Verwerkersvoorwaarden Gjald Bedrijfsvoering B.V.

Deze voorwaarden zijn onlosmakelijk verbonden met alle overeenkomsten die Gjald Bedrijfsvoering B.V. sluit met betrekking tot (AFAS) software optimalisatie, - implementatie of – integratie.

Partijen:

1. **Gjald Bedrijfsvoering B.V.**, hierna te noemen: "**VERWERKER**";

en

2. Afnemer, hierna te noemen "**VERANTWOORDELIJKE**";

hierna gezamenlijk te noemen: "**Partijen**".

OVERWEGINGEN:

A. VERANTWOORDELIJKE en VERWERKER een overeenkomst hebben gesloten, hierna de "**Overeenkomst**". In het kader van de uitvoering van de Overeenkomst verleent VERWERKER diensten aan VERANTWOORDELIJKE;

B. VERWERKER in het kader van de uitvoering van de Overeenkomst ook Persoonsgegevens verwerkt voor VERANTWOORDELIJKE;

C. Partijen wettelijk verplicht zijn afspraken te maken en vast te leggen met betrekking tot de verwerking van Persoonsgegevens door VERWERKER;

D. de bepalingen van deze Verwerkersvoorwaarden vóórgaan op alle andere afspraken die tussen Partijen gelden en betrekking hebben op de verwerking van Persoonsgegevens door VERWERKER voor VERANTWOORDELIJKE.

PARTIJEN ZIJN HET VOLGENDE OVEREENGEKOMEN:

Artikel 1. Definities

Naast de wettelijke definities hebben de volgende termen de volgende betekenis:

"*AP*"	Autoriteit Persoonsgegevens, ook College Bescherming Persoonsgegevens genoemd, de toezichthoudende autoriteit voor de naleving van de geldende privacywetgeving;
"*AVG*"	Algemene Verordening Gegevensbescherming, voluit: Verordening (EU) 2016/679 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;
"*Betrokkene*"	de natuurlijke persoon waarop de Persoonsgegevens die VERWERKER verwerkt voor VERANTWOORDELIJKE en/of haar opdrachtgevers in het kader van de uitvoering van de Overeenkomst betrekking hebben;
"*Beveiligingsincident*"	een 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 doorgezonden, opgeslagen of anderszins verwerkte Persoonsgegevens;
"*Verwerkersvoorwaarden*"	de onderhavige overeenkomst inclusief alle bijlagen die onlosmakelijk hieraan zijn verbonden;
"*Bijlage*"	iedere bijlage bij deze Verwerkersvoorwaarden, welke een onlosmakelijk deel daarvan uitmaakt;
"*Derde*"	een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de Betrokkene, noch de VERANTWOORDELIJKE, noch de VERWERKER, noch de personen die onder rechtstreeks gezag van de VERANTWOORDELIJKE of de VERWERKER gemachtigd zijn om de Persoonsgegevens te verwerken;
"*Diensten*"	alle diensten die VERWERKER aan VERANTWOORDELIJKE verleent, zoals omschreven in de Overeenkomst;
"*EER*"	Europese Economische Ruimte;
"*Persoonsgegevens*"	alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon die VERWERKER ontvangt van of verwerkt voor VERANTWOORDELIJKE in het kader van de uitvoering van de Overeenkomst;
"*Sub-verwerker*"	een partij die door VERWERKER wordt ingeschakeld voor de uitvoering van de Overeenkomst en de daarbij horende verwerking van Persoonsgegevens;
"*Wbp*"	Wet bescherming persoonsgegevens;
"*Verwerken*"	elke handeling of elk geheel van handelingen met betrekking tot Persoonsgegevens, 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. Algemeen

2.1 VERANTWOORDELIJKE wordt ten aanzien van de Persoonsgegevens beschouwd als verantwoordelijke in de zin van de Wbp en verwerkingsverantwoordelijke in de zin van de AVG. VERWERKER is bewerker in de zin van de Wbp en verwerker in de zin van de AVG. Indien de voormelde terminologie op enig moment mocht afwijken van de gangbare of wettelijke terminologie, laat dit de inhoud van deze Verwerkersvoorwaarden en de juridische verhouding tussen Partijen onverlet.

