

Subverwerkersovereenkomst RSR/Leverancier inzake Klantenservice RSR Studentenreisproduct

De Ondergetekenden:

De besloten vennootschap Regisseur Studenten Reisrecht B.V., handelsregister 30276696, gevestigd te Amersfoort, Koningin Wilhelminalaan 35, rechtsgeldig vertegenwoordigd door L.S. van der Eijck, Directeur, hierna te noemen 'RSR',

en

De besloten vennootschap XXX, handelsregister XXX, gevestigd te XXX, XXX, en ten deze rechtsgeldig vertegenwoordigd door XXX, hierna te noemen 'Leverancier',

Gezamenlijk ook aan te duiden als "Partijen"

Overwegingen:

1. RSR is de rechtspersoon die in opdracht van de OV-bedrijven tot taak heeft de digitale administratie van het reisproduct voor studerenden op de OV-chipkaart te voeren. OV-bedrijven zijn 'verantwoordelijke' in de zin van de Algemene Verordening Gegevensbescherming (AVG). De Minister is 'Verantwoordelijke' in de zin van de AVG voor zover het gegevens betreft die verwerkt worden ten behoeve van het studentenreisproduct ingevolge de Wet Studiefinanciering 2000. RSR is daarmee hun gemeenschappelijke 'verwerker'.
2. De digitale administratie van RSR is vormgegeven volgens het 'Privacy by Design'-concept, met dien verstande dat RSR waarborgt dat het Burger Service Nummer (BSN) van studenten blijft afgeschermd voor verdere verwerking in het openbaar vervoer.
3. Voor de uitvoering van werkzaamheden maakt RSR gebruik van diensten van derden, onder goedkeuring door de Dienst Uitvoering Onderwijs (DUO).
4. Leverancier werkt in opdracht van RSR teneinde de distributie en beheer van studentenreisproducten op een effectieve en efficiënte manier te realiseren. Hiertoe hebben partijen op <datum> de 'Overeenkomst Klantenservice RSR Studentenreisproduct' gesloten.
5. Partijen wensen de verwerking van persoonsgegevens in het kader van genoemde dienstverleningsovereenkomst in deze subverwerkersovereenkomst te regelen. In deze subverwerkersovereenkomst heeft Leverancier de rol van 'subverwerker'.
6. Leverancier verwerkt persoonsgegevens volgens een gegevensset die is gelimiteerd tot de gegevens die noodzakelijk zijn voor het uitvoeren van de opgedragen werkzaamheden.
7. RSR en Leverancier maken middels deze overeenkomst afspraken die in het verlengde liggen van artikel 28 lid 3 AVG en de in dit kader gesloten verwerkersovereenkomsten met DUO en de OV-bedrijven.

KOMEN PARTIJEN ALS VOLGT OVEREEN:

Artikel 1 – Onderwerp van deze overeenkomst

1. In deze subverwerkersovereenkomst regelen Partijen de verwerking van persoonsgegevens door Leverancier in het kader van de Overeenkomst Klantenservice RSR Studentenreisproduct dd.....
2. De aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van persoonsgegevens, betrokkenen en ontvangers zijn in Bijlage 1 omschreven.

Artikel 2 - Omvang verwerkingsbevoegdheid Leverancier

1. RSR verstrekt Leverancier niet meer persoonsgegevens dan de gegevensset die noodzakelijk is voor het uitvoeren van de opgedragen werkzaamheden.
2. Leverancier verwerkt de persoonsgegevens uitsluitend in opdracht en op basis van schriftelijke instructies van Opdrachtgever behoudens afwijkende wettelijke voorschriften die op Leverancier van toepassing zijn.
3. Indien een instructie als bedoeld in het eerste lid naar het oordeel van Leverancier in strijd is met een wettelijk voorschrift inzake gegevensbescherming, stelt hij RSR daarvan voorafgaand aan de verwerking in kennis, tenzij een wettelijk voorschrift deze kennisgeving verbiedt.
4. Indien Leverancier op grond van een wettelijk voorschrift persoonsgegevens dient te verstrekken, informeert hij RSR onmiddellijk, en zo mogelijk voorafgaand aan de verstrekking.
5. Leverancier heeft geen zeggenschap over het doel van en de middelen voor de verwerking van persoonsgegevens.

