1e lijn support
administratie@aditum-arbo.nl
088-277 88 28

2e lijn support
support@planningsagenda.nl
0548-234 111

Verwerkersovereenkomst

De partijen zijn gelijk aan de partijen vermeld in de werkopdracht inclusief basiscontract arbodienstverlening onder nummer

Klant (Werkgever), hierna te noemen: ‘Opdrachtgever’

Bedrijfsarts, hierna te noemen: ‘Opdrachtgever’

En

Aditum Arbo B.V., hierna te noemen: ‘Opdrachtnemer’

Ondergetekenden gezamenlijk aangeduid als “Partijen”;

OVERWEGEN DAT:

A. Opdrachtnemer diensten ten behoeve van Opdrachtgevers verricht, zoals beschreven in de werkopdracht inclusief basiscontract arbodienstverlening onder nr.:
B. Partijen in het kader van de uitvoering van de hiervoor bedoelde overeenkomst persoonsgegevens verwerken in de zin van de Algemene Verordening Gegevensbescherming (hierna: ‘AVG’), waarvoor Opdrachtgevers ‘verwerkingsverantwoordelijken’ zijn in de zin van de AVG.
C. Opdrachtnemer de betreffende gegevens louter in opdracht van Opdrachtgevers verwerkt en niet voor eigen doeleinden.
D. Opdrachtnemer in dat kader is aan te merken als ‘verwerker’ in de zin van de AVG.
E. Partijen de opdracht tot en nadere afspraken omtrent de verwerking van persoonsgegevens wensen vast te leggen in deze Verwerkersovereenkomst.
F. Deze Verwerkersovereenkomst van toepassing is op alle rechtsverhoudingen die tussen Partijen zijn aangegaan voor zover op grond daarvan persoonsgegevens worden verwerkt.

EN ZIJN OVEREENGEKOMEN:

Definities

1.1. In deze Verwerkersovereenkomst worden de hierna volgende begrippen gehanteerd.
1.2. *Verantwoordelijke*: de verwerkingsverantwoordelijke in de zin van artikel 4 sub 7 AVG oftewel de Opdrachtgever.
1.3. *Verwerker*: degene die ten behoeve van de Verantwoordelijke persoonsgegevens bewerkt in de zin van artikel 4 sub 8 AVG, oftewel de Opdrachtnemer.
1.4. *Betrokkene*: degene op wie een persoonsgegeven betrekking heeft, zoals bedoeld in artikel 4 sub 1 AVG.
1.5. *Derde*: ieder, niet is de Betrokkene, de Verantwoordelijke, de Verwerker, of enig persoon die onder rechtstreeks gezag van de Verantwoordelijke of de Verwerker gemachtigd is om persoonsgegevens te verwerken.
1.6. *Verwerken van persoonsgegevens*: het uitvoeren van een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, zoals is gedefinieerd in artikel 4 sub 2 AVG.
1.7. *Autoriteit Persoonsgegevens (of kortweg ‘AP’)*: de organisatie als bedoeld in artikel 6 Uitvoeringswet AVG.
1.8. *Verstrekken van persoonsgegevens*: de door de Verantwoordelijke aan Verwerker verstrekte gegevens ter verwerking ten behoeve van de Verantwoordelijke betreffende geïdentificeerde of identificeerbare gegevens van een natuurlijk persoon.
1.9. *Datalek of Beveiligingslek*: inbreuk in verband met persoonsgegevens, zoals bedoeld in artikel 4 sub 12 AVG.
1.10. *Verwerkersovereenkomst*: de onderhavige overeenkomst tussen Partijen.
1.11. *Hoofdovereenkomst*: de overeenkomst zoals is geduid in overweging A.

Onderwerp en reikwijdte van deze Verwerkersovereenkomst

2.1. Opdrachtnemer kan gedurende de uitvoering van de overeenkomst(en) ten behoeve van Opdrachtgever en ter voldoening aan enige wettelijke verplichting persoonsgegevens verwerken.
2.2. Een overzicht van de categorieën persoonsgegevens en de doeleinden waarvoor de persoonsgegevens ten behoeve van Opdrachtgever worden verwerkt is opgenomen in **Bijlage 1** bij deze Verwerkersovereenkomst.