2.2 Partijen verstrekken aan elkaar alle benodigde informatie en verlenen elkaar de medewerking die redelijkerwijs van de ander kan worden verwacht om een goede naleving van de geldende privacywet- en regelgeving en deze Verwerkersvoorwaarden mogelijk te maken.

2.3 Deze Verwerkersvoorwaarden maken onlosmakelijk onderdeel uit van de Overeenkomst. Daar waar de Overeenkomst afwijkt van hetgeen in deze Verwerkersvoorwaarden is bepaald, prevaleren deze Verwerkersvoorwaarden.

Artikel 3. Verwerken van Persoonsgegevens

3.1 VERWERKER zal de Persoonsgegevens in overeenstemming met de geldende wet- en regelgeving verwerken in haar hoedanigheid van verwerker en heeft de categorieën van betrokkenen, het soort Persoonsgegevens en de aard en het doel waarvoor de Persoonsgegevens worden verwerkt opgenomen in **Bijlage 1**. VERWERKER zal de Persoonsgegevens niet voor andere doeleinden of op andere wijze gebruiken dan voor het doel waarvoor de Persoonsgegevens zijn verstrekt of haar bekend zijn geworden.

3.2 VERWERKER zal de Persoonsgegevens uitsluitend verwerken op basis van de schriftelijke instructies van VERANTWOORDELIJKE in het kader van de uitvoering van de Overeenkomst en de verleende Diensten, dan wel in verband met een wettelijke verplichting.

3.3 VERWERKER zal de Persoonsgegevens niet aan een Derde verstrekken, tenzij deze uitwisseling plaatsvindt in opdracht van of met toestemming van VERANTWOORDELIJKE in het kader van de uitvoering van de Overeenkomst of wanneer dit voortvloeit uit een wettelijke verplichting.

3.4 VERWERKER zal, voor zover het in haar macht ligt, iedere redelijke inspanning verrichten om aan Derden ten minste dezelfde voorwaarden op te leggen als die welke ten aanzien van hem gelden op grond van deze Verwerkersvoorwaarden.

3.4 VERWERKER draagt er zorg voor dat de Persoonsgegevens niet buiten de EER worden verwerkt, tenzij VERANTWOORDELIJKE daar schriftelijke toestemming voor heeft gegeven.

Artikel 4. Geheimhouding

4.1 VERWERKER houdt de Persoonsgegevens die zij verwerkt in het kader van de uitvoering van de Overeenkomst geheim en zal, voor zover het in haar macht ligt, alle redelijke maatregelen treffen om geheimhouding van de Persoonsgegevens te waarborgen. VERWERKER zal iedere redelijke inspanning verrichten om de verplichting tot geheimhouding tevens op te leggen aan haar personeel en alle door haar ingeschakelde (hulp)personen.

4.2 De in dit artikel bedoelde geheimhoudingsplicht geldt niet indien VERANTWOORDELIJKE schriftelijk toestemming heeft gegeven om de Persoonsgegevens aan een Derde te verstrekken, of een wettelijke verplichting bestaat om de Persoonsgegevens aan een Derde te verstrekken.

Artikel 5. Beveiliging Persoonsgegevens

5.1 VERANTWOORDELIJKE zal in overeenstemming met de geldende wettelijke regels de beveiliging van de Persoonsgegevens waarborgen en daartoe passende technische en organisatorische maatregelen treffen.

5.2 VERWERKER zal in overeenstemming met de geldende wet- en regelgeving technische en organisatorische maatregelen treffen, in stand houden en zo nodig aanpassen om een op het risico afgestemd beveiligingsniveau te waarborgen.

