VERWERKERSOVEREENKOMST UITVOERING VAN DOELGROEPENVERVOER |

DE ONDERGETEKENDEN:

1. De gemeenschappelijke regeling Omnibuzz, statutair gevestigd te 6135 KB Sittard en kantoorhoudende te 6135 KB Sittard aan de Geerweg 3, te dezen rechtsgeldig vertegenwoordigd door haar directeur, de heer mr. G.M.F Vreuls, hierna te noemen: "Verwerkingsverantwoordelijke";

en

2. De [naam], statutair gevestigd te [plaats] en kantoorhoudende te [adres], te dezen rechtsgeldig vertegenwoordigd door [naam, functie], hierna te noemen: "Verwerker";

Verwerkingsverantwoordelijke en Verwerker hierna gezamenlijk: "Partijen";

IN AANMERKING NEMENDE:

A. dat Partijen op [datum] de raamovereenkomst inzake de uitvoering van doelgroepenvervoer met elkaar hebben gesloten (de "Hoofdovereenkomst") en dat de Verwerkingsverantwoordelijke in dit kader diverse werkzaamheden aan Verwerker heeft opgedragen, waaronder de daadwerkelijke uitvoering van het vervoer van Jeugdwetvervoer;

B. dat in het kader van de daadwerkelijke uitvoering van het personenvervoer door de Verwerker naast gewone Persoonsgegevens ook bijzondere Persoonsgegevens, waaronder medische gegevens, van Jeugdwetvervoer geïndiceerde klanten door Verwerker ten behoeve van het vervoer worden verwerkt;

C. dat de Verwerkingsverantwoordelijke op grond van artikel 28 lid 1 Algemene Verordening Gegevensbescherming ("AVG") verplicht is te waarborgen dat de Verwerker bij de verwerking voldoende technische en organisatorische beveiligingsmaatregelen treft;

D. dat Partijen op grond van artikel 28 lid 3 AVG in deze Verwerkersovereenkomst nadere afspraken wensen te maken met betrekking tot de registratie van bijzondere Persoonsgegevens door Verwerker in het kader van de uitvoering van zijn opdracht;

KOMEN HET VOLGENDE OVEREEN:

Artikel 1 Definities

In deze overeenkomst worden de volgende definities gebruikt:

1.1 Bijlagen: aanhangsels bij deze overeenkomst, die na door beide partijen te zijn geparafeerd, deel uitmaken van deze overeenkomst.

1.2 Normen en standaarden: de door de Verwerkingsverantwoordelijke vastgestelde normen en standaarden ter zake van methoden, technieken, procedures, projecten en documentatievoorschriften welke bij de uitvoering van de werkzaamheden door de Verwerker zullen worden gevolgd als vastgelegd in bijlage 1.

1.3 AVG: Algemene Verordening Gegevensbescherming (Verordening (EU) 2016/679).

1.4 Toezichthouder: de Autoriteit Persoonsgegevens (AP) is het zelfstandig bestuursorgaan dat in Nederland toezicht houdt op het verwerken van persoonsgegevens.

1.5 Verwerking van persoonsgegevens of het verwerken van persoonsgegevens, Verwerkingsverantwoordelijke, Verwerker, Betrokkene, Functionaris Gegevensbescherming, Persoonsgegevens: de definitie die de AVG daaraan geeft.

1.6 Derde: ieder, niet zijnde de betrokkene, de verantwoordelijke, de verwerker, of enig persoon die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd is om persoonsgegevens te verwerken.

1.7 Datalek: een inbreuk op de beveiliging, zoals bedoeld in artikel 4 lid 12 AVG.

Artikel 2 Ingangsdatum en duur

2.1 Deze Verwerkersovereenkomst gaat in op het moment van ondertekening door beide Partijen en duurt voort zolang de Verwerker Persoonsgegevens voor de Verwerkingsverantwoordelijke verwerkt, ook nadat Verwerker is opgehouden diensten aan Verwerkingsverantwoordelijke te verlenen of werkzaamheden voor Verwerkingsverantwoordelijke uit te voeren.

Artikel 3 Type persoonsgegevens en categorieën van betrokkenen

3.1 De Persoonsgegevens die de Verwerker voor de Verwerkingsverantwoordelijke verwerkt zijn van Jeugdwetvervoer geïndiceerde klanten en betreffen zowel gewone Persoonsgegevens als bijzondere Persoonsgegevens. In bijlage 2 wordt aangegeven welk type Persoonsgegevens de Verwerker voor de Verwerkingsverantwoordelijke verwerkt.

Artikel 4 Doel, inhoud en condities van de verwerking

4.1. De Verwerker verwerkt de Persoonsgegevens uitsluitend ten behoeve van en in opdracht van Verwerkingsverantwoordelijke en ter uitvoering van de Hoofdovereenkomst.

4.2 De Verwerker verwerkt in het kader van de uitvoering van de Hoofdovereenkomst de Persoonsgegevens uitsluitend voor de in bijlage 3 omschreven doeleinden. Verwerker zal de Persoonsgegevens niet voor enig ander doel verwerken, behoudens afwijkende wettelijke verplichtingen.

4.3 De Verwerker zal alle noodzakelijke medewerking, kennis en advies verstrekken dan wel verlenen aan Verwerkingsverantwoordelijke met betrekking tot op Verwerkingsverantwoordelijke en/of Verwerker rustende wettelijke verplichtingen.

4.4 De Verwerker verbindt zich om in het kader van die werkzaamheden de door of via de Verwerkingsverantwoordelijke ter beschikking gestelde Persoonsgegevens zorgvuldig te verwerken.

