

Verwerkersovereenkomst

IT die voor
zich spreekt.

Betrouwbaar, veilig en compliant

Verklaring van vertrouwelijkheid

Dit document bevat vertrouwelijke informatie, eigendom van de VTM Groep B.V. (hierna te noemen VTM). De informatie wordt alleen aan uw organisatie verstrekt om u in staat te stellen de producten en diensten van VTM in detail te evalueren. Dit document (inbegrepen delen ervan) mag niet worden getoond of overgedragen buiten uw organisatie zonder voorafgaande schriftelijke toestemming van een hiertoe bevoegde vertegenwoordiger van VTM en mag niet in enige vorm worden gereproduceerd of vermenigvuldigd voor andere doeleinden dan voor intern gebruik binnen uw organisatie ten behoeve van eerder genoemde evaluatie.

Disclaimer

Hoewel dit document met de grootst mogelijke zorg is samengesteld kunnen aan dit document geen rechten worden ontleend. VTM aanvaardt geen aansprakelijkheid voor mogelijke fouten en tekortkomingen. Prijzen en voorwaarden kunnen aan veranderingen onderhevig zijn

Inhoud

De ondergetekenden.....	4
Overwegende dat:.....	4
Zijn het volgende overeengekomen:.....	4
1. Bijlagen en definities.....	4
2. Verwerking van persoonsgegevens.....	5
3 Beveiliging van persoonsgegevens.....	6
4. Datalekken en meldplicht.....	6
5. Verzoeken van betrokkenen.....	7
6. Vertrouwelijkheid.....	7
7. Toegang en controle.....	7
8. Aansprakelijkheid.....	8
9. Sub-verwerkers.....	8
10. Doorgifte aan derde landen.....	9
11. Bewaren van persoonsgegevens.....	9
12. Geldigheid, duur en beëindiging van de verwerkersovereenkomst.....	9
13. Toepasselijk recht en geschillenbeslechting.....	10
Ondertekening.....	11
Bijlage 1 – categorieën, soort, aard, doel en contactgegevens.....	12
Bijlage 2 – Beschrijving informatiebeveiliging VTM.....	14
Bijlage 3 – Procedure meldplicht datalekken.....	18
Bijlage 4 – vragenlijst bij de procedure meldplicht datalekken.....	19
Bijlage 5 – Algemene voorwaarden.....	22

De ondergetekenden

Deze verwerkersovereenkomst is een optionele aanvulling op de hoofdovereenkomst om de aanvullende voorwaarden met betrekking tot de verwerking van Persoonsgegevens te beschrijven en is een overeenkomst tussen VTM Services B.V., statutair gevestigd te Maasdijk, Nederland, geregistreerd adres Honderdland 190, 2676 LT Maasdijk, hierna te noemen Verwerker; en u of de entiteit die u vertegenwoordigt als de gegevensbeheerder, hierna te noemen Verwerkingsverantwoordelijke, hierna gezamenlijk te noemen Partijen of afzonderlijk te noemen Partij.

Overwegende dat:

- a. Verwerker met Verwerkingsverantwoordelijke een overeenkomst heeft gesloten inzake de levering van IT & Telecom diensten aan Verwerkingsverantwoordelijke, waaronder maar niet beperkt tot advies, configuratie, connectiviteit en beheer ("**Overeenkomst**"). Verwerker verwerkt bij deze diensten mogelijk Persoonsgegevens, waarvoor Verwerkingsverantwoordelijke verantwoordelijk is;
- b. Partijen in het kader van de Algemene Verordening Gegevensbescherming ("**AVG**") en de Uitvoeringswet AVG ("**UAVG**") wettelijk verplicht zijn afspraken te maken en vast te leggen met betrekking tot de Verwerking van Persoonsgegevens door Verwerker;
- c. De bepalingen van deze overeenkomst ("**Verwerkersovereenkomst**") vóór gaan op alle andere afspraken die tussen Partijen gelden en betrekking hebben op de verwerking van Persoonsgegevens door Verwerker voor Verwerkingsverantwoordelijke.

Zijn het volgende overeengekomen:

1. Bijlagen en definities

I.I De considerans en de hierna te noemen bijlagen, maken integraal deel uit van deze verwerkersovereenkomst:

- a) Bijlage I: een beschrijving van de categorieën van Betrokkenen, het soort Persoonsgegevens en de aard en het doel waarvoor de Persoonsgegevens worden verwerkt.
- b) Bijlage 2: een beschrijving van de door Verwerker getroffen beveiligingsmaatregelen. Verwerker kan de beschrijving van beveiligingsmaatregelen van tijd tot tijd eenzijdig wijzigen en/of aanpassen aan bijvoorbeeld de stand van de techniek. Verwerker zal Verwerkingsverantwoordelijke over een wijziging en/of aanpassing van beveiligingsmaatregelen informeren.
- c) Bijlage 3: de door Partijen gebruikte Procedure Meldplicht Datalekken. Deze bijlage zal in ieder geval worden aangepast indien de regelgeving omtrent de Meldplicht Datalekken of de uitleg daarvan wijzigt.

- d) Bijlage 4: de vragenlijst bij de procedure meldplicht datalekken.
- e) Bijlage 5: Algemene Voorwaarden.

1.2 Op deze verwerkersovereenkomst zijn de reeds geldende algemene voorwaarden van Verwerker ("NLdigital Voorwaarden 2020") van de betreffende onderliggende leveringsovereenkomst van toepassing. Indien er sprake is van tegenstrijdigheid tussen de algemene voorwaarden van deze verwerkersovereenkomst, prevaleert deze verwerkersovereenkomst. Eventuele tegenstrijdigheid laat de toepassing van de overige bepalingen van de algemene voorwaarden van verwerker onverlet.

1.3 Met een hoofdletter geschreven begrippen hebben de betekenis zoals omschreven in deze Verwerkersovereenkomst. Daarnaast hebben de met een hoofdletter geschreven begrippen "Persoonsgegevens", "Inbreuk in verband met Persoonsgegevens", "Verwerking", "Verwerkingsverantwoordelijke", "Verwerker", "Betrokkene" en "Derde" de inhoudelijke betekenis die artikel 4 van de AVG hieraan geeft.

2. Verwerking van persoonsgegevens

2.1 Verwerker verwerkt de Persoonsgegevens uitsluitend in opdracht van Verwerkingsverantwoordelijke in het kader van de in overweging sub B genoemde diensten, plus die doeleinden die daarmee redelijkerwijs samenhangen.

2.2 De categorieën van Betrokkenen, het soort Persoonsgegevens, de aard en het doel waarvoor de Persoonsgegevens worden verwerkt zijn door verwerkingsverantwoordelijke opgenomen in Bijlage I.

2.3 De Verwerking vindt plaats onder de verantwoordelijkheid en conform de instructies van Verwerkingsverantwoordelijke, tenzij Verwerker in verband met een wettelijke verplichting verplicht is om anders te handelen. Indien een instructie naar de mening van Verwerker een inbreuk maakt op de AVG en/of de UAVG, stelt Verwerker Verwerkingsverantwoordelijke daarvan onmiddellijk in kennis.

2.4 Verwerkingsverantwoordelijke heeft en houdt zelfstandige en volledige zeggenschap over het doel en de middelen van de Verwerking van de Persoonsgegevens. In het bijzonder staat Verwerkingsverantwoordelijke ervoor in dat er tijdens de duur van de Overeenkomst sprake is en blijft van een rechtmatige grondslag voor de Verwerking van de Persoonsgegevens en vrijwaart Verwerker hieromtrent.

2.5 Verwerker treft maatregelen om ervoor te zorgen dat haar medewerkers die toegang hebben tot de Persoonsgegevens, (i) deze slechts in opdracht van Verwerkingsverantwoordelijke verwerken en (ii) gebonden zijn aan een geheimhoudingsplicht.

3 Beveiliging van persoonsgegevens

3.1 Verwerker zal waar zij in opdracht van Verwerkingsverantwoordelijke Persoonsgegevens verwerkt gedurende de looptijd van deze Verwerkersovereenkomst passende technische en organisatorische maatregelen treffen, in stand houden en zo nodig aanpassen, om de Persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking. Deze maatregelen zullen, rekening houdend met de stand van de techniek en de kosten betrekking hebbende op de implementatie en tenuitvoerlegging van de maatregelen, een passend beveiligingsniveau bieden gelet op de risico's die de Verwerking van de Persoonsgegevens, gezien de aard daarvan, met zich meebrengen. Voor een actuele beschrijving van de technische en organisatorische maatregelen die Verwerker in opdracht van Verwerkingsverantwoordelijke neemt wordt verwezen naar Bijlage 2 bij deze Verwerkersovereenkomst.

4. Datalekken en meldplicht

4.1 Indien Verwerker een Inbreuk in verband met Persoonsgegevens zoals bedoeld op grond van artikel 4 lid 12 AVG ("**Datalek**") vaststelt, zal Verwerker Verwerkingsverantwoordelijke daarover zonder onredelijke vertraging informeren. De eerste melding is een vroegtijdige waarschuwing die zo snel mogelijk, maar in ieder geval binnen 24 uur na waarneming van het incident plaatsvindt. Dit nadat de verwerker het datalek heeft ontdekt of nadat zij daarover door haar sub-verwerkers is geïnformeerd.

4.2 In geval van een Datalek zal Verwerker in overeenstemming met artikel 33 lid 2 AVG alle redelijke maatregelen treffen om de gevolgen van het Datalek te beperken en/of een nieuw incident te voorkomen, tegen vergoeding van de redelijke kosten door Verwerkingsverantwoordelijke. Verwerker zal daarbij redelijkerwijs medewerking verlenen aan Verwerkingsverantwoordelijke om het Datalek te beoordelen en de Verwerkingsverantwoordelijke in staat te stellen te kunnen voldoen aan haar eventuele wettelijke meldplicht(en) aan de Autoriteit Persoonsgegevens en Betrokkene(n).

4.3 De melding van een Datalek aan de Autoriteit Persoonsgegevens en (eventueel) Betrokkene(n) is altijd de verantwoordelijkheid van Verwerkingsverantwoordelijke. Verwerker is nimmer aansprakelijk voor de op Verwerkingsverantwoordelijke rustende correcte en tijdige meldplicht in de zin van de AVG. In geval Verwerkingsverantwoordelijke voornemens is een Datalek dat zich heeft voorgedaan bij Verwerker te melden bij de Autoriteit Persoonsgegevens en/of Betrokkene(n), zal deze melding in overleg met Verwerker door Verwerkingsverantwoordelijke worden verricht.

4.4 Het (bij)houden van een register van Datalekken is altijd de verantwoordelijkheid van Verwerkingsverantwoordelijke.

4.5 Partijen leggen hun afspraken over de informatie-uitwisseling in verband met Datalekken vast in een "Procedure Meldplicht Datalekken" in Bijlage 3.

5. Verzoeken van betrokkenen

5.1 Indien Verwerker een verzoek of bezwaar van een Betrokkene ontvangt, zoals een verzoek om informatie, inzage, rectificatie, gegevenswissing, verwerkingsbeperking, overdracht van de Persoonsgegevens, zoals bedoeld in hoofdstuk III AVG, stuurt Verwerker dat verzoek zonder onredelijke vertraging door naar Verwerkingsverantwoordelijke.

5.2 Verwerker verleent Verwerkingsverantwoordelijke alle redelijke medewerking om ervoor te zorgen dat Verwerkingsverantwoordelijke binnen de wettelijke termijnen kan voldoen aan de verplichtingen op grond van de geldende wet- en regelgeving. De redelijke kosten voor deze medewerking zullen door Verwerkingsverantwoordelijke aan Verwerker worden vergoed.

6. Vertrouwelijkheid

6.1 Verwerker is gehouden alle Persoonsgegevens die hem bij de uitvoering van zijn werkzaamheden bekend raken, geheim te houden. Verwerker zal de verplichting tot geheimhouding tevens opleggen aan haar personeel en eventuele sub-Verwerkers.

6.2 De in dit artikel bedoelde geheimhoudingsplicht geldt niet indien Verwerkingsverantwoordelijke uitdrukkelijk 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.

7. Toegang en controle

7.1 De zeggenschap over de Persoonsgegevens blijft volledig berusten bij Verwerkingsverantwoordelijke. Op verzoek van Verwerkingsverantwoordelijke en tegen vergoeding van de kosten zal Verwerker alle of een gedeelte van de Persoonsgegevens in gangbaar formaat ter beschikking stellen aan Verwerkingsverantwoordelijke.

7.2 Verwerkingsverantwoordelijke heeft het recht om maximaal één keer per jaar, met een aanzegging van twee weken, binnen reguliere kantoortijden, door onafhankelijke deskundigen, een audit te laten uitvoeren inzake de Verwerking van Persoonsgegevens door Verwerker ter controle op de naleving van de Verwerkersovereenkomst. De kosten van dergelijke audits zijn voor rekening van Verwerkingsverantwoordelijke. Ook eventuele audits op verzoek van Verwerkingsverantwoordelijke bij sub-Verwerkers zijn voor rekening van Verwerkingsverantwoordelijke. Verwerker zal alle redelijke medewerking verlenen aan een audit, waaronder het verlenen van toegang tot gebouwen en databases en het ter beschikking stellen van alle relevante informatie.

7.3 Een audit van Verwerkingsverantwoordelijke als omschreven in het vorige artikellid, zal zich altijd beperken tot de systemen van Verwerker die voor de Verwerkingen worden gebruikt. Verwerkingsverantwoordelijke zal de bij de controle gevonden informatie geheimhouden en alleen gebruiken om de naleving door Verwerker van de verplichtingen uit deze Verwerkersovereenkomst te controleren en de informatie of delen daarvan zo snel als mogelijk wissen. Verwerkingsverantwoordelijke staat ervoor in dat eventuele ingeschakelde Derde(n) deze verplichtingen ook op zich nemen. Indien een door

Verwerkingsverantwoordelijke ingeschakelde Derde een instructie geeft die naar mening van Verwerker inbreuk oplevert op de AVG, dan stelt Verwerker Verwerkingsverantwoordelijke daarvan onmiddellijk in kennis

7.4 Op verzoek van Verwerkingsverantwoordelijke en vergoeding van de kosten van Verwerker zal Verwerker redelijke medewerking verlenen bij de uitvoering van Privacy Impact Assessments (artikel 35 AVG) en voorafgaande controle door de toezichthoudende autoriteit (artikel 36 AVG).

8. Aansprakelijkheid

8.1 De aansprakelijkheid van Verwerker voor schade als gevolg van een toerekenbare tekortkoming in de nakoming van de Verwerkersovereenkomst, dan wel uit onrechtmatige daad of anderszins, wordt geregeld in de toepasselijke Algemene Voorwaarden van Verwerker.

8.2 Verwerkingsverantwoordelijke garandeert dat de opdracht tot Verwerking van de Persoonsgegevens in overeenstemming is met de geldende wet- en regelgeving. Verwerker is niet aansprakelijk voor schade die het gevolg is van het door Verwerkingsverantwoordelijke niet naleven van de AVG, UAVG of andere wet- of regelgeving.

8.3 Verwerkingsverantwoordelijke vrijwaart Verwerker voor:

Boetes en/of dwangsommen van of namens de Autoriteit Persoonsgegevens en/of andere bevoegde autoriteiten die aan Verwerker worden opgelegd en waarbij vast is komen te staan dat deze zijn toe te schrijven aan het niet naleven van de AVG, UAVG of andere wet- of regelgeving door Verwerkingsverantwoordelijke;

Aanspraken van Betrokkene(n) en/of Derde(n) op grond van schade als bedoeld in artikel 8.2.

De vrijwaringen gelden ook voor de kosten die Verwerker in verband met de boetes en/of dwangsommen en/of aanspraken moet maken, bijvoorbeeld in een eventuele juridische procedure.

9. Sub-verwerkers

9.1 Verwerkingsverantwoordelijke staat Verwerker op basis van algemene toestemming (op grond van artikel 28 lid 2 AVG) toe de Persoonsgegevens door anderen dan eigen personeel (sub-Verwerkers) te laten verwerken in het kader van de diensten van Verwerker. De door Verwerker aangewezen sub-Verwerker(s) dienen minimaal te voldoen aan de bepalingen uit deze Verwerkersovereenkomst en alle voortvloeiende verplichtingen uit de AVG en de UAVG.

9.2 Met ondertekening van deze Verwerkersovereenkomst geeft Verwerkingsverantwoordelijke toestemming voor het inschakelen van sub-Verwerkers door Verwerker. Indien Verwerker een sub-Verwerker wenst in te schakelen, zal Verwerker Verwerkingsverantwoordelijke hierover vooraf inlichten en Verwerkingsverantwoordelijke de mogelijkheid bieden om hiertegen bezwaar te maken. De sub-Verwerkers die thans door Verwerker zijn ingeschakeld, zijn genoemd in bijlage I.

10. Doorgifte aan derde landen

10.I Het is Verwerker toegestaan om Persoonsgegevens te verwerken of te laten verwerken buiten de Europese Economische Ruimte (Europese Unie, Noorwegen, Liechtenstein, IJsland) onder de voorwaarde dat ofwel (i) voor het betreffende land een adequaatheidsbesluit geldt of (ii) met de ontvanger een overeenkomst is gesloten waarin de door de Europese Commissie vastgestelde modelbepalingen zijn opgenomen.

11. Bewaren van persoonsgegevens

11.I Verwerker zal de Persoonsgegevens die hij verwerkt in het kader van de Overeenkomst niet langer bewaren dan noodzakelijk. Uitgangspunt daarbij is dat het bewaren van Persoonsgegevens niet langer noodzakelijk is nadat het verlenen van de diensten uit hoofde van de Overeenkomst is voltooid, tenzij de Verwerker op andere gronden gehouden is de Persoonsgegevens te bewaren. Verwerker zal Verwerkingsverantwoordelijke informeren wanneer hij de Persoonsgegevens niettemin langer wenst te bewaren, onder vermelding van de redenen hiertoe, evenals de wettelijke grondslag voor dit bewaren.

12. Geldigheid, duur en beëindiging van de verwerkersovereenkomst

12.I Deze Verwerkersovereenkomst is geldig vanaf datum ondertekening door beide Partijen, voor de duur van de Overeenkomst inzake de diensten die geleverd worden door Verwerker aan Verwerkingsverantwoordelijke als vermeld onder overweging sub B, met dien verstande dat de duur van de Verwerkersovereenkomst naar rato wordt verlengd zolang het terug leveren dan wel vernietigen van gegevens overeenkomstig artikel 12.4 nog niet is voltooid.

12.2 Wijzigingen van deze Verwerkersovereenkomst zijn slechts geldig indien deze door wederzijdse instemming van Verwerkingsverantwoordelijke en Verwerker schriftelijk zijn overeengekomen.

12.3 Een wijziging in de verwerkte Persoonsgegevens of in de betrouwbaarheidseisen, de privacyregelgeving of de eisen van Verwerkingsverantwoordelijke kan aanleiding zijn om deze Verwerkersovereenkomst aan te vullen of te wijzigen. Indien dit leidt tot significante aanpassingen in de Overeenkomst, of wanneer Verwerker niet kan voorzien in een passend niveau van bescherming, kan dit voor Verwerker reden zijn om de Overeenkomst te beëindigen.

12.4 Beëindiging van de Verwerkersovereenkomst leidt ertoe dat de Verwerkte Persoonsgegevens binnen een redelijke termijn, naar keuze van Verwerkingsverantwoordelijke, worden geretourneerd c.q. overgedragen dan wel vernietiging. Verwerker zal hangende de keuze van Verwerkingsverantwoordelijke de Persoonsgegevens blijven bewaren voor rekening en risico van Verwerkingsverantwoordelijke en met dien verstande dat Verwerkingsverantwoordelijke zijn keuze binnen een periode van één maand kenbaar moet maken aan Verwerker. De eventuele kosten van het verzamelen en overdragen dan wel vernietigen van Persoonsgegevens bij het eindigen van de Overeenkomst zijn voor rekening van Verwerkingsverantwoordelijke. Op verzoek van Verwerkingsverantwoordelijke geeft Verwerker vooraf een kosteninschatting.

12.5 Verwerker kan afwijken van het in artikel 12.4 bepaalde, voor zover ten aanzien van Persoonsgegevens een wettelijke bewaartermijn zou gelden of voor zover dat noodzakelijk is om tegenover Verwerkingsverantwoordelijke nakoming van zijn verplichtingen te bewijzen.

12.6 In deze Verwerkersovereenkomst opgenomen verplichtingen die naar hun aard bedoeld zijn om voort te duren na het eindigen van deze Verwerkersovereenkomst, waaronder maar niet beperkt tot de artikelen over geheimhouding en aansprakelijkheid, blijven van toepassing, ook nadat deze Verwerkersovereenkomst is geëindigd.

13. Toepasselijk recht en geschillenbeslechting

13.1 Deze Verwerkersovereenkomst en de uitvoering daarvan wordt beheerst door Nederlands recht.

13.2 Geschillen, welke tussen partijen ontstaan in verband met deze Verwerkersovereenkomst, zullen bij uitsluiting worden voorgelegd aan de bevoegde rechter van de Rechtbank Den Haag.

Ondertekening

Aldus opgesteld en in tweevoud getekend te Maasdijk.

Verwerkingsverantwoordelijke

Locatie, datum : «Woonplaats (Plaats)», datum
Naam organisatie : «Naam»
Naam vertegenwoordiger : de heer / mevrouw
«Initialen voorvoegsel achternaam»
Functie vertegenwoordiger : «Functienaam»

Handtekening :

Verwerker

Locatie, datum : Maasdijk, datum
Naam organisatie : VTM Services B.V.
Naam vertegenwoordiger : De heer J. Schnetz
Functie vertegenwoordiger : Operationeel Directeur
Handtekening :

Bijlage 1 – categorieën, soort, aard, doel en contactgegevens

A. Categorieën Betrokkenen

De personen waarop de Persoonsgegevens betrekking hebben zijn in ieder geval:

- Klanten of Medewerkers van Verwerkingsverantwoordelijke

B. Soort Persoonsgegevens

De Persoonsgegevens die door Verwerker worden verwerkt zijn in ieder geval:

- Naam, Telefoonnummers en Emailadressen.

C. Aard en doel van de verwerking

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

- 1) haalbaarheidsonderzoek van een mogelijke samenwerking tussen VTM en klant;
- 2) inventarisatie van de ICT- en /of Telecom omgeving bij klant;
- 3) implementatie van ICT- en Telecomproducten en diensten bij klant;
- 4) beheren, monitoren, onderhouden en beveiligen van ICT- en Telecom omgeving/componenten bij klant;

D. Gegevens sub-verwerkers

Verwerker maakt voor de diensten thans gebruik van de volgende sub-verwerkers:

Verwerker	Beschrijving werkzaamheden
Microsoft Corporation	We hebben onze services ondergebracht bij de datacenters van Microsoft Azure. Microsoft is gevestigd in Dublin. Deze datacenters zijn gevestigd in Nederland en de back-up bevindt zich in Ierland. Microsoft zorgt voor de beveiliging en beschermt jouw en onze data tegen onder andere diefstal en hard- en softwareproblemen.
AFAS Software B.V.	We maken gebruik van de ERP Software van AFAS Software B.V.. AFAS is gevestigd in Nederland. De datacenters zijn tevens gevestigd in Nederland en de back-up bevindt zich in Nederland. AFAS zorgt voor de beveiliging en beschermt jouw en onze data tegen onder andere diefstal en hard- en softwareproblemen.
N-able Technologies LTD	We maken voor onze Back-up diensten gebruik van de Cove Data Protection™ Software van N-Able Technologies. N-Able is gevestigd in de United Kingdom.

	De datacenters zijn wereldwijd verspreid. N-Able zorgt voor de beveiliging en beschermt jouw en onze data tegen onder andere diefstal en hard- en softwareproblemen.
Salesbuildr	We maken voor onze offertes gebruik van Salesbuildr. Salesbuildr is gevestigd in Nederland. De datacenters zijn gevestigd in Nederland en Duitsland. Salesbuildr voert geautomatiseerde back-ups uit over de hele infrastructuur. Alle back-up processen worden door Salesbuildr actief gemonitord met geautomatiseerde waarschuwingen. Salesbuildr zorgt voor de beveiliging en beschermt jouw en onze data tegen onder andere diefstal en hard- en softwareproblemen.

E. Contactgegevens

Voor vragen of opmerkingen over de Verwerkersovereenkomst en Bijlagen is de contactpersoon van

VERANTWOORDELIJKE :

.....

VERWERKER : VTM Services B.V.

0174 527320

Versie 2.1

Bijlage 2 – Beschrijving informatiebeveiliging VTM

Om de vertrouwelijkheid en de geheimhouding van gegevens te waarborgen heeft VTM diverse technische en organisatorische maatregelen genomen. Dit conform de verschillende ISO-certificeringen die we in bezit hebben. Dit betreffen de ISO27001 (informatiebeveiliging), NEN7510 (informatiebeveiliging in de Zorgsector) en ISO9001 (Kwaliteit). Deze beveiligingsmaatregelen dienen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau te bieden gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen.

Domein	Technische/ organisatorische maatregel
Veilig personeelsbeleid	Vertrouwelijkheidsverplichtingen Medewerkers van de verwerker zijn onderworpen aan vertrouwelijkheidsverplichtingen en deze verplichtingen worden formeel opgenomen in arbeidsovereenkomsten. Bij indiensttreding van een nieuwe medewerker vragen we standaard een VOG (Verklaring Omtrent het Gedrag), algemeen screeningsprofiel, aan voor de volgende functies: - Leidinggevende functies - Technische functies - Financiële functies Voor deze functies wordt de VOG elke 3 jaar opnieuw aangevraagd. Beveiligingstraining De verwerker stelt haar medewerkers op de hoogte van de relevante beveiligingsprocedures voor het beschermen van klantendata en hun rol daarbij. Beëindiging. Toegangsrechten worden bij beëindiging van de samenwerking tijdig ingetrokken, in overeenstemming met formele beveiligingsadministratieprocedures.
Beheer van bedrijfsmiddelen	Inventaris van bedrijfsmiddelen De verwerker houdt een inventaris bij van alle ICT-materiaal en media in gebruik. Toegang tot de inventarissen is beperkt tot hiervoor geautoriseerde medewerkers. Behandeling van bedrijfsmiddelen Data op draagbare apparaten is versleuteld. – De verwerker beschikt over procedures voor het

	veilig vernietigen van media en afgedrukt materiaal die vertrouwelijke data bevatten.
Cryptografie	Versleuteling van vertrouwelijke data gebeurt volgens crypto grafische standaarden. Data uitwisseling tussen systemen van VTM en derden gaat uitsluitend via beveiligde kanalen. Hierbij wordt TLS-encryptie (minimaal TLS versie 1.2) gebruikt.
Fysieke beveiliging en beveiliging van de omgeving	Fysieke toegang tot faciliteiten - VTM beperkt de toegang tot faciliteiten waar vertrouwelijke informatie wordt verwerkt tot geïdentificeerde, geautoriseerde personen. - Fysieke toegang tot datacentra wordt uitsluitend toegekend volgens een formele autorisatieprocedure, en toegangsrechten worden periodiek beoordeeld Bescherming tegen verstoringen. VTM gebruikt verschillende systemen die voldoen aan industriestandaarden om zijn datacentra te beschermen tegen gegevensverlies als gevolg van stroomuitval en brand.
Toegangscontrole	Toegangsbeleid VTM hanteert een toegangscontrolebeleid op basis van 'need-to-know'- en 'least privileges'-beginselen. Toegangsautorisatie Elk individu die toegang heeft tot systemen die klantgegevens bevatten, heeft een aparte, unieke ID-gebruikersnaam. - De verwerker beperkt de toegang tot klantgegevens tot die personen die dergelijke toegang nodig hebben om hun functie uit te voeren. Authenticatie De verwerker maakt gebruik van standaardpraktijken die voldoen aan industriestandaarden om gebruikers te identificeren en te authentifieren die zich proberen toegang te verschaffen tot de netwerk- of informatiesystemen van de verwerker, waaronder sterke authenticatie. - Indien authenticatiemechanismen gebaseerd zijn op wachtwoorden, dan vereist de verwerker dat de wachtwoorden ten minste acht tekens lang en

	voldoende complex zijn. – Gedeactiveerde of verlopen ID's / gebruikersnamen worden niet toegekend aan andere personen. – Accounts worden vergrendeld bij herhaalde pogingen om met behulp van een ongeldig wachtwoord toegang te krijgen tot het informatiesysteem. Netwerkttoegang De verwerker implementeert de nodige controlemaatregelen (bv. firewalls, security appliances, netwerk segmentatie) die een redelijke mate van zekerheid bieden dat toegang tot zijn netwerk op gepaste wijze wordt beschermd.
Beveiliging van de bedrijfsactiviteiten (operationele beveiliging)	Gegevensherstel VTM maakt op periodieke basis, maar in geen geval minder vaak dan één keer per week (tenzij tijdens die periode geen gegevens bijgewerkt werden), back-ups van klantgegevens voor hersteldoeleinden. – VTM bewaart kopieën van klantgegevens en gegevensherstelprocedures op een andere plaats dan waar de primaire computerapparatuur die de klantgegevens verwerkt, zich bevindt. Beveiligingsupdates Beveiligingsupdates worden opgevolgd en geïnstalleerd volgens een gedocumenteerd patch managementproces.
Communicatie beveiliging	Netwerksegregatie VTM heeft een netwerksegmentatiebeleid en controles ingevoerd om te vermijden dat personen toegang krijgen tot communicatie en systemen waarvoor ze geen autorisatie hebben. Transfer buiten eigen netwerk VTM versleutelt klantgegevens die worden verzonden via publieke, niet-vertrouwde netwerken. Informatieoverdracht. Overdracht van klantgegevens aan derde partijen geschiedt enkel na het sluiten van een formele schriftelijke overeenkomst.
Verwerving, ontwikkeling en onderhoud van informatiesystemen	Beveiligingsvereisten. De vereisten voor de bescherming van gegevens en systemen worden geanalyseerd en

	gespecificeerd. Controle over wijzigingen. VTM heeft een formeel wijzigingsbeheerproces geïmplementeerd om ervoor te zorgen dat wijzigingen in operationele systemen en toepassingen plaatsvinden op een gecontroleerde wijze.
Verwerkersrelaties	Keuze van verwerkers VTM evalueert de beveiliging en privacy praktijken van een verwerker/partner met betrekking tot gegevensverwerking. Contractuele verplichtingen (sub) Verwerkers met toegang tot klantgegevens zijn onderworpen aan verplichtingen inzake gegevensbescherming en deze worden formeel opgenomen in verwerkerscontracten.
Beheer van informatiebeveiligingsincidenten	Incident response VTM houdt een register van beveiligingsinbreuken bij met een beschrijving van de inbreuk, het tijdstip, de gevolgen van de inbreuk, de naam van de melder en van degene aan wie de inbreuk werd gemeld. Notificatie van incidenten In geval van een informatiebeveiligingsincident dat impact heeft op de vertrouwelijkheid of integriteit van klantgegevens, zal VTM, de klant hiervan zo snel mogelijk maar in ieder geval binnen 24 uur na waarneming van het incident informeren (zoals beschreven in de overeenkomst).
Bedrijf continuïteit	Noodherstel VTM handhaaft een noodherstelplan voor de datacentra waar zich informatiesystemen van VTM bevinden die klantgegevens verwerken. Redundantie De redundante opslag en procedures voor gegevensherstel van VTM zijn ontworpen met als doel klantgegevens te herstellen in hun laatste geback-up staat voor het tijdstip waarop ze verloren gegaan zijn of vernietigd werden.

Bijlage 3 – Procedure meldplicht datalekken

Tussen Partijen zijn met betrekking tot de meldplicht datalekken de volgende afspraken gemaakt:

- 1) Verwerker registreert Datalekken voor zover deze worden geconstateerd door haar diensten;
- 2) In geval van een Datalek informeert Verwerker Verwerkingsverantwoordelijke zonder onredelijke vertraging en zal de relevante informatie over het Datalek melden aan de hand van de in bijlage 4 opgenomen vragenlijst;
- 3) Verwerkingsverantwoordelijke zal beoordelen of een melding verricht dient te worden bij de Autoriteit Persoonsgegevens dan wel Betrokkene(n). Verwerkingsverantwoordelijke zal daarbij in overleg treden met Verwerker;
- 4) Voordat Verwerkingsverantwoordelijke de melding bij de Autoriteit Persoonsgegevens dan wel Betrokkene(n) verricht zal Verwerkingsverantwoordelijke de inhoud van de melding met Verwerker bespreken;
- 5) Indien Verwerkingsverantwoordelijke oordeelt dat tevens Betrokkene(n) geïnformeerd dienen te worden, zal Verwerkingsverantwoordelijke de inhoud van die informatie met Verwerker bespreken.

Bijlage 4 - vragenlijst bij de procedure meldplicht datalekken

De contactpersonen bij Verwerkingsverantwoordelijke voor de meldplicht datalekken zijn:

[A + gegevens]

[B + gegevens]

Verwerker zal bij een Datalek de volgende vragen beantwoorden:

Geef een omschrijving van het Datalek:

.....

De persoonsgegevens van hoeveel personen zijn getroffen door het Datalek?

.....

Omschrijf de groep personen waarop de Persoonsgegevens betrekking hebben.

.....

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 Datalek:

.....

Wanneer is het Datalek 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. ransomware 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 geleeke 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 Datalek? Zo ja, welke uit welke landen:

.....

Bijlage 5 – Algemene voorwaarden

De NLdigital Voorwaarden 2020 zijn van toepassing, gedeponneerd bij de Rechtbank Midden-Nederland, locatie Utrecht. Deze voorwaarden kunt u hier raadplegen en downloaden: <https://www.vtmgroep.nl/algemene-voorwaarden>. Indien gewenst sturen wij u deze kosteloos toe.