede technische en organisatorische beveiliging van persoonsgegevens. Niettemin kan niet uitgesloten worden dat op enig moment een inbreuk op de beveiliging van Persoonsgegevens optreedt, bij Verwerkingsverantwoordelijke of bij Verwerker. Partijen onderkennen voorts dat een inbreuk zo snel mogelijk opgemerkt moet worden en bekend moet worden gemaakt aan de andere Partij, opdat maatregelen getroffen kunnen worden ter beperking van de gevolgen van de inbreuk en melding aan de toezichthouder kan worden overwogen.

- 1.** Opmerken van technische inbreuken
  - 1.1** Verwerker en Verwerkingsverantwoordelijke verplichten zich om op de door hen beheerde systemen, systemen in werking te hebben en te houden bestemd om technische inbreuken op de beveiliging op te merken.
- 2.** Opmerken van organisatorische inbreuken
  - 2.1** Verwerker en Verwerkingsverantwoordelijke verplichten zich om een intern protocol datalekken te hebben, opdat inbreuken op de beveiliging als gevolg van menselijk handelen tijdig bekend worden. In dit protocol worden medewerkers ten minste verplicht om elke inbreuk onmiddellijk (dat wil zeggen binnen 1 uur nadat de inbreuk zich heeft voorgedaan) te melden bij hun direct leidinggevende. Verwerkingsverantwoordelijke en Verwerker zullen ervoor zorgen dat de medewerkers aan de inhoud van genoemd protocol gebonden zijn.
- 3.** Melding en beoordeling van inbreuken
  - 3.1** Verwerker is verplicht om elke inbreuk te melden aan Verwerkingsverantwoordelijke. De melding geschiedt per e-mail aan de directie van Verwerkingsverantwoordelijke en, zo deze er is, aan de FG van Verwerkingsverantwoordelijke.
  - 3.2** Na melding bij de Verwerkingsverantwoordelijke beoordeelt en beslist zij of er een melding bij de Autoriteit Persoonsgegevens, althans de krachtens artikel 55 AVG bevoegde toezichthouder zal doen. Indien tot het doen van een melding wordt besloten, verstrekt Verwerkingsverantwoordelijke een kopie van de melding aan Verwerker. Indien in een concreet geval wordt besloten om geen melding aan de Autoriteit, althans de bevoegde toezichthouder, en/of de Betrokkenen te doen, vrijwaart Verwerkingsverantwoordelijke Verwerker voor alle schade die als gevolg van het besluit om niet te melden mocht worden geleden.
  - 3.3** Of Verwerkingsverantwoordelijke een melding doet tevens aan de Betrokkenen is afhankelijk van de vraag of de gelekte gegevens al dan niet (goed) waren versleuteld of het datalek om andere redenen (waarschijnlijk) ongunstige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene(n). De beoordeling en beantwoording van deze vraag is voorbehouden aan Verwerkingsverantwoordelijke.
  - 3.4** Verwerker zal niet zelf overgaan tot het verrichten van een melding aan de Autoriteit Persoonsgegevens, althans de bevoegde toezichthouder en/of Betrokkenen.