4.5 Partijen onderkennen dat Verwerker naast zijn rol als Verwerker, mogelijkerwijs deels ook als (gezamenlijk) Verwerkingsverantwoordelijke moet worden aangemerkt. Ook op die verhouding blijven de bepalingen uit deze Verwerkersovereenkomst onverkort van toepassing.

Artikel 5 Verplichtingen Verwerker

5.1 De Verwerker verwerkt de Persoonsgegevens uitsluitend op basis van schriftelijke instructies van de Verwerkingsverantwoordelijke, conform artikel 28 lid 3 onderdeel a AVG.

5.2 De Verwerker heeft geen zelfstandige zeggenschap over de ter beschikking gestelde en de te verwerken Persoonsgegevens in zijn hoedanigheid als Verwerker. Zo neemt hij geen beslissingen over ontvangst en gebruik van de Persoonsgegevens, de verstrekking aan Derden en de duur van de opslag van gegevens. De zeggenschap over de Persoonsgegevens verstrekt onder deze Verwerkersovereenkomst komt nimmer bij de Verwerker te berusten.

5.3 De Verwerker zal bij de verwerking van Persoonsgegevens in het kader van de uitvoering van de Hoofdovereenkomst handelen in overeenstemming met de toepasselijke wet- en regelgeving betreffende de verwerking van persoonsgegevens, waaronder de AVG.

5.4 De Verwerker zal alle redelijke instructies van de contactpersoon, zoals bedoeld in artikel 13.3, opvolgen, behoudens afwijkende wettelijke verplichtingen. Indien deze afwijkende wettelijke verplichtingen er zijn wordt de Verantwoordelijke hiervan, voorafgaand aan de verwerking, schriftelijk op de hoogte gebracht door de Verwerker.

5.5 De Verwerker zal te allen tijde op eerste verzoek van de contactpersoon, als bedoeld in artikel 13.3, door de Verwerkingsverantwoordelijke ter beschikking gestelde Persoonsgegevens met betrekking tot deze Verwerkersovereenkomst ter hand stellen.

5.6 De Verwerker stelt de Verwerkingsverantwoordelijke te allen tijde in staat om binnen de wettelijke termijnen te voldoen aan zijn verplichtingen op grond van de AVG. De Verwerker zal de Verwerkingsverantwoordelijke in dit kader zijn volledige medewerking verlenen. Onder de verplichtingen van de Verwerkingsverantwoordelijke vallen onder andere het kunnen voldoen aan de volgende rechten van betrokkenen, zoals, maar niet beperkt tot een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van Persoonsgegevens en het uitvoeren van een gehonoreerd aangetekend verzet. Ingeval van een ontvangen verzoek van een betrokkene zal Verwerker de Verwerkingsverantwoordelijke hierover onmiddellijk informeren en met hem overleggen, wie op het verzoek zal reageren. De Verwerker zal in een voorkomend geval onmiddellijk de Persoonsgegevens corrigeren of anderszins aanpassen, in overeenstemming met de instructies van de Verwerkingsverantwoordelijke.

5.7 De Verwerker werkt op verzoek van Verwerkingsverantwoordelijke te allen tijde mee aan een gegevensbeschermingseffectbeoordeling (DPIA).

5.8 De Verwerker houdt een register bij van alle categorieën van verwerkingsactiviteiten die zij ten behoeve van Verwerkingsverantwoordelijke heeft verricht in de zin van artikel 30 lid 2 AVG.

De Verwerker verstrekt dit register op eerste verzoek van Verwerkingsverantwoordelijke aan Verwerkingsverantwoordelijke.

Artikel 6 Geheimhoudingsplicht

6.1 De Verwerker treft maatregelen om ervoor te zorgen dat de Persoonsgegevens conform artikel 32 lid 4 AVG voor derden geheim worden gehouden. Personen in dienst van, dan wel werkzaam ten behoeve van de Verwerker, evenals de Verwerker zelf, zijn verplicht tot geheimhouding met betrekking tot de Persoonsgegevens waarvan zij kennis kunnen nemen, behoudens voor zover een bij, of krachtens de wet gegeven voorschrift tot verstrekking verplicht of indien de Verwerkingsverantwoordelijke vooraf zijn schriftelijke toestemming hiervoor heeft verleend. Medewerkers die niet in dienst zijn bij de Verwerker hebben een geheimhoudingsverklaring ondertekend.

6.2 Indien de Verwerker op grond van een wettelijke verplichting gegevens dient te verstrekken, zal de Verwerker de grondslag van het verzoek en de identiteit van de verzoeker verifiëren en zal de Verwerker de Verwerkingsverantwoordelijke onmiddellijk, voorafgaand aan de verstrekking, ter zake informeren. Tenzij wettelijke bepalingen dit verbieden.

6.3 De geheimhoudingsverplichtingen voortvloeiende uit dit artikel 6 blijven na het einde van deze Verwerkersovereenkomst onverminderd van kracht.

Artikel 7 Beveiligingsmaatregelen en controle

7.1 De Verwerker neemt conform artikel 32 AVG en rekening houdend 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, alle passende technische en organisatorische maatregelen om de Persoonsgegevens welke worden verwerkt ten dienste van de Verwerkingsverantwoordelijke te beveiligen en beveiligd te houden tegen verlies of tegen enige vorm van onrechtmatige verwerking. De wijze van beveiliging wordt nader omschreven in bijlage 5.

7.2 De Verwerker zorgt ervoor dat de technische en organisatorische maatregelen periodiek worden geëvalueerd en indien nodig worden geactualiseerd. Verwerkingsverantwoordelijke wordt van significante wijzigingen schriftelijk op de hoogte gesteld en heeft de mogelijkheid om hiertegen bezwaar te maken. De Verwerker rapporteert jaarlijks op verzoek van de Verwerkersverantwoordelijke over de opzet en werking van het stelsel van maatregelen en procedures, gericht op naleving van deze Verwerkersovereenkomst.

7.3 De Verwerkingsverantwoordelijke is te allen tijde gerechtigd de verwerking van Persoonsgegevens te (doen) controleren. De Verwerker is verplicht de Verwerkingsverantwoordelijke, de Toezichthouder, of, de onder geheimhouding controlerende instantie in opdracht van Verwerkingsverantwoordelijke toe te laten en verplicht medewerking te verlenen zodat de controle daadwerkelijk uitgevoerd kan worden.

7.4 De Verwerker verbindt zich om binnen een door de Verwerkingsverantwoordelijke te bepalen termijn de Verwerkingsverantwoordelijke, of de door de Verwerkingsverantwoordelijke ingeschakelde derde, te voorzien van de verlangde informatie. Hierdoor kan de Verwerkingsverantwoordelijke, of de door de Verwerkingsverantwoordelijke ingeschakelde derde, zich een oordeel vormen over de naleving door de

Verwerker van deze Verwerkersovereenkomst. De Verwerkingsverantwoordelijke, of de door de Verwerkingsverantwoordelijke ingeschakelde derde, is gehouden alle informatie betreffende deze controles vertrouwelijk te behandelen.

7.5 De Verwerker staat er voor in de door de Verwerkingsverantwoordelijke of ingeschakelde derde aangegeven aanbevelingen ter verbetering binnen de daartoe door de Verwerkingsverantwoordelijke te bepalen redelijke termijn uit te voeren.

7.6 Naast rapportages door de Verwerker en controles door de Verwerkingsverantwoordelijke of controlerende instantie in opdracht van de Verwerkingsverantwoordelijke, kunnen beide partijen ook overeenkomen gebruik te maken van een Third Party Memorandum (TPM) opgesteld door een onafhankelijke externe deskundige.

7.7 De redelijke kosten van de controle worden gedragen door de partij die de kosten maakt, tenzij uit de controle blijkt dat de Verwerker enig punt uit deze Verwerkersovereenkomst niet heeft nageleefd. In dat geval worden de kosten van de controle gedragen door de Verwerker.

Artikel 8 Meldplicht datalekken en beveiligingsincidenten

8.1 Indien zich ten aanzien van de door Verwerker verwerkte Persoonsgegevens een (vermoedelijk) datalek in de zin van de toepasselijke wet- en regelgeving voordoet, zal Verwerker hiervan onmiddellijk – doch uiterlijk binnen 24 uur na ontdekking – telefonisch en per e-mail de Verwerkingsverantwoordelijke op de hoogte brengen, opdat de Verwerkingsverantwoordelijke het datalek tijdig bij de Toezichthouder en eventueel de betrokkene(n) kan melden.

8.2 De Verwerker verstrekt aan de Verwerkingsverantwoordelijke op diens eerste verzoek alle inlichtingen die de Verwerkingsverantwoordelijke noodzakelijk acht om het incident te kunnen beoordelen. Daarbij verschaft de Verwerker in ieder geval de informatie aan de Verwerkingsverantwoordelijke zoals omschreven in bijlage 4. De Verwerker zal alle noodzakelijke medewerking verlenen aan het zo nodig, op de kortst mogelijke termijn, verschaffen van aanvullende informatie aan de toezichthouder(s) en/of betrokkene(n).

8.3 Ook nadat de melding is gedaan, zal Verwerker de Verwerkingsverantwoordelijke regelmatig informeren over nieuwe ontwikkelingen rond het incident en van de maatregelen die Verwerker treft om de gevolgen van het incident te beperken en herhaling te voorkomen.

8.4 De Verwerkingsverantwoordelijke mag bij elk datalek gebruik maken van zijn auditrecht zoals bedoeld in artikel 7 van deze Verwerkersovereenkomst.

8.5 De Verwerker zal redelijkerwijs alle maatregelen treffen die nodig zijn om het datalek op te heffen dan wel alle gevolgen daarvan voor zowel de betrokkene(n) als Verwerkingsverantwoordelijke te minimaliseren, indien mogelijk in overleg met de Verwerkingsverantwoordelijke.

8.6 De Verwerker beschikt over een gedegen plan van aanpak betreffende de omgang met en afhandeling van inbreuken en zal de Verwerkingsverantwoordelijke, op diens verzoek inzage verschaffen in het plan. Verwerker stelt de Verwerkingsverantwoordelijke op de hoogte van materiële wijzigingen in het plan van aanpak.

8.7 De Verwerker zal het doen van meldingen aan de toezichthouder(s) overlaten aan de Verwerkingsverantwoordelijke.

8.8 De Verwerker houdt een gedetailleerd logboek bij van alle (vermoedens van) inbreuken op de beveiliging, evenals de maatregelen die in vervolg op dergelijke inbreuken zijn genomen waarin minimaal de informatie zoals bedoeld in bijlage 4 is opgenomen, en geeft daar op eerste verzoek van de Verwerkingsverantwoordelijke inzage in.

Artikel 9 Inschakeling sub-verwerkers

9.1 De Verwerker is gerechtigd om zijn activiteiten die bestaan uit het verwerken van Persoonsgegevens uit te besteden aan sub-verwerkers gevestigd binnen de Europese Economische Ruimte (EER), mits deze minimaal voldoen aan de gestelde eisen (zie ook artikel 9.2). De Verwerker zal de Verwerkingsverantwoordelijke tijdig informeren over diens sub-verwerkers en wijzigingen daarin. De Verwerkingsverantwoordelijke heeft het recht op redelijke gronden bezwaar te maken tegen deze uitbesteding. Bij het aangaan van de Hoofdovereenkomst en het ondertekenen van deze Verwerkersovereenkomst zullen de gecontracteerde sub-verwerkers, die op het moment van ondertekening bekend zijn, worden opgenomen in bijlage 6.