5.3 Partijen zullen bij het treffen van beveiligingsmaatregelen rekening houden met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen.

5.5 Indien VERANTWOORDELIJKE een beoordeling wenst uit te voeren van een beoogde verwerkingsactiviteit in het kader van de uitvoering van de Overeenkomst zal VERWERKER, voor zover het in haar macht ligt, iedere redelijke inspanning verrichten om deze beoordeling in overeenstemming met de geldende wet- en regelgeving uit te kunnen voeren. Tevens zal VERWERKER, voor zover het in haar macht ligt, iedere redelijke inspanning verrichten, indien een voorafgaande raadpleging van de AP nodig is op grond van de geldende wet- en regelgeving.

5.6 In **Bijlage 2** zijn de afspraken tussen Partijen vastgelegd over de concrete technische en organisatorische beveiligingsmaatregelen. Deze maatregelen worden periodiek geëvalueerd en indien nodig aangepast.

Artikel 6. Controle

6.1 VERANTWOORDELIJKE heeft het recht om een audit te laten uitvoeren inzake de verwerking van Persoonsgegevens door VERWERKER ter controle op de naleving van deze Verwerkersvoorwaarden. VERWERKER zal alle medewerking verlenen aan een audit, waaronder het verlenen van toegang tot gebouwen en databases en het ter beschikking stellen van alle relevante informatie.

6.2 VERWERKER zal in overleg met VERANTWOORDELIJKE de aanbevelingen zo spoedig mogelijk uitvoeren. Indien de aanpassingen het gevolg zijn van een tekortkoming in de nakoming van

de beveiligingseisen uit de Verwerkersvoorwaarden, dan zal VERWERKER deze kosten voor haar rekening nemen.

6.3 In geval van een onderzoek door de AP of een andere bevoegde autoriteit zal VERWERKER alle medewerking verlenen en VERANTWOORDELIJKE zo snel mogelijk informeren.

Artikel 7. Beveiligingsincidenten

7.1 VERWERKER informeert VERANTWOORDELIJKE onverwijld nadat VERWERKER kennis heeft genomen van een Beveiligingsincident met betrekking tot de verwerking van de Persoonsgegevens.

7.2 In geval van een Beveiligingsincident zal VERWERKER, voor zover het in haar macht ligt, alle redelijke maatregelen treffen om de gevolgen van het incident te beperken en/of een nieuw incident te voorkomen. VERWERKER zal iedere redelijke inspanning verlenen aan VERANTWOORDELIJKE om het Beveiligingsincident te beoordelen en te kunnen voldoen aan haar eventuele wettelijke meldplicht en haar eventuele plicht tot het informeren van Betrokkenen.

7.3 Partijen leggen hun afspraken over de informatie-uitwisseling in verband met incidenten vast in een “Procedure Meldplicht Datalekken” in **Bijlage 3**. Deze bijlage kan te allen tijde in overleg door Partijen worden gewijzigd. De bijlage zal in ieder geval worden aangepast, indien de regelgeving omtrent de Meldplicht Datalekken of de uitleg daarvan wijzigt.

7.4 In geval van een Beveiligingsincident bij VERWERKER dat leidt tot een meldplicht of een informatieplicht voor VERANTWOORDELIJKE, zal de melding in overleg met VERWERKER door VERANTWOORDELIJKE worden verricht.

Artikel 8. Verzoeken van Betrokkenen

8.1 Indien VERWERKER een verzoek of bezwaar van een Betrokkene ontvangt, zoals een verzoek om informatie, inzage, rectificatie, gegevenswissing, verwerkingsbeperking, overdracht van de Persoonsgegevens, stuurt VERWERKER dat verzoek door naar VERANTWOORDELIJKE.

8.2 VERWERKER verleent VERANTWOORDELIJKE, voor zover het in haar macht ligt, alle redelijke medewerking om ervoor te zorgen dat VERANTWOORDELIJKE binnen de wettelijke termijnen kan voldoen aan de verplichtingen op grond van de geldende wet- en regelgeving.

Artikel 9. Sub-verwerkers

9.1 VERWERKER heeft bij de verwerking van de Persoonsgegevens de mogelijkheid om, na voorafgaande schriftelijke toestemming van VERANTWOORDELIJKE, Sub-verwerkers in te schakelen.

9.2 VERWERKER zal iedere redelijke inspanning verrichten om ervoor te zorgen dat zij met de door haar ingeschakelde Sub-verwerkers een overeenkomst sluit die in overeenstemming is met de relevante wet- en regelgeving en deze Verwerkersvoorwaarden en die ten minste dezelfde eisen stelt als deze Verwerkersvoorwaarden aan VERWERKER stelt. VERWERKER zal in dat kader in ieder geval iedere Sub-verwerkers contractueel de geheimhoudingsverplichtingen, meldingsverplichtingen en beveiligingsmaatregelen na laten leven met betrekking tot de verwerking van de Persoonsgegevens.

Artikel 10. Toegang tot de Persoonsgegevens

10.1 De zeggenschap over de Persoonsgegevens blijft volledig berusten bij VERANTWOORDELIJKE. Op verzoek van VERANTWOORDELIJKE zal VERWERKER alle of een gedeelte van de Persoonsgegevens in gangbaar formaat ter beschikking stellen aan VERANTWOORDELIJKE.

10.2 VERWERKER zal iedere redelijke inspanning verrichten om ervoor te zorgen dat VERANTWOORDELIJKE te allen tijde toegang behoudt tot de Persoonsgegevens. Voor zover het in de macht van VERWERKER ligt, zal VERWERKER ervoor inspannen dat VERANTWOORDELIJKE ook in geval van faillissement of surséance van betaling van VERWERKER toegang blijft houden tot de Persoonsgegevens.

Artikel 11. Aansprakelijkheid en vrijwaring

11.1 Indien VERANTWOORDELIJKE tekortschiet in de nakoming van de Verwerkersvoorwaarden, is VERANTWOORDELIJKE aansprakelijk voor alle schade en buitengerechtelijke en gerechtelijke kosten die VERWERKER daardoor lijdt of heeft geleden.

11.2 VERANTWOORDELIJKE stelt VERWERKER schadeloos voor alle claims, acties, aanspraken van Derden en voor verliezen, schade of kosten die aan de zijde van VERWERKER vallen en die rechtstreeks of indirect voortvloeien uit of tot stand komen in verband met een tekortkoming van deze Verwerkersvoorwaarden door VERANTWOORDELIJKE en/of het niet-naleven van de geldende wet- en regelgeving door VERWERKER.

11.3 VERANTWOORDELIJKE vrijwaart VERWERKER voor schades en/of boetes en/of dwangsommen van of namens de AP en/of andere autoriteiten die aan VERWERKER worden opgelegd en welke zijn toe te schrijven aan overtredingen van de geldende wetgeving door VERANTWOORDELIJKE en/of een tekortkoming door VERANTWOORDELIJKE in de nakoming van deze Verwerkersvoorwaarden.

11.4 In geval van overtreding en/of niet-naleving door VERANTWOORDELIJKE van hetgeen in deze Verwerkersvoorwaarden is bepaald, en indien als gevolg hiervan VERWERKER een boete van de AP of een andere autoriteit opgelegd krijgt, dient een bedrag gelijk aan het boetebedrag door VERANTWOORDELIJKE VERWERKER aan VERWERKER te worden voldaan, vermeerderd met alle rentes en buitengerechtelijke en gerechtelijke kosten die VERWERKER als gevolg van de overtreding en/of de niet-naleving heeft gemaakt. Deze vordering is onmiddellijk opeisbaar en is niet voor verrekening vatbaar. Het voorgaande laat het recht van VERWERKER onverlet om van VERANTWOORDELIJKE – naast betaling van de boete – nakoming en/of volledige schadevergoeding te vorderen.

