

**Bijlage 8 –
Concept Verwerkersovereenkomst
Verduurzamen woningen
Gemeente Zaanstad**

Kenmerk: 2026-403

Verwerkersovereenkomst

Verduurzamen woningen Gemeente Zaanstad

Kenmerk: 2026-403

Gemeente Zaanstad, waarvan <XXhet college van Burgemeester en Wethouders/de Gemeenteraad> de verwerkingsverantwoordelijke is, verder te noemen Verwerkingsverantwoordelijke, hierbij rechtsgeldig vertegenwoordigd door de <XXheer of mevrouw> <persoonsnaam>, <functie>

en

<BedrijfXX>, gevestigd te <plaatsnaam>, KVK-nummer <nummer> verder te noemen Verwerker, hierbij rechtsgeldig vertegenwoordigd door de <de heer of mevrouw>, <persoonsnaam> , <functie> ,

hierna afzonderlijk te noemen "Partij", of gezamenlijk "Partijen"

Overwogen het volgende:

- a) Partijen hebben op <datum> een Overeenkomst, hierna Hoofdovereenkomst, afgesloten, op grond waarvan Verwerker de volgende diensten levert aan de Verwerkingsverantwoordelijke: zoals dit is beschreven in de Hoofdovereenkomst Verduurzamen woningen Gemeente Zaanstad met Kenmerk: 2026-403;
- 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 (UAVG) van toepassing;
- d) Partijen willen in aanvulling op de AVG en de UAVG de volgende afspraken over de verwerking van Persoonsgegevens vastleggen in deze verwerkersovereenkomst (hierna: de Verwerkersovereenkomst);

En komen het volgende overeen:

Artikel 1 Definities

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

Artikel 2 Ingangsdatum en duur

- 2.1 Deze Verwerkersovereenkomst gaat in op het moment dat de Hoofdovereenkomst tot stand is gekomen, tenzij Partijen anders overeenkomen.
- 2.2 Deze Verwerkersovereenkomst eindigt op het moment dat Verwerker de verwerking van Persoonsgegevens op grond van de Hoofdovereenkomst heeft beëindigd en de afspraken over het teruggeven en/of wissen van Persoonsgegevens zijn nagekomen.
- 2.3 Wanneer Partijen een (nieuwe) Verwerkersovereenkomst overeenkomen, betekent dat dat de oude Verwerkersovereenkomst komt te vervallen.

Artikel 3 Onderwerp van deze Verwerkersovereenkomst

- 3.1 Verwerker verwerkt de door of via Verwerkingsverantwoordelijke ter beschikking gestelde Persoonsgegevens uitsluitend in opdracht van Verwerkingsverantwoordelijke voor de uitvoering van de Hoofdovereenkomst en uitsluitend overeenkomstig schriftelijke instructies van Verwerkingsverantwoordelijke, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke wettelijke bepaling hem tot verwerking verplicht. In dat geval zal Verwerker Verwerkingsverantwoordelijke, voorafgaand aan de verwerking, daarvan zonder onredelijke vertraging in kennis stellen, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.
- 3.2 De door Verwerker uit te voeren verwerkingen staan beschreven in tabel 1 van Bijlage 1.

Artikel 4 Inhoudelijke afspraken

4.1 Beveiligingsmaatregelen

Verwerker zorgt voor passende technische en organisatorische maatregelen om de Persoonsgegevens goed te beveiligen, zoals bedoeld in artikel 32 AVG. De wijze waarop Verwerker de passende technische en organisatorische maatregelen aantoont, staat in Bijlage 2.

4.2 Audits

Verwerker verleent alle benodigde medewerking aan audits uitgevoerd door een gecertificeerde auditor over de nakoming van de afspraken binnen deze Verwerkersovereenkomst en Bijlagen, tenzij Verwerker door middel van een geldige certificering, die periodiek door een geaccrediteerde instelling wordt getoetst, heeft aangetoond dat Verwerker de gemaakte afspraken nakomt. De kosten van deze audit worden gedragen door Verwerkingsverantwoordelijke (zowel eigen kosten als kosten van Verwerker), tenzij de auditor één of meer tekortkomingen van niet ondergeschikte aard van Verwerker constateert die ten nadele zijn van Verwerkingsverantwoordelijke.

4.3 Verwerking buiten de EER

Verwerker mag Persoonsgegevens buiten de Europese Economische Ruimte (laten) verwerken wanneer is voldaan aan de voorwaarden van artikel 45 of 46 AVG. Wanneer er sprake is van een verwerking buiten de EER, dan stelt Verwerker Verwerkingsverantwoordelijke daarvan vooraf op de hoogte.

4.4 Geheimhouding

Personen die werken voor (sub)Verwerker en (sub)Verwerker zelf, moeten Persoonsgegevens waarmee zij werken geheimhouden. De personen die werken voor Verwerker en subverwerkers hebben daarom een geheimhoudingsverklaring getekend, of zich op een andere manier schriftelijk gebonden aan de geheimhouding.

4.5 Subverwerkers

De ten tijde van het afsluiten van deze Verwerkersovereenkomst bekende subverwerkers vermeldt Verwerker in tabel 3 van Bijlage 1. Verwerkingsverantwoordelijke verleent hierbij algemene toestemming voor de inschakeling van subverwerkers. Verwerker houdt na de start van de werkzaamheden Verwerkingsverantwoordelijke op de hoogte van de beoogde inschakeling van nieuwe subverwerkers. Bij de inschakeling van subverwerkers blijven de artikelen 28.2 en 28.4 AVG onverkort van kracht.

4.6 Rechten van betrokkenen

Als een betrokkene een beroep doet op zijn rechten zoals genoemd in artikel 12 t/m 22 AVG, helpt Verwerker Verwerkingsverantwoordelijke om daarop binnen de wettelijke termijnen een beslissing te nemen.

4.7 Gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging

Op verzoek van Verwerkingsverantwoordelijke werkt Verwerker altijd mee aan een gegevensbeschermingseffectbeoordeling (DPIA) en een voorafgaande raadpleging als bedoeld in artikel 35 en 36 AVG.

Artikel 5 Inbreuk in verband met Persoonsgegevens

5.1 Verwerker zal Verwerkingsverantwoordelijke zonder onredelijke vertraging, maar uiterlijk binnen 24 uur, informeren na vaststelling van een (vermoedelijke) Inbreuk in verband met Persoonsgegevens. Verwerker vermeldt hierbij voor zover bekend de vermeende oorzaak van de (vermoedelijke) Inbreuk, de categorie persoonsgegevens, de categorie betrokkenen en het aantal betrokkenen.

5.2 In geval van een Inbreuk neemt Verwerker zonder onredelijke vertraging alle maatregelen om de Inbreuk te herstellen, de gevolgen daarvan te beperken en verdere Inbreuken te voorkomen en houdt de Verwerkingsverantwoordelijke hiervan voortdurend op de hoogte.

5.3 Verwerker heeft een gedetailleerd logboek van de Inbreuken en de maatregelen die op Inbreuken zijn genomen. Verwerkingsverantwoordelijke mag dat inzien, wanneer deze daarom vraagt.

5.4 Verwerkingsverantwoordelijke beslist of de Inbreuk moet worden gemeld bij de toezichthoudende autoriteit en/of Betrokkene. Verwerker ondersteunt de Verwerkingsverantwoordelijke waar nodig bij de melding aan de toezichthoudende autoriteit en/of Betrokkene.

Artikel 6 Aansprakelijkheid

- 6.1 Eventuele in de Hoofdovereenkomst overeengekomen beperkingen van de aansprakelijkheid hebben ook betrekking op de Verwerkersovereenkomst.

Artikel 7 Beëindigen verwerkersovereenkomst

- 7.1 Partijen moeten in de Hoofdovereenkomst afspraken maken over de beëindiging van de Hoofdovereenkomst en de daaruit voortvloeiende teruggave en wissing van Persoonsgegevens.
- 7.2 De geheimhouding geldt ook nog na beëindiging van deze Verwerkersovereenkomst.

Artikel 8 Overige bepalingen

- 8.1 Op deze overeenkomst is Nederlands recht van toepassing. Alle geschillen, ook als alleen één Partij vindt dat er een geschil is, zullen in eerste instantie worden voorgelegd aan dezelfde bevoegde rechter als genoemd in de Hoofdovereenkomst.

Ondertekening

Aldus overeengekomen en in tweevoud ondertekend,

Ingangsdatum: <XX.....>

Gemeente Zaanstad

De burgemeester van Gemeente Zaanstad

namens deze: <XXnaam, functie>

plaats: <.....>

datum: <.....>

<Naam organisatieXX>

namens deze: <XXnaam, functie>

plaats: <.....>

datum: <.....>

Bijlage 1: Overzicht van te verwerken persoonsgegevens, contactgegevens partijen en overzicht ingeschakelde subverwerkers

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

Naam verwerking/Welke dienst en/of product	Verwerkings-doeleinden	Categorieën van Betrokkenen	(Bijzondere) Persoonsgegevens	Verwerkings-locatie	Doorgifte-instrument (indien van toepassing)	Aanvullende maatregelen (indien van toepassing)

2. Contactgegevens

Contactpersoon Verwerkingsverantwoordelijke (NB: Ook buiten kantooruren)	Naam: Contactgegevens:
Contactpersoon Verwerker (NB: Ook buiten kantooruren)	Naam: Contactgegevens:
Contactgegevens Gemeente Zaanstad	telefoonnummer: XXX e-mailadres : privacy@zaanstad.nl

3. Ingeschakelde subverwerkers

Naam en contactgegevens subverwerker	KvK-nummer	Uitbestede verwerkingen	Toepassing (geautomatiseerd systeem)	Verwerkings-locatie	Doorgifte-instrument	Aanvullende maatregelen (indien van toepassing)

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

Bijlage 2: Aantonen passend niveau van beveiliging

Normenstelsel

- ☐ De verwerker werkt volgens een algemeen erkende norm voor informatiebeveiliging, te weten: (vermeld normenstelsel, zoals bijvoorbeeld NEN7510, NEN/ISO 27001, PCI/DSS) en is volgens deze norm wel/niet gecertificeerd.
 - ☐ Datum laatste certificering:
- ☐ De verwerker werkt volgens een algemeen erkende overheidsnorm zoals de BIO2, of vergelijkbaar, te weten:
- ☐ De verwerker werkt volgens een andere norm, te weten:

Toereikendheid

De toereikendheid van de informatiebeveiliging blijkt uit het volgende:

- ☐ Verwerker verstrekt een actueel en geldig certificaat en verklaring van toepasselijkheid (VVT);
- ☐ Rapportages van periodieke externe controles zoals audits, pentesten of TPM's (bijv. ISAE3xxx SOC type II);
- ☐ Een assurance rapport (TPM) van een auditor die is aangesloten bij NOREA;
- ☐ Eigen controles of eigen mededelingen over de beveiligingsmaatregelen zoals hieronder beschreven (in lijn met de aanpak uit hoofdstuk 4.4 uit de BIO2, een ICV):

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

Aansluiting bij goedgekeurde gedragscode

- ☐ Verwerker is aangesloten bij een door een toezichthoudende autoriteit goedgekeurde gedragscode, te weten

NB: Substantiële wijzigingen in het bovenstaande en achteruitgang van de voorwaarden geven partijen op korte termijn aan elkaar door.

Toelichting bijlagen

Bijlage 1:

De verwerker vult bijlage 1 in. Als deze daarbij hulp nodig heeft, kan de verwerker de hulp inroepen van de verwerkingsverantwoordelijke.

Tabel 1: In het eerste deel wordt ingevuld:

- Welke verwerking: zie hiervoor: <https://www.informatiebeveiligingsdienst.nl/product/vooringevuld-verwerkingsregister-gemeenten/> Zie onder Kolom 'H'.
- Verwerkingsdoeleinden, zie hiervoor: <https://www.informatiebeveiligingsdienst.nl/product/vooringevuld-verwerkingsregister-gemeenten/> Zie onder Kolom 'L'.
- Categorieën van betrokkenen: dit zijn voorbeelden van categorieën van betrokkenen:
 - Aanvragers/Indieners
 - Belanghebbenden
 - Bestuurders/Raadsleden
 - Ambtenaren gemeente
 - Websitebezoekers
 - Personeel leveranciers
 - Scholieren
 - Studenten
 - Ouderen
 - Gehandicapten
 - Kinderen
- Categorieën persoonsgegevens: dit zijn voorbeelden van categorieën persoonsgegevens:

Arbeidsgegevens	Functie, werktijden
Beeldmateriaal	Videomateriaal, audiomateriaal
Contactgegevens	e-mailadres, telefoonnummer, adres
Identiteitsgegevens	Identificatienr., paspoortnr., BTW nummer ZZP-er
Inloggegevens	Gebruikersnaam, wachtwoord
Internetgegevens	IP-adres, online surfgedrag, cookies
Locatiegegevens	Lengtegraad, breedtegraad
Persoonlijke gegevens	Naam, geboortedatum, geboorteplaats, geslacht, gezinssamenstelling

Bijzondere en gevoelige persoonsgegevens

Biometrische gegevens met het oog op de unieke identificatie van een persoon
BSN
Financiële gegevens
Genetische gegevens
Gezondheidsgegevens
Lidmaatschap van een vakbond
Politieke opvattingen
Ras of etnische afkomst
Religieuze of levensbeschouwelijke overtuigingen
Seksueel gedrag of seksuele gerichtheid
Strafrechtelijke persoonsgegevens

Verwerkingslocatie

Het moet duidelijk zijn waar de verwerking plaatsvindt. Als persoonsgegevens worden doorgegeven naar (of toegankelijk zijn in) een land buiten de EER moet dat hier ook worden aangegeven.

Doorgifte-instrument

Als er sprake is van een verwerking buiten de EER moet aangegeven worden welk doorgifte-instrument wordt gebruikt. De mogelijke doorgifte-instrumenten zijn:

1. Adequaatheidsbesluit;
2. Specifieke uitzonderingen (art. 49);
3. Standaard bepalingen (standard contractual clauses SCCs);
4. Bindende bedrijfsvoorschriften (binding corporate rules, BCRs);
5. Gedragsregels (codes of conduct; certification mechanisms);
6. Ad hoc modelcontractbepalingen (ad hoc contractual clauses).

Aanvullende maatregelen

- Indien gebruik wordt gemaakt van doorgifte-instrumenten 3 t/m 6 worden, conform de aanbevelingen van de EDPB (Recommendations 01/2020), aanvullende technische, organisatorische en contractuele maatregelen getroffen om een aan de AVG gelijkwaardig beschermingsniveau te waarborgen.
- De aanvullende maatregelen worden vastgesteld op basis van een risicoafweging, rekening houdend met de aard van de persoonsgegevens, de verwerkingsactiviteiten en het derde land. Hiermee wordt beoogd een beschermingsniveau te realiseren dat materieel gelijkwaardig is aan het beschermingsniveau binnen de EER.
- Technische maatregelen (voorbeelden)
 - Encryptie van persoonsgegevens tijdens opslag en overdracht
 - Beheer van encryptiesleutels binnen de EER
 - Toegangsbeperkingen op basis van need-to-know en/of least privilege
 - Logging en monitoring van toegang tot persoonsgegevens
 - Logische scheiding van gegevens
 - Pseudonimisering of anonimisering waar mogelijk
- Organisatorische maatregelen (voorbeelden)
 - Beleidsregels die toegang vanuit derde landen beperken
 - Training en bewustwording van medewerkers
 - Procedures voor beoordeling en afhandeling van verzoeken van buitenlandse autoriteiten
 - Incident- en datalekprocedures gericht op internationale doorgifte
- Contractuele maatregelen (voorbeelden)
 - Verwerking uitsluitend op schriftelijke instructie van de verwerkingsverantwoordelijke
 - Informatieplicht bij verzoeken van buitenlandse autoriteiten, voor zover wettelijk toegestaan
 - Verplichting tot juridische toetsing en betwisting van dergelijke verzoeken
 - Beperking van verdere doorgifte aan (sub)verwerkers
 - Audit- en controlebevoegdheden voor de verwerkingsverantwoordelijke

Hieronder een voorbeeld :

Naam verwerking/W elke dienst en/of product	Verwerking s- doeleinden	Categorieën van betrokkenen	(Bijzondere) persoonsgegevens	Verwerking s-locatie	Doorgifte instrument (indien van toepassing)	Aanvullend e maatregelen (indien van toepassing)

Tabel 2: hier wordt ingevuld:

- Wie zijn (ook buiten kantooruren!) de contactpersonen van de verwerkingsverantwoordelijke, de verwerker en de IBD. Zorg voor een gemeentelijk e-mailadres dat niet wijzigt als de gemeentelijke contactpersoon niet meer in dienst is. Dus bijvoorbeeld: privacy@naamgemeente.nl.
- In het geval er meerdere gemeenten bij het incident zijn betrokken, informeren partijen ook de IBD. De IBD is telefonisch 24 uur per dag bereikbaar. De mail van de IBD wordt niet 24 uur per dag gelezen.

Tabel 3:

- Indien er sprake is van een of meerdere subverwerkers, dan vult de verwerker de tabel voor iedere subverwerker met de volgende gegevens:
 - **de naam en de contactgegevens subverwerker:** Vermeld de volledige handelsnaam van de subverwerker en relevante contactgegevens;
 - **het Kvk-nummer**
 - **Uitbestede verwerkingen:** Hier wordt aangegeven welke categorieën van verwerkingen de subverwerker uitvoert. De verwerker selecteert uitsluitend de categorieën die feitelijk van toepassing zijn. Onderstaande categorieën zijn juridisch herleidbaar tot artikel 4, lid 2 AVG. Categorieën uitbestede verwerkingen:
 - Opslaan en hosten van persoonsgegevens: Hieronder valt het vastleggen en opslaan van persoonsgegevens, ongeacht de vorm (digitaal of fysiek). Dit betreft onder meer opslag op servers, databases, archieven of andere opslagmedia.
 - Beschikbaar stellen van persoonsgegevens ten behoeve van uitvoering van diensten: Hieronder valt het raadplegen en gebruiken van persoonsgegevens zodat de dienstverlening aan de verwerkingsverantwoordelijke kan worden uitgevoerd, bijvoorbeeld inzage, verwerking of weergave van gegevens.
 - Technisch, organisatorisch of operationeel beheer met mogelijke toegang tot persoonsgegevens: Hieronder valt beheer waarbij toegang tot persoonsgegevens mogelijk is, zoals onderhoud, ondersteuning, kwaliteitscontrole, beveiliging of incidentafhandeling. Dit kan zowel geautomatiseerd als handmatig plaatsvinden.
 - Vastleggen, wijzigen of actualiseren van persoonsgegevens: Hieronder valt het bijwerken, corrigeren of aanvullen van persoonsgegevens op instructie van de verwerkingsverantwoordelijke.
 - Ordenen, structureren of combineren van persoonsgegevens: Hieronder valt het structureren, rubriceren, koppelen of anderszins organiseren van persoonsgegevens ten behoeve van de overeengekomen dienstverlening.
 - Back-ups, herstel en continuïteitsvoorzieningen: Hieronder vallen het maken van back-ups, het bewaren daarvan, en het herstellen van persoonsgegevens bij incidenten of calamiteiten.
 - Verstrekken of ter beschikking stellen van persoonsgegevens: Hieronder valt het doorgeven of beschikbaar stellen van persoonsgegevens aan de verwerkingsverantwoordelijke of, indien toegestaan, aan andere partijen op instructie van de verwerkingsverantwoordelijke.
 - Afschermen, beveiligen en beperken van toegang tot persoonsgegevens: Hieronder vallen beveiligingsmaatregelen zoals toegangsbeperkingen, autorisaties, logging en monitoring.
 - Verwijderen en vernietigen van persoonsgegevens: Hieronder valt het wissen of vernietigen van persoonsgegevens na beëindiging van de dienstverlening of op instructie van de verwerkingsverantwoordelijke.
 - **Toepassing (geautomatiseerd systeem)**
Vermeld het systeem, de applicatie of de omgeving waarin de uitbestede verwerkingen plaatsvinden. Dit kan zowel een geautomatiseerd systeem als een fysieke of hybride omgeving zijn.
 - **Verwerkingslocatie**
Vermeld het land of de landen waar de verwerking feitelijk plaatsvindt. Indien persoonsgegevens worden doorgegeven aan of toegankelijk zijn vanuit landen buiten de EER, moet dit expliciet worden vermeld.
 - **Doorgifte instrument**
Zie toelichting bij Bijlage 1 tabel 1
 - **Aanvullende maatregelen**
Zie toelichting bij Bijlage 1 tabel 1

Voorbeeld

4. Ingeschakelde subverwerkers

Naam en contactgegevens subverwerker	KvK-nummer	Uitbestede verwerkingen	Toepassing (geautomatiseerd systeem)	Verwerkingslocatie	Doorgifte instrument	Aanvullende maatregelen (indien van toepassing)
		•				

--	--	--	--	--	--	--

Bijlage 2:

Bijlage 2 is een praktische uitwerking van artikel 32 AVG. Dus verwerker moet hier aangeven welke passende technische en organisatorische maatregelen hij heeft genomen die een op het risico afgestemd beveiligingsniveau waarborgen. Dus de verwerker geeft aan welk normenstelsel hij voldoet, hoe de toereikendheid van de informatiebeveiliging is gewaarborgd. In dat kader kan verwerker aangeven of hij is aangesloten bij een door de AP goedgekeurde gedragscode.

Normenstelsel: Hier wordt een keuze gemaakt voor het normenstelsel dat van toepassing is op de verwerking waarover de overeenkomst wordt afgesloten. Dit is bij voorkeur de BIO2 maar, indien verwerker kan aantonen dat hij voldoet aan een andere vergelijkbare norm, kan die hier ook worden ingevuld om de punten 1 en 2 van deze bijlage met elkaar in één lijn te brengen.

Toereikendheid: Omdat het onder de AVG belangrijk is om te kunnen aantonen dat de verwerking voldoet aan de afgesproken eisen over een niveau van beveiliging dat past bij de verwerking, wordt hier aangegeven hoe een verwerker dit kan aantonen. Hierbij zijn diverse mogelijkheden aan te kruisen. Waar relevant verstrekt¹ Verwerker bewijsstukken (zoals een geldig certificaat, verklaring van toepasselijkheid en andere bewijsstukken) waaruit blijkt dat wordt voldaan aan opgegeven normen, certificeringen, etc. Tenzij het zonder meer verstrekken de informatieveiligheid van Verwerker ernstig verlaagt.

Het is aan de verwerkingsverantwoordelijke om te beoordelen of deze verantwoording voldoende is voor de betreffende verwerking en ook aan verwerker om actief te controleren of aan deze paragraaf van de bijlage gevolg wordt gegeven. Voor meer informatie over hoe je kunt bepalen of een certificaat valide is, kunt u de IBD factsheet over [assurance](#) lezen.

Verder kan de verwerker aangeven of deze is aangesloten bij een goedgekeurde gedragscode.

¹ Hardcopy, via de mail, of via een link.