

Aanvullende Overeenkomst inzake de deling van gegevens

**Aanvullende Overeenkomst inzake de deling
van gegevens**

Behorende bij:

**Dienstverleningsovereenkomst "Onderzoek
inkoop PBM voor VWS", met kenmerk 2846242,
getekend d.d. 20 juli 2021**

Aanvullende Overeenkomst inzake de deling van gegevens

Ondergetekenden:

1. De Staat der Nederlanden, met zetel te Den Haag, vertegenwoordigd door de Minister van Medische Zaken en Sport, waarbij de Minister wordt vertegenwoordigd door [naam en functie persoon], hierna te noemen: "ministerie van VWS"

en

2. Deloitte Forensic & Dispute Services B.V., statutair gevestigd te Rotterdam, kantoorhoudende te Gustav Mahlerlaan 2970, 1081 LA Amsterdam, te dezen rechtsgeldig vertegenwoordigd door [naam en functie persoon], hierna te noemen: „Deloitte“;

elk afzonderlijk een "Partij", en tezamen "Partijen".

Overwegende dat:

- A. Partijen op 20 juli 2021 een schriftelijke Dienstverleningsovereenkomst zijn aangegaan, bekend als "Onderzoek inkoop PBM voor VWS", met kenmerk 2846242, ingegaan met terugwerkende kracht per 18 juni 2021, hierna te noemen: "Hoofdovereenkomst".
- B. Partijen ter uitvoering van de Hoofdovereenkomst en meer specifiek artikel 14 van de bij die Hoofdovereenkomst geldende ARVODI-bepalingen, een aanvullende overeenkomst wensen overeen te komen met betrekking tot de verwerking van gegevens en de daarbij behorende naleving van de AVG (zoals hierna gedefinieerd) en andere toepasselijke wetgeving inzake gegevensbescherming en privacy (hierna: Aanvullende Overeenkomst).
- C. Deloitte de diensten verleent, zoals beschreven in de Opdrachtbrief in paragraaf 2, zijnde document 3 van de Hoofdovereenkomst, als onafhankelijk en onpartijdig onderzoeker.
- D. Partijen erkennen dat Deloitte gelet op haar rol als onafhankelijk en onpartijdig onderzoeker in de uitvoering van de Hoofdovereenkomst zal optreden als een afzonderlijke verwerkingsverantwoordelijke met betrekking tot de Persoonsgegevens die zij verwerkt ter uitvoering van die Hoofdovereenkomst en zelfstandig voldoet aan de voorwaarden voortvloeiende uit de AVG.
- E. Het ministerie van VWS wenst bepaalde Gegevens (zoals hierna gedefinieerd) ter beschikking te stellen, en Deloitte de van het ministerie van VWS ontvangen Gegevens kan gebruiken in samenhang met het Toegestane Doel (zoals hierna gedefinieerd), met inachtneming van de voorwaarden van deze Aanvullende Overeenkomst (zoals hierna gedefinieerd) en alle toepasselijke wet- en regelgeving;

komen Partijen hierbij overeen als volgt.

Aanvullende Overeenkomst inzake de deling van gegevens

1. Definities

De in deze Aanvullende Overeenkomst inzake de deling van gegevens gebruikte woorden of formuleringen hebben zowel in het enkelvoud als het meervoud de volgende betekenis:

- **Aanvullende Overeenkomst:** deze aanvullende overeenkomst inzake de uitwisseling van gegevens, behorende bij de Hoofdovereenkomst.
- **ARVODI-2018:** Algemene Rijksvoorwaarden voor het verstrekken van opdrachten tot het verrichten van Diensten 2018.
- **AVG:** de afkorting AVG staat voor Algemene Verordening Gegevensbescherming (EU 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens).
- **Betrokkene:** degene op wie Persoonsgegevens betrekking hebben.
- **Bijlage:** de bijlagen bij deze Aanvullende Overeenkomst, die daar onlosmakelijk deel van uitmaken.
- **BVA VWS:** Beveiligingsautoriteit VWS Concern.
- **Gegevens:** Gegevens in de zin van de gegevensverzameling, zoals verstrekt door het ministerie van VWS ten behoeve van de uitvoering van de Hoofdovereenkomst.
- **Hoofdovereenkomst:** de Dienstverleningsovereenkomst tussen het ministerie van VWS en Deloitte, zijn de "Onderzoek inkoop PBM voor VWS", met kenmerk 2846242.
- **Persoonsgegevens:** Informatie in de Gegevens zoals verstrekt door het ministerie van VWS over een geïdentificeerde of identificeerbare natuurlijke persoon die in het kader van de uitvoering van de Hoofdovereenkomst door Deloitte wordt verwerkt.
- **Toegestane Doel:** het uitvoeren van het onderzoek zoals beschreven in de Hoofdovereenkomst, en het rapporteren van de resultaten van het onderzoek, uitsluitend voor het in de Hoofdovereenkomst overeengekomen doel.