11.5 Indien VERWERKER aansprakelijk is jegens VERANTWOORDELIJKE voor schade uit welke hoofde dan ook, is VERWERKER alleen aansprakelijk voor directe schade die VERANTWOORDELIJKE lijdt als gevolg van een aan VERWERKER toerekenbare tekortkoming en/of onrechtmatige daad. De totale aansprakelijkheid van VERWERKER onder deze Verwerkersvoorwaarden zal nooit meer bedragen dan het bedrag dat de verzekeraar van VERWERKER in een voorkomend geval uitkeert en dan wel nooit meer bedragen dan € 1.000.000,00.

11.6 VERWERKER is nooit aansprakelijk voor gevolgschade, waaronder mede begrepen zuivere vermogensschade, gederfde winst, en immateriële schade. In het bijzonder is VERWERKER niet aansprakelijk voor schade in verband met en/of als gevolg van:

a. beëindiging of wijziging van de geleverde dienst;
b. communicatiegebreken in verband met hardware-, software-, netwerk- of andere computerproblemen;
c. het gebruik van door VERANTWOORDELIJKE voorgeschreven gegevens of databestanden;
d. verlies, verminking of vernietiging van gegevens of databestanden; en/of,
e. ontoegankelijkheid van de dienst van VERWERKER.

11.7 Voor zover nakoming niet blijvend onmogelijk is, ontstaat de aansprakelijkheid van VERWERKER wegens toerekenbare tekortkoming in de nakoming van de Verwerkersvoorwaarden slechts indien VERANTWOORDELIJKE VERWERKER onverwijld en deugdelijk schriftelijk in gebreke stelt, waarbij een redelijke termijn ter zuivering van de tekortkoming wordt gesteld, en VERWERKER ook na die termijn toerekenbaar tekort blijft schieten in de nakoming van haar verplichtingen. De ingebrekestelling dient een zo volledig en gedetailleerd mogelijke omschrijving van de tekortkoming te bevatten, zodat VERWERKER in staat is adequaat te reageren.

11.8 Voorwaarde voor het ontstaan van enig recht op schadevergoeding is steeds dat VERANTWOORDELIJKE de schade zo spoedig mogelijk na het ontstaan daarvan schriftelijk bij VERWERKER meldt. Ieder vordering tot schadevergoeding jegens VERWERKER vervalt door het enkele verloop van zes (6) maanden na het ontstaan van de vordering

Artikel 12. Duur en beëindiging

12.1 Deze Verwerkersvoorwaarden eindigen van rechtswege bij beëindiging van de Overeenkomst. Verplichtingen met een duurkarakter blijven tussen Partijen in stand, zoals onder meer maar niet uitsluitend de geheimhoudingsverplichting uit artikel 4 van de Verwerkersvoorwaarden.

12.2 VERWERKER zal bij beëindiging van de Overeenkomst, voor zover het in haar macht ligt, iedere redelijke inspanning verrichten om op verzoek van VERANTWOORDELIJKE de Persoonsgegevens in een gangbaar formaat ter beschikking stellen aan VERANTWOORDELIJKE of aan een door VERANTWOORDELIJKE aangewezen Derde.

12.3 VERWERKER zal, voor zover het in haar macht ligt, iedere redelijke inspanning verrichten om na overdracht van de Persoonsgegevens aan VERANTWOORDELIJKE de nog aanwezige Persoonsgegevens te vernietigen, tenzij een langere opslag wettelijk verplicht is. VERWERKER zal eveneens, voor zover het in haar macht ligt, iedere redelijke inspanning verrichten om ervoor te zorgen dat de Persoonsgegevens bij de Sub-verwerkers zullen worden vernietigd.