Uitvoering verwerking

3.1. Opdrachtnemer zal optreden als Verwerker en Opdrachtgever als Verantwoordelijke. Voor het medisch dossier met C gegevens is uitsluitend de betreffende behandelend Bedrijfsarts de Verwerkingsverantwoordelijke. Opdrachtnemer staat ervoor in dat het medisch dossier zich in een afgescheiden beveiligd deel van het systeem bevindt, waar Opdrachtgever op geen enkel wijze inzage of toegang tot heeft noch zal verkrijgen.

3.2. Opdrachtnemer garandeert dat zij ten behoeve van Opdrachtgever uitsluitend persoonsgegevens zal verwerken voor zover dit noodzakelijk is voor de uitvoering van de Hoofdovereenkomst en voor zover dit overeenkomstig de aard en het doel van de Hoofdovereenkomst is en niet anders dan op basis van instructies van Opdrachtgever in haar rol als Verantwoordelijke. Overige verwerkingen zullen uitsluitend worden uitgevoerd als daartoe een wettelijke verplichting bestaat of daarvoor een ambtelijk bevel is gegeven, waarover Opdrachtgever zal worden geïnformeerd, tenzij een wettelijke verplichting of ambtelijk bevel dit verhindert. In geen geval zal Opdrachtnemer persoonsgegevens verwerken voor eigen doeleinden.

3.3. Opdrachtnemer zal alle redelijke instructies van Opdrachtgever in verband met de verwerking van de persoonsgegevens opvolgen. Opdrachtnemer stelt Opdrachtgever op de hoogte indien naar haar oordeel instructies in strijd zijn met de toepasselijke regelgeving met betrekking tot de verwerking van persoonsgegevens.

3.4. Opdrachtnemer zal de persoonsgegevens aantoonbaar, op behoorlijke en zorgvuldige wijze en in overeenstemming met de op hem als Verwerker op grond van de AVG en overige regelgeving rustende verplichtingen verwerken. Indien er sprake is van het verwerken van bijzondere persoonsgegevens als bedoeld in artikel 9 AVG, zal Opdrachtnemer zich tevens houden aan de bepalingen die op grond van boek 7, titel 7, afdeling 5 BW (de Wet inzake de geneeskundige behandelingsovereenkomst, of kortweg: 'WGBO') van toepassing zijn.

3.5. Opdrachtnemer zal, tenzij hij hiervoor uitdrukkelijke voorafgaande schriftelijke toestemming heeft verkregen van Opdrachtgever, geen persoonsgegevens verwerken of laten verwerken door hemzelf of door derden in landen buiten de Europese Economische Ruimte ('EER'). Opdrachtnemer stelt (de in **Bijlage 2** genoemde medewerker van) Opdrachtgever onmiddellijk schriftelijk op de hoogte van alle (geplande) permanente of tijdelijke doorgiftes van persoonsgegevens naar een land buiten de Europese Economische Ruimte en zal pas uitvoering geven aan dergelijke (geplande) doorgiftes na schriftelijke toestemming van Opdrachtgever. Opdrachtgever heeft te allen tijde het recht om aanvullende voorwaarden te verbinden aan haar toestemming voor een dergelijke verwerking.

3.6. Onverminderd enige andere contractuele geheimhoudingverplichting die op Opdrachtnemer rust, garandeert Opdrachtnemer dat zij alle persoonsgegevens als strikt vertrouwelijk zal behandelen en dat zij al haar werknemers, vertegenwoordigers en/of onderaannemers die betrokken zijn bij de verwerking van de persoonsgegevens van de vertrouwelijke aard van dergelijke (persoons)gegevens op de hoogte zal stellen en hen zal verplichten eenzelfde vertrouwelijkheid in acht te nemen.

3.7. Opdrachtnemer zal haar volledige en tijdige medewerking verlenen aan Opdrachtgever om (i) na goedkeuring en in opdracht van Opdrachtgever betrokkenen toegang te laten krijgen tot de hun betreffende persoonsgegevens; (ii) persoonsgegevens te verwijderen of te corrigeren of over te dragen; (iii) aan te tonen dat persoonsgegevens verwijderd of gecorrigeerd of overgedragen zijn indien zij incorrect zijn (of, ingeval Opdrachtgever het er niet mee eens is dat persoonsgegevens incorrect zijn, het feit vast te leggen dat de betrokkene zijn persoonsgegevens als incorrect beschouwt); en (iv) Opdrachtgever anderszins in de gelegenheid te stellen om aan haar verplichtingen uit hoofde van de AVG of andere toepasselijke regelgeving op het gebied van verwerking van persoonsgegevens te voldoen.