Artikel 3 – Doorwerking AVG

Leverancier verplicht zich om ten aanzien van persoonsgegevens die de Minister via RSR aan haar ter beschikking stelt ter uitvoering van deze overeenkomst alle voorschriften zoals voortvloeiend uit de AVG, alsmede alle andere op privacybescherming betrekking hebbende wetten en regelingen, na te leven.

Artikel 4 – Bijstand vanwege rechten van betrokkenen

Leverancier verleent RSR bijstand bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III AVG vastgelegde rechten van de betrokkene te beantwoorden.

Artikel 5 – Categorieën gegevens

RSR verstrekt Leverancier niet meer persoonsgegevens dan de gegevensset die noodzakelijk is voor het uitvoeren van de opgedragen werkzaamheden.
De gegevensset die voor de uitvoering van deze overeenkomst noodzakelijk is, is opgenomen in bijlage 1.

Artikel 6 - Informatiebeveiliging en geheimhouding

1. Partijen verstaan onder 'informatiebeveiliging': passende technische en organisatorische maatregelen die de continuïteit, beschikbaarheid, integriteit en vertrouwelijkheid van hier overeengekomen gegevensverwerking waarborgen (zie ook Bijlage 2), inclusief de verplichting tot geheimhouding door medewerkers bij Leverancier en andere personen die in aanraking (kunnen) komen met de persoonsgegevens zoals bedoeld in deze overeenkomst en in de van toepassing verklaarde Algemene Inkoopvoorwaarden RSR 2023.
Leverancier treft de technische en organisatorische beveiligingsmaatregelen zoals opgenomen in Bijlage 2 van deze subverwerkersovereenkomst.
2. Leverancier toont op verzoek van RSR aan dat zijn personeel zich ertoe heeft verbonden vertrouwelijkheid en geheimhouding in acht te nemen.
3. Geheimhoudingsverplichtingen gelden niet voor zover zij de goede nakoming van deze subverwerkersovereenkomst zouden hinderen, indien sprake is van een wettelijke verplichting (o.a. de artikelen 32 tot en met 36 van de AVG) om gegevens te verstrekken of bij compliance toetsing door een daarvoor door RSR aangewezen onafhankelijke partij.
4. Partijen erkennen dat het waarborgen van een passend beveiligingsniveau voortdurend kan dwingen tot het treffen van aanvullende beveiligingsmaatregelen. Leverancier waarborgt een op het risico afgestemd beveiligingsniveau. Inschrijver waarborgt dat de beveiliging voldoet aan de nieuwste van toepassing zijnde normen.
5. Indien en voor zover RSR daarom uitdrukkelijk schriftelijk verzoekt, zal Leverancier aanvullende maatregelen treffen met het oog op de beveiliging van de persoonsgegevens.
6. Leverancier verwerkt persoonsgegevens niet buiten de Europese Unie, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming heeft verkregen van RSR en behoudens afwijkende wettelijke verplichtingen.
7. Leverancier verwerkt de gegevens volgens de code voor Informatiebeveiliging - ISO 27001 (of vergelijkbaar) en stuurt op eerste schriftelijk verzoek een kopie van het certificaat aan RSR. Leverancier laat certificeringen jaarlijks extern auditen door een onafhankelijke EDP-auditor. RSR draagt de kosten voor de audit. Leverancier dient echter kosteloos mee te werken met de audit.
8. Leverancier garandeert dat de data, zoals genoemd in Bijlage 1, te allen tijde beschikbaar is voor RSR.
9. Leverancier neemt voldoende maatregelen tegen aanvallen van buitenaf (zoals bijvoorbeeld een reverse proxy oplossing tegen een DDOS-aanval), en overige ongewenste en ongevoegde toegang van zowel interne medewerkers als externen.
10. Leverancier richt een procedure in voor het beschermen van de gegevens bij verplaatsen van de gegevens of het vervangen van apparatuur waarbij in geval van een incident inzage is in de omvang en oorzaak.
11. De toegang tot de apparatuur moet dusdanig beveiligd zijn dat ongevoegden geen veranderingen kunnen aanbrengen in de (systeem-)instellingen en/of eventuele

opgeslagen gegevens en deze ook niet kunnen inzien of verwijderen.

12. Het systeem dient te ondersteunen dat alle gebruikers in kunnen loggen middels een inlognaam en sterk wachtwoord op een veilige manier. Voor het beschermen van bijzondere persoonsgegevens wordt 2-factor authenticatie toegepast. Er wordt een passende authenticatietechniek gekozen om de geclaimde identiteit van een gebruiker te bewijzen.
13. De autorisaties dienen passend te kunnen worden ingericht (rechten en beperkingen) voor specifieke gebruikersrollen waarbij de details en striktheid van de maatregelen een afspiegeling zijn van de classificatie.
14. Beveiliging van de communicatie tussen applicaties waarbij persoonsgegevens uitgewisseld worden van adequate beveiliging te worden voorzien. Persoonsgegevens of andere gevoelige gegevens mogen enkel verzonden worden door ze tijdens de gehele transportketen over een publiek netwerk te beveiligen met een actueel versleutelingalgoritme. Voor webverkeer is dit HTTPS (certificaat, TLS, minimale CSR sleutellengte van 2048 bits).
15. Persoonsgegevens worden versleuteld opgeslagen.
16. Omgeving van Opdrachtgever is afgeschermd op het netwerk van andere klanten van Inschrijver.
17. Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard voor een periode van 18 maanden en regelmatig te worden beoordeeld. Deze logbestanden dienen te worden beschermd tegen onbevoegde toegang en vervalsing.
18. Technieken voor beveiligd programmeren behoren zowel te worden gebruikt voor nieuwe ontwikkelingen als in scenario's voor hergebruik waarvan de normen die voor de ontwikkeling zijn toegepast niet bekend zijn of niet consistent zijn met de huidige 'best practices'.
19. Conflicterende taken en verantwoordelijkheden worden gescheiden. Voor beheertaken worden unieke gebruikersidentificaties gebruikt, zodat gebruikers kunnen worden gekoppeld aan en verantwoordelijk gesteld kunnen worden voor hun acties. Speciale toegangsrechten worden op basis van noodzaak tot gebruik en per gebeurtenis toegekend. Speciale verslaglegging wordt hiervan bijgehouden.

Artikel 7 – Informatieplichten en inbreuken i.v.m. persoonsgegevens

1. Leverancier stelt RSR onverwijld, dat wil zeggen direct bij constatering van een inbreuk in verband met persoonsgegevens, op de hoogte. Leverancier vermeldt hierbij :
 - a. de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;

- b. de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
- c. de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
- d. de maatregelen die Leverancier voorstelt of heeft genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

De meldplicht geldt voor alle inbreuken in verband met persoonsgegevens die zijn omschreven in lid 3 van dit artikel.

- 2. Leverancier zal te allen tijde een deugdelijk onderzoek verrichten naar het incident en passende vervolgstappen nemen ten aanzien van het incident, om deze zodoende in de toekomst te voorkomen. De melding van het beveiligingsincident aan RSR ontslaat Leverancier niet van zijn verplichtingen uit hoofde van de op dat moment geldende wet- en regelgeving. Het nalaten van het invoeren van passende maatregelen om toekomstige incidenten te voorkomen wordt gezien als een tekortkoming in de nakoming.
- 3. Onder "inbreuk in verband met persoonsgegevens" in artikel 7.1 wordt in ieder geval het volgende verstaan:
 - i) een onderzoek naar of beslaglegging door bevoegde autoriteiten of gerechtelijke instanties van de persoonsgegevens, of een vermoeden dat zulks gaat plaatsvinden;
 - ii) een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.
- 4. Leverancier zal te allen tijde geschreven procedures voorhanden hebben, die haar in staat stellen om RSR van een onmiddellijke reactie over een inbreuk in verband met persoonsgegevens te voorzien, de getroffen en nog te treffen maatregelen om schade te beperken en herhaling te voorkomen kenbaar te maken, en om effectief samen te werken met RSR om het incident af te handelen. Leverancier zal RSR voorzien van een exemplaar van dergelijke procedures indien RSR daar schriftelijk om verzoekt.
- 5. Partijen dragen elk de door henzelf in verband met de melding aan de bevoegde toezichthoudende autoriteit en betrokkene te maken kosten.

Artikel 8- Controle

- 1. De Leverancier zal bij aanvang van de Overeenkomst en daarna steeds op eerste schriftelijke verzoek RSR informeren over de genomen technische en organisatorische beveiligingsmaatregelen.

2. De RSR is gerechtigd periodiek te (laten) controleren of de Leverancier niet enkel zijn verplichtingen op grond van wet- en regelgeving op het gebied van de bescherming van persoonsgegevens nakomt, maar ook de verplichtingen die uit deze subverwerkersovereenkomst voortvloeien. Onderdeel van deze controle kan zijn een zogenaamde (on)aangekondigde penetratietest op de website. De Leverancier is gehouden alle medewerking te verlenen.
3. Leverancier levert volledige medewerking aan tests en audits die door RSR of een door RSR aan te wijzen partij zullen worden uitgevoerd.
4. Leverancier informeert RSR over haar auditbeleid, controlemaatregelen en auditresultaten. Leverancier informeert RSR als zij niet voldoet aan de afgesproken standaarden. Leverancier krijgt een redelijke periode om weer aan de standaard te voldoen.
5. Leverancier laat minimaal een keer per jaar een audit/penetratietest uitvoeren door een onafhankelijke derde partij en maakt het resultaat hiervan aan de opdrachtgever bekend. De kosten voor het meewerken aan deze audit worden gedragen door Leverancier.
6. Mutaties worden op basis van gebruiker, datum en tijd vastgelegd in een niet-muteerbaar logbestand en RSR kan deze zelf opvragen via een rapportage.
7. In het verlengde van 14.1 AVG, ziet RSR toe op de naleving van de in deze overeenkomst gemaakte afspraken.
8. Leverancier laat jaarlijks vóór november een onafhankelijke en objectieve audit uitvoeren door een geaccrediteerde auditor op basis van de in artikel 7 genoemde SLA waarmee RSR kan vaststellen dat Leverancier aan alle uit deze overeenkomst voortvloeiende verplichtingen voldoet. Dit leidt tot de jaarlijkse Third Party mededeling zoals genoemd in artikel 6 lid 3 van de Overeenkomst Klantenservice RSR Studentenreisproduct. Onderdeel van de auditaanpak is dat Leverancier tevens auditverklaringen overlegt van ingeschakelde subverwerkers.

Artikel 9 – Aansprakelijkheid en vrijwaring

1. Leverancier is jegens RSR aansprakelijk voor alle schade als gevolg van het niet, niet tijdig of niet behoorlijk nakomen van zijn of haar verplichtingen voortvloeiende uit deze subverwerkersovereenkomst.
2. Leverancier vrijwaart RSR tegen aanspraken van derden, die in verband staan met een toerekenbare tekortkoming van de verplichtingen uit hoofde van deze subverwerkersovereenkomst.

Artikel 10 – Privacy Officer

Voor alle aangelegenheden, inclusief de meldingen op basis van artikel 7, treedt de Privacy Officer van RSR op. De contactgegevens van de Privacy Officer zijn te vinden in Bijlage 2 van de SLA.

Artikel 11 – Service Level Agreement (SLA)

1. In de Overeenkomst SLA Klantenservice Studentenreisproduct is een aparte Service Level Agreement (SLA) opgenomen en zijn operationele afspraken gemaakt waarbij RSR ketenpartners kan aanwijzen met wie Leverancier onder zo nodig nader te bepalen voorwaarden samenwerkt.
2. De SLA bevat *Key Performance Indicators* (KPI's) om de kwaliteit van de in de dienstverleningsovereenkomst overeengekomen werkzaamheden te borgen.
3. De eisen, vervat in de KPI's van de SLA zijn de basis voor onafhankelijke audits op de naleving van de overeengekomen informatiebeveiligingsmaatregelen. De kwaliteit van de dienstverlening en het beveiligingsniveau in de SLA voldoen minimaal aan de NEN-ISO/IEC 27001 norm (of vergelijkbaar) en Leverancier stelt hiervoor een certificaat beschikbaar aan Opdrachtgever.

Artikel 12 – Inschakeling subverwerkers

1. Leverancier kan subverwerkers inschakelen na voorafgaande schriftelijke goedkeuring te hebben ontvangen van RSR. Leverancier blijft steeds verantwoordelijk voor het handelen van ingeschakelde subverwerkers voor zover dit van invloed is op de goede uitvoering van deze overeenkomst en de bescherming van persoonsgegevens.
2. Voor goedkeuring is vereist dat een subverwerkersverzoek vooraf schriftelijk aan RSR kenbaar wordt gemaakt. Een verzoek dient de namen van de subverwerkers te bevatten, evenals de activiteiten waarvoor zij worden gecontracteerd. RSR zal goedkeuring alleen onthouden als daar zwaarwegende redenen voor zijn. Een overzicht van de subverwerkers is opgenomen als Bijlage 3.
3. Wanneer Leverancier, met inachtneming van het bepaalde in artikel 8 van deze subverwerkersovereenkomst en artikel 23 Algemene Inkoopvoorwaarden RSR 2024, een andere verwerker inschakelt om ten behoeve van Opdrachtgever verwerkingsactiviteiten te verrichten, worden aan deze andere verwerker bij een overeenkomst dezelfde verplichtingen inzake gegevensbescherming opgelegd als die welke in deze Verwerkersovereenkomst zijn opgenomen. Zij zal zich voorafgaand en gedurende de samenwerking met subverwerkers, ervan vergewissen dat deze voldoen aan hun verplichtingen.
4. In aanvulling op lid 3 van dit artikel zal Leverancier op verzoek van de Opdrachtgever een kopie van een dergelijke subverwerkingsovereenkomst en van alle latere wijzigingen daarvan verstrekken aan RSR. Voor zover nodig ter bescherming van bedrijfsgeheimen of andere vertrouwelijke informatie, met inbegrip van persoonsgegevens, kan Leverancier de tekst van de overeenkomst bewerken alvorens de kopie te delen.
5. Het is subverwerkers niet toegestaan om op hun beurt onderaannemers in te schakelen, behalve in de gevallen dat RSR daarvoor schriftelijke toestemming heeft gegeven. Leverancier dient dit verbod te hebben opgenomen in de subverwerkersovereenkomsten die zij aangaat met andere subverwerkers.
6. Niettegenstaande de toestemming van RSR, zal Leverancier volledig aansprakelijk blijven jegens RSR voor het nakomen van de verplichtingen van de subverwerker en

voor de gevolgen van het uitbesteden aan derden. Leverancier zal RSR vrijwaren en schadeloos stellen voor aanspraken van derden op RSR.

Artikel 13 – Aansprakelijkheid

1. Partijen zijn wettelijk gehouden tot de betaling van schadevergoeding, stopzetting van activiteiten of herstel van fouten voor zover sprake is van verwijtbaar gedrag en schade die hen redelijkerwijs dient te worden toegerekend.
2. Beide Partijen zijn gerechtigd om bewijs aan te reiken waaruit blijkt dat schade niet aan de betreffende Partij kan worden toegerekend, waardoor deze geheel of gedeeltelijk van zijn aansprakelijkheid kan worden ontheven.
3. De partij die aantoonbaar tekortschiet in de nakoming van diens verplichtingen wordt door de andere partij schriftelijk of per email in gebreke gesteld. Hierbij wordt de nalatige partij een redelijke termijn gegund om alsnog de verplichtingen na te komen.
4. Bij niet nakoming van de verplichting binnen de in de vorige volzin genoemde termijn kan de benadeelde partij de nalatige partij aansprakelijk stellen voor vergoeding van de geleden schade.
5. Partijen zijn jegens elkaar nimmer gehouden tot het vergoeden van enige indirecte en/of immateriële schade zoals verlies van huidige en toekomstige omzet of winst, verlies van data, verlies van contracten, verlies van goodwill, vertraging of andere economische schade.

Artikel 14 – Terugbezorgen en/of wissen persoonsgegevens

Na afloop van de Overeenkomst draagt Leverancier, naar gelang de keuze van RSR op een binnen de markt geaccepteerde format, zorg voor het terugbezorgen aan RSR en/of het wissen van alle persoonsgegevens, met inachtneming van hetgeen gesteld is in art. 19 van de Algemene Inkoopvoorwaarden 2023. Leverancier verwijdert kopieën op eigen kosten en toont bewijs hiervan aan Opdrachtgever, behoudens afwijkende wettelijke voorschriften.

Artikel 15 – Looptijd en ontbindende voorwaarde

1. Deze subverwerkersovereenkomst treedt in werking op 01-04-2024 en wordt aangegaan voor de duur van de Overeenkomst inzake Klantenservice RSR Studentenreisproduct en eindigt niet eerder dan nadat Leverancier alle persoonsgegevens die deze in het kader van de dienstverleningsovereenkomst heeft verwerkt heeft gewist of (terug)bezorgd aan RSR of aan een door RSR aangewezen partij.
2. Voorwaarde voor effectuering van de met deze overeenkomst gepaard gaande gegevensuitwisselingen is de Hoofdovereenkomst Studenten OV-chipkaart geldend vanaf 1 januari 2010 tussen de Staat der Nederlanden (ten deze vertegenwoordigd door het Ministerie van Onderwijs, Cultuur en Wetenschappen) en het Openbaar Vervoer. Bij beëindiging van deze overeenkomst is de onderhavige subverwerkersovereenkomst en eventuele subverwerkersovereenkomsten van onderleveranciers eveneens van rechtswege beëindigd. Bij beëindiging van de

Overeenkomst Dienstverlening digitale administratie Studentenreisproduct ten behoeve van de door Leverancier te verrichten werkzaamheden, tussen Leverancier en RSR zal deze overeenkomst gelijktijdig van rechtswege zijn beëindigd.

Artikel 16 – Toepasselijk recht en geschillenbeslechting

Op deze overeenkomst is Nederlands recht van toepassing.

Alle geschillen die ontstaan naar aanleiding van deze overeenkomst zullen, voor zover niet anders door de wet is voorgeschreven, zijn onderworpen aan het oordeel van de bevoegde rechter te Utrecht.

De volgende bijlagen maken deel uit van deze subverwerkersovereenkomst:

- I. Gegevensset
- II. Beveiliging van persoonsgegevens bij elektronische verzending
- III. Door RSR goedgekeurde subverwerkers van Leverancier

Aldus overeengekomen en in tweevoud ondertekend op XXX te Amersfoort,

XXX
XXX

Leverancier

Mw. L.S. van der Eijck
Directeur RSR

Bijlage 1 - Gegevensset

BSN student
Geslacht
voorletters / voornaam
achternaam
adres / postcode / woonplaats
emailadres
geboortedatum
telefoonnummer
persoonlijk OV-chipkaartnummer
anonieme OV-chipkaartnummer
OV-chipkaart geldig tot datum
bankrekeningnummer
tenaamstelling bankrekening
individuele probleemomschrijving
verzonden e-mails

Bijlage 2 - Beveiliging van persoonsgegevens bij elektronische verzending

In deze bijlage is voor zowel de verzendende als ontvangende partij aangegeven welke technische en organisatorische maatregelen dienen te worden genomen alvorens kan worden overgegaan tot de uitwisseling van **persoonsgegevens** middels elektronische verzending.

Eisen ten aanzien van de verzendende partij:

- De verzendende partij is primair verantwoordelijk voor eventuele inbreuken op de privacy gedurende het transport van de verzendende partij naar de ontvangende partij;
- De verzendende partij dient er voor zorg te dragen dat de gegevens voor verzending op een zodanige wijze zijn versleuteld dat raadpleging door anderen dan de ontvangende partij in redelijkheid niet mogelijk moet worden geacht;
- De verzendende partij dient zich er voor verzending van te vergewissen middels raadpleging van de ontvanger dat de ontvangende partij inderdaad bereikbaar is op het door de verzendende partij gehanteerde ontvangstadres voor elektronische verzending;
- De verzendende partij dient zo spoedig mogelijk na verzending contact op te nemen met de ontvangende partij om te controleren of de gegevens inderdaad zijn aangekomen.

Eisen ten aanzien van de ontvangende partij:

- De ontvangende partij dient de verzendende partij te voorzien van een adres voor de ontvangst van de elektronisch verzonden gegevens;
- De ontvangende partij dient er voor zorg te dragen dat dit adres slechts toegankelijk is voor personen die gerechtigd zijn de gegevens te raadplegen vanuit hun functie dan wel betrokkenheid bij de uitvoering van de opdracht.
- De ontvangende partij dient er voor zorg te dragen dat ontsleuteling van de gegevens slechts mogelijk is door personen die tot raadpleging van de gegevens gerechtigd zijn in verband met hun rol ter uitvoering van de opdracht.

Eisen ten aanzien van beide partijen:

- Beide partijen dragen er zorg voor dat alle betrokkenen binnen hun organisaties die toegang hebben tot de gegevens een geheimhoudingsverklaring hebben ondertekend die mede deze gegevens omvat.
- Beide partijen zijn verplicht om indien er een vermoeden bestaat dat (een gedeelte van de) gegevens tijdens de verzending op enig moment voor anderen dan partijen toegankelijk zijn geweest dit te melden bij de andere partij.
- Beide partijen zullen elkaar bij een dergelijk vermoeden over en weer van alle informatie voorzien die noodzakelijk is om na te kunnen gaan of de gegevens inderdaad toegankelijk zijn geweest voor anderen en of dezen ook gebruik hebben gemaakt van deze toegankelijkheid.

Bijlage 3 – Door RSR goedgekeurde subverwerkers van Leverancier

Bedrijfsnaam en KVK-nr	Vestigingsadres	Hoofdbeschrijving van activiteit