12.4 Deze Verwerkersvoorwaarden vervangen alle vorige Verwerkersvoorwaarden(en), die tussen Partijen zijn gesloten.

12.5 Niettegenstaande enige bepaling in de Overeenkomst als gevolg van faillissement of surseance van betaling blijft deze Verwerkersvoorwaarden onverminderd van kracht ten aanzien van de Persoonsgegevens die in het kader van de uitvoering van de Overeenkomst en/of deze Verwerkersvoorwaarden zijn verstrekt. De Verwerkersvoorwaarden kan in dat geval eenzijdig door middel van een schriftelijke verklaring door VERWERKER worden ontbonden.

Artikel 13. Toepasselijk recht / Bevoegde rechter

13.1 Op deze Verwerkersvoorwaarden is uitsluitend Nederlands recht van toepassing.

13.2 Alle geschillen die ontstaan naar aanleiding van deze Verwerkersvoorwaarden worden beslecht op dezelfde wijze als opgenomen in de Overeenkomst.

BIJLAGE 1

A. Categorieën Betrokkenen
De personen waarop de Persoonsgegevens betrekking hebben zijn in ieder geval:
- medewerkers van afnemer
- stakeholders van afnemer voor zover opgenomen in de software
- leveranciers van afnemer
- klanten van afnemer

B. Soort Persoonsgegevens
De Persoonsgegevens die door VERWERKER worden verwerkt zijn in ieder geval:

- (Bedrijfs)Naam - E-mailadres - Geslacht - Telefoonnummer - NAW-gegevens (straat, huisnummer, toevoeging, postcode en plaats) - BSN - KvK-nummer – Geboortedatum - Profielfoto - IP-adres - Factuurgegevens - Financiële data - Grootboekrekeningen - Grootboekmutaties en eventueel gekoppelde documenten - Gewerkte uren – Salarisgegevens in de breedste zin van het woord – alle overige persoonsgegevens voor zover die door Afnemer in de software zijn opgeslagen.

Daarnaast is het mogelijk dat medewerkers van verwerker in contact komen met bijzondere persoonsgegevens voor zover die door Afnemer in de software zijn opgeslagen zoals politieke voorkeur en ras.

C. Aard en doel van de verwerking
De aard van de verwerking is raadplegen en in voorkomende gevallen tijdelijk exporteren en opslaan ten behoeven van databewerking.

De Persoonsgegevens worden in ieder geval voor de volgende doelen verwerkt:

- inrichtingsdoeleinden van de software
- optimalisatiedoeleinden van de software
- migratiedoeleinden van de software

BIJLAGE 2

Omschrijving van de technische en organisatorische beveiligingsmaatregelen die door de VERWERKER zijn geïmplementeerd

Zoals opgenomen in art. 5 worden hieronder de afspraken tussen partijen vastgelegd over de concrete technische en organisatorische beveiligingsmaatregelen. De getroffen maatregelen zijn opgenomen in deze Bijlage en worden aangevuld of gewijzigd indien dat nodig is. VERANTWOORDELIJKE acht genoemde maatregelen passend voor de verwerking van de Persoonsgegevens.

A. Beveiligingsniveau

VERWERKER maakt gebruik van een beveiligd citrix platform van waaruit software omgevingen van afnemers benaderd worden. Deze worden derhalve nooit rechtstreeks vanaf het internet door middel van een desktop of laptop benaderd. Gegevens van VERANTWOORDELIJKE worden derhalve altijd indien nodig opgeslagen op het beveiligde netwerk van VERWERKER en zijn derhalve optimaal beveiligd tegen gegevensverlies als gevolg van diefstal van hardware.

Het Citrix platform maakt gebruik van SSL versleutelde techniek encryptie van data en kan alleen via tweeweg authenticatie (token) benaderd worden. Hiermee is verzeker dat alleen door VERWERKER geautoriseerde en bevoegde medewerkers de omgeving kunnen benaderen.