Beveiliging persoonsgegevens en controle

4.1. De uitwisseling van persoonsgegevens tussen Partijen vindt zo veel mogelijk versleuteld plaats. Voor zover sprake is van toegang via internet tot een applicatie waarin medische gegevens worden verwerkt, zal deze toegang niet anders plaatsvinden dan middels meervoudige authenticatie.

4.2. Onverminderd de beveiligingsnormen die Partijen op mogelijk andere wijze zijn overeengekomen, zal Opdrachtnemer passende technische en organisatorische beveiligingsmaatregelen nemen die gezien de huidige stand der techniek en de daarmee gemoeide kosten overeenstemmen met de aard van de te verwerken persoonsgegevens, ter bescherming van de persoonsgegevens tegen verlies, onbevoegde kennisname, verminking of onrechtmatige verwerking, alsmede om de (tijdige) beschikbaarheid van de gegevens te garanderen. Deze maatregelen omvatten in ieder geval:

a) maatregelen om te waarborgen dat enkel bevoegd personeel toegang heeft tot de persoonsgegevens voor de doeleinden die zijn uiteengezet in **Bijlage 1**;
b) maatregelen waarbij de Verwerker haar medewerkers, onderaannemers uitsluitend toegang geeft tot persoonsgegevens via op naam gestelde accounts, waarbij het gebruik van die accounts adequaat gelogd wordt en waarbij de betreffende accounts alleen toegang geven tot die persoonsgegevens waartoe de toegang voor de betreffende persoon noodzakelijk is;
c) maatregelen om de persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, onopzettelijk verlies of wijziging, onbevoegde of onrechtmatige opslag verwerking, toegang of openbaarmaking, waaronder, maar niet beperkt tot encryptie van (opgeslagen) gegevens;
d) maatregelen om zwakke plekken te identificeren ten aanzien van de verwerking van persoonsgegevens in de systemen die worden ingezet voor het verlenen van diensten aan Opdrachtgever;
e) maatregelen om de tijdige beschikbaarheid van de gegevens te garanderen, een en ander zoals nader uitgewerkt in **Bijlage 3** en in de Hoofdovereenkomst;
f) de overige maatregelen die Partijen in **Bijlage 3** en in de Hoofdovereenkomst zijn overeengekomen.

4.3. Opdrachtnemer onderwerpt periodiek haar activiteiten met betrekking tot informatieveiligheid en privacy beleid aan een (externe) audit.

4.4. Opdrachtgever is te allen tijde gerechtigd de verwerking van persoonsgegevens te controleren. Opdrachtnemer is verplicht Opdrachtgever of een in opdracht van Opdrachtgever controlerende instantie toe te laten en medewerking te verlenen, zodat de controle daadwerkelijk uitgevoerd kan worden.

4.5. Opdrachtgever heeft het recht toe te (laten) zien op de naleving van de hiervoor onder 4.1 en 4.2 genoemde maatregelen. Opdrachtnemer stelt Opdrachtgever, indien Opdrachtgever daarom verzoekt, hiertoe in elk geval eenmaal per jaar in de gelegenheid op een door Partijen in gezamenlijk overleg nader te bepalen tijdstip en verder indien Opdrachtgever daar aanleiding toe ziet naar aanleiding van (vermoeden van) informatie- of privacy-incidenten, zulks te (laten) controleren. Opdrachtnemer zal eventuele door Opdrachtgever naar aanleiding van een dergelijke controle in redelijkheid gegeven instructies tot aanpassing van het beveiligingsbeleid binnen een redelijke termijn opvolgen.

4.6. De kosten voor de hiervoor in dit artikel 4 bedoelde controle komen voor rekening van Opdrachtgever, tenzij uit de audit aantoonbaar voortvloeit dat Opdrachtnemer wezenlijk tekortschiet in de nakoming van haar (beveiligings-)verplichtingen.