9.2 De Verwerker blijft ook in het geval van uitbesteding van de verwerking van Persoonsgegevens aan sub-verwerkers conform artikel 28 lid 4 AVG te allen tijde aanspreekpunt en volledig verantwoordelijk voor de naleving van de bepalingen uit deze Verwerkersovereenkomst door de sub-verwerker. De Verwerker garandeert dat de door hem ingeschakelde sub-verwerkers schriftelijk minimaal dezelfde plichten op zich nemen als tussen de Verwerkingsverantwoordelijke en de Verwerker zijn overeengekomen en zal de Verwerkingsverantwoordelijke, op diens verzoek, inzage verschaffen in de met de sub-verwerkers gesloten overeenkomsten, waarin deze plichten zijn opgenomen.

9.3 De Verwerker mag de Persoonsgegevens uitsluitend verwerken in EER landen. Doorgifte naar andere landen is uitsluitend toegestaan na voorafgaande schriftelijke toestemming van de Verwerkingsverantwoordelijke en met inachtneming van de toepasselijke wet- en regelgeving.

9.4 De Verwerker houdt een actueel register bij van de door hem ingeschakelde sub-verwerkers, waarin de identiteit, vestigingsplaats en een beschrijving van de werkzaamheden van de sub-verwerkers zijn opgenomen, alsmede eventuele door de Verwerkingsverantwoordelijke gestelde aanvullende voorwaarden. Dit register kan door de Verwerkingsverantwoordelijke te allen tijde worden opgevraagd.

Artikel 10 Wijziging en beëindigen Verwerkersovereenkomst

10.1 Wijziging van deze Verwerkersovereenkomst kan slechts schriftelijk plaatsvinden middels een door beide Partijen geaccordeerd voorstel.

10.2 Zodra de Verwerkersovereenkomst is beëindigd, zal de Verwerker naar keuze van de Verwerkingsverantwoordelijke conform artikel 28 lid 3 onderdeel g AVG:

(i) alle of een door Verwerkingsverantwoordelijke bepaald gedeelte van haar in het kader van deze Verwerkersovereenkomst ter beschikking gestelde Persoonsgegevens aan de Verwerkingsverantwoordelijke retourneren en bestaande kopieën verwijderen;

(ii) de Persoonsgegevens die zij van de Verwerkingsverantwoordelijke heeft ontvangen op alle locaties vernietigen conform de instructies van Verwerkingsverantwoordelijke te vernietigen, waarbij Verwerker de deugdelijke vernietiging van de Persoonsgegevens conform de instructies van de Verwerkingsverantwoordelijke aan Verwerkingsverantwoordelijke aantoonbaar dient te maken.. De vernietigingswijze zal een voor de desbetreffende gegevensdrager veilige en algemeen geaccepteerd vernietigingswijze betreffen, waarbij het maken van onnodige extra kosten zal proberen te worden voorkomen.

De Verwerkingsverantwoordelijke kan zo nodig nadere eisen stellen aan de wijze van beschikbaarstelling, waaronder eisen aan het bestandsformaat, dan wel vernietiging. Deze werkzaamheden moeten, binnen een nader overeen te komen redelijke termijn, uitgevoerd worden en hiervan wordt een verslag gemaakt.

10.3 De Verwerker zal te allen tijde de in het vorig lid beschreven dataportabiliteit waarborgen zodanig dat er geen sprake is van verlies van functionaliteit of (delen van) de gegevens.

10.4 De Verwerkingsverantwoordelijke en de Verwerker treden met elkaar in overleg over wijzigingen in deze Verwerkersovereenkomst als een wijziging in regelgeving of een wijziging in de uitleg van regelgeving daartoe aanleiding geven.

Artikel 11 Aansprakelijkheid

11.1 De Verwerker is jegens de Verwerkingsverantwoordelijke aansprakelijk voor schade of nadeel voortvloeiende uit het niet nakomen van deze Verwerkersovereenkomst, daaronder begrepen wanneer bij de verwerking niet wordt voldaan aan de specifiek tot de Verwerker gerichte verplichtingen opgenomen in deze Verwerkersovereenkomst en/of indien de Verwerker in strijd handelt met de toepasselijke wet- en/of regelgeving, waaronder de AVG, of buiten de rechtmatige instructies van de Verwerkingsverantwoordelijke heeft gehandeld. Onder Verwerker dient in het verband van dit artikel te worden verstaan de Verwerker, haar werknemers en/of door haar ingeschakelde derden, waaronder sub-verwerkers.

11.2 De Verwerker vrijwaart de Verwerkingsverantwoordelijke voor alle schade, boetes, claims van derden (waaronder betrokkenen) of (ander) nadeel en kosten van Verwerkingsverantwoordelijke in dat geval, voor zover ontstaan als gevolg van een handelen of nalaten van de Verwerker in het kader van de verwerking van Persoonsgegevens.

Artikel 12 Toepasselijk recht

12.1 Op deze Verwerkersovereenkomst en op alle geschillen die daaruit mochten voortvloeien of daarmee mochten samenhangen, is uitsluitend Nederlands recht van toepassing.

12.2 Alle geschillen die ontstaan naar aanleiding van deze Verwerkersovereenkomst zullen worden voorgelegd aan de bevoegde rechter van het arrondissement waarin de Verwerkingsverantwoordelijke is gevestigd. Het staat Partijen vrij om alvorens hun geschil(len) aan de civiele rechter voor te leggen en mits beide Partijen hiermee schriftelijk instemmen hun geschil(len) aan een mediator voor te leggen om gezamenlijk tot een oplossing te komen.

Artikel 13 Overige bepalingen

13.1 De Verwerkersovereenkomst bevat de gehele overeenkomst tussen Partijen met betrekking tot het onderwerp ervan en treedt in de plaats van elke andere afspraak tussen Partijen hierover. In geval van strijdigheid van afspraken tussen de Hoofdovereenkomst en deze Verwerkersovereenkomst, gaan de bepalingen – voor wat betreft het verwerken van Persoonsgegevens – van deze Verwerkersovereenkomst voor.

13.2 Indien één of meer bepalingen van deze Verwerkersovereenkomst nietig zijn of vernietigd worden, laat dat de geldigheid van de overige bepalingen onverlet. Partijen zijn gehouden om nietige of vernietigde bepalingen te vervangen door wel geldige bepalingen met zoveel mogelijk dezelfde strekking.

13.3 Namens de Verwerkingsverantwoordelijke treedt [invullen naam] als contactpersoon op, functie [invullen functie], e-mailadres: [invullen e-mailadres] en telefoonnummer mobiel: [invullen telefoonnummer], vast: [invullen telefoonnummer].
Bij diens afwezigheid treedt [invullen naam] als contactpersoon op, functie [invullen functie], e-mailadres: [invullen e-mailadres] en telefoonnummer mobiel: [invullen telefoonnummer] vast: [invullen telefoonnummer].

Namens de Verwerker treedt [invullen naam] als contactpersoon op, functie [invullen functie], e-mailadres: [invullen e-mailadres] en telefoonnummer mobiel: [invullen telefoonnummer], vast: [invullen telefoonnummer].
Bij diens afwezigheid treedt [invullen naam] als contactpersoon op, functie [invullen functie], e-mailadres: [invullen e-mailadres] en telefoonnummer mobiel: [invullen telefoonnummer], vast: [invullen telefoonnummer].

- handtekeningenpagina volgt -

Aldus in tweevoud overeengekomen,

Voor Verwerkingsverantwoordelijke:	Voor Verwerker:
Naam: G.M.F. Vreuls	Naam:
Functie: Directeur	Functie:
Datum: _____	Datum:_____

Bijlage 1: Beschrijving beveiliging ter uitwerking van artikel 1 lid 2.

1. Normenstelsel

a. De informatiebeveiliging vindt plaats volgens algemeen erkende normen, namelijk: *de overheidsnorm BIO, zoals nader omschreven in bijlage 5.*

2. De toereikende van de informatiebeveiliging blijkt uit:

a. Certificering
b. Periodieke externe controles en audit.
c. Rapportages met conclusies over de bevindingen van de uitgevoerde DPIA en Audit.
d. Eigen controles of eigen mededelingen.

3. Uit de certificering of periodieke externe controles of uit de audits of uit de eigen controles blijkt of kan afgeleid worden dat de beveiliging voldoet aan of gelijkwaardig is met de toelichting (bijlage 5) en de daarin omschreven elementen.

LET OP: gemotiveerd afwijken is toegestaan!

Paraaf:

Bijlage 2: Soort Persoonsgegevens die de Verwerker voor de Verwerkingsverantwoordelijke verwerkt artikel 3 lid 1.

De Verwerker verwerkt voor de Verwerkingsverantwoordelijke van de Jeugdwetvervoer geïndiceerde burgers zowel ten aanzien van gewone Persoonsgegevens als bijzondere Persoonsgegevens.

De gewone Persoonsgegevens hebben betrekking op:

1.	Identificatiegegevens waaronder:	de namen, adressen, geboortedatum, gegevens van de vertegenwoordiger, pasnummer en klantnummer.
2.	Gerechtelijke gegevens waaronder:	beschikking bewind, curatorschap.
3.	Financiële gegevens waaronder:	bankrekeninggegevens en factuurnummer, openstaande vorderingen.
4.	Communicatiegegevens, waaronder:	telefoonnummers en e-mailadressen.
5.	Locatiegegevens, waaronder:	Ritgegevens.
6.	Saldo:	Saldobudget van de zones
7.	BSN gegevens	
8.	Pasfoto.	

De bijzondere Persoonsgegevens hebben betrekking op:

1. Reisspecificaties waaronder:

   Klant categorie: Individueel of groepsvervoer ;
   Vervoersindicatie: Met begeleiding of zonder begeleiding, soort begeleiding, met hulpmiddel of zonder hulpmiddel en soort hulpmiddel;
   Indicatie: Kamer-Kamer vervoer, direct vervoer, individueel vervoer of voorin (zitplaats);
   Rolstoel: soort rolstoel.

Paraaf:

Bijlage 3: Omschrijving werkzaamheden ter uitwerking van artikel 4 lid 2

In deze bijlage worden de doelen van de Verwerking van de Persoonsgegevens door Verwerker nader omschreven.

In het kader van de Hoofdovereenkomst verwerkt Verwerker Persoonsgegevens uitsluitend voor het volgende doel of de volgende doeleinden:
- voor administratiedoeleinden ter uitvoering van het transport van Jeugdwetvervoer geïndiceerde klanten;
- en daaraan gerelateerde of voor de uitvoering van het transport benodigde werkzaamheden.

Verder te noemen verwerkingsdoeleinden kunnen tussen de Verwerker en de Verwerkingsverantwoordelijke alleen schriftelijk worden overeengekomen en in deze bijlage worden toegevoegd.

Bijlage 4: Inlichtingen om incidenten te beoordelen ter uitwerking van artikel 8.

De Verwerker zal de volgende inlichtingen verschaffen die noodzakelijk zijn voor de Verwerkingsverantwoordelijke om het incident te kunnen beoordelen en de melding te maken bij de Toezichthouder.

