Inhoud

Verwerkersovereenkomst

Contractnummer: […].

De ondergetekenden:

1. De Raad voor Rechtsbijstand, waarvan de zetel is gevestigd te 's-Hertogenbosch,
te dezen vertegenwoordigd door [functienaam en naam ondertekenaar]
hierna te noemen: Opdrachtgever,

en

2. [volledige naam en rechtsvorm contractant],
(statutair) gevestigd te [plaats],
te dezen vertegenwoordigd door
..... *(en .....)* [naam ondertekenaar]
hierna te noemen: Opdrachtnemer,

hierna gezamenlijk te noemen: Partijen;

OVERWEGENDE DAT:

- voor zover Opdrachtnemer Persoonsgegevens verwerkt ten behoeve van Opdrachtgever in het kader van de Overeenkomst, Opdrachtgever krachtens artikel 4, onderdeel 7 en onderdeel 8, van de Algemene Verordening Gegevensbescherming (EU) 2016/679 kwalificeert als Verwerkingsverantwoordelijke voor de Verwerking van Persoonsgegevens en Opdrachtnemer als Verwerker;

- Partijen in deze Verwerkersovereenkomst, zoals bedoeld in artikel 28, derde lid, van de Verordening, hun afspraken over de Verwerking van Persoonsgegevens door Opdrachtnemer wensen vast te leggen.

KOMEN OVEREEN:

Artikel 1. Begrippen

In deze Verwerkersovereenkomst wordt een aantal begrippen met een beginhoofdletter gebruikt. Aan deze begrippen komt de betekenis toe die hieraan wordt gegeven in de Algemene Verordening Gegevensbescherming.

1.1 Betrokkene: de natuurlijke persoon op wie een Persoonsgegeven betrekking heeft.

1.2 Inbreuk in verband met Persoonsgegevens: 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.

1.3 Overeenkomst: de hoofdovereenkomst tussen Opdrachtgever en Opdrachtnemer [titel] van [datum], met kenmerk [kenmerk].

1.4 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, die Opdrachtnemer in het kader van de Overeenkomst ten behoeve van Opdrachtgever verwerkt.

1.5 Verordening: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van de Richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming).

1.6 Verwerkersovereenkomst: deze overeenkomst inclusief overwegingen en bijbehorende bijlagen.

1.7 Verwerking: een bewerking of een geheel van bewerkingen in het kader van de Overeenkomst 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, verspreiding of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Artikel 2. Voorwerp van deze Verwerkersovereenkomst

2.1 Deze Verwerkersovereenkomst regelt de Verwerking van Persoonsgegevens door Opdrachtnemer in het kader van de Overeenkomst.

2.2 De aard en het doel van de Verwerking, het soort Persoonsgegevens en de categorieën van Persoonsgegevens, Betrokkenen en ontvangers zijn in Bijlage 1 omschreven.

2.3 Opdrachtnemer garandeert de toepassing van passende technische en organisatorische maatregelen, opdat de Verwerking aan de vereisten van de Verordening voldoet en de bescherming van de rechten van de Betrokkene is gewaarborgd.

2.4 Opdrachtnemer garandeert te voldoen aan de vereisten van de toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

Artikel 3. Inwerkingtreding en duur

3.1 Deze Verwerkersovereenkomst treedt in werking op het moment waarop deze door Partijen is ondertekend.

3.2 Deze Verwerkersovereenkomst eindigt nadat en voor zover Opdrachtnemer alle Persoonsgegevens overeenkomstig artikel 10 heeft gewist of terugbezorgd.

3.3 Geen van Partijen kan deze Verwerkersovereenkomst tussentijds opzeggen.

3.4 Bij beëindiging van deze overeenkomst:
a. Blijven lopende verplichtingen gelden (o.a. Geheimhouding (artikel 6), Meldplicht datalekken (artikel 9);
b. Werkt Opdrachtnemer mee aan de adequate overdracht van werkzaamheden aan een opvolgende Opdrachtnemer.

