Bijlage 3 Afspraken voor Privacy & Informatiebeveiliging

1. Overzicht te bewerken persoonsgegevens & contact functionaris

Naam verwerking/ Welke dienst en/of product	Verwerkings-doeleinden	Categorieën van betrokkenen	(Bijzondere) persoons gegevens	Aanvullende Beschermings Maatregelen	Contact Func - tionaris

2. Aantonen passend niveau van beveiliging

Normenstelsel

□ De zelfstandig verwerkigsverantwoordelijke werkt volgens een algemeen erkende norm voor informatiebeveiliging, te weten:

…….. (vermeld normenstelsel, zoals bijvoorbeeld BIO 2.0/ISO 27001, ISO 9001, Blik op Werk) en is volgens deze norm wel/niet gecertificeerd.

o Kopie Datum laatste certificering: …….

De beveiligingsmaatregelen sluiten aan bij de **Baseline Informatiebeveiliging Overheid (BIO 2.0)**, ten minste op het voor de gemeentelijke keten vastgestelde Baseline-niveau (BBN2). Dit omvat onder meer:

- **Multi-Factor Authenticatie (MFA)** voor alle systemen waarin cliëntgegevens worden verwerkt.
- **Versleuteling (Encryption)** van persoonsgegevens, zowel tijdens transport (*in transit*, via TLS 1.3) als tijdens opslag (*at rest*).
- **Logische toegangsbeveiliging** op basis van het *need-to-know* principe.

□ De zelfstandig verwerkingsverantwoordelijke werkt volgens ISO9001

……..

□ De zelfstandig verwerkingsverantwoordelijke werkt volgens het Keurmerk Blik op werk

……..

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

Toereikendheid

De toereikendheid van de informatiebeveiliging blijkt uit het volgende:

□ Zelfstandig verwerkingsverantwoordelijek verstrekt een actueel en geldig certificaat en verklaring van toepasselijkheid (VVT);

□ 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/NOLOC;
□ 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.

□ Zelfstandig verwerkingsverantwoordelijke is aangesloten bij een door een toezichthoudende autoriteit goedgekeurde gedragscode, te weten: