Modelovereenkomst Gegevensuitwisseling tussen Zelfstandige Verwerkingsverantwoordelijken op grond van uitvoering <naam uitvoering wettelijke regeling/Hoofdovereenkomst>

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

en

<Naam organisatie>, gevestigd te <plaatsnaam>, KVK-nummer <nummer> Verwerkingsverantwoordelijke, hierbij rechtsgeldig vertegenwoordigd door de <de heer of mevrouw>, <persoonsnaam>, <functie>,

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

Overwegen het volgende:

a) Partijen <maak keuze: voeren beide op grond van <naam wettelijke regeling> taken uit of <hebben op <datum> de <titel hoofdovereenkomst>, hierna naam Hoofdovereenkomst/, afgesloten>,
b) Partijen zullen ter uitvoering van de hiervoor vermelde <taken/afspraken> Persoonsgegevens verwerken;
c) Op de verwerking van Persoonsgegevens door Partijen zijn de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG) van toepassing;
d) Partijen zijn ieder Verwerkingsverantwoordelijke als bedoeld in artikel 4, aanhef en onder 7, AVG voor de verwerkingen die zij uitvoeren;
e) Partijen stellen vast dat zij beide ieder voor zich verwerkingsverantwoordelijke zijn voor hun eigen deel van de verwerking, als bedoeld in artikel 3.2 van deze overeenkomst.
f) Partijen willen in aanvulling op de AVG en de UAVG de volgende afspraken vastleggen over de verwerking van Persoonsgegevens;

Artikel 1 Definities

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

Artikel 2 Ingangsdatum en duur

2.1 Deze overeenkomst gaat in op het moment dat de Hoofdovereenkomst tot stand is gekomen, tenzij Partijen anders overeenkomen.
2.2 Deze overeenkomst eindigt op het moment dat Partijen de verwerking van Persoonsgegevens hebben beëindigd.

Artikel 3 Onderwerp van deze Overeenkomst

3.1 Partijen verwerken de door of via Partijen ter beschikking gestelde Persoonsgegevens uitsluitend voor de uitvoering van de hierboven genoemde <Hoofdovereenkomst> en daarmee voor <doel> .
3.2 Iedere Partij vult de door haar uit te voeren leveringen aan de andere Partij in tabel 1 van Bijlage 1 in.

Artikel 4 Inhoudelijke afspraken

4.1 **Beveiligingsmaatregelen**
Partijen zorgen ervoor dat passende technische en organisatorische maatregelen worden genomen om de Persoonsgegevens goed te beveiligen ten aanzien van de levering van Persoonsgegevens, overeenkomstig artikel 32 AVG. Deze maatregelen garanderen een passend beveiligingsniveau bij de verwerkingen genoemd in Bijlage 1..

4.2 **Geheimhouding**
Personen die werken voor Partijen moeten Persoonsgegevens waarmee zij werken geheimhouden. De personen die werken voor Partijen en eventueel ingeschakelde derden hebben daarom een geheimhoudingsverklaring getekend, of zich op een andere manier schriftelijk gebonden aan de geheimhouding.

4.3 **Verwerkers**
Partijen houden - indien van toepassing - bij welke verwerkers zijn ingeschakeld bij de uitwisseling van de Persoonsgegevens.

4.4 **Rechten van betrokkenen**
Als Betrokkene een beroep doet op zijn rechten, zoals genoemd in artikel 12 t/m 22 AVG, kan deze zich richten tot de Partij die Verwerkingsverantwoordelijke is voor de desbetreffende verwerking (zie Bijlage 1). Mocht een Betrokkene zich tot de verkeerde Verwerkingsverantwoordelijke richten, dan zorgt de Partij die het verzoek ontvangt, dat dit verzoek naar de juiste Partij wordt verzonden. Partijen zullen elkaar zo nodig redelijkerwijs ondersteunen bij het tijdig afhandelen van de hierboven genoemde verzoeken.

4.5 **Gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging**
Op verzoek van een Partij werkt de andere Partij 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 tijdens de uitwisseling

5.1 Partijen zullen elkaar dan over en weer zo snel mogelijk, maar uiterlijk binnen 24 uur, informeren na vaststelling van een (vermoedelijke) Inbreuk in verband met Persoonsgegevens. Partijen vermelden 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 nemen Partijen zonder onredelijke vertraging alle maatregelen om de Inbreuk te herstellen, de gevolgen daarvan te beperken en verdere Inbreuken te voorkomen.

5.3 Partijen maken na een geconstateerde Inbreuk afspraken over welke Partij de melding doet bij de toezichthoudende autoriteit en/of de Betrokkene(n).

Artikel 6 Beëindigen Overeenkomst

6.1 Partijen maken - indien noodzakelijk - in de Hoofdovereenkomst afspraken over de teruggave en wissing van Persoonsgegevens.

6.2 De geheimhouding geldt ook nog na beëindiging van deze Overeenkomst.

Artikel 7 Overige bepalingen

7.1 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 de bevoegde rechter. Partijen kunnen onderling ook zelf vooraf en bevoegde rechter aanwijzen (forumkeuze).

7.2 Deze Overeenkomst maakt onlosmakelijk deel uit van de Hoofdovereenkomst.

Ondertekening
Aldus overeengekomen en ondertekend,

Ingangsdatum: <……>

Gemeente Oisterwijk
namens deze: <naam, functie>

plaats: Oisterwijk

datum: <……>

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

plaats: <……>

datum: <……>

Bijlage 1: Overzicht van te verwerken persoonsgegevens

1. **Iedere Partij vult de cyclus van de levering van Persoonsgegevens in.**

   Levering/verstrekking van persoonsgegevens, doeleinden categorieën van betrokkenen, soort persoonsgegevens en eventuele doorgifte naar derde landen.

Verstrekking/ levering	**Verwerkings-doeleinden**	**Grondslag**	**Categorieën van Betrokkenen**	**Categorieën Persoons-gegevens (waaronder bijzondere persoons-gegevens)**	**Doorgifte naar derde landen**	**Doorgifte-instrument**	**Aanvullende maatregelen (indien van toepassing)**
Toelichting: aangeven dat het om de leveringen van A->B en van B->A gaat							

2. Contactgegevens Gemeente Oisterwijk

Contactpersoon Verwerkingsverantwoordelijke (NB: Ook buiten kantooruren)	Naam: Contactgegevens:
Functionaris Gegevensbescherming (FG)	Naam: Ingrid Blazer Contactgegevens: fg@goirle.nl tel: 06 53 73 46 70
Privacy en Security Officer (PO)	Naam: Julia Pawlik Contactgegevens: j.pawlik@hilvarenbeek.n; tel: 013 50 58 344
Privacy en Security Officer (PO)	Naam Xander Hendrickx Contactgegevens: x.hendrickx@hilvarenbeek.nl tel: 013 50 58 324
Chief Information Security Officer (CISO)	Naam: Marco de Bruin Contactgegevens: marco.de.bruin@goirle.nl tel: 013 70 20 801

Contactgegevens <naam Partij>

Contactpersoon Verwerkingsverantwoordelijke (NB: Ook buiten kantooruren)	Naam: Contactgegevens:

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

Bijlage 2: Aantonen passend niveau van beveiliging

NB: Iedere Partij vult Bijlage 2 in voor de verwerkingen waar de partij verantwoordelijk is.

Gemeente Oisterwijk

□ Verwerkingsverantwoordelijke werkt volgens een algemeen erkende overheidsnorm, te weten: Baseline Informatiebeveiliging Overheid (BIO).

Toereikendheid
De toereikendheid van de informatiebeveiliging blijkt uit het volgende:

- Verklaring van toepasselijkheid (VVT): ENSIA/BIO verantwoording
- Rapportages van periodieke externe controles zoals audits, pentesten, TPM's en ISAE-rapport.
- Een assurance rapport van een auditor die is aangesloten bij NOREA;
- Eigen controles of eigen mededelingen over de beveiligingsmaatregelen in de vorm van een rapportage aan de horizontale en verticale toezichthouders.

NB: 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.

Naam wederpartij

□ De verwerkingsverantwoordelijke 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.

□ De verwerkingsverantwoordelijke werkt volgens een algemeen erkende overheidsnorm zoals de BIO, of vergelijkbaar, te weten:
……..,

□ De verwerkingsverantwoordelijke werkt volgens een andere norm, te weten:
……..

Toereikendheid
De toereikendheid van de informatiebeveiliging blijkt uit het volgende:

□ Certificering 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 BIO, een ICV):
……

NB: 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.

Aansluiting bij goedgekeurde gedragscode
□ Verwerkingsverantwoordelijke is aangesloten bij een door een toezichthoudende autoriteit goedgekeurde gedragscode, te weten
……

Bijlage 3: Inlichtingen om incidenten te beoordelen ter uitwerking van art. 5

Datalekprocedure Gemeente Oisterwijk
De wederpartij zal alle inlichtingen verschaffen die de gemeente noodzakelijk acht om het incident te kunnen beoordelen. Daarbij verschaft de wederpartij in ieder geval de volgende informatie:

- Wat de (vermeende) oorzaak is van de inbreuk;
- Wat het (vooralsnog bekende en/of te verwachten) gevolg is;
- Wat de (voorgestelde) oplossing is;
- Contactgegevens voor de opvolging van de melding;
- Aantal personen waarvan gegevens betrokken zijn bij de inbreuk (indien geen exact aantal bekend is: het minimale en maximale aantal personen waarvan gegevens betrokken zijn bij de inbreuk);
- Een omschrijving van de groep personen van wie gegevens betrokken zijn bij de inbreuk;
- Het soort of de soorten persoonsgegevens die betrokken zijn bij de inbreuk;
- De datum waarop de inbreuk heeft plaatsgevonden (indien geen exacte datum bekend is: De periode waarbinnen de inbreuk heeft plaatsgevonden);
- De datum en het tijdstip waarop de inbreuk bekend is geworden bij wederpartij of bij een door hem ingeschakelde derde of onderaannemer;
- Of de gegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk zijn gemaakt voor onbevoegden;
- Wat de reeds ondernomen maatregelen zijn om de inbreuk te beëindigen en om de gevolgen van de inbreuk te beperken.

Datalekken / incidenten dienen gemeld te worden via het emailadres: datalek@oisterwijk.nl