Artikel 4. Omvang verwerkingsbevoegdheid Opdrachtnemer

4.1 Opdrachtnemer Verwerkt de Persoonsgegevens uitsluitend in opdracht en op basis van schriftelijke instructies van Opdrachtgever behoudens afwijkende wettelijke voorschriften die op Opdrachtnemer van toepassing zijn.

4.2 Indien een instructie als bedoeld in het eerste lid naar het oordeel van Opdrachtnemer in strijd is met een wettelijk voorschrift inzake gegevensbescherming, stelt hij Opdrachtgever daarvan voorafgaand aan de Verwerking in kennis, tenzij een wettelijk voorschrift deze kennisgeving verbiedt.

4.3 Indien Opdrachtnemer op grond van een wettelijk voorschrift Persoonsgegevens dient te verstrekken, informeert hij Opdrachtgever onmiddellijk, en zo mogelijk voorafgaand aan de verstrekking.

4.4 Opdrachtnemer heeft geen zeggenschap over het doel van en de middelen voor de Verwerking van Persoonsgegevens.

Artikel 5. Beveiliging van de Verwerking

5.1 Onverminderd artikel 2.3 treft Opdrachtnemer de technische en organisatorische beveiligingsmaatregelen naar de stand van techniek zoals beschreven in Bijlage 2.

5.2 Partijen erkennen dat het waarborgen van een passend beveiligingsniveau voortdurend kan dwingen tot het treffen van aanvullende beveiligingsmaatregelen. Opdrachtnemer waarborgt een op het risico afgestemd beveiligingsniveau.

5.3 Indien en voor zover Opdrachtgever daarom uitdrukkelijk schriftelijk verzoekt, zal Opdrachtnemer aanvullende maatregelen treffen met het oog op de beveiliging van de Persoonsgegevens.

5.4 Opdrachtnemer Verwerkt Persoonsgegevens niet buiten de Europese Unie, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming heeft verkregen van Opdrachtgever en behoudens afwijkende wettelijke verplichtingen.

5.5 Opdrachtnemer informeert Opdrachtgever onmiddellijk zodra hij kennis heeft genomen van onrechtmatige Verwerkingen van Persoonsgegevens of inbreuken op beveiligingsmaatregelen zoals

genoemd in het eerste en tweede lid. Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zodra (gedeeltelijk) bekend, in stappen worden verstrekt.

5.6 Opdrachtnemer verleent Opdrachtgever bijstand bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36 van de Verordening.

Artikel 6. Geheimhouding door personeel van Opdrachtnemer

6.1 De Persoonsgegevens hebben een vertrouwelijk karakter als bedoeld in de op deze overeenkomst van toepassing zijnde Algemene Voorwaarden van Opdrachtgever.

6.2 Opdrachtnemer toont op verzoek van Opdrachtgever aan dat zijn Personeel zich ertoe heeft verbonden vertrouwelijkheid in acht te nemen als bedoeld in de op deze overeenkomst van toepassing zijnde Algemene Voorwaarden van Opdrachtgever.

Artikel 7. Subverwerkers

7.1 Opdrachtnemer schakelt geen andere personen of organisaties in voor de Verwerking, tenzij Opdrachtgever daarmee schriftelijk instemt. Aan de toestemming kan hij voorwaarden verbinden. Opdrachtgever onthoudt deze toestemming niet op onredelijke gronden.

7.2 Stemt Opdrachtgever in met de inzet van andere personen of organisaties, dan sluit Opdrachtnemer met deze subverwerkers overeenkomsten met daarin dezelfde verplichtingen inzake gegevensbescherming als die in deze Verwerkersovereenkomst zijn opgenomen.

7.3 Als subverwerkers hun verplichtingen voor beveiliging niet nakomen, blijft Opdrachtnemer volledig aansprakelijk voor eventuele schade.

Artikel 8. Bijstand vanwege rechten van Betrokkene

Opdrachtnemer verleent Opdrachtgever bijstand bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III van de Verordening vastgelegde rechten van de Betrokkene te beantwoorden.

Artikel 9. Inbreuk in verband met Persoonsgegevens

9.1 Opdrachtnemer informeert Opdrachtgever onmiddellijk, zodra hij kennis heeft genomen van een Inbreuk in verband met Persoonsgegevens, overeenkomstig de afspraken zoals vastgelegd in Bijlage 3. Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zodra (gedeeltelijk) bekend, in stappen worden verstrekt.

9.2 Opdrachtnemer informeert Opdrachtgever ook na een melding op grond van het eerste lid over ontwikkelingen betreffende de Inbreuk in verband met Persoonsgegevens.

9.3 Partijen dragen elk de door henzelf in verband met de melding aan de bevoegde toezichthoudende autoriteit en Betrokkene te maken kosten.

Artikel 10. Retourneren of verwijderen Persoonsgegevens

10.1 Na afloop van de Overeenkomst draagt Opdrachtnemer, naar gelang de keuze van Opdrachtgever, zorg voor het retourneren aan Opdrachtgever en/of het verwijderen van alle Persoonsgegevens. Opdrachtnemer verwijdert kopieën, behoudens afwijkende wettelijke

voorschriften. De Persoonsgegevens worden als volgt geretourneerd: [bestandsformaat] [wijze] [adres].

10.2 Opdrachtnemer [verwijdert en/of retourneert] de Persoonsgegevens binnen [aantal] [dagen/weken] na afloop van de Overeenkomst, bij gebreke waarvan Opdrachtnemer een onmiddellijk opeisbare boete verschuldigd is van 10% van de opdrachtwaarde, met een minimum van € 1.000,-. Per dag dat de overtreding voortduurt verbeurt Opdrachtnemer een boete van € 1.000,- met een maximum van € 50.000,-. Voor de opeisbaarheid van deze boete(s) is geen ingebrekestelling vereist en geldt onverminderd enig ander aan Opdrachtgever toekomend recht, waaronder het recht op volledige schadevergoeding.

Artikel 11. Informatieverplichting en audit

11.1 Opdrachtnemer stelt alle informatie ter beschikking die nodig is om aan te tonen dat de verplichtingen uit deze Verwerkersovereenkomst zijn en worden nagekomen.

11.2 Opdrachtnemer verleent alle benodigde medewerking aan audits.

11.3 ***<OPTIONEEL>*** Opdrachtgever ~~laat~~ kan eenmaal per […] een audit laten uitvoeren door een onafhankelijke partij.

OF

11.3 ***<OPTIONEEL>*** Opdrachtnemer verstrekt met een frequentie van eenmaal per […], uiterlijk op [datum(s)] aan Opdrachtgever een verklaring van een onafhankelijke externe deskundige, waarin deze een oordeel geeft over de genoemde naleving.

Artikel 12. Toepasselijk recht en geschillenbeslechting

12.1 De Verwerkersovereenkomst en de uitvoering daarvan worden beheerst door het Nederlands recht.

12.2 Eventuele geschillen die tussen Partijen ontstaan, verband houdende met deze Verwerkersovereenkomst, worden voorgelegd aan de bevoegde rechter voor het arrondissement waarin de Verwerkingsverantwoordelijke gevestigd is.

Artikel 13. Slotbepalingen

13.1 Deze Verwerkersovereenkomst maakt onderdeel uit van de Overeenkomst. Alle rechten en verplichtingen uit de Overeenkomst zijn daarom ook van toepassing op de Verwerkersovereenkomst.

13.2 Bij eventuele tegenstrijdigheden tussen de bepalingen in de Verwerkersovereenkomst en de Overeenkomst, gelden de bepalingen uit deze Verwerkersovereenkomst ten aanzien van de verwerking van Persoonsgegevens.

13.3 Afwijkingen van deze Verwerkersovereenkomst zijn slechts geldig wanneer Partijen dit samen schriftelijk afspreken.

Aldus op de laatste van de twee hierna genoemde data overeengekomen en in tweevoud ondertekend,

's-Hertogenbosch, [datum] [Plaats], [datum]

[functienaam en naam ondertekenaar] [naam Opdrachtnemer]

namens deze,
[functienaam ondertekenaar]

[naam ondertekenaar] [functie en naam ondertekenaar]

Bijlage 1. De Verwerking van Persoonsgegevens

In deze bijlage moet in ieder geval het volgende worden gespecificeerd:

Het onderwerp/aard van de Verwerking	
Het doel van de Verwerking	
Verwerkte Persoonsgegevens:	
Beschrijving categorieën Persoonsgegevens	
Beschrijving categorieën Betrokkenen	
Beschrijving categorieën ontvangers van Persoonsgegevens	
Subverwerkers	
Locatie verwerkingen	
Bewaartermijn	
Doorgifte	Niet van toepassing / Indien van toepassing benoem hier ook het doorgifte instrument:

Bijlage 2. IB maatregelen

Toelichting
Met deze checklist betreffende het vaststellen van passende technische en organisatorische maatregelen wordt invulling gegeven aan de wettelijke bepalingen uit artikel 32 en 35 van de AVG. Deze bijlage is bedoeld om vast te stellen in hoeverre vastgestelde normen inzake verwerking van persoonsgegevens zijn getroffen en in hoeverre deze passend zijn. In de onderstaande tabel zijn vastgestelde normen weergegeven. Deze bijlage bevat onderdelen die moeten worden nagelopen a.d.h.v. een risico gebaseerde benadering. De partijen worden geacht eventuele restrisico's te vermelden. In onderstaande tabel wordt aangeven of de onderdelen aantoonbaar gedocumenteerd zijn of welke restrisico's aanwezig zijn.

I. Informatiebeveiligingsnorm

Verwerker toont aan dat het niveau van informatiebeveiliging toereikend is. Dit blijkt uit.

		Aanwezig	**Toelichting**	**N.v.t.**
	Zijn ISO certificeringen aanwezig of andere relevante certificeringen?	ISO 27001 ISAE 3402 Anders, nl.		
	Wat is de scope van de ISO certificering of andere relevante certificeringen?			
	Tot wanneer is de hiervoor bedoelde certificering geldig?			
	Indien u beschikt over de hiervoor bedoelde certificering(en), graag de gepubliceerde vindplaats dan wel bewijs als bijlage toevoegen.			

Indien in Deel I de toereikendheid niet wordt aangetoond, moet Deel II worden ingevuld.

II. Organisatorische en technische beveiligingsmaatregelen
(geef aan wat van toepassing is)

A	**Beleid**	**Aanwezig**	**Niet aanwezig/ toelichting**	**N.v.t.**
	Is er een Informatiebeveiligingsbeleid?			
	Is er een Privacybeleid?			
	Is er beleid over beveiligingsincidenten/datalekken?			
	Is er beleid over continuïteit van de informatievoorziening/dienstverlening?			
	Is er beleid voor gebruik van bedrijfslaptops/telefoons/telewerken?			
B	**Organisatie**			
	Kan een in control verklaring informatiebeveiliging worden overlegd? Is er zicht op mogelijke kwetsbaarheden in systemen / netwerkbeveiliging en hoe wordt dit beheerd?			
	Heeft uw organisatie Informatiebeveiligingspersoneel in dienst (zoals een CISO)?			
	Heeft het personeel een VOG? Is geheimhouding opgenomen in contracten van personeel?			

