

Ondergetekenden

Het College van Burgemeester en Wethouders van de gemeente Baarn, verder te noemen de verwerkingsverantwoordelijke, hierbij rechtsgeldig vertegenwoordigd door,

En

< naam organisatie> , verder te noemen Verwerker, hierbij rechtsgeldig vertegenwoordigd door <naam, functie>,

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

Overwegen het volgende:

- a) Partijen op _____, hierna Hoofdovereenkomst, hebben afgesloten, op grond waarvan Verwerker de volgende dienst(en) levert aan de Verwerkingsverantwoordelijke;
- 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 van toepassing;
- d) Partijen willen in aanvulling op de AVG en de Uitvoeringswet AVG de volgende afspraken over de verwerking van Persoonsgegevens vastleggen in deze Verwerkersovereenkomst.

Artikel 1. Definities

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

Artikel 2. Ingangsdatum en duur van de overeenkomst

- 2.1 Deze verwerkersovereenkomst gaat in op het moment van ondertekening en geldt zolang de Hoofdovereenkomst van kracht is, of zolang nog niet is voldaan aan de eisen van artikel 7.1 van deze verwerkersovereenkomst.

Artikel 3. Onderwerp van de overeenkomst

- 3.1 Verwerker verwerkt de door of via Verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens uitsluitend in opdracht van Verwerkingsverantwoordelijke voor de uitvoering van de Hoofdovereenkomst, behalve als wettelijke verplichtingen of bindende uitspraken van bevoegde organen, anders bepalen.
- 3.2 De door Verwerker uit te voeren verwerkingen staan in Bijlage 1, die Verwerker met behulp van Verwerkingsverantwoordelijke invult.

Artikel 4. Verwerker

- 4.1 Verwerker moet zorgen voor passende technische en organisatorische maatregelen om de gegevens goed te beveiligen, zoals bedoeld in artikel 32 AVG. Verwerker toont dit aan in Bijlage 2.
- 4.2 Verwerker mag niets beslissen over de persoonsgegevens die hij heeft ontvangen voor de uitvoering van de Hoofdovereenkomst. Zo neemt hij geen beslissingen over de ontvangst en het gebruik van deze gegevens, de verstrekking aan derden en de duur van de opslag van gegevens. Verwerker verwerkt gegevens alleen volgens de schriftelijke instructies van verwerkingsverantwoordelijke.
- 4.3 Personen die werken voor Verwerker, en Verwerker zelf, moeten de Persoonsgegevens waarmee zij werken geheimhouden, behalve als er een wettelijke uitzondering is. De personen die werken voor Verwerker hebben daarom een geheimhoudingsverklaring getekend. De geheimhouding geldt ook nog na afloop van deze Verwerkersovereenkomst.
- 4.4 Verwerker mag - met toestemming van Verwerkingsverantwoordelijke - voor de uitvoering van de werkzaamheden een andere verwerker inschakelen. Verwerker laat voor de ingangsdatum aan Verwerkingsverantwoordelijke weten wie de andere ingeschakelde verwerkers zijn. Verwerker vult daarvoor tabel 3 van Bijlage 1 in en houdt deze actueel. Verwerkingsverantwoordelijke is bevoegd om binnen 30 dagen tegen deze verandering bezwaar te maken. Verwerker draagt er zorg voor dat de betreffende derde tenminste dezelfde verplichtingen op zich neemt als genomen door Verwerker in deze overeenkomst.
- 4.5 Als Betrokkene een beroep doet op zijn rechten (o.a. inzage, correctie, verwijdering), helpt Verwerker Verantwoordelijke om daarop binnen de wettelijke termijnen een beslissing te nemen.
- 4.6 Verwerker zal aan verwerkingsverantwoordelijke alle noodzakelijke medewerking verlenen als Verwerkingsverantwoordelijke een gegevensbeschermingseffectbeoordeling, of een audit wil (laten) uitvoeren of noodzakelijke informatie nodig heeft en de hulp van Verwerker daarbij nodig heeft

Artikel 5. Inbreuk in verband met Persoonsgegevens

- 5.1 Verwerker zal Verwerkingsverantwoordelijke zo snel mogelijk, maar uiterlijk 48 uur na ontdekking van een inbreuk in verband met persoonsgegevens, hierover informeren. Daarbij versterkt Verwerker zonder onredelijke vertraging alle noodzakelijke informatie, medewerking en toegang aan Verwerkingsverantwoordelijke, zodat laatstgenoemde de Inbreuk op tijd kan melden aan de Autoriteit Persoonsgegevens en/of Betrokkene overeenkomstig de AVG.
- 5.2 In geval van een Inbreuk neemt Verwerker zo snel mogelijk alle maatregelen om de Inbreuk te herstellen, de gevolgen van de inbreuk te beperken en verdere inbreuken te voorkomen.
- 5.3 Verwerker heeft een gedegen plan van aanpak over de omgang met en de afhandeling van Inbreuken en zal Verwerkingsverantwoordelijke, op zijn verzoek, dat plan laten zien (bijlage 4).
- 5.4 Verwerker heeft een gedetailleerd logboek van alle Inbreuken en de maatregelen die op Inbreuken zijn genomen. Verwerkingsverantwoordelijke mag dat inzien, wanneer deze daarom vraagt.
- 5.5 Verwerkingsverantwoordelijke beslist of deze de Inbreuk moet melden bij de toezichthoudende autoriteit en/of Betrokkene.

Artikel 6. Aansprakelijkheid

- 6.1 De Partij die toerekenbaar tekortschiet in de nakoming van zijn verplichtingen, is tegenover de andere Partij aansprakelijk voor de door deze geleden en/of te lijden schade.
- 6.2 De aansprakelijkheid van verwerker is beperkt tot het verzekerde bedrag, van minimaal EUR 1.000.000,-- per gebeurtenis.
- 6.3 De verwerker is voldoende verzekerd en verstrekt op verzoek de polis aan de gemeente.
- 6.4 Bij gebreke van voldoende dekking of uitkering is de aansprakelijkheid beperkt tot 4 maal de contractwaarde, waarbij de aansprakelijkheid nooit meer bedraagt dan € 5.000.000,-

Artikel 7. Beëindigen verwerkersovereenkomst

- 7.1 Na afloop van de werkzaamheden, zal Verwerker op verzoek van Verwerkingsverantwoordelijke de ter beschikking gestelde persoonsgegevens aan Verwerkingsverantwoordelijke teruggeven en/of vernietigen.
- 7.2 Verwerkingsverantwoordelijke kan nadere redelijke eisen stellen aan de wijze van beschikbaarstelling, waaronder eisen aan het bestandsformaat, dan wel vernietiging. Deze werkzaamheden moeten, binnen een nader overeen te komen redelijke termijn, uitgevoerd worden.
- 7.3 Verwerker maakt hiervan een verslag en geeft dit Verwerkersverantwoordelijke.

Artikel 8. Overige bepalingen

- 8.1 Alle geschillen, ook als alleen één Partij vindt dat er een geschil is, zullen in eerste instantie worden voorgelegd aan de bevoegde rechter van de Rechtbank Midden-Nederland
- 8.2 Alle rechten en verplichtingen uit de Hoofdovereenkomst, waaronder begrepen de van toepassing zijnde algemene voorwaarden, zijn voor het overige aanvullend van toepassing op de verwerking van Persoonsgegevens

Ondertekening

Aldus in tweevoud opgesteld,

Gemeente <naam gemeente>
namens deze:<naam, functie>
plaats: <.....>

<Naam organisatie>
namens deze: <naam, functie>
plaats: <.....>

Bijlage 1: Overzicht van te verwerken persoonsgegevens

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

Naam verwerking	Verwerkingsdoeleinden	Categorieën van betrokkenen	(Bijzondere) Persoonsgegevens	Doorgifte naar derde landen

2. Contactgegevens

Contactpersoon Verwerkingsverantwoordelijke (NB: Ook buiten kantooruren)	Naam: < > Contactgegevens:
Contactpersoon Verwerker (NB: Ook buitenkantooruren)	Naam: Contactgegevens:
Contactgegevens IBD	Telefoonnummer: 070-373 8011

3. Ingeschakelde subverwerkers

Naam subverwerker	Contactgegevens subverwerker	Uitbestede verwerkingen
Geen		

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

Bijlage 2: Aantonen passend niveau van beveiliging

1. Normenstelsel

☐ De informatiebeveiliging vindt plaats volgens algemeen erkende normen, namelijk:

.....

.....(vermeld normenstelsel, zoals bijvoorbeeld NEN7510, NEN/ISO 27001, PCI/DSS).

☐ De informatiebeveiliging vindt plaats volgens een algemeen erkende overheidsnorm zoals de BIG (of de BIR, BIO) of vergelijkbaar, namelijk:

.....

2. De toereikendheid van de informatiebeveiliging blijkt uit:

☐ Periodieke externe controles zoals audits of TPM's (bijv. ISAE3xxx SOC type II);

☐ Een Assurance rapport van een auditor die is aangesloten bij NOREA;

☐ Data Pro Certificaat

☐ Eigen controles of eigen mededelingen over de beveiligingsmaatregelen zoals hieronder beschreven:

.....

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

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