2. Bekendmaking en reikwijdte Gegevens

- 2.1 Met inachtneming van de voorwaarden van de Aanvullende Overeenkomst zal het ministerie van VWS bepaalde Gegevens aan Deloitte verstrekken zoals beschreven in Bijlage 1.
 - 2.2 Deloitte erkent dat de Gegevens door het ministerie van VWS worden verstrekt in de staat waarin zij zich op dat moment bevinden ("as is") zonder enigerlei garantie van toereikende kwaliteit of geschiktheid voor een bepaald doel of gebruik, en zonder enige andere uitdrukkelijke of impliciete garantie, tenzij anders overeengekomen.
 - 2.3 Het ministerie van VWS verklaart de Gegevens uitsluitend aan Deloitte te zullen verstrekken voor het Toegestane Doel.
-

Aanvullende Overeenkomst inzake de deling van gegevens

- 2.4 Het ministerie van VWS verstrekt uitsluitend die Gegevens voor zover die nodig zijn voor de uit te voeren opdracht.
- 2.5 Partijen verlenen elkaar redelijke medewerking en bijstand met betrekking tot (ten minste):
- Verzoeken van betrokkenen en andere communicatie met betrokkenen die betrekking hebben op de verwerking van hun Persoonsgegevens; en
 - Elke communicatie met een toezichthoudende autoriteit.

3. Geheimhouding

~~De~~ Persoonsgegevens hebben een vertrouwelijk karakter als bedoeld in artikel 13.1 van de ARVODI-2018.

- 3.2 Deloitte toont op verzoek van het ministerie van VWS aan dat zijn Personeel zich ertoe heeft verbonden vertrouwelijkheid in acht te nemen als bedoeld in artikel 13.2 van de ARVODI-2018.

4. Gegevensbescherming

~~De~~ ministerie van VWS ziet erop toe dat alle Gegevens in overeenstemming met toepasselijke wet- en regelgeving worden verkregen uit de systemen toebehorende aan en/of onder verantwoordelijkheid vallende van het ministerie van VWS, en verklaart tot verstrekking van die Gegevens bevoegd te zijn.

- 4.2 Deloitte garandeert dat alle werkzaamheden waarbij Gegevens worden gebruikt, zullen worden verricht in overeenstemming met alle toepasselijke wet- en regelgeving, richtlijnen, optimale werkwijzen en goedkeuringen in het kader van het onderzoek.
- 4.3 Deloitte zal passende technische en organisatorische maatregelen nemen ter waarborging van een niveau van veiligheid dat is afgestemd op het risico, zodat het gebruik van de verstrekte Gegevens in overeenstemming is met de vereisten op grond van de EU-wetgeving inzake bescherming van gegevens en andere toepasselijke wet- en regelgeving inzake de verwerking van persoonsgegevens, en de bescherming van de rechten van betrokkenen is gewaarborgd.
- 4.4 Deloitte ziet erop toe dat alle Personeel met toegang tot de Gegevens zullen handelen in overeenstemming met het bepaalde in deze Overeenkomst en met alle overige wet- en

Aanvullende Overeenkomst inzake de deling van gegevens

regelgeving op het gebied van gegevensbescherming en - beveiliging. Deloitte zal ervoor zorgen dat uitsluitend diegenen van zijn werknemers die rechtstreeks betrokken zijn bij het Toegestane Doel toegang hebben tot de Gegevens en dat zij gebonden zullen zijn aan geheimhoudings- en gebruikersverklaringen en - beperkingen die in grote mate vergelijkbaar zijn met en ten minste even streng zijn als die waarin deze Overeenkomst voorziet.

