Standaard Verwerkersovereenkomst Veiligheidsregio Brabant Noord

Toelichting op de Standaard Verwerkersovereenkomst

De Standaard Verwerkersovereenkomst is een uitwerking van de Baseline Informatiebeveiliging Overheid (BIO2) en de Algemene Verordening Gegevensbescherming (AVG). De BIO is bestuurlijk vastgesteld als gezamenlijke norm voor informatiebeveiliging voor alle Nederlandse overheden. De BIO2 is gebaseerd op de laatste versie van de ISO 27001 en de ISO 27002.

Doel

Veiligheidsregio Brabant Noord en leveranciers willen bij de uitvoering van hun taken en diensten komen tot een goede en rechtmatige dienstverlening. Als bij de uitvoering van deze taken en diensten persoonsgegevens worden verwerkt dan willen Veiligheidsregio Brabant Noord en leveranciers de verplichtingen op grond van de AVG nakomen. Daarbij willen Partijen uitgaan van wederzijds vertrouwen.

Het doel van deze standaard verwerkersovereenkomst is het Veiligheidsregio Brabant Noord en hun leveranciers makkelijker te maken om tot afspraken te komen over de verwerking van persoonsgegevens. Deze standaard wordt gebruikt als aanvulling op een hoofdovereenkomst om op grond van de AVG (artikel 28.3 en 28.9) nadere afspraken te maken en vast te leggen over de omgang met persoonsgegevens.

Rangorde

De rangorde van de verschillende documenten (o.a. inkoopdocumenten, hoofdovereenkomst, verwerkersovereenkomst) wordt geregeld in de hoofdovereenkomst.

Doelgroep

Dit document is van belang voor het management van Veiligheidsregio Brabant Noord, de systeemeigenaren, de proceseigenaren, inkopers, privacyfunctionarissen en informatiebeveiligers.

Verwerkersovereenkomst uitvoering Busvervoer Risk Factory

Veiligheidsregio Brabant Noord, waarvan het dagelijks bestuur de verwerkingsverantwoordelijke is, verder te noemen Verwerkingsverantwoordelijke, hierbij rechtsgeldig vertegenwoordigd door de <heer of mevrouw> <persoonsnaam>, <functie>

en

<Bedrijf>, gevestigd te <plaatsnaam>, KVK-nummer <nummer>verder te noemen Verwerker, hierbij rechtsgeldig vertegenwoordigd door de <de heer of mevrouw>, <persoonsnaam> , <functie>,

hierna afzonderlijk te noemen “Partij”, of gezamenlijk “Partijen”

Overwegen het volgende:

a) Partijen hebben op <datum> de <titel hoofdovereenkomst> hierna Hoofdovereenkomst, afgesloten, op grond waarvan Verwerker de volgende dienst(en) levert aan de Verwerkingsverantwoordelijke: busvervoer Risk Factory.

b) Verwerker verwerkt voor de uitvoering van de Hoofdovereenkomst Persoonsgegevens voor Verwerkingsverantwoordelijke;
c) Op de verwerking van Persoonsgegevens door Verwerker zijn de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG) van toepassing;
d) Partijen willen in aanvulling op de AVG en de UAVG de volgende afspraken over de verwerking van Persoonsgegevens vastleggen in deze verwerkersovereenkomst (hierna: de Verwerkersovereenkomst);

En komen het volgende overeen:

Artikel 1 Definities

1.1 Begrippen uit de AVG en de UAVG die in deze Verwerkersovereenkomst worden gebruikt, hebben dezelfde betekenis.
1.2 Bijlagen: aanhangsels bij deze Verwerkersovereenkomst, die onlosmakelijk deel uitmaken van deze Verwerkersovereenkomst.

Artikel 2 Ingangsdatum en duur

2.1 Deze Verwerkersovereenkomst gaat in op het moment dat de Hoofdovereenkomst tot stand is gekomen, tenzij Partijen anders overeenkomen.
2.2 Deze Verwerkersovereenkomst eindigt op het moment dat Verwerker de verwerking van Persoonsgegevens op grond van de Hoofdovereenkomst heeft beëindigd en de afspraken over het teruggeven en/of wissen van Persoonsgegevens zijn nagekomen.
2.3 Wanneer Partijen een (nieuwe) Verwerkersovereenkomst overeenkomen, betekent dat dat de oude Verwerkersovereenkomst komt te vervallen.