4.7. Partijen erkennen dat beveiligingseisen voortdurend veranderen en dat een effectieve beveiliging frequente evaluatie en regelmatige verbetering van verouderde beveiligingsmaatregelen vereist. Opdrachtnemer zal daarom de maatregelen zoals geïmplementeerd op basis van dit artikel voortdurend evalueren en verscherpen, aanvullen of verbeteren, om te blijven voldoen aan haar verplichtingen onder dit artikel. Opdrachtnemer zal aan Opdrachtgever tenminste eenmaal per jaar schriftelijk verslaglegging van doen toekomen.

Monitoring, informatieplichten en incidentenmanagement

5.1. Opdrachtnemer zal actief monitoren op inbreuken op de beveiligingsmaatregelen en over de resultaten van de monitoring in overeenstemming met dit artikel rapporteren aan Opdrachtgever.

5.2. Zodra zich een incident met betrekking tot de verwerking van de persoonsgegevens voordoet, heeft voorgedaan, of zou kunnen voordoen, is Opdrachtnemer verplicht Opdrachtgever als Verantwoordelijke daarvan onverwijld en in ieder geval binnen 24 uur in kennis te stellen en daarbij alle relevante informatie te verstrekken omtrent de aard van het incident, het risico dat gegevens onrechtmatig verwerkt zijn of kunnen worden en de maatregelen die getroffen zijn of zullen worden om het incident op te lossen dan wel de gevolgen/schade zoveel mogelijk te beperken.

5.3. Opdrachtgever is, onverminderd de overige verplichtingen uit dit artikel, verplicht om de eventuele negatieve gevolgen die voortvloeien uit een incident zo snel mogelijk ongedaan te maken dan wel de verdere gevolgen te minimaliseren.

5.4. Opdrachtnemer zal Opdrachtgever te allen tijde haar medewerking verlenen en zal de instructies van Opdrachtgever opvolgen, met als doel Opdrachtgever in staat te stellen een deugdelijk onderzoek te verrichten naar het incident, een correcte respons te formuleren en passende vervolgstappen te nemen ten aanzien van het incident, waaronder begrepen het informeren van de AP en/of de betrokkene zoals bepaald in artikel 5 lid 8 van deze Verwerkersovereenkomst.

5.5. Onder 'incident' wordt in elk geval het volgende verstaan:

a) een klacht of (informatie)verzoek van een Betrokkene of een Derde met betrekking tot de verwerking van persoonsgegevens door Opdrachtnemer;
b) een onderzoek naar of beslaglegging door overheidsfunctionarissen op de persoonsgegevens of een vermoeden dat dit gaat plaatsvinden;
c) iedere ongeautoriseerde toegang, verwerking, verwijdering, verminking, verlies of enige vorm van onrechtmatige verwerking van de persoonsgegevens;
d) een inbreuk op de beveiliging en/of de vertrouwelijkheid, zoals uiteengezet in artikel 3 en 4 van deze Verwerkersovereenkomst, althans ieder ander incident, dat (mogelijk) leidt tot onopzettelijke of onrechtmatige vernietiging, verlies, wijziging, onbevoegde openbaarmaking van – of toegang tot – de persoonsgegevens, of enige aanwijzing dat een dergelijke inbreuk zal plaatsvinden of heeft plaatsgevonden.

5.6. Opdrachtnemer zal te allen tijde geschreven procedures voorhanden hebben die hem in staat stellen om Opdrachtgever van een onmiddellijke reactie over een incident te voorzien, en om effectief samen te werken met Opdrachtgever om het incident af te handelen en zal Opdrachtgever voorzien van een exemplaar van dergelijke procedures indien Opdrachtgever daarom verzoekt.

5.7. Meldingen die worden gedaan op grond van dit artikel worden gericht aan de (in **Bijlage 2)** opgenomen werknemer van) Opdrachtgever of, indien relevant, aan een andere door Opdrachtgever tijdens de duur van deze Verwerkersovereenkomst schriftelijk bekendgemaakte andere werknemer van Opdrachtgever.

5.8. Opdrachtgever zal, indien naar haar oordeel noodzakelijk, betrokkenen en andere derden waaronder de AP informeren over incidenten. Het is Opdrachtnemer niet toegestaan informatie te verstrekken over incidenten aan betrokkenen of andere derde partijen, behoudens voor zover Opdrachtnemer daartoe wettelijk verplicht is.

Gebruik onderaannemers

6.1. Opdrachtnemer kan haar activiteiten die (deels) bestaan uit het verwerken van persoonsgegevens of die vereisen dat persoonsgegevens verwerkt worden, geheel of ten dele uitbesteden aan derden ('subverwerkers'). Een overzicht van de subverwerkers is vermeld in (**Bijlage 1**).

6.2. Opdrachtnemer zal aan de door hem ingeschakelde derde dezelfde of strengere verplichtingen opleggen als voor hemzelf uit deze Verwerkersovereenkomst en de AVG voortvloeien en ziet toe op de naleving daarvan door de derde. De betreffende afspraken met de derde zullen schriftelijk worden vastgelegd.

Aansprakelijkheid

7.1 Indien een van de Partijen tekortschiet in de nakoming van enige verplichting uit hoofde van deze Verwerkersovereenkomst, kan de andere partij haar in gebreke stellen. Een partij zal niet eerder in verzuim zijn, dan nadat de ene de andere partij schriftelijk in gebreke heeft gesteld en aan die andere partij een redelijke termijn heeft gegund tot nakoming van de betreffende verplichting of tot het doen van een redelijk voorstel tot vergoeden van de schade.

7.2. Opdrachtnemer is aansprakelijk voor toerekenbare tekortkomingen waarvoor zij in verzuim is. Iedere aansprakelijkheid van Opdrachtnemer is beperkt tot vergoeding van directe schade tot maximaal het bedrag dat op grond van de door Opdrachtnemer afgesloten aansprakelijkheidsverzekering wordt uitgekeerd. Indien de aansprakelijkheidsverzekering geen aanspraak geeft op enig bedrag dan is de aansprakelijkheid van Opdrachtnemer beperkt tot een maximum van 100.000 euro.
De beperkingen komen te vervallen indien en voor zover de schade het gevolg is van opzet of bewuste roekeloosheid van medewerkers van Opdrachtnemer.

7.3. Naast Opdrachtnemer kunnen ook alle personen die betrokken zijn of betrokken zijn geweest bij de uitvoering van de Verwerkersovereenkomst en de subwerkers een beroep doen op artikel 7.2.

Duur en beëindiging

8.1. Deze Verwerkersovereenkomst gaat in op het moment van ondertekening door Partijen.

8.2. De duur van deze Verwerkersovereenkomst is gelijk aan de duur van de Hoofdovereenkomst, tenzij Partijen anders zijn overeengekomen.

8.3. Er bestaat samenhang tussen de Verwerkersovereenkomst en de Hoofdovereenkomst. Dat wil zeggen dat beëindiging van de Verwerkersovereenkomst, op welke grond dan ook (opzegging/ontbinding), tot gevolg heeft dat de Hoofdovereenkomst eveneens op dezelfde grond beëindigd wordt (en vice versa), tenzij partijen in voorkomend geval schriftelijk anders overeenkomen.

8.4. Verplichtingen welke naar hun aard bestemd zijn om ook na beëindiging van deze Verwerkersovereenkomst voort te duren, blijven na beëindiging van de Verwerkersovereenkomst gelden. Tot deze bepalingen behoren onder meer die welke voortvloeien uit de bepalingen betreffende bewaarplicht, geheimhouding, aansprakelijkheid en toepasselijk recht.

8.5. Wijziging van deze Verwerkersovereenkomst kan slechts schriftelijk plaatsvinden door middel van een door Partijen ondertekend amendement.

8.6. Ieder der partijen is gerechtigd, onverminderd hetgeen daartoe bepaald is in de Hoofdovereenkomst, de uitvoering van deze Verwerkersovereenkomst en de daarmee samenhangende Hoofdovereenkomst op te schorten, dan wel zonder rechterlijke tussenkomst met onmiddellijke ingang te ontbinden, indien:
   a) de andere partij wordt ontbonden of anderszins ophoudt te bestaan;
   b) de andere partij aantoonbaar tekortschiet in de nakoming van de verplichtingen die voortvloeien uit deze Verwerkersovereenkomst en die ernstige toerekenbare tekortkoming niet binnen 30 dagen is hersteld na een daartoe strekkende schriftelijke ingebrekestelling;
   c) de andere partij in staat van faillissement wordt verklaard of surséance van betaling aanvraagt.

8.7. Opdrachtgever is gerechtigd deze Verwerkersovereenkomst en de Hoofdovereenkomst per direct te ontbinden indien Opdrachtnemer te kennen geeft niet (langer) te kunnen voldoen aan de betrouwbaarheidseisen die op grond van ontwikkelingen in de wet en/of de rechtspraak aan de verwerking van de persoonsgegevens worden gesteld. Artikel 9 lid 2 is van overeenkomstige toepassing.

Bewaartermijnen, teruggave en vernietiging van persoonsgegevens

9.1. Opdrachtnemer bewaart de persoonsgegevens niet langer dan strikt noodzakelijk en in geen geval langer dan tot het einde van deze Verwerkersovereenkomst of, indien tussen partijen een bewaartermijn is overeengekomen, niet langer dan deze termijn, tenzij sprake is van een wettelijke bewaarplicht.

9.2. Bij beëindiging van deze Verwerkersovereenkomst, of indien van toepassing aan het einde van de overeengekomen of wettelijke bewaartermijn, of op schriftelijk verzoek van Opdrachtgever, zal Opdrachtnemer, kosteloos, naar keuze van Opdrachtgever, de persoonsgegevens vernietigen of teruggeven in een gangbaar formaat, zoals, maar niet beperkt tot XML of CSV aan Opdrachtgever. Indien teruggave, vernietiging of verwijdering niet mogelijk zijn, stelt Opdrachtnemer Opdrachtgever daarvan onmiddellijk op de hoogte. In dat geval garandeert Opdrachtnemer dat hij de persoonsgegevens vertrouwelijk zal behandelen en niet langer zal verwerken.

9.3. Bij het einde van deze Verwerkersovereenkomst zal Opdrachtnemer alle subverwerkers die betrokken zijn bij het verwerken van persoonsgegevens op de hoogte stellen van de beëindiging van deze Verwerkersovereenkomst. De verplichtingen uit artikel 9.2 zijn van overeenkomstige toepassing op de deze subverwerkers.

Slotbepalingen

10.1. De overwegingen maken onderdeel uit van deze Verwerkersovereenkomst.

10.2. In het geval van strijdigheid tussen de bepalingen uit deze Verwerkersovereenkomst en de bepalingen uit de Hoofdovereenkomst, zullen de bepalingen van de Verwerkersovereenkomst leidend zijn.

10.3. Op deze Verwerkersovereenkomst is louter Nederlands recht van toepassing.

10.4. Eventuele conflicten zullen eerst met elkaar besproken worden waarbij beide partijen zich inspannen om deze in goed overleg met elkaar op te lossen.

10.5. Geschillen over of in verband met deze Verwerkersovereenkomst worden uitsluitend voorgelegd aan de bevoegde rechter in het arrondissement van de Opdrachtnemer.

10.6. In alle gevallen waarin deze Verwerkersovereenkomst niet voorziet beslissen Partijen in onderling overleg.

Aldus overeengekomen en ondertekend via de Hoofdovereenkomst.

Bijlage 1: Beschrijving verwerkingen persoonsgegevens

1. Het soort Persoonsgegevens

☒ e-mailadres
☒ voornaam
☒ achternaam
☒ adres
☒ postcode
☒ woonplaats
☒ telefoonnummer
☒ geslacht
☒ geboortedatum
☒ BSN
☒ klantnummer
☒ relatienummer
☒ gezondheid

2. Categorieën van Betrokkenen

☒ klanten / cliënten
☒ patiënten
☒ zakelijke contactpersonen

3. Doeleinde(n) verwerking:

Opdrachtgever verwerkt persoonsgegevens in het kader van het voeren van een medisch dossier en/of het verrichten van werkzaamheden in het kader van arbeidsgeneeskundige gezondheidsbevordering zoals bedoeld in de Arbowet.

4. Beschrijving verwerking(en) en middelen

Opdrachtnemer zal de hiervoor genoemde persoonsgegevens verwerken in verband met de activiteiten die zij onderneemt ter uitvoering van de overeenkomst. Opdrachtgever wijst de middelen voor de verwerking van de persoonsgegevens aan.

5. Subverwerkers

Naam sub-verwerker:	**Onderdeel dienstverlening**	**Inzage in de volgende Persoonsgegevens:**
Planningsagenda.nl B.V.	Beheer en support	Alle personeelsgegevens
Exonet B.V.	Hosting en onderhoud productieomgeving	Alleen via back-ups mogelijk
Cloud VPS	Hosting en onderhoud ontwikkel-, test- en acceptatieomgeving.	Geen

Bijlage 2: Contactgegevens

In geval van ‘incidenten’/datalekken dient door Opdrachtnemer contact opgenomen te worden met de Functionaris voor Gegevensbescherming en/of de privacy officer van opdrachtgever

Zie Hoofdovereenkomst.

Bijlage 3: TECHNISCHE EN ORGANISATORISCHE MAATREGELEN

Verwerker past de volgende maatregelen toe bij verwerkingen voor Verwerkersverantwoordelijke:

1. Fysieke toegangscontrole

Passende maatregelen om onbevoegden de toegang tot gegevensverwerkingssystemen, waarin persoonsgegevens worden verwerkt, te verhinderen.

- ☒ alarmsysteem
- ☒ alarmsysteem met verbinding naar bewaking of politie
- ☐ bescherming van gebouwen
- ☒ automatisch systeem voor toegangscontrole
- ☐ scheiding van werk- en bezoekruimtes
- ☐ chipkaart-/transpondervergrendeling
- ☐ sluitsysteem met behulp van een code
- ☐ handmatige vergrendeling
- ☐ biometrische beveiliging
- ☐ videobewaking van ingangen
- ☐ foto-elektrische beveiliging/bewegingsmelder
- ☐ veiligheidssloten
- ☒ gecontroleerde sleuteluitgave
- ☐ gezekerde lucht- en lichtschachten
- ☐ bewakingspersoneel
- ☐ toegangscontrole bij de portier
- ☒ registratie van de bezoekers
- ☐ identificatie van de bezoekers
- ☐ zorgvuldige selectie beveiligingspersoneel
- ☒ zorgvuldige selectie schoonmaakpersoneel
- ☐ verplicht dragen van een pasje

2. Digitale toegangscontrole

Maatregelen om te voorkomen dat een gegevensverwerkingssysteem kan worden gebruikt door onbevoegden.

- ☒ toewijzing van gebruikersrechten
- ☒ hanteren van gebruikersprofielen
- ☒ wachtwoordbeleid (lengte, opmaak, roulatie)
- ☐ hanteren van noodwachtwoorden
- ☒ authenticatie door gebruikersnamen/wachtwoorden
- ☒ meerfactorauthenticatie (2FA)
- ☒ protocol voor thuiswerken
- ☐ authenticatie door biometrische methoden
- ☒ hanteren van elektronische handtekening
- ☒ toewijzing van gebruikersprofielen
- ☐ vergrendeling voor de behuizing
- ☒ gebruik van VPN technologie
- ☒ vergrendeling van externe interfaces
- ☒ encryptie van een mobiele gegevensdrager
- ☒ gebruik van antivirussoftware
- ☒ gebruik van Intrusion Detection Systems
- ☒ encryptie van mobiele gegevensdragers
- ☒ encryptie van mobiele devices (smartphones)
- ☒ gebruik van een hardware firewall
- ☒ gebruik van een software firewall
- ☒ gebruik van Mobile Device Management
- ☒ regeling voor updaten software en firmware

3. Toegangscontrole persoonsgegevens

Maatregelen om ervoor te zorgen dat bevoegde gebruikers uitsluitend toegang kunnen krijgen tot de persoonsgegevens, waarvoor zij gemachtigd zijn en ter voorkoming van verdere onbevoegde verwerkingen.

- ☒ hanteren van een autorisatiesysteem
- ☒ rechtenbeheer door een systeembeheerder
- ☒ screening van de (interne) systeembeheerder
- ☒ registreren van toegangen tot applicaties
- ☒ registreren van toegangen tot gegevens
- ☒ veilige opslag van gegevensdragers
- ☒ fysieke schijf wissen voor hergebruik
- ☒ correcte vernietiging van gegevensdragers
- ☒ gebruik van papierversnipperaars of vernietigingsdiensten
- ☒ registratie van de vernietiging

4. Doorgiftecontrole

Maatregelen om ervoor te zorgen dat persoonsgegevens in de elektronische verzending of tijdens het transport of opslag op gegevensdragers niet kunnen worden gelezen, verwerkt of verwijderd door onbevoegden en dat gecontroleerd en aangetoond kan worden aan wie een doorgifte van persoonsgegevens heeft plaatsgevonden.

- ☒ gebruik van VPN-tunnels
- ☒ gebruik van SSL-/TLS-verbindingen
- ☒ gebruik van proxy servers
- ☒ gebruik van e-mailencryptie
- ☐ zorgvuldige selectie van personeel en vervoer bij transport
- ☐ gebruik van veilige transportverpakkingen en -houders
- ☒ openbaarmaking van gegevens in anonieme vorm
- ☒ openbaarmaking van gegevens in pseudonieme vorm
- ☐ creatie van een overzicht van de regelmatige ontvangst- en leveringsactiviteiten
- ☒ documentatie van de ontvangers van gegevens
- ☒ documentatie van (de termijnen van) geplande overdrachten
- ☒ gebruik van het vierogenprincipe (gesplitste wachtwoorden)

5. Invoeringscontrole

Maatregelen die verzekeren dat achteraf kan worden aangetoond of, wanneer en door wie persoonsgegevens in gegevensverwerkingssystemen zijn ingevoerd, gewijzigd of verwijderd.

- ☒ protocollen voor invoering, wijziging en verwijdering van gegevens
- ☒ protocollen voor het afhandelen van verzoeken tot wijziging, beperking of verwijdering van gegevens
- ☒ traceerbaarheid van invoering, wijziging of verwijdering van gegevens door individuele gebruikersnamen
- ☒ time stamping van verwerkingen
- ☒ hanteren van gebruikersrechten voor het verwerken van gegevens op basis van autorisatie
- ☒ overzichten van met welke applicaties gegevens kunnen worden ingevoerd, veranderd en verwijderd
- ☒ opslag van formulieren en bronnen, waarvan de opgeslagen gegevens zijn afgeleid

6. Opdrachtcontrole

Maatregelen die verzekeren dat persoonsgegevens die in opdracht verwerkt worden alleen volgens de instructies van de opdrachtgevers kunnen worden verwerkt.

- ☒ hanteren van verwerkersovereenkomsten
- ☒ schriftelijke instructies aan de opdrachtnemers
- ☒ zorgvuldige keuze van opdrachtnemers
- ☒ opdrachtnemer heeft een functionaris voor de gegevensbescherming aangewezen
- ☒ effectieve controle op de opdrachtnemer
- ☐ contractuele boetes voor overtredingen
- ☒ voorafgaand onderzoek over de documentatie van de veiligheidsmaatregelen bij de opdrachtnemer
- ☒ verplichting tot geheimhouding van de gegevens voor werknemers
- ☒ verplichting tot geheimhouding van de gegevens voor opdrachtnemers
- ☒ vernietiging van de gegevens na beëindiging van de dienst
- ☒ continue controle van de opdrachtnemers en zijn werkzaamheden

7. Beschikbaarheidscontrole

Maatregelen die beschikbaarheid en continuïteit waarborgen. ☒ noodstroomvoorziening voor servers

☒ controle van de temperatuur en de luchtvochtigheid in de serverruimte
☒ vuur- en rookalarmsysteem
☒ brandblussystemen/brandblussers in de serverruimte
☒ back-up- en een herstelplan
☒ opslag van back-upgegevens op een beveiligde, externe server
☒ tests van back-ups en dataherstel
☒ serverruimtes boven NAP in overstromingsgebieden
☒ serverruimtes niet onder sanitaire voorzieningen
☒ klimaatcontrole in serverruimtes
☒ bescherming stekkerdozen in serverruimtes
☒ aanwezigheid noodplan
☒ archiveringssysteem
☒ spamfilter

8. Scheiding van gegevens

Maatregelen die verzekeren dat voor verschillende doeleinden de verzamelde gegevens afzonderlijk verwerkt kunnen worden. ☒ fysiek gescheiden opslagsystemen of afzonderlijke gegevensdragers

☒ hanteren van een autorisatieconcept
☒ vastleggen van het doel van verwerking in de tributen van datasets
☒ vastleggen van de databankrechten
☒ hanteren van logische toegangsscheiding
☒ encryptie van datasets die worden verwerkt voor hetzelfde doel
☒ scheiding van productie- en testsystemen
☒ scheiding van gewone en gevoelige persoonsgegevens
☒ scheiding van brongegevens en gepseudonimiseerde of geanonimiseerde gegevens in aparte, beveiligde systemen
☒ privacy by design/privacy by default

9. Overige maatregelen

Overige maatregelen.

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____