- 4.5 Deloitte verklaart derden geen toegang te zullen verlenen tot (een deel van de) gegevens of daarvan afgeleide identificeerbare gegevens, tenzij anders overeengekomen.
- 4.6 Deloitte dient het ministerie van VWS te informeren over inbreuken in verband met Persoonsgegevens of een redelijk vermoeden daarvan zonder onredelijke vertraging, doch uiterlijk binnen 24 uur na ontdekking ervan. Ten behoeve van het informeren zal Deloitte gebruik maken van de contactgegevens in Bijlage 4.
- 4.7 In verband met het bepaalde in artikel 6.15 onderdeel c) van de Hoofdovereenkomst, zal Deloitte na vijf jaar na de datum waarop het onderzoek is afgerond middels oplevering van het definitieve eindrapport, dan wel na beëindiging van deze Overeenkomst, in overleg treden met de Functionaris Gegevensbescherming van het ministerie van VWS over het teruggeven van brongegevens of het verwijderen uit haar beheeromgeving van de brongegevens. Binnen 12 maanden na publicatie van het definitieve eindrapport door Opdrachtgever, zullen Opdrachtgever en Opdrachtnemer in overleg treden om de persoonsgegevens binnen de brondata zodanig te beveiligen dat hierbij de belangen van betrokkenen binnen redelijke grenzen gewaarborgd kunnen worden.

5. Slotbepalingen

- 5.1 Deze Aanvullende Overeenkomst eindigt op het moment de Hoofdovereenkomst wordt beëindigd.
- 5.2 Zodra de Hoofdovereenkomst wordt beëindigd of eindigt, om welke reden dan ook, blijven de relevante bepalingen van deze Aanvullende Overeenkomst van kracht zolang er door Deloitte Persoonsgegevens worden verwerkt, waarna deze Aanvullende Overeenkomst van rechtswege eindigt.
- 5.3 Bij tegenstrijdigheid tussen de bepalingen uit de Hoofdovereenkomst en de Aanvullende Overeenkomst, prevaleren de bepalingen uit de Hoofdovereenkomst, met dien verstande dat de bepalingen die betrekking hebben op de rechten en plichten voortvloeiende uit de AVG prevaleren boven de bepalingen uit de Hoofdovereenkomst.

Aanvullende Overeenkomst inzake de deling van gegevens

Ondertekend door Partijen:

Aldus overeengekomen en ondertekend in tweevoud,

DE MINISTER/STAATSSECRETARIS VAN/VOOR
[naam portefeuille]

Deloitte Forensic & Dispute Services BV

namens deze,
[functienaam ondertekenaar]

namens deze,

5.1.2e

5.1.2e

5.1.2e

5.1.2e

30/9-21

Aanvullende Overeenkomst inzake de deling van gegevens

Bijlage 1 Toepassingsgebied en beschrijving van Persoonsgegevens en verwerkingsdoel(en)

Betrokkenen:

Ambtenaren en (ingehuurde) derden die onder de verantwoordelijkheid van het ministerie van VWS vallen en/of vielen, of waarvan het ministerie de persoonsgegevens onder zich heeft, die betrokken waren bij het inkoopproces van persoonlijke beschermingsmiddelen in de periode 1 januari 2020 tot 1 juni 2021 door VWS en/of LCH.

Toegestane doeleinden:

De verwerking van persoonsgegevens in verband met het uitvoeren van het onderzoek zoals beschreven in de Hoofdovereenkomst, en het rapporteren van de resultaten van het onderzoek, uitsluitend voor het in de Hoofdovereenkomst overeengekomen doel.

Categorieën van Persoonsgegevens:

Gewone Persoonsgegevens als bedoeld in de AVG, waarbij onder meer verwerkt wordt:

- Naam
- Functie en periode van bekleden van functie
- Emailadres
- Telefoonnummer

De Gegevens omvatten in bredere zin:

- de (zakelijke) emailbestanden,
- de (zakelijke) correspondentie,
- de (zakelijke) communicatie, zoals chatberichten en sms-berichten,
- de persoonlijke gegevensmap(pen) op het zakelijke netwerk/de server toebehorende aan het ministerie van VWS en/of SSC-ICT,
- en soortgelijke bestanden, documenten, correspondentie en/of communicatie.

Van betrokkenen wordt door Deloitte een lijst bijgehouden met daarbij aangetekend welke data is verkregen van het ministerie van VWS.

De Bewaarperiode:

De bewaarperiode is in artikel 3.7 van deze Aanvullende Overeenkomst vastgelegd.

Ontvanger:

De Persoonsgegevens kunnen worden verstrekt aan Deloitte Forensic & Dispute Services BV zoals vereist voor de toegestane doeleinden.

Locatie

De gegevens zullen door Deloitte Forensic & Dispute Services BV en de (direct) gelieerde bedrijven binnen het Deloitte Netwerk enkel binnen de Europese Unie verwerkt worden.

Aanvullende Overeenkomst inzake de deling van gegevens

Bijlage 2 Overzicht van veiligheidsmaatregelen

Technische en organisatorische maatregelen

Partijen nemen de volgende technische en organisatorische maatregelen om de Persoonsgegevens te beschermen tegen onopzettelijke of onwettige vernietiging, of onopzettelijk verlies, wijziging, ongeoorloofde openbaarmaking of toegang.

Deloitte is gecertificeerd voor ISO27001. Op verzoek van opdrachtgever zal Deloitte het certificaat en de Verklaring van Toepasselijkheid overleggen.

Deloitte heeft op verzoek van het ministerie van VWS Toets maatregelen VIR-BI ingeleverd. Deze is akkoord bevonden voor het niveau Departementaal Vertrouwelijk.

Inspectie fysieke beveiligingsmaatregelen

De BVA VWS zal, nadat het onderzoek is afgerond (of in een fase is beland waar de onafhankelijkheid van het onderzoek niet meer ter discussie kan worden gesteld), van Deloitte een uitnodiging ontvangen om op de relevante locatie een inspectie uit te voeren op de door Deloitte beschreven 'fysieke' beveiligingsmaatregelen. Doelstelling van de inspectie is het (steekproefsgewijs) vaststellen of er eenzelfde fysiek beveiligingsniveau aanwezig is als bij de Rijksdienst.

Kopie (netto)databestand BVA

Er worden twee kopieën gemaakt van het (netto)databestand dat aan Deloitte zal worden meegegeven. Een van deze kopieën is voor de BVA. Deze (BVA)kopie zal in een sealbag in de kluis van de BVA worden opgeslagen. De BVA zal de kopie die ontvangen is pas na afloop van het onderzoek (laten) beoordelen, als daar aanleiding voor is, op aanwezigheid van bijzondere informatie. Doel is het vaststellen of er sprake is geweest van compromittatie van bijzondere informatie omdat deze bijzondere informatie buiten de Rijksdienst is gebracht. Mocht er aanleiding zijn, vanwege een geconstateerd incident, de kopie al tijdens het onderzoek te raadplegen dan zal dit in onderlinge afstemming met Deloitte gebeuren (om waar mogelijk te voorkomen dat de onafhankelijkheid van het onderzoek ter discussie kan komen te staan).

Aanvullende Overeenkomst inzake de deling van gegevens

Bijlage 3 Mitigerende maatregelen bij aantreffen bijzondere informatie en/of bijzondere categorieën persoonsgegevens

Bijzondere informatie

Op het moment dat Deloitte de constatering doet dat er in de dataset die zij in haar bezit heeft, en die buiten de (fysieke omgeving van de) Rijksdienst is gebracht, bijzondere informatie aanwezig is (rubricering Departementaal Vertrouwelijk en/of Staatsgeheim) en deze bijzondere informatie heeft geen relatie met het onderzoek dan zal dit door Deloitte gemeld worden bij de BVA VWS (via het piketnummer 5.1.2e

In onderlinge afstemming zal dan besproken worden wat de te nemen vervolgstappen zijn.

Alleen documenten waar duidelijk in de header staat 'Departementaal Vertrouwelijk' of 'STAATSGEHEIM Confidentieel' (of hoger), en daardoor herkenbaar zijn voor Deloitte, vallen onder deze afspraak. In beginsel zouden er in de (netto)dataset geen documenten aanwezig kunnen zijn die de classificatie STAATSGEHEIM Confidentieel (of hoger) hebben.

Bijzondere categorieën persoonsgegevens

Indien na levering van de Gegevens door Deloitte bijzondere categorieën persoonsgegevens als bedoeld in artikel 9 van de AVG worden aangetroffen in de geleverde dataset worden de volgende maatregelen getroffen:

- Het anonimiseren van de aangetroffen informatie, dan wel
- Indien de informatie niet van belang is voor het onderzoek, het vernietigen van die informatie.

Bij het aantreffen van meerdere documenten met bijzondere categorieën persoonsgegevens, kan Deloitte onderzoek instellen of dit in de toekomst voorkomen kan worden door aanpassing van de filtercriteria.

Aanvullende Overeenkomst inzake de deling van gegevens

Bijlage 4 Afspraken inzake Inbreuken in verband met Persoonsgegevens

Met Inbreuk in verband met Persoonsgegevens wordt bedoeld: ongewenste toegang tot of vernietiging, wijziging of publicatie van Persoonsgegevens bij Opdrachtnemer. Een Inbreuk in verband met Persoonsgegevens betreft derhalve niet alleen het lekken van Persoonsgegevens, maar ook de onrechtmatige verwerking van Persoonsgegevens.

Het ministerie van VWS spreekt van een Inbreuk in verband met Persoonsgegevens indien er sprake is van een inbreuk in verband met de beveiliging van Persoonsgegevens. Indien er sprake is van een Inbreuk in verband met Persoonsgegevens worden de Persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking, dat wil zeggen: aan datgene waartegen de beveiligingsmaatregelen moeten beschermen.

Melding van inbreuken in verband met Persoonsgegevens en/of incidenten in verband met beveiliging

Deloitte is verantwoordelijk voor de verwerking van de verstrekte Gegevens ten behoeve van de uitvoering van de Hoofdovereenkomst zoals beschreven in Bijlage 1 vanaf het moment van verstrekking van die Gegevens door het ministerie van VWS aan Deloitte. Deloitte is verantwoordelijk indien er sprake is van een inbreuk in verband met die verstrekte Persoonsgegevens. Deloitte is verantwoordelijk voor het vaststellen en melden van inbreuken in verband met Persoonsgegevens aan de Autoriteit Persoonsgegevens, alsmede voor het melden van inbreuken in verband met Persoonsgegevens aan de betrokkenen.

Indien Deloitte het ministerie van VWS dient te informeren in verband met artikel 4.6, dient de volgende informatie te worden verstrekt:

Contactgegevens contactpersoon

[invullen VWS]

Gegevens inzake de inbreuk in verband met Persoonsgegevens

- Geef een samenvatting van het incident waarbij de inbreuk op de beveiliging van Persoonsgegevens heeft plaatsgevonden
- Van hoeveel personen zijn Persoonsgegevens betrokken bij de inbreuk? (Vermeld het aantal.)
 - a) Minimum: [invullen]
 - b) Maximum: [invullen]
- Beschrijf de groep mensen wier Persoonsgegevens bij de inbreuk zijn betrokken
- Wanneer heeft de inbreuk plaatsgevonden? (Kies een van de volgende mogelijkheden en vul aan waar nodig).
 - a) Op [datum]
 - b) Tussen [begindatum periode] en [einddatum periode]
 - c) Nog niet bekend

Aanvullende Overeenkomst inzake de deling van gegevens

- Wat is de aard van de inbreuk? (Meerdere opties mogelijk)
 - a) Lezen (vertrouwelijkheid)
 - b) Kopiëren
 - c) Wijzigen (integriteit)
 - d) Wissen of vernietigen (beschikbaarheid)
 - e) Diefstal
 - f) Nog niet bekend

- Om wat voor Persoonsgegevens gaat het? (Meerdere opties mogelijk)
 - a) NAW-gegevens
 - b) Telefoonnummers
 - c) E-mailadressen of andere adressen voor elektronische communicatie
 - d) Toegangs- of identificatiegegevens (zoals inlognaam / wachtwoord of klantnummer)
 - e) Bijzondere Persoonsgegevens (zoals ras, etnische afkomst, strafblad, politieke overtuiging, vakbondslidmaatschap, religie, seksueel leven, medische gegevens)
 - f) Overige informatie, namelijk [invullen]

- Wat zijn de mogelijke gevolgen van de inbreuk voor de privacy van de betrokkenen? (Meerdere opties mogelijk)
 - a) Stigmatisering of uitsluiting
 - b) Schade aan de gezondheid
 - c) Blootstelling aan (identiteits)fraude
 - d) Blootstelling aan spam of phishing
 - e) Anders, namelijk [invullen]

Deloitte dient (redelijke vermoedens van) inbreuken in verband met Persoonsgegevens onmiddellijk doch uiterlijk binnen 24 uur na ontdekking aan de CISO & Privacy Officer van het ministerie van VWS te melden op 5.1.2e@minvws.nl, of per telefoon op [5.1.2e](tel:5.1.2e)

Bij het doen van een melding dient Deloitte uitdrukkelijk te vermelden dat de melding een inbreuk in verband met Persoonsgegevens betreft.