B. Maatregelen van VERWERKER om te zorgen dat uitsluitend bevoegd personeel toegang heeft tot de Persoonsgegevens:

- In de aanmeldpagina is ‘brute force protection’ ingebouwd, zodat wachtwoorden niet oneindig geprobeerd kunnen worden.
- Alle communicatie tussen de PC en de citrix omgeving is encrypted (256-bits) en de beveiligde SSL verbinding is gecertificeerd.
- Alleen ‘sterke’ wachtwoorden zijn toegestaan (minimaal 8 karakters, minimaal 1 cijfer, minimaal 1 hoofdletter).
- Alle wachtwoorden worden versleuteld (gehashed) opgeslagen. Medewerkers van VERWERKER kunnen geen wachtwoorden van gebruikers achterhalen.
- Medewerkers van VERWERKER zijn contractueel gebonden aan geheimhouding van al datgene wat zij gedurende hun werkzaamheden kennis van kunnen nemen.
- VERWERKER draagt er zorg voor dat alleen medewerkers die betrokken zijn bij een specifieke opdracht voor VERANTWOORDELIJKE de gegevens kunnen benaderen. De inlog van de software is alleen bekend bij betrokkenen bij de opdracht en kan niet door andere medewerkers van VERWERKER worden achterhaald.

BIJLAGE 3 “Procedure Meldplicht Datalekken”

Tussen Partijen zijn met betrekking tot de Meldplicht Datalekken de volgende afspraken gemaakt:

1) VERWERKER registreert alle Beveiligingsincidenten;
2) In geval van een Beveiligingsincident informeert VERWERKER VERANTWOORDELIJKE onverwijld en zal de relevante informatie over het incident melden aan de hand van de hieronder opgenomen vragenlijst;
3) VERANTWOORDELIJKE zal beoordelen of een melding verricht dient te worden bij de AP. VERANTWOORDELIJKE zal daarbij in overleg treden met VERWERKER;
4) Voordat VERANTWOORDELIJKE de melding bij de AP verricht zal VERANTWOORDELIJKE de inhoud van de melding met VERWERKER bespreken;
5) Indien VERANTWOORDELIJKE oordeelt dat tevens betrokkenen geïnformeerd dienen te worden,

Vragenlijst Beveiligingsincident – bij de Procedure Meldplicht Datalekken

Deze lijst is gebaseerd op het meldformulier van de AP

De contactpersonen bij VERANTWOORDELIJKE voor de Meldplicht Datalekken zijn:

[A + gegevens]
[B + gegevens]

VERWERKER zal bij een Beveiligingsincident de volgende vragen beantwoorden:

☐ **Geef een omschrijving van het Beveiligingsincident:**

……..
(bijvoorbeeld "gestolen laptop met klantgegevens" of "een hack op systeem [X]" of "inloggegevens verstuurd naar ontvanger Y ipv X")

☐ **De persoonsgegevens van hoeveel personen zijn getroffen door het Beveiligingsincident?**

……..
(geef een minimum en maximum aantal aan)

☐ **Omschrijf de groep personen waarop de Persoonsgegevens betrekking hebben.**

……..
(bijvoorbeeld sollicitanten of cliënten van VERANTWOORDELIJKE)

Is er sprake van één van deze specifieke groepen personen (omcirkel het antwoord):

Ouderen: JA / NEE
Kinderen: JA / NEE
Zieken of mensen met een verstandelijke beperking: JA / NEE

☐ **Datum en tijdstip van het incident:**

……..
(kan een vast tijdstip zijn of een periode, als dit niet bekend is "onbekend" invullen)

☐ **Wanneer is het Beveiligingsincident ontdekt?**

……..

☐ **Wat is de aard van de inbreuk? Omcirkel de antwoorden en vul in waar nodig**

Kan een onbevoegde de gegevens lezen: JA / NEE
Kunnen/zijn de gegevens (worden) gekopieerd door een onbevoegde: JA / NEE
Kunnen/zijn de (bron)gegevens (worden) gewijzigd (bijv. hack in het systeem): JA / NEE
Kunnen/zijn de (bron)gegevens (worden) verwijderd of vernietigd (bijv. ransom ware of brand datacenter): JA / NEE
Zijn de gegevens gestolen: JA / NEE
Overig: ……
(invullen, of als de aard niet bekend is: "onbekend" invullen)

- **Om welk type gegevens gaat het? Omcirkel de antwoorden en vul in waar nodig:**

Naam-, adres- en woonplaatsgegevens: JA / NEE
Telefoonnummer: JA / NEE
E-mailadres of andere adres voor elektronische communicatie: JA / NEE
Inloggegevens (gebruikersnaam/wachtwoord, klantnummer of ander identificatienummer): JA / NEE,
zo ja; welke gegevens zijn het: ……(invullen)
Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer): JA / NEE
Burgerservicenummer (BSN) of sofinummer: JA / NEE
Paspoortkopieën of kopieën van andere legitimatiebewijzen: JA / NEE
Geslacht: JA / NEE
Geboortedatum en/of leeftijd: JA / NEE
(Pas)foto: JA / NEE
Geboorteland: JA / NEE
Medische gegevens (waaronder ook medicijnen of medische hulpmiddelen): JA / NEE
Biometrische gegevens (bijv. vingerafdruk, DNA): JA / NEE,
zo ja; welke gegevens zijn het: …… (invullen)
Gegevens over schulden/kredieten: JA / NEE
Inkomensgegevens: JA / NEE
Gegevens over iemands betalingsverkeer: JA / NEE
Gegevens over wettelijke vertegenwoordiging (bewindvoerder/mentor): JA / NEE
Verslavingsgegevens: JA / NEE
School/werkprestaties: JA / NEE
Gegevens over relationele problemen: JA / NEE
Gegevens over (vermoeden van) mishandeling: JA / NEE
Religie: JA / NEE
Strafrechtelijke gegevens (ook bijv. straatverboden): JA / NEE
Politieke overtuiging: JA / NEE
Vakbondslidmaatschap: JA / NEE
Seksuele voorkeur/geaardheid: JA / NEE
Overige gegevens: …… (invullen)

- **Welke gevolgen kan de inbreuk hebben voor de getroffen personen? Omcirkel de antwoorden en vul in waar nodig:**

Stigmatisering of uitsluiting: JA / NEE
Schade aan de gezondheid: JA / NEE
Kans op identiteitsfraude: JA / NEE
Kans op financiële schade (bijv. fraude met creditcardgegevens): JA / NEE
Blootstelling aan spam of phishing: JA / NEE
Andere gevolgen, namelijk: …….. (invullen)

- **Omschrijf welke technische en organisatorische maatregelen zijn getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?**

……..

- **Zijn de gelekte Persoonsgegevens beveiligd? Omcirkel de antwoorden en vul in waar nodig:**

Zijn de gegevens versleuteld: JA /NEE,

zo ja; welke versleuteling: ……. (invullen)
geldt deze versleuteling voor alle Persoonsgegevens of voor een deel? Indien voor een deel, voor welk deel: …… (invullen)

Zijn de gegevens gehasht: JA /NEE,
zo ja; op welke wijze: ……. (invullen)

Kunnen de gegevens vanaf afstand worden gewist: JA /NEE,
zo ja; is dat gebeurd en wanneer is dat gebeurd: …… (invullen)

Zijn de gegevens op een andere manier onbegrijpelijk of ontoegankelijk gemaakt: JA /NEE,
zo ja; op welke manier: ……. (invullen)

☐ **Zijn er Persoonsgegevens van personen in andere EU-landen getroffen door het Beveiligingsincident? Zo ja, welke uit welke landen:**

……..