Daarbij gaat het in ieder geval om de volgende informatie :

- De aard van de inbreuk, waar mogelijk onder vermelding van de categorieën van betrokkenen;
- Een zo exact mogelijke opgave van de Persoonsgegevens waar het om gaat;
- Wat de (vermeende) oorzaak is van de inbreuk;
- Wat het (vooralsnog bekende en/of te verwachten) gevolg is;
- Wat de (voorgestelde) oplossing is;
- Contactgegevens voor de opvolging van de melding;
- Aantal personen waarvan gegevens betrokken zijn bij de inbreuk (indien geen exact aantal bekend is: het minimale en maximale aantal personen waarvan gegevens betrokken zijn bij de inbreuk);
- Een omschrijving van de groep personen van wie gegevens betrokken zijn bij de inbreuk;
- Het soort of de soorten persoonsgegevens die betrokken zijn bij de inbreuk;
- Omschrijving van de groep mogelijke onbevoegde ontvangers;
- De datum waarop de inbreuk heeft plaatsgevonden (indien geen exacte datum bekend is: De periode waarbinnen de inbreuk heeft plaatsgevonden);
- De datum en het tijdstip waarop de inbreuk bekend is geworden bij verwerker of bij een door hem ingeschakelde derde of onderaannemer;
- Of de gegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk zijn gemaakt voor onbevoegden;
- Wat de reeds ondernomen maatregelen zijn om de inbreuk te beëindigen
- en om de gevolgen van de inbreuk te beperken.

Kan nog verder worden aangevuld.

Paraaf:

Bijlage 5: Uitwerking wijze van beveiliging (artikel 7)

Beveiligingsbeleid

nr	Maatregel verwerker
5.1.1.1	De verwerker heeft een eigen vastgesteld en gepubliceerd informatie beveiligingsbeleid.

Organisatie van informatiebeveiliging

nr	Maatregel verwerker
6.1.5.1	Medewerkers die te maken hebben met persoonsinformatie van de verantwoordelijke dienen een geheimhoudingsverklaring te ondertekenen. Hierbij wordt tevens vastgelegd dat na beëindiging van de functie, de betreffende persoon gehouden blijft aan die geheimhouding.
6.1.8.2	Periodieke beveiligingsaudits, (minimaal eens per twee jaar) worden uitgevoerd volgens afspraken met de verwerkingsverantwoordelijke.
6.2.1.7	Over het naleven van de afspraken wordt jaarlijks gerapporteerd aan de verantwoordelijke.
6.2.3.1	Maatregelen uit de verwerkersovereenkomst zijn geïmplementeerd.

Beheer van bedrijfsmiddelen

nr	Maatregel verwerker
7.2.2.1	De verwerker heeft maatregelen genomen zo dat niet geautoriseerden geen kennis kunnen nemen van persoonsgegevens.

Personele beveiliging

nr	Maatregel verwerker
8.1.1.2	Het personeel van de verwerker of derden moeten kennis hebben van de verantwoordelijkheden ten aanzien van de bewerking van de persoonsgegevens voor de verantwoordelijke.
8.1.2.1	Voor personen is een recente Verklaring Omtrent het Gedrag (VOG) vereist met punten die door de verwerkingsverantwoordelijke zijn aangedragen. Tenzij dit centraal in het contract geregeld
8.3.3.1	Toegangsrechten van medewerkers van de verwerker worden direct geblokkeerd als geen toegang voor de bewerking van de persoonsgegevens noodzakelijk is.

Fysieke beveiliging

nr	Maatregel verwerker
9.1.2.1	Toegang tot beveiligde zones of gebouwen waar persoonsgegevens van de verantwoordelijke zich bevinden is alleen mogelijk na autorisatie daartoe.
9.1.3.1	Papieren documenten en mobiele gegevensdragers die persoonsgegevens of andere vertrouwelijke gegevens van de verantwoordelijke bevatten worden beveiligd opgeslagen.
9.2.7.1	Apparatuur, informatie en programmatuur met persoonsgegevens van de verwerkingsverantwoordelijke mogen niet zonder toestemming vooraf van de locatie van de verwerker worden meegenomen.

Beheer van communicatie en bedienprocessen

nr	Maatregel verwerker
10.3.1.1	De ICT-voorzieningen voldoen aan het voor de dienst overeengekomen niveau van beschikbaarheid. Er worden voorzieningen geïmplementeerd om de beschikbaarheid van componenten te bewaken (bijvoorbeeld de controle op aanwezigheid van een component en metingen die het gebruik van een component vaststellen). Op basis van voorspellingen van het gebruik wordt actie genomen om tijdig de benodigde uitbreiding van capaciteit te bewerkstelligen.
10.3.2.2	Acceptatiecriteria voor het testen van de beveiliging betreft minimaal de meest recente OWASP top-10. De verwerker toont aan dat de door verwerker geleverde (web)applicatie geen kwetsbaarheden bevat uit de top-10.
10.6.1.2	Gegevensuitwisseling tussen vertrouwde en niet vertrouwde zones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware.
10.6.1.3	Bij transport van vertrouwelijke informatie over niet vertrouwde netwerken tussen de verwerker en de verantwoordelijke, zoals over het internet, dient altijd geschikte encryptie te worden toegepast. De cryptografische beveiligingsvoorzieningen en componenten voldoen aan algemeen gangbare beveiligingscriteria (zoals FIPS 140-2 en waar mogelijk NBV).
10.6.2.1	Beveiligingskenmerken, niveaus van dienstverlening en beheer eisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in elke overeenkomst voor netwerkdiensten, zowel voor diensten die intern worden geleverd als voor uitbestede diensten door een verwerker.
10.7.2.1	Het verwijderen cq. vernietigen van vertrouwelijke data en de vernietiging van verwijderbare media gebeurt conform landelijke wet- en regelgeving.
10.8.2.2	Verantwoordelijkheid en aansprakelijkheid in het geval van informatiebeveiligingsincidenten zijn beschreven, evenals procedures over melding van incidenten van de verwerker naar de verantwoordelijke.

Paraaf:

10.8.3.1	De verwerker neemt maatregelen om vertrouwelijke informatie te beschermen, zoals: • Versleuteling. • Bescherming door fysieke maatregelen, zoals afgesloten containers. • Gebruik van verpakkingsmateriaal waaraan te zien is of getracht is het te openen • Persoonlijke aflevering. • Opsplitsing van zendingen in meerdere delen en eventueel verzending via verschillende routes.
10.10.1.1	Door de verwerker worden rapportages van logbestanden gemaakt die periodiek worden beoordeeld. Deze periode dient te worden gerelateerd aan de mogelijkheid van misbruik en de schade die kan optreden.
10.10.1.2	Een logregel bevat minimaal: • Een tot een natuurlijk persoon herleidbare gebruikersnaam of ID. • De gebeurtenis (zie 10.10.2.1). • Waar mogelijk de identiteit van het werkstation of de locatie. • Het object waarop de handeling werd uitgevoerd. • Het resultaat van de handeling. De datum en het tijdstip van de gebeurtenis.
10.10.1.3	In een logregel wordt in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, et cetera).
10.10.2.1	De volgende gebeurtenissen worden in ieder geval opgenomen in de logging: • Gebruik van technische beheerfuncties, zoals het wijzigingen van configuratie of instelling: uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore. • Gebruik van functioneel beheerfuncties, zoals het wijzigingen van configuratie en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets (waaronder databases). • Handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoord reset, uitgifte en intrekken van cryptosleutels. • Beveiligingsincidenten (zoals de aanwezigheid van malware, testen op vulnerabilities, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van security services). • Verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens executie van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of systemen). Handelingen van gebruikers, zoals goede en foute inlogpogingen, systeemtoegang, gebruik van online transacties en toegang tot bestanden door systeembeheerders.
10.10.3.3	Logbestanden worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden.
10.10.3.5	De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met een minimum van drie maanden, conform de wensen van de verwerkingsverantwoordelijke. Bij een (vermoed) informatiebeveiligingsincident is de bewaartermijn minimaal drie jaar
10.10.6.1	Er worden maatregelen genomen om er voor te zorgen dat de logbestanden die verzameld worden aan elkaar te relateren zijn, op basis van het tijdstip waarin ze zijn opgetreden.

Toegangsbeveiliging

nr	**Maatregel verwerker**
11.3.1.1	Aan de gebruikers is een set gedragsregels aangereikt met daarin minimaal het volgende: • Wachtwoorden worden niet opgeschreven. • Gebruikers delen hun wachtwoord nooit met anderen. • Wachtwoorden mogen niet opeenvolgend zijn. • Een wachtwoord wordt onmiddellijk gewijzigd indien het vermoeden bestaat dat het bekend is geworden aan een derde. • Wachtwoorden worden niet gebruikt in automatische inlogprocedures (bijvoorbeeld opgeslagen onder een functietoets of in een macro). Uitzondering zijn wachtwoordmanagers die met een sterk wachtwoord zijn beveiligd.
11.4.2.1	Als externe toegang nodig is tot de persoonsgegevens van de verantwoordelijke door eigen personeel, of personeel van de verwerker, dienen geschikte authenticatie methodes te worden gebruikt.
11.4.5.5	Zonering wordt ingericht met voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke (hardening van voorzieningen).
11.5.1.1	Toegang tot de persoonsgegevens van de verantwoordelijke wordt verleend op basis van twee-factor authenticatie.
11.5.1.2	Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatiegegevens.
11.5.1.3	Voorafgaand aan het aanmelden wordt aan de gebruiker een melding getoond dat alleen geautoriseerd gebruik is toegestaan voor expliciet door de organisatie vastgestelde doeleinden.
11.5.1.4	Bij een succesvol loginproces wordt de datum en tijd van de voorgaande login of loginpoging getoond. Deze informatie kan de gebruiker enige informatie verschaffen over de authentici
11.5.1.5	Nadat voor een gebruikersnaam 3 keer een foutief wachtwoord gegeven is, wordt het account minimaal 10 minuten geblokkeerd. Indien er geen lock-out periode ingesteld kan worden, dan wordt het account geblokkeerd totdat de gebruiker verzoekt deze lock-out op te heffen of het wachtwoord te resetten.
11.5.2.1	Bij uitgifte van authenticatiemiddelen wordt minimaal de identiteit vastgesteld, evenals het feit dat de gebruiker recht heeft op het authenticatiemiddel
11.5.3.1	Er wordt automatisch gecontroleerd op goed gebruik van wachtwoorden (onder andere voldoende sterke wachtwoorden, regelmatige wijziging, directe wijziging van initieel wachtwoord).

Paraaf:

nr	Maatregel verwerker
11.5.5.1	De periode van inactiviteit van een werkstation is vastgesteld op maximaal 15 minuten. Daarna wordt de PC vergrendeld. Bij remote desktop sessies geldt dat na maximaal 15 minuten inactiviteit de sessie verbroken wordt.
11.5.6.1	De toegang voor onderhoud op afstand door een leverancier wordt alleen opengesteld op basis van een wijzigingsverzoek of storingsmelding, met 2-factor authenticatie en tunneling.
11.6.1.1	In de soort toegangsregels wordt ten minste onderscheid gemaakt tussen lees – en schrijfbevoegdheden
11.6.1.2	Managementsoftware heeft de mogelijkheid gebruikerssessies af te sluiten.
11.6.1.3	Bij extern gebruik vanuit een niet vertrouwde omgeving vindt sterke authenticatie (two-factor) van gebruikers plaats.

Verwerving, onderhoud en ontwikkeling

nr	Maatregel verwerker
12.1.1.1	In projecten ten behoeve van systemen voor de verwerkingsverantwoordelijke wordt een beveiligingsrisicoanalyse en maatregelbepaling opgenomen als onderdeel van het ontwerp. Ook bij wijzigingen worden de veiligheidsconsequenties meegenomen
12.1.1.2	De Beveiligingsrichtlijnen voor Webapplicaties van het NCSC worden toegepast bij analyse, ontwikkeling en testen van het informatiesysteem. Waar relevant worden ook andere standaarden en richtlijnen gebruikt.
12.2.1.1	Er moeten controles worden uitgevoerd op de invoer van gegevens. Daarbij wordt minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledige gegevens, gegevens die niet aan het juiste format voldoen, toevoegen van parameters (SQL -Injectie) en inconsistentie van gegevens.
12.2.2.1	Er bestaan voldoende mogelijkheden om reeds ingevoerde gegevens te kunnen corrigeren door er gegevens aan te kunnen toevoegen.
12.2.3.1	Er behoren eisen en geschikte beheersmaatregelen te worden vastgesteld en geïmplementeerd, voor het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten in toepassingen.
12.3.1.1	De gebruikte cryptografische algoritmen voor versleuteling zijn als open standaard gedocumenteerd en zijn door onafhankelijke betrouwbare deskundigen getoetst.
12.3.2.1	In het sleutelbeheer is minimaal aandacht besteed aan het proces, de actoren en hun verantwoordelijkheden.
12.4.1.1	Alleen geautoriseerd personeel kan functies en software installeren of activeren.
12.5.1.1	Er is aantoonbaar wijzigingsmanagement ingericht volgens gangbare best practices, zoals ITIL en voor applicaties ASL.
12.5.2.1	Van aanpassingen (zoals updates) aan softwarematige componenten van de technische infrastructuur wordt vastgesteld dat deze de juiste werking van de technische componenten niet in gevaar brengen en de beveiliging zoals afgesproken met de verantwoordelijke te niet doen.
12.5.4.1	Op het grensvlak van een vertrouwde en een niet vertrouwde omgeving vindt content -scanning Plaats.
12.5.4.2	Er dient een proces te zijn om aan de verantwoordelijke te melden dat (persoons) informatie is uitgelekt. Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen vastgesteld, in combinatie met een reactie- en escalatieprocedure voor incidenten, waarin de handelingen worden vastgelegd die moeten worden genomen na het ontvangen van een rapport van een beveiligingsincident.
12.6.1.1	Er is een proces ingericht voor het beheer van technische kwetsbaarheden. Dit omvat minimaal het melden van incidenten aan de verantwoordelijke, het uitvoeren van periodieke penetratietests, het uitvoeren van risicoanalyses van kwetsbaarheden en patching van systemen en hardware.
12.6.1.4	Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is worden zo spoedig mogelijk doorgevoerd, echter minimaal binnen één week. Minder kritische beveiliging-updates/patches moeten worden ingepland bij de eerst volgende onderhoudsronde.

Beheer van incidenten

nr	Maatregel verwerker
13.1.1.1	Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen aan de Verwerkingsverantwoordelijke vastgesteld, in combinatie met een Reactie - en escalatieprocedure voor incidenten, waarin de handelingen worden vastgelegd die moeten worden genomen na het ontvangen van een rapport van een beveiligingsincident.
13.1.1.5	Vermissing of diefstal van apparatuur of media die gegevens van de verantwoordelijke kunnen bevatten wordt altijd ook aangemerkt als informatiebeveiligingsincident.
13.2.2.1	De informatie verkregen uit het beoordelen van beveiligingsmeldingen wordt geëvalueerd met als doel beheersmaatregelen te verbeteren. (PDCA-Cyclus)
13.1.1.4	Alle beveiligingsincidenten worden vastgelegd in een systeem en geëscaleerd aan de verwerkingsverantwoordelijke
13.2.3.1	Voor een vervolgprocedure naar aanleiding van een beveiligingsincident behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd in overeenstemming met de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

Naleving

nr	Maatregel verwerker
15.1.3.1	De registraties van de verantwoordelijke behoren te worden beschermd tegen verlies, vernietiging en vervalsing, in overeenstemming met wettelijke en regelgevende eisen, contractuele verplichtingen en bedrijfsmatige eisen.
15.1.4.1	De bescherming van gegevens en privacy behoort te worden bewerkstelligd in overeenstemming met relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen.

Paraaf:

15.1.6.1	Er is vastgesteld aan welke overeenkomsten, wetten en voorschriften de toepassing van cryptografische technieken moet voldoen. Zie ook 12.3.
15.2.1.1	De verwerker is verantwoordelijk voor uitvoering en beveiligingsprocedures en toetsing daarop (onder andere de jaarlijkse in control verklaring). Conform deze verwerkersovereenkomst en andere contractuele eisen zorgt de verwerker voor het toezicht op de uitvoering van het beveiligingsbeleid ten behoeve van de gegevens van de verantwoordelijke. Daarbij behoren ook periodieke beveiligingsaudits. Deze kunnen worden uitgevoerd door, of vanwege de verantwoordelijke.
15.2.2.1	Informatiesystemen van de verwerker ten behoeve van de verantwoordelijke worden regelmatig gecontroleerd op naleving van beveiligingsnormen. Dit kan door bijvoorbeeld kwetsbaarheidsanalyses en penetratietesten.

Paraaf:

Bijlage 6: Lijst sub-verwerker bij aangaan Verwerkersovereenkomst

Paraaf: