BIJLAGE 6 – CONCEPT VERWERKERSOVEREENKOMST

Partijen

Gemeentelijke Gezondheidsdienst Groningen (hierna te noemen: GGD Groningen), gevestigd te Groningen, KVK nummer 62089781, ten deze rechtsgeldig vertegenwoordigd door de heer. J. Koopman, Directeur Publieke Gezondheid, hierna te noemen: verantwoordelijke

en

XXXXXX (hierna te noemen: XXXXXX), gevestigd te XXXXXX, KVK-nummer XXXXXX, ten deze rechtsgeldig vertegenwoordigd door de heer/mevrouw XXXXXX, <functie>, hierna te noemen; verwerker,

overwegende:

1. dat XXXXXX is aan te merken als verwerker in de zin van de Algemene verordening gegevensbescherming (hierna: AVG) en GGD Groningen is aan te merken als verantwoordelijke in de zin van de AVG, aangezien XXXXXX ten behoeve van GGD Groningen gegevens verwerkt, zonder aan rechtstreeks gezag van GGD Groningen te zijn onderworpen en de verantwoordelijke het doel van en de middelen voor de verwerking van de persoonsgegevens vaststelt;

2. dat in dit kader persoonsgegevens worden verwerkt;

3. dat verwerker op grond van zijn dienstverlening, zoals opgenomen in de hoofdovereenkomst XXXXXX te maken krijgt met persoonsgegevens;

4. dat de gegevens die door de verantwoordelijke aan de verwerker worden verstrekt privacygevoelig zijn en zowel verantwoordelijke als verwerker groot belang hechten aan het beschermen van de privacy;

5. dat de AVG de verantwoordelijke in de zin van die wet verplicht een verwerkersovereenkomst te sluiten met een verwerker;

6. dat de AVG aan de verantwoordelijke de plicht oplegt om ervoor zorg te dragen dat de verwerker voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen;

7. dat de AVG daarnaast aan de verantwoordelijke de plicht oplegt om toe te zien op de naleving van die maatregelen;

verklaren te zijn overeengekomen als volgt:

Artikel 1: Opvolgen van opdracht en instructies door verwerker
1. De verwerker verwerkt de persoonsgegevens slechts in opdracht van de verantwoordelijke, behoudens afwijkende wettelijke verplichtingen.
2. De verwerker verwerkt gegevens ten behoeve van de verantwoordelijke, overeenkomstig diens instructies en onder diens verantwoordelijkheid.
3. De verwerker heeft geen zeggenschap over het doel en de middelen voor de verwerking van persoonsgegevens. Zo neemt hij geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en de duur van de opslag van gegevens. De zeggenschap over de persoonsgegevens verstrekt onder deze overeenkomst komt nimmer bij de verwerker te berusten.
4. Naast de verplichting van de verwerker om de instructies van de verantwoordelijke te volgen, dient hij ook zorg te dragen voor de naleving van de voorwaarden die – met name op grond van de AVG – worden gesteld aan het verwerken van persoonsgegevens.
5. De verwerker stelt de verantwoordelijke in de gelegenheid de verwerking van persoonsgegevens te controleren.

Artikel 2: Beveiligingsmaatregelen
1. De verwerker neemt alle passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen een passend beveiligingsniveau, gelet op de aard van de persoonsgegevens die de verwerker verwerkt.
2. De verantwoordelijke heeft het recht om toe te zien op de naleving en werking van de beveiligingsmaatregelen.

Artikel 3: Meldplicht datalekken
1. De verwerker meldt een data lek volgens de definitie van de AVG onverwijld (uiterlijk binnen 24 uur na constatering dat een beveiligingsincident mogelijk onder de meldplicht valt) aan de verantwoordelijke. Hierbij worden de bepalingen uit de beleidsregels ‘De meldplicht datalekken in de AVG in acht genomen;
2. De verwerker houdt de verantwoordelijke op de hoogte van eventuele nieuwe ontwikkelingen rond het incident, en van de maatregelen die de verwerker treft om aan zijn kant de gevolgen van het incident te beperken en herhaling te voorkomen.

Artikel 4: Geheimhouding
De verwerker is verplicht tot geheimhouding van de persoonsgegevens die hij van de verantwoordelijke ontvangt, behoudens voor zover een wettelijk voorschrift de verwerker tot mededelen verplicht en behoudens de gegevensverstrekking die plaatsvindt in opdracht van de verantwoordelijke. De verwerker besteedt zijn verplichtingen die voortvloeien uit de hoofdovereenkomst niet uit aan derden, tenzij de verantwoordelijke daarvoor uitdrukkelijk schriftelijk toestemming heeft gegeven.

Artikel 5: Medewerkers van de verwerker
De verplichtingen van de verwerker die uit deze overeenkomst voortvloeien, gelden ook voor degenen die persoonsgegevens verwerken onder het gezag van de verwerker.

Artikel 6: Overige bepalingen
1. De overeenkomst wordt aangegaan voor de periode dat de hoofdovereenkomst van kracht is.
2. Deze overeenkomst kan slechts met instemming van partijen worden gewijzigd. Deze wijziging heeft eerst werking tussen partijen indien zij schriftelijk tussen partijen is overeengekomen.
3. De verwerker bewaart de persoonsgegevens die hij van de verantwoordelijke heeft ontvangen niet langer dan strikt noodzakelijk. Hij vernietigt de persoonsgegevens na goedkeuring door de verantwoordelijke.
4. De verwerker zal de verantwoordelijke bijstand verlenen bij het vervullen van diens verplichtingen op grond van de van toepassing zijnde wetgeving inzake bescherming van persoonsgegevens, waaronder verzoeken van betrokkenen die hun wensen uit te oefenen.
5. De verwerker geeft geen persoonsgegevens door naar landen buiten de Europese Economische Ruimte.
6. De verwerker draagt zorg dat na beëindiging van deze overeenkomst, naargelang van de keuze van de verantwoordelijke, dat alle persoonsgegevens zijn gewist dan wel zijn terugbezorgd aan de verantwoordelijke, en dat bestaande kopieën zijn verwijderd, tenzij opslag hiervan wettelijk verplicht is.

Artikel 7: Aansprakelijkheid
1. Indien verwerker tekortschiet in de nakoming van de verplichting uit deze overeenkomst
kan verantwoordelijke hem in gebreke stellen. Verwerker is echter onmiddellijk in gebreke
als de nakoming van desbetreffende verplichting anders dan door overmacht binnen de overeengekomen termijn, reeds blijvend onmogelijk is. Ingebrekestelling geschiedt schriftelijk, waarbij aan verwerker een redelijke termijn wordt gegund om alsnog zijn verplichtingen na te komen. Deze termijn is een fatale termijn. Indien nakoming binnen deze termijn uitblijft, is verwerker in verzuim. Art. 82 AVG is van toepassing.

Artikel 8: Beschrijving van te verwerken persoonsgegevens
De beschrijving van de te verwerken persoonsgegevens en de beveiliging ervan zijn opgenomen in bijlagen A, B en C. Deze bijlagen maken onderdeel uit van deze overeenkomst.

Artikel 9: Toepasselijk recht
Op deze overeenkomst en op alle geschillen die daaruit mogen voortvloeien of daarmee mogen samenhangen, is het Nederlands recht van toepassing.

Aldus overeengekomen, in tweevoud opgemaakt en ondertekend,

Namens GGD Groningen,	Namens XXXXXX
De heer mr. dr. J. Koopman Directeur Publieke Gezondheid	De heer/mevrouw XXXXXX <functie>
Datum:	Datum:

Bijlage A Beschrijving van de verwerking van persoonsgegevens

Te verwerken persoonsgegevens (kruis aan welke van toepassing is/zijn)

☐ Naam
☐ Adres
☐ Postcode
☐ Emailgegevens
☐ Telefoonnummer
☐ Geboortedatum of leeftijd
☐ Huwelijkse status
☐ Geslacht
☐ Opleiding
☐ Financiële gegevens
☐ Kentekengegevens
☐ Ras of etniciteit
☐ Politieke opvattingen
☐ Religieuze of levensbeschouwelijke overtuigingen
☐ Lidmaatschap van een vakbond
☐ Gegevens over iemands seksuele gedrag of seksuele gerichtheid
☐ Door de overheid uitgegeven Identificatie Nummers, zoals BSN
☐ (kopieën van identiteitsbewijzen, zoals rijbewijs of paspoort
☐ Strafrechtelijke gegevens
☐ Medische gegevens
☐ Overige (graag kort beschrijven welke persoonsgegevens u verwerkt):
.....

.....

.....

Voor welk doel worden de persoonsgegevens gebruikt? (omschrijf duidelijk het doel/de doelen van de verwerking van persoonsgegeven).

Bijlage B Beschrijving van de beveiliging van persoonsgegevens

1. De informatiebeveiliging vindt plaats volgens één van de algemeen erkende normen of overheidsnormen (kruis aan wat van toepassing is):
   ☐NEN7510
   ☐NEN/ISO 27001
   ☐PCI/DSS
   ☐Baseline Informatiebeveiliging Gemeenten
   ☐Baseline Informatiebeveiliging Rijksdienst
   ☐Vergelijkbaar, nl. ……

2. Het voldoen aan de eisen van de informatiebeveiliging blijkt uit (kruis aan wat van toepassing is en voeg deze bij de overeenkomst):
   ☐Certificering
   ☐Periodieke externe controles zoals audits of TPM's op verzoek van verantwoordelijke
   ☐Een Assurance rapport met conclusies over de bevindingen van de auditor
   ☐ISAE 3402 type 2 verklaring en documentatie ter ondersteuning
   ☐Eigen controles

3. Bewerker stelt de volgende documenten ter beschikking waaruit bescherming van persoonsgegevens blijkt (kruis aan wat van toepassing is):
   ☐Certificering
   ☐Een Assurance rapport met conclusies over de bevindingen van de auditor
   ☐ISAE 3402 type 2 verklaring (jaarlijks)
   ☐Service Level Agreement
   ☐Eigen controles, zoals ….

4. Specifieke bepalingen over de bescherming van persoonsgegevens:
   Ingeschakelde subverwerkers

Naam en contactgegevens subverwerker	**KvK-nummer**	**Uitbestede verwerkingen**	**Toepassing**

5. Contactgegevens

Contactpersoon GGD Groningen	Bij Inbreuk in verband met persoonsgegevens ex artikel 4 sub 12 AVG in verband met Persoonsgegevens: FG@ggd.groningen.nl Telefoon: 050-3674000 (vragen naar de functionaris gegevensbescherming
Contactpersoon XXXXXX	Naam: XXXXXX

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

Bijlage C Afspraken betreffende Inbreuk in verband met persoonsgegevens ex artikel 4 sub 12 AVG in verband met Persoonsgegevens

1) Wanneer zich bij Verwerker Inbreuk in verband met persoonsgegevens voordoen in de zin van artikel 4 sub 12 als aangeduid sub ii definitie Inbreuk in verband met persoonsgegevens, dan wel Verwerker daarmee bekend raakt, levert Verwerker de volgende informatie binnen 24 uur aan de Verwerkingsverantwoordelijke.

2) Contactgegevens melder
Naam, functie, emailadres, telefoonnummer

3) Gegevens over het Inbreuk in verband met persoonsgegevens
Geef een samenvatting van de Inbreuk in verband met persoonsgegevens en in hoeverre de beveiliging van de persoonsgegevens in het gedrang is;

4) Van hoeveel personen zijn Persoonsgegevens betrokken bij de inbreuk? (Vul de aantallen in.)
a) Minimaal: (vul aan)
b) Maximaal: (vul aan)

5) Omschrijf de groep mensen van wie Persoonsgegevens zijn betrokken bij de inbreuk;

6) Wanneer vond de inbreuk plaats? (Kies een van de volgende opties en vul waar nodig aan.)
a) Op (datum)
b) Tussen (begindatum periode) en (einddatum periode)
c) Nog niet bekend

7) Wat is de aard van de inbreuk? (U kunt meerdere mogelijkheden aankruisen.)
a) Lezen (vertrouwelijkheid)
b) Kopiëren
c) Veranderen (integriteit)
d) Verwijderen of vernietigen (beschikbaarheid)
e) Diefstal
f) Nog niet bekend

8) Om welk type Persoonsgegevens gaat het? (U kunt meerdere mogelijkheden aankruisen.)
a) Naam -, adres - en woonplaatsgegevens
b) Telefoonnummers
c) E - mailadressen of andere adressen voor elektronische communicatie
d) Toegangs - of identificatiegegevens (bijvoorbeeld inlognaam/wachtwoord of huisarts/ zorggroepnummer)
e) Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)
f) Burgerservicenummer (BSN)
g) Paspoortkopieën of kopieën van andere legitimatiebewijzen

h) Geslacht, geboortedatum en/of leeftijd
i) Bijzondere Persoonsgegevens (bijvoorbeeld ras, etniciteit, criminele gegevens, politieke overtuiging, vakbondslidmaatschap, religie, seksuele leven, gegevens over de gezondheid)
j) Overige gegevens, namelijk (vul aan)

9) Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen?
(U kunt meerdere mogelijkheden aankruisen.)
a) Stigmatisering of uitsluiting
b) Schade aan de gezondheid
c) Blootstelling aan (identiteits)fraude
d) Blootstelling aan spam of phishing
e) Anders, namelijk (vul aan)

10) Vervolgacties naar aanleiding van het Datalek
Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?

11) Technische beschermingsmaatregelen
Zijn de Persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden? (Kies een van de volgende opties en vul waar nodig aan.)
a) Ja
b) Nee
c) Deels, namelijk: (vul aan)

Als de Persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd? (Beantwoord deze vraag als u bij de vorige vraag gekozen heeft voor optie a of optie c. Als u gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen toe.)

12) Internationale aspecten
Heeft de inbreuk betrekking op personen in andere EU-landen? (Kies een van de volgende opties.)
a) Ja
b) Nee
c) Nog niet bekend