Verwerkersovereenkomst

GGD regio Utrecht

Inhoudsopgave

Verwerkersovereenkomst :

Datum :

Contractspartijen:

1. De GGD regio Utrecht, gevestigd en kantoorhoudende aan De Dreef 5, 3706 BR te Zeist, en ingeschreven in het handelsregister onder nummer 50909185 te dezen rechtsgeldig vertegenwoordigd door de Directeur Publieke Gezondheid van GGD regio Utrecht, drs. N. (Nicolette) Rigter, hierna te noemen: **Verwerkingsverantwoordelijke,**

en:

2. [naam] gevestigd te [plaats], en ingeschreven in het handelsregister onder nummer [nummer] te dezen rechtsgeldig vertegenwoordigd door [naam en functie], hierna te noemen: **Verwerker**.

gezamenlijk aan te duiden als: **"Partijen";**

Overwegende dat:
Partijen hebben op_____een Overeenkomst met betrekking tot_____gesloten. Ter uitvoering van onze Overeenkomst worden Persoonsgegevens verwerkt.

Partijen leggen in deze Verwerkersovereenkomst en de daarbij behorende bijlagen:

1. Overzicht met verwerkingen van persoonsgegevens en verwerkingsdoelen
2. Overzicht met beveiligingsmaatregelen
3. Proces rondom het melden van Datalekken en de te verstrekken informatie

vast wat Verwerker wel en niet mag doen met de Persoonsgegevens.

1. Definities:

De hierna en hiervoor gebruikte begrippen volgen uit de Algemene Verordening Gegevensbescherming (EU 2016/679) die vanaf 25 mei 2018 van toepassing is en hebben de volgende betekenis:

1.1 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon

1.2 Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;

1.3 Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen;

1.4 Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;

1.5 Subverwerker: de partij die door de Verwerker wordt ingeschakeld als Verwerker ten behoeve van de Verwerking van de Persoonsgegevens in het kader van deze Verwerkersovereenkomst en het hoofdovereenkomst;

1.6 Betrokkene: geïdentificeerde of identificeerbaar natuurlijk persoon op wie de verwerkte persoonsgegeven betrekking hebben;

1.7 Verwerkersovereenkomst: deze overeenkomst inclusief de bijlagen;

1.8 Overeenkomst: de hoofdovereenkomst waar deze Verwerkersovereenkomst uit voortvloeit;

1.9 Datalek: 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 gegevens;

1.10 Gegevensbeschermingseffectbeoordeling: het uitvoeren van een beoordeling, voorafgaand aan het uitvoeren van de verwerking, van het effect van de beoogde verwerkingsactiviteiten op de bescherming van de persoonsgegevens.

1.11 Toezichthoudende autoriteit: een onafhankelijke overheidsinstantie verantwoordelijk voor het toezicht op de naleving van de wet in verband met de verwerking van Persoonsgegevens. In Nederland is dit de Autoriteit Persoonsgegevens;

2. Totstandkoming, duur en beëindiging van deze Verwerkersovereenkomst

2.1 Deze Verwerkersovereenkomst treedt in werking op de datum waarop Partijen deze ondertekenen.
2.2 Deze Verwerkersovereenkomst is onderdeel van de Overeenkomst en zal gelden voor zolang de Overeenkomst duurt.
2.3 Indien de Overeenkomst eindigt, eindigt deze Verwerkersovereenkomst automatisch; de Verwerkersovereenkomst kan niet apart worden opgezegd.
2.4 Na beëindiging van deze Verwerkersovereenkomst zullen de lopende verplichtingen voor Verwerker, zoals het melden van Datalekken, waarbij de Persoonsgegevens van Verwerkingsverantwoordelijke betrokken zijn, en de plicht tot geheimhouding blijven voortduren.

3. Verwerken Persoonsgegevens

3.1 Verwerker zal alleen Persoonsgegevens verwerken in opdracht van Verwerkingsverantwoordelijke en heeft geen zeggenschap over de Persoonsgegevens. Verwerker volgt instructies hierover op en mag de Persoonsgegevens niet op een andere manier verwerken, tenzij Verwerkingsverantwoordelijke daar van te voren toestemming of opdracht voor geeft.
3.2 In Bijlage 1 wordt opgenomen welke Persoonsgegevens Verwerker precies zal verwerken en voor welke verwerkingsdoeleinden.
3.3 Verwerker houdt zich aan de wet en verwerkt de gegevens op een behoorlijke, zorgvuldige en transparante wijze.
3.4 Verwerker mag zonder voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke geen andere personen of organisaties inschakelen bij het verwerken van de Persoonsgegevens.
3.5 Wanneer Verwerker met toestemming van Verwerkingsverantwoordelijke andere organisaties inschakelt, moeten zij minimaal voldoen aan de eisen die zijn opgenomen in deze Verwerkersovereenkomst.
3.6 Wanneer Verwerkingsverantwoordelijke een verzoek krijg van een Betrokkene die zijn of haar privacy rechten wil uitoefenen, werkt Verwerker daar binnen een termijn van 14 dagen aan mee. Deze rechten bestaan uit een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming, bezwaar maken tegen de verwerking van de persoonsgegevens en een verzoek tot overdraagbaarheid van de eigen Persoonsgegevens.
3.7 Wanneer Verwerkingsverantwoordelijke Verwerker verzoekt om informatie te geven, dan zal hij de informatie verstrekken die Verwerkingsverantwoordelijke nodig heeft voor het uitvoeren van een Gegevensbeschermingseffectbeoordeling. Verwerkingsverantwoordelijke heeft dit nodig om in te kunnen schatten wat het risico van de verwerking is die Verwerker uitvoert.

4. Beveiligen van Persoonsgegevens

4.1 Verwerker zorgt ervoor dat de Persoonsgegevens voldoende zijn beveiligd. Om verlies en onrechtmatige verwerkingen te voorkomen neem hij passende technische en organisatorische maatregelen.
4.2 Deze maatregelen zijn afgestemd op het risico van de verwerking. Een overzicht van deze maatregelen en het beleid daarover neemt Verwerker op in Bijlage 2.
4.3 Ter controle zal Verwerker ieder jaar een rapportage sturen waarin de genomen beveiligingsmaatregelen staan en de eventuele aandachts- en/of verbeterpunten. Hiervoor zal Verwerker aan Verwerkingsverantwoordelijke geen kosten in rekening brengen.
4.4 Verwerkingsverantwoordelijke mag een inspectie of audit in de organisatie van Verwerker laten uitvoeren om te bepalen of het verwerken van de Persoonsgegevens aan de wet en de afspraken uit deze Verwerkersovereenkomst voldoet. Hierbij zal Verwerker medewerking verlenen, waaronder het verstrekken van toegang tot gebouwen en databases en het ter beschikking stellen van alle relevante informatie.
4.5 De kosten voor de uitvoering van deze audit zullen voor rekening van Verwerker komen wanneer blijkt dat Verwerker zich niet aan de verplichtingen in deze Verwerkersovereenkomst houdt.
4.6 De controle op de algehele verwerking van Persoonsgegevens door Verwerker kan, naast de audit mogelijkheid, ook gebeuren via zelfevaluatie. Verwerker zal hierbij aan Verwerkingsverantwoordelijke een rapport verstrekken waarin hij aantoont dat er wordt voldaan aan de wet en de afspraken uit deze Verwerkersovereenkomst. Deze rapportage dient te worden ondertekend door een directielid binnen de organisatie van Verwerker.
4.7 Wanneer Verwerkingsverantwoordelijke of Verwerker vindt dat een wijziging in de te nemen beveiligingsmaatregelen noodzakelijk is, treden Partijen in overleg over de wijziging daarvan. De kosten voor het wijzigen van de beveiligingsmaatregelen komen voor de rekening van degene die de kosten maakt.

5. Exporteren Persoonsgegevens

5.1 Verwerker mag geen Persoonsgegevens laten verwerken door andere personen of organisaties buiten de Europese Economische Ruimte (EER), zonder daarvoor voorafgaande schriftelijke toestemming te hebben verkregen van Verwerkingsverantwoordelijke.

6. Geheimhouding

6.1 Verwerker zal de aan hem verstrekte Persoonsgegevens geheim houden, tenzij dit op basis van een wettelijke verplichting niet mogelijk is.
6.2 Verwerker zal ervoor zorgen dat ook ingeschakelde personeel en hulppersonen zich aan deze geheimhouding houden, door een geheimhoudingsplicht in de (arbeids-) contracten op te nemen.

7. Datalekken

7.1 In geval van een ontdekking van een (mogelijk) Datalek zal Verwerker Verwerkingsverantwoordelijke hierover informeren binnen 24 uur aan de Privacy Officer van Verwerkingsverantwoordelijke via famuradin@ggdru.nl en de informatie verstrekken die is aangegeven in Bijlage 3, zodat Verwerkingsverantwoordelijke indien nodig een melding bij de Toezichthouder kan doen.

7.2 Na de melding van een Datalek, zal de Verwerkingsverantwoordelijke op de hoogte worden gehouden van nieuwe ontwikkelingen rondom het Datalek en de maatregelen die Verwerker heeft getroffen om de omvang van het Datalek te beperken en te beëindigen en een soortgelijk incident in de toekomst te kunnen voorkomen.

7.3 Het niet toegestaan dat Verwerker een melding van een Datalek doet aan de Toezichthouder en ook mag Verwerker de Betrokkenen niet informeren over het Datalek. Dit is de verantwoordelijkheid van Verwerkingsverantwoordelijke.

7.4 Eventuele kosten die gemaakt worden om het Datalek op te lossen en in de toekomst te kunnen voorkomen, komen voor rekening van degene die de kosten maakt.

8. Aansprakelijkheid

8.1 Als Verwerker de verplichtingen uit deze Verwerkersovereenkomst niet nakomt, stelt Verwerkingsverantwoordelijke hem daarvoor aansprakelijk.

8.2 Verwerker is aansprakelijk voor alle schade geleden door het niet nakomen van de wet en de bepalingen uit deze Verwerkersovereenkomst, voor zover dit is ontstaan door zijn werkzaamheden.

8.3 Indien Verwerker de verplichtingen in deze Verwerkersovereenkomst overtreedt, is Verwerker aan Verwerkingsverantwoordelijke een direct opeisbare boete verschuldigd van €50.000,- voor iedere overtreding en €2.500,-. voor iedere dag dat je de overtreding begaat. Daarnaast behoudt Verwerkingsverantwoordelijke het recht om schadevergoeding te vorderen.

8.4 Verwerker is aansprakelijk voor de aan Verwerkingsverantwoordelijke opgelegde bestuurlijke boete door de Toezichthouder als de geleden schade het gevolg is van onrechtmatig of nalatig handelen door Verwerker.

8.5 Verwerkingsverantwoordelijke is niet aansprakelijk voor aanspraken van Betrokkenen of andere personen en organisaties waar Verwerker de samenwerking mee is aangegaan of waarvan Verwerker Persoonsgegevens verwerkt, als dit het gevolg is van onrechtmatig of nalatig handelen van Verwerker.

9. Teruggave Persoonsgegevens en bewaartermijn

9.1 Na het beëindigen van deze Verwerkersovereenkomst geef Verwerker de Persoonsgegevens terug, in een voor de Verantwoordelijke leesbare vorm. Eventuele achter gebleven Persoonsgegevens zullen op een zorgvuldige en veilige manier worden vernietigd.

9.2 De Persoonsgegevens die Verwerker verwerkt volgens deze Verwerkersovereenkomst zullen worden vernietigd na verstrijken van de wettelijke bewaartermijn en/of op verzoek van Verwerkingsverantwoordelijke.

9.3 Verwerker zal na de teruggave en/of vernietiging van de Persoonsgegevens schriftelijk aan Verwerkingsverantwoordelijke verklaren dat hij de Persoonsgegevens niet langer heeft.

10. Slotbepalingen

10.1 Deze Verwerkersovereenkomst is onderdeel van de Overeenkomst. Alle rechten en verplichtingen uit de Overeenkomst zijn daarom ook van toepassing op de Verwerkersovereenkomst.
10.2 Bij eventuele tegenstrijdigheden tussen de bepalingen in de Verwerkersovereenkomst en de Overeenkomst, gelden de bepalingen uit deze Verwerkersovereenkomst.
10.3 Afwijkingen van deze Verwerkersovereenkomst zijn slechts geldig wanneer Partijen dit samen schriftelijk afspreken.
10.4 Op deze Verwerkersovereenkomst en op de werkzaamheden, is het Nederlandse recht van toepassing.
10.5 Over eventuele geschillen tussen ons bepaald de rechter in de rechtbank binnen het gebied waar het bedrijf van Verwerkingsverantwoordelijke gevestigd is.

Aldus door ons overeengekomen en ondertekend

Verantwoordelijke

Ondertekend voor en namens : _____

Naam : _____

Functie : _____

Datum en plaats : _____

Handtekening : _____

Verwerker

Ondertekend voor en namens : _____

Naam : _____

Functie : _____

Datum en plaats : _____

Handtekening : _____

Bijlage 1:

Overzicht met verwerkingen van persoonsgegevens en verwerkingsdoelen

Beschrijving van verwerkingsactiviteiten door Verwerker:	
Categorie(ën) van betrokkenen:	
Soort persoonsgegevens:	
Verwerkte persoonsgegevens:	
Verwerkingsdoelen:	
Verwerkingsverantwoordelijke:	
Verwerker:	
Subverwerkers:	
Locatie verwerkingen:	
Bewaartermijn:	

Bijlage 2:
Overzicht met beveiligingsmaatregelen

Hier moet een overzicht van de beveiligingsnormen opgenomen worden die Verwerker neemt. Denk aan:

Technische beveiligingsmaatregelen

- ☐ Up to date virusscan
- ☐ Beveiligde USB-sticks
- ☐ Accurate beveiliging medewerkerstelefoon
- ☐ Bitlocker toegangsmechanisme
- ☐ Unieke inlogcode en wachtwoord (regelmatig aanpassen)
- ☐ Versleutelde email
- ☐ Geen onbeveiligde externe harde schijven
- ☐ Geen onbeveiligde back ups maken
- ☐ Geen documenten op privé laptop op slaan

Organisatorische beveiligingsmaatregelen

- ☐ Clean desk policy
- ☐ Laptop niet onbemand achterlaten
- ☐ Laptop nooit achterlaten in de auto
- ☐ Privacy screens medewerkers
- ☐ Oude documenten op juiste manier vernietigen
- ☐ Zorgvuldig gebruik van USB-sticks

Bijlage 3:

Proces rondom het melden van Datalekken en de te verstrekken informatie

Verwerker zal alle inlichtingen verschaffen die Verwerkingsverantwoordelijke noodzakelijk acht om het incident te kunnen beoordelen. Daarbij verschaft Verwerker in ieder geval de volgende informatie aan de Verwerkingsverantwoordelijke;

1. **Geef een samenvatting van het beveiligingslek / beveiligingsincident / datalek: wat is er gebeurd?**
   Vermeld hier ook de naam van het betrokken systeem.
2. **Wat is het (vooralsnog bekende en/of te verwachten) gevolg?**
3. **Welke typen persoonsgegevens zijn betrokken bij het beveiligingsincident?**
   Zoals, maar niet beperkt tot, naam, adres, e-mailadres, IP-nummer, Burgerservicenummer, pasfoto en ieder ander tot een persoon te herleiden gegeven.
4. **Van hoeveel personen zijn de persoonsgegevens betrokken bij het beveiligingsincident?**
   Geef een minimum en maximum aantal personen.
5. **Omschrijving groep personen om wiens gegevens het gaat.**
   Bijzondere aandacht verdienen gegevens van een kwetsbare groepen personen, zoals kinderen.
6. **Zijn de contactgegevens van de betrokken personen bekend?**
   Het kan zijn dat betrokkenen geïnformeerd moeten worden over het datalek, kunnen we deze personen in dat geval bereiken?
7. **Wat is de oorzaak (root cause) van het beveiligingsincident?**
8. **Op welke datum of in welke periode heeft het beveiligingsincident plaats kunnen vinden?**
   Geef dit zo specifiek mogelijk aan.
9. **Welke beveiligingsmaatregelen zijn er getroffen na het datalek?**

<u>Waar meld je het beveiligingsincident?</u>
Als een (mogelijk) beveiligingsincident is ontdekt, neem direct contact op met de Privacy Officer:

Faazila Muradin
Privacy Officer
GGD regio Utrecht
E-mail: famuradin@ggdru.nl
Tel: 06-18916577

Functionaris Gegevensbescherming
GGD regio Utrecht
E-mail: fg@ggdru.nl
Tel: 030-6086086