Artikel 3 Onderwerp van deze Verwerkersovereenkomst

3.1 Verwerker verwerkt de door of via Verwerkingsverantwoordelijke ter beschikking gestelde Persoonsgegevens uitsluitend in opdracht van Verwerkingsverantwoordelijke voor de uitvoering van de Hoofdovereenkomst en uitsluitend overeenkomstig schriftelijke instructies van Verwerkingsverantwoordelijke, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke wettelijke bepaling hem tot verwerking verplicht. In dat geval zal Verwerker Verwerkingsverantwoordelijke, voorafgaand aan de verwerking, daarvan zonder onredelijke vertraging in kennis stellen, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.
3.2 De door Verwerker uit te voeren verwerkingen staan beschreven in tabel 1 van Bijlage 1.

Artikel 4 Inhoudelijke afspraken

4.1 **Beveiligingsmaatregelen**
Verwerker zorgt voor passende technische en organisatorische maatregelen om de Persoonsgegevens

goed te beveiligen, zoals bedoeld in artikel 32 AVG. De wijze waarop Verwerker de passende technische en organisatorische maatregelen aantoont, staat in Bijlage 2.

4.2 **Audits**
Verwerker verleent alle benodigde medewerking aan audits uitgevoerd door een gecertificeerde auditor over de nakoming van de afspraken binnen deze Verwerkersovereenkomst en Bijlagen, tenzij Verwerker door middel van een geldige certificering, die periodiek door een geaccrediteerde instelling wordt getoetst, heeft aangetoond dat Verwerker de gemaakte afspraken nakomt. De kosten van deze audit worden gedragen door Verwerkingsverantwoordelijke (zowel eigen kosten als kosten van Verwerker), tenzij de auditor één of meer tekortkomingen van niet ondergeschikte aard van Verwerker constateert die ten nadele zijn van Verwerkingsverantwoordelijke.

4.3 **Verwerking buiten de EER**
Verwerker mag Persoonsgegevens buiten de Europese Economische Ruimte (laten) verwerken wanneer is voldaan aan de voorwaarden van artikel 45 of 46 AVG. Wanneer er sprake is van een verwerking buiten de EER, dan stelt Verwerker Verwerkingsverantwoordelijke daarvan vooraf op de hoogte.

4.4 **Geheimhouding**
Personen die werken voor (sub)Verwerker en (sub)Verwerker zelf, moeten Persoonsgegevens waarmee zij werken geheimhouden. De personen die werken voor Verwerker en subverwerkers hebben daarom een geheimhoudingsverklaring getekend, of zich op een andere manier schriftelijk gebonden aan de geheimhouding.

4.5 **Subverwerkers**
De ten tijde van het afsluiten van deze Verwerkersovereenkomst bekende subverwerkers vermeldt Verwerker in tabel 3 van Bijlage 1. Verwerkingsverantwoordelijke verleent hierbij algemene toestemming voor de inschakeling van subverwerkers. Verwerker houdt na de start van de werkzaamheden Verwerkingsverantwoordelijke op de hoogte van de beoogde inschakeling van nieuwe subverwerkers. Bij de inschakeling van subverwerkers blijven de artikelen 28.2 en 28.4 AVG onverkort van kracht.

4.6 **Rechten van betrokkenen**
Als een betrokkene een beroep doet op zijn rechten zoals genoemd in artikel 12 t/m 22 AVG, helpt Verwerker Verwerkingsverantwoordelijke om daarop binnen de wettelijke termijnen een beslissing te nemen.

4.7 **Gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging**
Op verzoek van Verwerkingsverantwoordelijke werkt Verwerker altijd mee aan een gegevensbeschermingseffectbeoordeling (DPIA) en een voorafgaande raadpleging als bedoeld in artikel 35 en 36 AVG.

Artikel 5 Inbreuk in verband met Persoonsgegevens

5.1 Verwerker zal Verwerkingsverantwoordelijke zonder onredelijke vertraging, maar uiterlijk binnen 24 uur, informeren na vaststelling van een (vermoedelijke) Inbreuk in verband met Persoonsgegevens. Verwerker vermeldt hierbij voor zover bekend de vermeende oorzaak van de (vermoedelijke) Inbreuk, de categorie persoonsgegevens, de categorie betrokkenen en het aantal betrokkenen.

5.2 In geval van een Inbreuk neemt Verwerker zonder onredelijke vertraging alle maatregelen om de Inbreuk te herstellen, de gevolgen daarvan te beperken en verdere Inbreuken te voorkomen en houdt de Verwerkingsverantwoordelijke hiervan voortdurend op de hoogte.

5.3 Verwerker heeft een gedetailleerd logboek van de Inbreuken en de maatregelen die op Inbreuken zijn genomen. Verwerkingsverantwoordelijke mag dat inzien, wanneer deze daarom vraagt.

5.4 Verwerkingsverantwoordelijke beslist of de Inbreuk moet worden gemeld bij de toezichthoudende autoriteit en/of Betrokkene. Verwerker ondersteunt de Verwerkingsverantwoordelijke waar nodig bij de melding aan de toezichthoudende autoriteit en/of Betrokkene.

Artikel 6 Aansprakelijkheid

6.1 Eventuele in de Hoofdovereenkomst overeengekomen beperkingen van de aansprakelijkheid hebben ook betrekking op de Verwerkersovereenkomst.

Artikel 7 Beëindigen verwerkersovereenkomst

7.1 Partijen moeten in de Hoofdovereenkomst afspraken maken over de beëindiging van de Hoofdovereenkomst en de daaruit voortvloeiende teruggave en wissing van Persoonsgegevens.

7.2 De geheimhouding geldt ook nog na beëindiging van deze Verwerkersovereenkomst.

Artikel 8 Overige bepalingen

8.1 Op deze overeenkomst is Nederlands recht van toepassing. Alle geschillen, ook als alleen één Partij vindt dat er een geschil is, zullen in eerste instantie worden voorgelegd aan dezelfde bevoegde rechter als genoemd in de Hoofdovereenkomst.

Ondertekening

Aldus overeengekomen en in tweevoud ondertekend,

Ingangsdatum: <……>

Veiligheidsregio Brabant Noord	**<Naam organisatie>**
namens deze**:** <naam, functie>	namens deze: <naam, functie>
plaats: <……>	plaats: <……>
datum: <……>	datum: <……>

Bijlage 1: Overzicht van te verwerken persoonsgegevens, contactgegevens partijen en overzicht ingeschakelde subverwerkers

1. Naam verwerking, doeleinden categorieën van betrokkenen, categorieën persoonsgegevens en eventuele doorgifte naar derde landen.

Naam verwerking/ Welke dienst en/of product	Verwerkings-doeleinden	Categorieën van Betrokkenen	(Bijzondere) Persoons-gegevens	Verwerkings-locatie	Doorgifte-instrument (indien van toepassing)	Aanvullende maatregelen (indien van toepassing)

2. Contactgegevens

Contactpersoon Verwerkingsverantwoordelijke (van VRBN)	Naam: Functie: e-mailadres: telefoonnummer:
Contactpersoon Verwerker (van leverancier)	Naam: Functie e-mailadres: telefoonnummer:
Contactgegevens Functionaris Gegevensbescherming	e-mailadres: privacy@vrbn.nl

3. Ingeschakelde subverwerkers

Naam en	KvK-	Uitbestede	Toepassing	Verwerkings-	Doorgifte	Aanvullende

contactgegevens subverwerker	nummer	verwerkingen	(geautomatiseerd systeem)	locatie	instrument	maatregelen (indien van toepassing)

NB: Substantiële wijzigingen in bovenstaande tabellen geven partijen op korte termijn aan elkaar door.

Bijlage 2: Aantonen passend niveau van beveiliging

Normenstelsel

□ De verwerker werkt volgens een algemeen erkende norm voor informatiebeveiliging, te weten:
…… (vermeld normenstelsel, zoals bijvoorbeeld NEN7510, NEN/ISO 27001, PCI/DSS) en is volgens deze norm wel/niet gecertificeerd.

- Datum laatste certificering: ……

□ De verwerker werkt volgens een algemeen erkende overheidsnorm zoals de BIO2, of vergelijkbaar, te weten:
……..,

□ De verwerker werkt volgens een andere norm, te weten:
……..

Toereikendheid

De toereikendheid van de informatiebeveiliging blijkt uit het volgende:

□ Verwerker verstrekt een actueel en geldig certificaat en verklaring van toepasselijkheid (VVT);
□ Rapportages van periodieke externe controles zoals audits, pentesten of TPM's (bijv. ISAE3xxx SOC type II);
□ Een assurance rapport (TPM) van een auditor die is aangesloten bij NOREA;
□ Eigen controles of eigen mededelingen over de beveiligingsmaatregelen zoals hieronder beschreven (in lijn met de aanpak uit hoofdstuk 4.4 uit de BIO2, een ICV):
……

NB: Uit de certificering/periodieke externe controles/audits of uit de eigen controles/beschrijvingen blijkt of kan worden afgeleid dat de beveiliging passend is bij de verwerking(en) genoemd in Bijlage 1.

Aansluiting bij goedgekeurde gedragscode

□ Verwerker is aangesloten bij een door een toezichthoudende autoriteit goedgekeurde gedragscode, te weten
……

NB: Substantiële wijzigingen in het bovenstaande en achteruitgang van de voorwaarden geven partijen op korte termijn aan elkaar door.