C	**Risicomanagement**			
	Vinden er periodieke risico-assessments plaats op het gebied van informatiebeveiliging?			
	Vinden er periodieke risico-assessments plaats op het gebied van privacy?			
D	**Toegang**			
	Bestaat er een autorisatieproces voor toegang tot systemen, informatie, gebouwen, werkruimten en speciale zones zodat medewerkers slechts toegang krijgen tot de voor hen relevante onderdelen en gegevens (logische toegangsbeveiliging)?			
	Vind er logging plaats? Wat wordt gelogd?			
	Is er een Auditmechanisme beschikbaar in de organisatie ?			
	Vind er periodieke controle /monitoring plaats op toegekende toegang ?			
	Is Multifactor Authenticatie toegepast?			
	Beschikt de organisatie over Back-up & Recovery (t.b.v. Business Continuity) ? Waar is de backup opgeslagen en hoe is deze beveiligd?			
F	**Beveiligingsmaatregelen**			
	Is er sprake van beveiligde elektronische uitwisseling van gegevens, minimaal door encryptie en andere vormen van beveiliging, waarbij uitlekken van gegevens wordt gesignaleerd en gegevens niet direct leesbaar zijn voor derden?			
	Worden gegevens enkel verstrekt vanuit en naar een beveiligd domein?			
	Bestaat Bescherming tegen malware, tegen inbraak en andere vormen van ontvreemding van informatie zodanig dat inbraakpogingen onmiddellijk worden gesignaleerd en de vertraging van inbraak afdoende is om diefstal van informatie te voorkomen, ook in geval van mobiele werkplekken?			
	Zijn er beschreven interne procedures opdat gegevens niet onbedoeld in handen van derden kunnen vallen ?			
	Zijn er beschreven interne procedures over omgang met externe media en beheer en gebruik daarvan.			
	Zijn er voor uitschakeling van de beveiliging zijn specifieke procedures ingericht die ongecontroleerd uitschakelen onmogelijk maken?			
G	**Overige**			
	Awareness training op gebied van Privacy en Informatiebeveiliging.			

	Voldoen ook leveranciers van de leverancier (subverwerkers) aan alle maatregelen waarbij hierboven 'ja' is aangegeven, en zijn hier afspraken over gemaakt?			

Bijlage 3. Afspraken betreffende Inbreuken in verband met Persoonsgegevens

Meld het (vermoedelijke) datalek onmiddellijk, maar uiterlijk binnen 24 uur na kennisneming van het Datalek. Dit kan via de e-mail aan privacy@rvr.org of telefonisch op telefoonnummer: 088-7871001.

Gebruik hiervoor bij voorkeur de onderstaande vragenlijst.

Beantwoording op de onderstaande vragen

Kunt u in ieder geval de volgende vragen zo volledig mogelijk en schriftelijk beantwoorden.

1. Geef een samenvatting van het beveiligingsincident/datalek (hierna: datalek): wat is er gebeurd? Vermeld hier ook de naam van het betrokken systeem.

2. Welke typen Persoonsgegevens zijn betrokken bij het mogelijke datalek?
   Zoals, maar niet beperkt tot, naam, adres, e-mailadres, telefoonnummer, IP-nummer, Burgerservicenummer, en ieder ander tot een persoon te herleiden gegeven.

3. Van hoeveel personen zijn de Persoonsgegevens betrokken bij het datalek?
   Geef a.u.b. een minimum en maximum aantal personen.

4. Kunt u een omschrijving geven van de groep personen om wiens gegevens het gaat.
   Geef aan of het gaat om medewerkersgegevens, gegevens van klanten, gegevens van internetgebruikers.

5. Zijn de contactgegevens van de betrokken personen bekend?
   Als de beoordeling uitwijst dat de Betrokkenen geïnformeerd moeten worden over het datalek hebben wij de contactgegevens nodig. Dit is het geval als het datalek waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Wij zullen u in dat geval vragen u de namen van de Betrokkenen die verband houden met het datalek te verstrekken.

6. Wat is de oorzaak van het Datalek?
   Heeft u een idee hoe het Datalek heeft kunnen ontstaan?

7. Wat zijn de waarschijnlijke gevolgen van het Datalek.
   Zoals, maar niet beperkt tot, onbevoegde toegang, misbruik van gegevens, wegvallen van essentiële dienst aan betrokkene, reputatieschade of stigmatisering.

8. Op welke datum of in welke periode heeft het Datalek plaats kunnen vinden?
   Geef dit a.u.b. zo specifiek mogelijk aan.

9. Welke maatregelen stelt u voor of heeft u al genomen om het Datalek aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan?

10. De naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen.