INFORMATIE
BEVEILIGINGS
DIENST

VNG Realisatie

Standaard Verwerkersovereenkomst Gemeenten

Verwerkersovereenkomst uitvoering <naam hoofdovereenkomst>

Gemeente <naam gemeente>, 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

<Bedrijf>, 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”

Overwegen het volgende:

a) Partijen hebben op <datum> de <titel hoofdovereenkomst>, hierna Hoofdovereenkomst, afgesloten, op grond waarvan Verwerker de volgende dienst(en) levert aan de Verwerkingsverantwoordelijke: <specificatie dienst(en)>;
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: <……>

Gemeente <naam gemeente>	**<Naam organisatie>**
De burgemeester van <naam gemeente>	
namens deze: <naam, functie>	namens deze: <naam, functie>
plaats: <……>	plaats: <……>
datum: <……>	datum: <……>

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

Verwerkingsverantwoordelijke laat Verwerker werkzaamheden verrichten. Als onderdeel van deze werkzaamheden kunnen gegevens van personen verwerkt worden. In deze bijlage is vastgelegd welke (categorieën van) persoonsgegevens van welke categorieën van Betrokkenen worden verwerkt, welke werkzaamheden Verwerker in dat kader voor Verwerkingsverantwoordelijke uitvoert en wat de verwerkingslocatie is. Voor zover van toepassing worden ook aanvullende maatregelen beschreven.

Deze bijlage is mede afhankelijk van (toekomstige) wijziging van functionaliteit van de Standaardprogrammatuur Stratech Perspectief Cloud en wijzigingen die het gevolg zijn van besluiten van de gemeente als Verwerkingsverantwoordelijk die (mede) betrekking hebben op de in deze bijlage vermelde gegevens welke daardoor kunnen wijzigingen.

De informatie in deze bijlage heeft betrekking op de Standaardprogrammatuur Stratech Perspectief Cloud.

Versiebeheer

DATUM	WIJZIGING
03-10-2024	Eerste versie.
12-03-2025	Subverwerkers van Interaction Next B.V. toegevoegd.
25-03-2025	Aanpassing wegens ISO norm transitie naar NEN-EN-ISO/IEC 27001:2023/A1:2024 nl en Verklaring van toepasselijkheid (VVT versie 2.2 van 24-02-2025).
08-05-2025	Bijlage 1 verder ingevuld.
14-10-2025	Wijziging naam subverwerker Interaction Next BV naar Xential BV
11-11-2025	Verwerking ‘Analyses’ verwijderd.
15-04-2026	Koppeling BI toegevoegd; Koppeling DataExport toegevoegd; Koppeling DDAS toegevoegd; Koppeling KvK (StUF NHR) toegevoegd; Koppeling VISH toegevoegd.

Betrokkenen (artikel 30 lid 1 sub c AVG)
Verwerkingsverantwoordelijke verwerkt gegevens waaronder persoonsgegevens van onderstaande categorieën van betrokkenen:

- Aanvragers (ook wel aangeduid als cliënten of schuldenaren);
- Partner(s) en kind(eren) van aanvragers;
- Schuldeisers.

Eventuele wijzigingen van categorieën van betrokkenen geven partijen op korte termijn aan elkaar door.

Persoonsgegevens (artikel 30 lid 1 sub c AVG)
Verwerkingsverantwoordelijke verwerkt gegevens van personen die afzonderlijk of gecombineerd redelijkerwijs een natuurlijk persoon identificeren (identificerende persoonsgegevens) en aanvullende (categorieën van) persoonsgegevens die betrekking hebben op de natuurlijk persoon.
Verwerkingsverantwoordelijke maakt daarvoor gebruik van de ICT Prestatie Stratech Perspectief Cloud.
Het betreft onderstaande (categorieën van) (persoons)gegevens betreffende:

- cliënten
  - persoonlijke gegevens;
  - contactgegevens;
  - financiële gegevens;
  - bijzondere persoonsgegevens:

- BSN[1].

- gebruikers
  - persoonlijke gegevens;
  - contactgegevens;
  - gelogde gegevens.

Eventuele wijzigingen van (categorieën van) persoonsgegevens geven partijen op korte termijn aan elkaar door.

Verwerkingsverantwoordelijke legt alleen (categorieën van) persoonsgegevens vast ten behoeve van de hiervoor genoemde categorieën van betrokkenen.

Verwerkingen (artikel 30 lid 2 sub b)
Verwerker verricht namens Verwerkingsverantwoordelijk de volgende categorieën van verwerkingen:

1. Dienstverlening op Afstand
   Dit betreft tot het hosten behorende beheerwerkzaamheden waarbij persoonsgegevens in de SaaS omgeving van Verwerker staan.
2. Interfacing
   Dit betreft geautomatiseerde verwerkingen vanuit de SaaS omgeving van Verwerker waarbij persoonsgegevens worden uitgewisseld (ontvangen of doorgezonden) met systemen van derden. De verantwoordelijkheid van verwerker ziet uitsluitend op door haar ontvangen persoonsgegevens die aan haar zijn doorgezonden en niet op persoonsgegevens die door verwerker zijn doorgezonden naar verwerkingsverantwoordelijke en/of derden, niet zijnde subverwerker(s).
3. Gebruikersondersteuning
   Dit betreft werkzaamheden in het kader van het voorkomen en opsporen van onvolkomenheden in de ICT Prestatie die door een (servicedesk) medewerker van Verwerker, vanaf locatie van Verwerker, worden uitgevoerd en waarbij de medewerker toegang heeft tot persoonsgegevens.
4. Implementatie diensten
   Dit betreft veelal implementatie diensten of andere werkzaamheden die door (een consultant van) Verwerker worden uitgevoerd en waarbij de medewerker (remote) toegang heeft tot persoonsgegevens.

Verwerkingslocatie
Verwerkingen door Verwerker vinden plaats binnen de EER. Er wordt daarom geen gebruik gemaakt van doorgifte-instrumenten. Verwerkingsverantwoordelijke laat Verwerker geen verwerking uitvoeren waarbij sprake is van doorgiften van persoonsgegevens aan een derde land of internationale organisatie.

Aanvullende maatregelen
Indien vanaf locatie van Verwerker op locatie van Verwerkingsverantwoordelijke werkzaamheden worden uitgevoerd door Verwerker, wordt dit gedaan via TeamViewer.

Contactgegevens (artikel 30 lid 2 sub a AVG)
De contactgegevens zijn opgenomen in de bijlage “DAP Stratech Perspectief Cloud” (hierna DAP) welke deel uitmaakt van de Overeenkomst.

Subverwerkers
Naam: Microsoft Corporation
KvK: (geen)
Contactgegevens: One Microsoft Place, South County Business Park, Carmanhall And Leopardstown, Dublin, D18 P521, Ierland
Verwerkingen: (beheer)werkzaamheden ten behoeve van de infrastructuur waarop de Standaardprogrammatuur Stratech Perspectief Cloud beschikbaar wordt gesteld
Toepassing: Azure diensten
Verwerkingslocatie: EER

[1] Wanneer daar een wettelijke basis voor is.

Doorgifte-instrument: Niet van toepassing
Aanvullende maatregelen: Niet van toepassing

Naam: Xential B.V.
KvK: 54466237
Contactgegevens: Oranjestraat 10, 7451 CC Holten
Verwerkingen: (beheer)werkzaamheden ten behoeve van de infrastructuur waarop de Derdenprogrammatuur Xential NGX beschikbaar wordt gesteld
Toepassing: Derdenprogrammatuur Xential NGX
Verwerkingslocatie: EER
Doorgifte-instrument: Niet van toepassing
Aanvullende maatregelen: Niet van toepassing
Subverwerkers van Xential B.V.: Amazon Web Services en ACC ICT

Naam: Isabel NV
KvK: -
Contactgegevens: Boulevard de l'Impératrice 13-15, Keizerinlaan 1000 Brussel
Verwerkingen: (beheer)werkzaamheden ten behoeve van betalingsverkeer
Toepassing: Ponto Connect
Verwerkingslocatie: EER
Doorgifte-instrument: Niet van toepassing
Aanvullende maatregelen: Niet van toepassing
Subverwerkers van Isabel NV: Amazon Web Services

Interfaces
Onderstaande opsomming biedt per interface een overzicht van de mogelijkheden tot uitwisseling van persoonsgegevens en is mede bedoeld als informatie om Verwerkingsverantwoordelijke te ondersteunen bij het beoordelen van zijn verantwoordelijkheden.

ONDERDEEL	BESCHRIJVING
Bestandsuitwisseling Client en Relaties	Stratech Perspectief Cloud verstrekt bestanden aan cliënten en relaties door middel van een e-mail met een uniek gegenereerde link en bijbehorend wachtwoord. De bestanden blijven versleuteld op de server totdat de relatie of cliënt het document heeft gedownload of de downloadlink is verlopen.
Koppeling BI	De Koppeling BI-API biedt de mogelijkheid om eenmaal per dag gegevens uit Stratech Perspectief Cloud te ontsluiten. Voor gegevensuitwisseling wordt de FSC-standaard gehanteerd. De gegevens zijn inhoudelijk gelijk aan de DDAS-informatie-uitwisseling met het CBS, waarbij clientgegevens geanonimiseerd zijn.

ONDERDEEL	BESCHRIJVING
Koppeling BKR (CKI)	Met de Koppeling BKR kunnen cliënten worden getoetst en kunnen kredieten en schuldregelingen worden geregistreerd in het Centraal Krediet Informatiesysteem (CKI). De volgende verwerkingen zijn mogelijk: • Toetsen CKI • Doortoetsen • Aanmelden contract bij het BKR • Afmelden contract bij het BKR • Registreren mutaties in de gegevens van het contract • Verwerken registraties De verbinding tussen Stratech Perspectief Cloud en het BKR is beveiligd volgens de door BKR vereiste normen, waarbij per deelnemer een client-side certificaat nodig is.
Koppeling BRP (StUF-BG)	Met de Koppeling BRP is het mogelijk gegevens, waaronder persoonsgegevens, op te halen uit de Basisregistratie Personen (BRP) en deze op te slaan in Stratech Perspectief Cloud. Het ophalen en actualiseren van gegevens uit de BRP verloopt via een gegevensmakelaar op basis van de standaard StUF-BG 3.10. Enkele algemene kenmerken van deze koppeling zijn: • Het ophalen van de (persoons)gegevens begint wanneer er een nieuw traject wordt aangemaakt. Op basis van het BSN- wordt het BRP-systeem bevraagd. • Per cliënt wordt een afnemersindicatie gestuurd. Vanaf dat moment ontvangt Stratech Perspectief Cloud een melding bij een wijziging van de persoon in de BRP. Het systeem haalt onder de naam van de begeleider de nieuwe gegevens op. • De koppeling wordt gelegd met één van de gangbare gegevensmakelaars, bijvoorbeeld Centric Key2datadistributie of PinkRoccade MakelaarSuite.
Koppeling DataExport	De DataExport-API koppeling maakt het mogelijk om eenmaal per dag alle gegevens in een ongefilterd formaat te exporteren vanuit Stratech Perspectief Cloud. Voor gegevensuitwisseling wordt de FSC-standaard gehanteerd. De gegevens betreffen uitsluitend de door de opdrachtgever ingevoerde informatie.
Koppeling DDAS (Data Delen Armoede en Schulden)	De Koppeling DDAS-API maakt het mogelijk om gegevens te delen met het CBS volgens de vastgestelde uitwisselspecificatie waarbij onder andere persoonsgegevens en Burgerservicenummers zijn inbegrepen. Hiermee kan een landelijk overzicht worden gecreëerd van problematieken rondom schulden en armoede en de bijbehorende ontwikkelingen. De gegevensuitwisseling vindt plaats via de FSC-standaard.

ONDERDEEL	BESCHRIJVING
Koppeling KvK (StUF NHR)	Met de Koppeling Kamer van Koophandel (StUF NHR) is het mogelijk om de Kamer van Koophandel te bevragen op basis van een KvK nummer. Wordt de relatie gevonden dan worden de volgende gegevens geregistreerd in Stratech Perspectief Cloud: naam, straat, huisnummer, toevoeging huisnummer, postcode, woonplaats. Voor de beveiliging van de communicatie met de KvK koppeling wordt gebruikgemaakt van TLS authenticatie.
Koppeling Microsoft Entra-ID en Microsoft 365	Met de Koppeling Microsoft Entra-ID wordt er op basis van Security Assertion Markup Language een koppeling gelegd tussen Perspectief en Entra-ID van opdrachtgever. **Proces** **Registratie:** Nieuwe applicatie wordt geregistreerd in Entra-ID met SAML-instellingen op basis van Stratech Perspectief Cloud. **Authenticatie:** Gebruiker logt in op Stratech Perspectief Cloud en wordt doorgestuurd naar Entra-ID. **Validatie:** Entra-ID valideert inloggegevens en genereert een SAML-assertie. **Toegang:** Stratech Perspectief Cloud gebruikt de assertie om de gebruiker toegang te verlenen. **Claims**: • Name • E-mail Address • Username • Mobile number • External ID • Surname

ONDERDEEL	BESCHRIJVING
Koppeling MS-Graph	Met de integratie van MS-Graph wordt toegang tot e-mailgegevens verschaft voor naadloze e-mailfunctionaliteit binnen Stratech Perspectief Cloud. **Proces** **Registratie:** Een nieuwe applicatie wordt geregistreerd in Entra-ID. **Authenticatie:** Toegang tot e-mailaccounts wordt verleend via OAuth 2.0-authenticatie. **Toestemming:** De applicatie verkrijgt toestemming om e-mailgegevens te benaderen via de Microsoft Graph API. **Integratie:** Stratech Perspectief Cloud maakt gebruik van de Microsoft Graph API om e-mailberichten te verzenden. **De relevante API-permissies zijn:** Mail.send – Application: verzendt e-mailberichten namens iedere gebruiker. User.read – Sign in and read user profile: aanmelden en gebruikersprofiel lezen. De toegangsrechten tot mailboxen dienen beperkt te worden tot uitsluitend de gebruikers van Stratech Perspectief Cloud.
Koppeling Ponto Connect	De Koppeling Ponto Connect biedt mogelijkheden voor het ontvangen van bankmutaties en het versturen van betaalopdrachten. Via de Ponto Connect koppeling ontvangt Stratech Perspectief Cloud bankmutaties waarin persoonsgegevens staan en kan Stratech Perspectief Cloud betaalopdrachten versturen waarin persoonsgegevens staan. De verbinding tussen Stratech Perspectief Cloud en Ponto Connect is beveiligd conform de door Ponto Connect vereiste beveiligingsnormen waaronder Oauth2 en tweezijdige SSL-verificatie. Daarnaast is er op deze koppeling op IP-adres niveau whitelisting toegepast aan de Stratech Perspectief Cloud zijde.

ONDERDEEL	BESCHRIJVING
Koppeling Schuldenknooppunt	De Koppeling Schuldenknooppunt (SKP) faciliteert gegevensuitwisseling tussen Stratech Perspectief Cloud en het Schuldenknooppunt via de SKP Rest API. De gegevens die worden uitgewisseld door deze module, zijn voorgeschreven door het Schuldenknooppunt. Stratech Perspectief Cloud ondersteunt versie 2 van de SB&SK flow. De verbinding tussen Stratech Perspectief Cloud en het Schuldenknooppunt is beveiligd volgens de beveiligingsnormen die door het Schuldenknooppunt zijn vastgesteld.
Koppeling VISH	Met de Koppeling VISH kunnen cliënten gemeld worden bij SNG (gerechtsdeurwaarders). Dit betekent dat op het juiste moment een signaal gegeven wordt dat de schuldenaar zich heeft aangemeld voor schuldhulpverlening en de invordering (tijdelijk) stopt. Hiermee worden onnodige kosten voorkomen en worden de schulden ook niet onnodig hoger. De verbinding tussen Stratech Perspectief Cloud en VISH is beveiligd volgens de door SNG vereiste normen. Er kan gebruik worden gemaakt van een PKIO-certificaat met OIN (in dat geval controleert SNG de uitgevende root en het OIN), of van een SNG-softwarecertificaat (bij een SNG-softwarecertificaat geeft SNG het certificaat zelf uit en nemen die op in hun administratie). Welke gegevens: Bij de dagelijkse aanlevering van de VISH-gegevens worden de Burgerservicenummers van personen in de schuldhulpverlening en optioneel de contactgegevens van de behandelaar aangeleverd. Dit gebeurt iedere werkdag.

ONDERDEEL	BESCHRIJVING
Koppeling Vroegsignalering	De Koppeling Vroegsignalering stelt opdrachtgevers in staat vroegtijdige signalen te toetsen aan lopende en recent (< 6 maanden) afgesloten trajecten in Stratech Perspectief Perspectief. Autorisatie vindt plaats op basis van gebruikersnaam en wachtwoord. Deze kunnen worden aangemaakt in de beheermodule. Het wachtwoord wordt eenmalig verstrekt via Stratech Perspectief Cloud. Een autorisatiebericht genereert een JWT-token. Met dit JWT-token kunnen de volgende twee berichten worden verzonden: 1. Opvragen van gegevens op basis van BSN. 2. Opvragen van gegevens op basis van adresgegevens. Daarnaast is er op deze koppeling op IP-adres niveau whitelisting toegepast aan de Stratech Perspectief Cloud zijde.
Koppeling Xential NGX	Via de koppeling met Xential NGX kunnen vooraf ingerichte sjablonen vanuit Stratech Perspectief Cloud worden gegenereerd met de benodigde data (mogelijk persoonsgegevens) in de vorm van brieven, rapporten, overeenkomsten, et cetera. De gegevens die voor een specifiek sjabloon benodigd zijn worden op het moment van genereren middels Rest-API met Oauth2 koppeling verstuurd naar Xential. Xential genereert het gevraagde document waarna Stratech Perspectief Cloud het bestand download en beveiligd opslaat. Xential bewaart de data alleen voor de tijd dat nodig is voor het genereren en afleveren van het document. Daarnaast is er op deze koppeling op IP-adres niveau whitelisting toegepast aan de Stratech Perspectief Cloud zijde.

ONDERDEEL	BESCHRIJVING
Koppeling Zaaksysteem (StUF ZKN)	Met de Koppeling Zaaksysteem (StUF ZKN) is het mogelijk om zaak- en documentgegevens vanuit Stratech Perspectief Cloud op te slaan in een zaaksysteem. Het uitwisselen van zaak- en documentgegevens tussen Stratech Perspectief Cloud en het zaaksysteem vindt plaats op basis van de standaard Zaak- en Documentservices 1.1. De zaak- en documentgegevens kunnen persoonsgegevens bevatten. Enkele algemene kenmerken van deze koppeling: ▪ Het traject van de cliënt in Stratech Perspectief Cloud staat gelijk aan de zaak in het zaaksysteem. ▪ Gegevens die op zaakniveau worden uitgewisseld zijn: NAW-cliënt, zaaktype, begin- en einddatum, begeleider, status en resultaat. ▪ In Stratech Perspectief Cloud gegenereerde en/of bewerkte brieven of los toegevoegde dossierstukken worden automatisch opgeslagen in het zaaksysteem. ▪ De volledige documentenlijst van de gekoppelde zaak kan in Stratech Perspectief Cloud getoond worden in het tabblad 'Dossier' van de cliënt. Ook wanneer er via een andere bron dan Stratech Perspectief Cloud documenten aan de zaak zijn toegevoegd, bijvoorbeeld door een postregistratie systeem. ▪ Documenten openen vanuit het cliëntdossier opent het document uit het zaaksysteem. Voor de beveiliging van de communicatie met het zaaksysteem wordt gebruikgemaakt van TLS authenticatie. Daarnaast is er op deze koppeling op IP-adres niveau whitelisting toegepast aan de Stratech Perspectief Cloud zijde.

ONDERDEEL	BESCHRIJVING
Vtlb-calculator	Voor de berekening van het vrij te laten bedrag (VTLB) wordt de voorgeschreven Programmatuur van de Vtlb-calculator (hierna calculator) van Bureau WSNP gebruikt. Stratech Perspectief Cloud zendt de vereiste gegevens naar de calculator. De calculator verzorgt vervolgens alles rondom de uitvoering van de berekening. De resultaten van de berekening zendt de calculator terug naar Stratech Perspectief Cloud. De met deze calculator uit te wisselen gegevens worden voorgeschreven door Bureau WSNP en staan onder andere vermeld in de technische documentatie van de calculator welke te vinden is op de website van Bureau WSNP. De calculator is een .dll bestand dat wordt ingeladen door Stratech Perspectief Cloud. De doorzending van gegevens tussen Stratech Perspectief Cloud en de calculator vindt daardoor plaats binnen het werkgeheugen van Stratech Perspectief Cloud. De calculator vereist toegang tot het internet. Bureau WSNP vermeldt op de website daarover het volgende: "*De VTLB-calculator vereist toegang tot het internet, aangezien de applicatie (via een server van de Raad voor Rechtsbijstand) een koppeling maakt met de burgertool bereken.uwBeslagvrijeVoet.nl. van Stichting Netwerk Gerechtsdeurwaarders. De gegevens die uitgewisseld worden (leefsituatie en inkomensgegevens) zijn anoniem en niet herleidbaar naar een persoon.*" De door de calculator gehanteerde beveiligingsmaatregelen worden bepaald door Bureau WSNP.

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

Bijlage 2: Aantonen passend niveau van beveiliging

Algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen als bedoeld in artikel 32 lid 1 AVG (artikel 30 lid 2 sub d AVG)

Normenstelsel

[X] De verwerker werkt volgens een algemeen erkende norm voor informatiebeveiliging, te weten:

NEN/ISO 27001 (vermeld normenstelsel, zoals bijvoorbeeld NEN7510, NEN/ISO 27001, PCI/DSS) en is volgens deze norm wel~~/niet~~ gecertificeerd.

- Datum laatste certificering: 4 maart 2025

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

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

Toereikendheid
De toereikendheid van de informatiebeveiliging blijkt uit het volgende:

[X] 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 BIO, 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 ……

ISO 27001 certificaat

DigiTrust
CERTIFICATION OF MANAGEMENT SYSTEMS

Management Systeem Certificaat

Dit certificaat met nummer DGT271721769 is uitgegeven voor het managementsysteem van:

Stratech Automatisering B.V.

Vestigingsadres: Pantheon 15, 7521PR te Enschede

Voldoet aan de eisen gesteld in de Informatie Beveiliging Management Systeem norm:

NEN-EN-ISO/IEC 27001:2023/A1:2024 nl

Voor het toepassingsgebied: Informatiebeveiliging gerelateerd aan het ontwikkelen van applicaties, het beschikbaar stellen van deze applicaties aan klanten via hosting, het ondersteunen van deze klanten bij het gebruik van de applicatie via service en consultancy, het adequaat beveiligen van de tot de applicatie behorende databank en de daarin opgeslagen (persoons)gegevens en ondersteunende processen voor veilig personeel en veilige voorzieningen.
Dit alles binnen de kaders van de met klant gesloten overeenkomst inclusief de van toepassing zijnde leveringsvoorwaarden en met uitsluiting van de eigen verantwoordelijkheid van een klant voor afdoende beveiliging van diens eigen systemen, gegevens (waaronder persoonsgegevens) en andere al dan niet gevoelige (bedrijfs)informatie.

In overeenstemming met de verklaring van toepasselijkheid versie 2.2 van 24 februari 2025.

Dit certificaat is alleen geldig in samenhang met het certificaataanhangsel met hetzelfde nummer, waarop de van toepassing zijnde locaties met betrekking tot dit certificaat vermeld zijn.

Dit certificaat is geldig vanaf:
4 maart 2025

Dit certificaat is geldig tot:
12 mei 2026

Datum eerste certificaat:
12 mei 2023

Dit certificaat vervangt nr:
DGT271721337

NAMENS

Marco Bijl
DigiTrust B.V.

MGMT. SYS.
RvA C 618

DigiTrust B.V.: Achtseweg Zuid 159R - 5651 GW Eindhoven - Nederland
Telefoon +31 88 224-5600 - sales@digitrust.nl - www.digitrust.nl - KvK 59396822

Deze afgifte is uitgevoerd in overeenstemming met en binnen de procedures van DigiTrust zoals ook bekend bij en gecontroleerd door de RvA. Dit certificaat is elektronisch uitgegeven, het is en blijft eigendom van DigiTrust. Het valt daarom onder en is gebonden aan de uitgifte condities van het contract.
Certificaten kunnen worden gevalideerd via de QR-code.

Pagina 1 van 2

CERTIFICAAT

DigiTrust
CERTIFICATION OF MANAGEMENT SYSTEMS

Behorende bij het certificaat met registratienummer: DGT271721769
Het informatiebeveiligingsmanagementsysteem van: Stratech Automatisering B.V.

Werkmaatschappijen en geregistreerde activiteiten

Stratech Automatisering B.V.
Informatiebeveiliging gerelateerd aan het ontwikkelen van applicaties, het beschikbaar stellen van deze applicaties aan klanten via hosting, het ondersteunen van deze klanten bij het gebruik van de applicatie via service en consultancy, het adequaat beveiligen van de tot de applicatie behorende databank en de daarin opgeslagen (persoons)gegevens en ondersteunende processen voor veilig personeel en veilige voorzieningen.
Dit alles binnen de kaders van de met klant gesloten overeenkomst inclusief de van toepassing zijnde leveringsvoorwaarden en met uitsluiting van de eigen verantwoordelijkheid van een klant voor afdoende beveiliging van diens eigen systemen, gegevens (waaronder persoonsgegevens) en andere al dan niet gevoelige (bedrijfs)informatie.

Stratech Opleiding & Advies B.V.
Pantheon 15, 7521 PR Enschede

DigiTrust B.V.: Achtseweg Zuid 159R - 5651 GW Eindhoven - Nederland
Telefoon +31 88 224-5600 - sales@digitrust.nl - www.digitrust.nl - KvK 59396822

Verklaring van toepasselijkheid (VVT)

ISO27001:2023/A1:2024(NL) Verklaring van toepasselijkheid Stratech Versie 2.2 Datum: 24-2-2025			Van toepassing?	Geïmplementeerd?	Van toepassing vanuit wet- en regelgeving	Van toepassing vanuit Contract en/of SLA	Risico analyse	Onderbouwing waarom niet van toepassing
Nr.	**Onderwerp**	**Beheersmaatregel**						
5	**Organisatorische beheersmaatregelen**							
5.1	Beleidsregels voor informatiebeveiliging	Informatiebeveiligingsbeleid en onderwerp specifieke beleidsregels moeten worden gedefinieerd, goedgekeurd door het management, gepubliceerd, gecommuniceerd aan en erkend door relevant personeel en relevante belanghebbenden en met geplande tussenpozen en als zich significante wijzigingen voordoen, worden beoordeeld.	Ja	Ja		X	X	
5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging	Rollen en verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie.	Ja	Ja		X	X	
5.3	Functiescheiding	Conflicterende taken en conflicterende verantwoordelijkheden moeten worden gescheiden.	Ja	Ja			X	
5.4	Management-verantwoordelijkheden	Het management moet van al het personeel eisen dat ze informatiebeveiliging toepassen overeenkomstig het vastgestelde informatiebeveiligingsbeleid, de onderwerpspecifieke beleidsregels en procedures van de organisatie	Ja	Ja			X	
5.5	Contact met overheidsinstanties	De organisatie moet contact met de relevante instanties leggen en onderhouden.	Ja	Ja			X	
5.6	Contact met speciale belangengroepen	De organisatie moet contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen leggen en onderhouden.	Ja	Ja			X	
5.7	Informatie en analyses over dreigingen	Informatie- met betrekking tot informatiebeveiligingsdreiging	Ja	Ja			X	

		en moet worden verzameld en geanalyseerd om informatie over dreigingen te produceren.						
5.8	Informatiebeveiliging en projectmanagement	Informatiebeveiliging moet worden geïntegreerd in projectmanagement.	Ja	Ja			X	
5.9	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	Er moet een inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van de eigenaren, worden opgesteld en onderhouden.	Ja	Ja			X	
5.10	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	Regels voor het aanvaardbaar gebruik van en procedures voor het omgaan met informatie en andere gerelateerde bedrijfsmiddelen moeten worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	Ja	Ja			X	
5.11	Retourneren van bedrijfsmiddelen	Personeel en andere belanghebbenden, al naargelang de situatie, moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst retourneren.	Ja	Ja			X	
5.12	Classificeren van informatie	Informatie moet worden geclassificeerd volgens de informatiebeveiligingsbehoeften van de organisatie, op basis van de eisen voor vertrouwelijkheid, integriteit, beschikbaarheid en relevante eisen van belanghebbenden.	Ja	Ja		X	X	
5.13	Labelen van informatie	Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Ja	Ja			X	
5.14	Overdragen van informatie	Er moeten regels, procedures of overeenkomsten voor informatieoverdracht zijn ingesteld voor alle soorten van communicatiefaciliteiten binnen de organisatie en tussen de organisatie en andere partijen.	Ja	Ja		X	X	
5.15	Toegangsbeveiliging	Er moeten regels op basis van bedrijfs- en informatiebeveiligingseisen worden vastgesteld en geïmplementeerd om de fysieke en logische toegang tot informatie en andere gerelateerde bedrijfsmiddelen te beheersen.	Ja	Ja		X	X	
5.16	Identiteitsbeheer	De volledige levenscyclus van identiteiten moet worden beheerd.	Ja	Ja			X	

5.17	Authenticatie-informatie	De toewijzing en het beheer van authenticatie-informatie moet worden beheerst door middel van een beheerproces waarvan het adviseren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.	Ja	Ja			X	
5.18	Toegangsrechten	Toegangsrechten voor informatie en andere gerelateerde bedrijfsmiddelen moeten worden verstrekt, beoordeeld, aangepast en verwijderd overeenkomstig het onderwerpspecifieke beleid en de regels inzake toegangsbeveiliging van de organisatie.	Ja	Ja			X	
5.19	Informatiebeveiliging en leveranciersrelaties	Er moeten processen en procedures worden vastgesteld en geïmplementeerd om de informatiebeveiligingsrisico's in verband met het gebruik van producten of diensten van de leverancier te beheersen.	Ja	Ja			X	
5.20	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Relevante informatiebeveiligingseisen moeten worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie worden overeengekomen.	Ja	Ja	X	X	X	
5.21	Beheren van informatiebeveiliging in de ICT-toeleveringsketen	Er moeten processen en procedures worden bepaald en geïmplementeerd om de informatiebeveiligingsrisico's in verband met de toeleveringsketen van ICT-producten en -diensten te beheersen.	Ja	Ja			X	
5.22	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	De organisatie moet de informatiebeveiligingspraktijken en de dienstverlening van leveranciers regelmatig monitoren, beoordelen, evalueren en veranderingen daaraan beheren.	Ja	Ja			X	
5.23	Informatiebeveiliging voor het gebruik van clouddiensten	Processen voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten moeten overeenkomstig de informatiebeveiligingseisen van de organisatie worden opgesteld.	Ja	Ja			X	
5.24	Plannen en voorbereiden van het beheer van informatiebeveiligings-incidenten	De organisatie moet plannen opstellen voor, en zich voorbereiden op, het beheren van informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatie[1]beveiligingsincidenten te definiëren, vast te stellen en te communiceren.	Ja	Ja			X	

5.25	Beoordelen van en besluiten over informatiebeveiligings-gebeurtenissen	De organisatie moet informatiebeveiligingsgebeurtenissen beoordelen en beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten.	Ja	Ja			X	
5.26	Reageren op informatiebeveiligings-incidenten	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Ja	Ja			X	
5.27	Leren van informatiebeveiligings-incidenten	Kennis die is opgedaan met informatiebeveiligingsincidenten moet worden gebruikt om de beheersmaatregelen voor informatiebeveiliging te versterken en te verbeteren.	Ja	Ja			X	
5.28	Verzamelen van bewijsmateriaal	De organisatie moet procedures vaststellen en implementeren voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs met betrekking tot informatiebeveiligingsgebeurtenissen.	Ja	Ja			X	
5.29	Informatiebeveiliging tijdens een verstoring	De organisatie moet plannen maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.	Ja	Ja			X	
5.30	ICT-gereedheid voor bedrijfscontinuïteit	De ICT-gereedheid moet worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoelstellingen en ICT-continuiteitseisen	Ja	Ja		X	X	
5.31	Wettelijke, statutaire, regelgevende en contractuele eisen	Wettelijke, statutaire, regelgevende en contractuele eisen die relevant zijn voor informatiebeveiliging en de aanpak van de organisatie om aan deze eisen te voldoen, moeten worden geïdentificeerd, gedocumenteerd en actueel gehouden.	Ja	Ja	X	X	X	
5.32	Intellectuele eigendomsrechten	De organisatie moet passende procedures implementeren om intellectuele eigendomsrechten te beschermen.	Ja	Ja	X		X	
5.33	Beschermen van registraties	Registraties moeten worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.	Ja	Ja	X		X	
5.34	Privacy en bescherming van persoonsgegevens	De organisatie moet de eisen met betrekking tot het behoud van privacy en de bescherming van persoonsgegevens volgens de toepasselijke wet- en regelgeving en contractuele eisen identificeren en eraan voldoen.	Ja	Ja	X	X	X	

5.35	Onafhankelijke beoordeling van informatiebeveiliging	De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan, met inbegrip van mensen, processen en technologieën, moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, worden beoordeeld.	Ja	Ja		X	X	
5.36	Naleving van beleid, regels en normen voor informatiebeveiliging	De naleving van het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en de normen van de organisatie moet regelmatig worden beoordeeld.	Ja	Ja	X	X	X	
5.37	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures voor informatieverwerkende faciliteiten moeten worden gedocumenteerd en beschikbaar worden gesteld aan het personeel dat ze nodig heeft.	Ja	Ja			X	
6	**Mensgerichte beheersmaatregelen**							
6.1	Screening	De achtergrond van alle kandidaten voor een dienstverband moet worden gecontroleerd voordat ze bij de organisatie in dienst treden en daarna op gezette tijden worden herhaald. Hierbij moet rekening worden gehouden met de toepasselijke wet- en regelgeving en ethische overwegingen, en deze controle moet in verhouding staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.	Ja	Ja			X	
6.2	Arbeidsovereenkomst	In arbeidsovereenkomsten moet worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging.	Ja	Ja		X	X	
6.3	Bewustwording van, opleiding en training in informatiebeveiliging	Personeel van de organisatie en relevante belanghebbenden moeten een passende bewustwording van, opleiding en training in informatiebeveiliging en regelmatige updates over het informatiebeveiligingsbeleid, onderwerpspecifieke beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie, krijgen	Ja	Ja		X	X	
6.4	Disciplinaire procedure	Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te ondernemen tegen personeel en andere belanghebbenden die zich	Ja	Ja		X	X	

		schuldig hebben gemaakt aan een schending van het informatiebeveiligingsbeleid.						
6.5	Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband, moeten worden gedefinieerd, gehandhaafd en gecommuniceerd aan relevant personeel en andere belanghebbenden.	Ja	Ja		X	X	
6.6	Vertrouwelijkheids- of geheimhoudings-overeenkomsten	Vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie inzake de bescherming van informatie weerspiegelen, moeten worden geïdentificeerd, gedocumenteerd, regelmatig worden beoordeeld en ondertekend door personeel en andere relevante belanghebbenden.	Ja	Ja		X	X	
6.7	Werken op afstand	Wanneer personeel op afstand werkt, moeten er beveiligingsmaatregelen worden geïmplementeerd om informatie te beschermen die buiten het gebouw en/of terrein van de organisatie wordt ingezien, verwerkt of opgeslagen.	Ja	Ja			X	
6.8	Melden van informatiebeveiligings-gebeurtenissen	De organisatie moet voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligings-gebeurtenissen tijdig via passende kanalen kan melden.	Ja	Ja		X	X	
7	**Fysieke beheersmaatregelen**							
7.1	Fysieke beveiligingszones	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, moeten worden beschermd door beveiligingszones te definiëren en te gebruiken	Ja	Ja			X	
7.2	Fysieke toegangsbeveiliging	Beveiligde zones moeten worden beschermd door passende toegangsbeveiligings-maatregelen en toegangspunten.	Ja	Ja		X	X	
7.3	Beveiligen van kantoren, ruimten en faciliteiten	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en geïmplementeerd.	Ja	Ja			X	
7.4	Monitoren van de fysieke beveiliging	Het gebouw en terrein moet voortdurend worden gemonitord op onbevoegde fysieke toegang.	Ja	Ja			X	
7.5	Beschermen tegen fysieke en omgevingsdreigingen	Er moet bescherming tegen fysieke en omgevingsdreigingen, zoals natuurrampen en andere	Ja	Ja			X	

		opzettelijke of onopzettelijke fysieke dreigingen voor de infrastructuur, worden ontworpen en geïmplementeerd.						
7.6	Werken in beveiligde zones	Voor het werken in beveiligde zones moeten beveiligingsmaatregelen worden ontwikkeld en geïmplementeerd.	Ja	Ja			X	
7.7	'Clear desk' en 'clear sereen'	Er moeten 'clear desk'-regels voor papieren documenten en verwijderbare opslagmedia en 'clear screen'-regels voor informatieverwerkende faciliteiten worden gedefinieerd en op passende wijze worden afgedwongen.	Ja	Ja			X	
7.8	Plaatsen en beschermen van apparatuur	Apparatuur moet veilig worden geplaatst en beschermd.	Ja	Ja			X	
7.9	Beveiligen van bedrijfsmiddelen buiten het terrein	Bedrijfsmiddelen buiten het gebouw en/of terrein moeten worden beschermd.	Ja	Ja			X	
7.10	Opslagmedia	Opslagmedia moeten worden beheerd gedurende hun volledige levenscyclus van aanschaf, gebruik, transport en verwijdering overeenkomstig het classificatieschema en de hanteringseisen van de organisatie.	Ja	Ja			X	
7.11	Nutsvoorzieningen	Informatieverwerkende faciliteiten moeten worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.	Ja	Ja			X	
7.12	Beveiligen van bekabeling	Voedingskabels en kabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen onderschepping, interferentie of beschadiging.	Ja	Ja			X	
7.13	Onderhoud van apparatuur	Apparatuur moet op de juiste wijze worden onderhouden om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te garanderen.	Ja	Ja			X	
7.14	Vellig verwijderen of hergebruiken van apparatuur	Onderdelen van de apparatuur die opslagmedia bevatten, moeten worden gecontroleerd om te waarborgen dat gevoelige gegevens en gelicentieerde software zijn verwijderd of veilig zijn overschreven voordat ze worden verwijderd of hergebruikt.	Ja	Ja			X	
8	**Technologische beheersmaatregelen**							
8.1	User endpoint devices	Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user	Ja	Ja			X	

		endpoint devices' moet worden beschermd.						
8.2	Speciale toegangsrechten	Het toewijzen en het gebruik van speciale toegangsrechten moet worden beperkt en beheerd.	Ja	Ja			X	
8.3	Beperking toegang tot informatie	De toegang tot informatie en andere gerelateerde bedrijfsmiddelen moet worden beperkt overeenkomstig het vastgestelde onderwerp specifieke beleid inzake toegangsbeveiliging.	Ja	Ja		X	X	
8.4	Toegangsbeveiliging op broncode	Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken moet op passende wijze worden beheerd.	Ja	Ja			X	
8.5	Beveiligde authenticatie	Er moeten beveiligde authenticatie technologieën en -procedures worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerpspecifieke beleid inzake toegangsbeveiliging.	Ja	Ja			X	
8.6	Capaciteitsbeheer	Het gebruik van middelen moet worden gemonitord en aangepast overeenkomstig de huidige en verwachte capaciteitseisen.	Ja	Ja			X	
8.7	Bescherming tegen malware	Bescherming tegen malware moet worden geïmplementeerd en ondersteund door een passend gebuikersbewustzijn.	Ja	Ja			X	
8.8	Beheer van technische kwetsbaarheden	Er moet informatie worden verkregen over technische kwetsbaarheden van in gebruik zijnde informatiesystemen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en er moeten passende maatregelen worden getroffen.	Ja	Ja			X	
8.9	Configuratiebeheer	Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken moeten worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.	Ja	Ja			X	
8.10	Wissen van informatie	In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie moet worden gewist als deze niet langer vereist is.	Ja	Ja			X	
8.11	Maskeren van gegevens	Gegevens moeten worden gemaskeerd overeenkomstig het onderwerpspecifieke beleid inzake toegangsbeveiliging en andere gerelateerde onderwerpspecifieke	Ja	Ja			X	

		beleidsregels, en bedrijfseisen van de organisatie, rekening houdend met de toepasselijke wetgeving.						
8.12	Voorkomen van gegevenslekken (data leakage prevention)	Maatregelen om gegevenslekken te voorkomen moeten worden toegepast in systemen, netwerken en andere apparaten waarop of waarmee gevoelige informatie wordt verwerkt, opgeslagen of getransporteerd.	Ja	Ja			X	
8.13	Back-up van informatie	Back-ups van informatie, software en systemen moeten worden bewaard en regelmatig worden getest overeenkomstig het overeengekomen onderwerpspecifieke beleid inzake back-ups.	Ja	Ja		X	X	
8.14	Redundantie van informatieverwerkende faciliteiten	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Ja	Ja		X	X	
8.15	Logging	Er moeten logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, worden geproduceerd, opgeslagen, beschermd en geanalyseerd.	Ja	Ja		X	X	
8.16	Monitoren van activiteiten	Netwerken, systemen en toepassingen moeten worden gemonitord op afwijkend gedrag en er moeten passende maatregelen worden getroffen om potentiële informatiebeveiligingsincident en te evalueren.	Ja	Ja		X	X	
8.17	Kloksynchronisatie	De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, moeten worden gesynchroniseerd met goedgekeurde tijdbronnen.	Ja	Ja			X	
8.18	Gebruik van speciale systeemhulpmiddelen	Het gebruik van systeemhulpmiddelen die in staat kunnen zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, moet worden beperkt en nauwkeurig worden gecontroleerd.	Ja	Ja			X	
8.19	Installeren van software op operationele systemen	Er moeten procedures en maatregelen worden geïmplementeerd om het installeren van software op operationele systemen op veilige wijze te beheren.	Ja	Ja			X	
8.20	Beveiliging netwerkcomponenten	Netwerken en netwerkapparaten moeten worden beveiligd, beheerd en beheerst om informatie in	Ja	Ja		X	X	

		systemen en toepassingen te beschermen.						
8.21	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten moeten worden geïdentificeerd, geïmplementeerd en gemonitord.	Ja	Ja		X	X	
8.22	Netwerksegmentatie	Groepen informatiediensten, gebruikers en informatiesystemen moeten in de netwerken van de organisatie worden gesegmenteerd.	Ja	Ja			X	
8.23	Toepassen van webfilters	De toegang tot externe websites moet worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.	Ja	Ja			X	
8.24	Gebruik van cryptografie	Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, moeten worden gedefinieerd en geïmplementeerd.	Ja	Ja		X	X	
8.25	Beveiligen tijdens de ontwikkelcyclus	Voor het veilig ontwikkelen van software en systemen moeten regels worden vastgesteld en toegepast.	Ja	Ja			X	
8.26	Toepassingsbeveiligings-eisen	Er moeten eisen aan de informatiebeveiliging worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.	Ja	Ja			X	
8.27	Veilige systeemarchitectuur en technische uitgangspunten	Uitgangspunten voor het ontwerpen van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle activiteiten betreffende het ontwikkelen van informatiesystemen.	Ja	Ja			X	
8.28	Vellig coderen	Er moeten principes voor veilig coderen worden toegepast op softwareontwikkeling.	Ja	Ja		X	X	
8.29	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Processen voor het testen van de beveiliging moeten worden gedefinieerd en geïmplementeerd in de ontwikkelcyclus.	Ja	Ja			X	
8.30	Uitbestede systeemontwikkeling	De organisatie moet de activiteiten in verband met uitbestede systeemontwikkeling sturen, bewaken en beoordelen.	Nee	Nvt				Software ontwikkeling is niet uitbesteedt.
8.31	Scheiding van ontwikkel-, test en productieomgevingen	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden en beveiligd.	Ja	Ja		X	X	
8.32	Wijzigingsbeheer	Wijzigingen in informatieverwerkende faciliteiten en informatiesystemen moeten onderworpen zijn aan	Ja	Ja			X	

		procedures voor wijzigingsbeheer.						
8.33	Testgegevens	Testgegevens moeten op passende wijze worden geselecteerd, beschermd en beheerd.	Ja	Ja			X	
8.34	Bescherming van informatiesystemen tijdens audits	Audittests en andere auditactiviteiten waarbij operationele systemen worden beoordeeld, moeten worden gepland en overeengekomen tussen de tester en het verantwoordelijke management.	Ja	Ja			X	

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

Toelichting bij de Standaard Verwerkersovereenkomst

De Standaard Verwerkersovereenkomst gemeenten is een nadere uitwerking voor gemeenten van de Baseline Informatiebeveiliging Overheid (BIO). De BIO is eind 2018 bestuurlijk vastgesteld als gezamenlijke norm voor informatiebeveiliging voor alle Nederlandse overheden.

Op 23 september 2025 heeft het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) de Baseline Informatiebeveiliging Overheid versie 2 (BIO2) bestuurlijk vastgesteld. De BIO2 vormt het nieuwe kader voor informatiebeveiliging binnen de overheid. Dit vernieuwde model is tot stand gekomen na een evaluatie van de huidige BIO en sluit aan op de ontwikkelingen rondom de NIS2-richtlijn. Hiermee geeft de BIO2 invulling aan de zorgplicht uit de NIS2-richtlijn voor de overheid. De BIO2 is onder leiding van BZK ontwikkeld in samenwerking met gemeenten, provincies, waterschappen en het rijk. De BIO2 is gebaseerd op de laatste versie van de ISO 27001 en de ISO 27002.

Doel

Gemeenten en leveranciers willen bij de uitvoering van hun taken en diensten komen tot een goede dienstverlening voor inwoners en bedrijven. Als bij de uitvoering van deze taken en diensten persoonsgegevens worden verwerkt dan willen gemeenten en leveranciers de verplichtingen op grond van de AVG nakomen. Daarbij willen Partijen uitgaan van wederzijds vertrouwen.

Het doel van deze standaard verwerkersovereenkomst is het gemeenten en hun leveranciers makkelijker te maken om tot afspraken te komen over de verwerking van persoonsgegevens. Deze standaard wordt gebruikt als aanvulling op een hoofdovereenkomst om op grond van de AVG (artikel 28.3 en 28.9) nadere afspraken te maken en vast te leggen over de omgang met persoonsgegevens.

Rangorde

De rangorde van de verschillende documenten (o.a. inkoopdocumenten, hoofdovereenkomst, verwerkersovereenkomst) wordt geregeld in de hoofdovereenkomst.

Beheer van deze standaard

VNG-Realisatie/IBD beheert deze standaard verwerkersovereenkomst. Zowel gemeenten als leveranciers kunnen verbetervoorstellen mailen naar privacy@vng.nl. Maximaal tweemaal per jaar beoordeelt de Beheergroep VWO (bestaande uit vertegenwoordigers van gemeenten en leveranciers), de verbetervoorstellen en zo nodig worden deze verwerkt in een volgende versie.

Hebt u vragen over het gebruik van deze standaard overeenkomst neem dan contact op met de IBD: privacy@vng.nl.

Doelgroep

Dit document is van belang voor het management van de gemeente, de systeemeigenaren, gemeentelijke inkopers, privacyfunctionarissen en informatiebeveiligers.

Relatie met overige documenten:

- GIBIT 2023;
- Addendum GIBIT 2023 Stratech;
- Baseline Informatiebeveiliging Overheid (BIO);
- Inkoopvoorwaarden en informatiebeveiligingseisen;
- Handreiking Service Level Agreements;
- Handreiking Geheimhoudingsverklaringen;
- Handreiking Screening Personeel BIO.

Inhoudsopgave

1. Inleiding

Bij de dienstverlening en bedrijfsvoering verwerken gemeenten persoonsgegevens. In voorkomende gevallen worden de verwerkingen uitgevoerd door derde partijen zoals andere overheidsorganisaties, semi-overheidsorganisaties en particuliere bedrijven. Bij de verwerking van persoonsgegevens is het van belang en zelfs wettelijk verplicht dat partijen hierover afspraken maken.

De IBD stelt vast dat gemeenten en leveranciers veel tijd en energie stoppen in het maken van afspraken hierover, maar dat het in veel gevallen niet lukt om tot overeenstemming te komen. De IBD ondersteunt - sinds de oprichting in 2013 - gemeenten en heeft daarom de volgende acties ondernomen:

- Het samen met gemeenten opstellen van een model verwerkersovereenkomst;
- Het ondersteunen van gebruikersverenigingen van gemeenten in de onderhandelingen met enkele grote leveranciers;
- Het opstellen van een factsheet over het opstellen van verwerkersovereenkomsten;
- Het opstellen van een factsheet over verwerkingsverantwoordelijken en verwerkers.

Deze acties hebben enig effect gehad, maar nog steeds ontbraken in veel gevallen sluitende afspraken. Opdrachtgevers en opdrachtnemers, verantwoordelijken en verwerkers achtten dit een hoogst onwenselijke situatie omdat het 1. strijdig is met de wet, 2. ongewenst is bij beveiligingsincidenten (datalekken) en 3. een verkeerd signaal geeft richting inwoners van de betrokken gemeente: de gemeente zou géén prioriteit geven aan een zorgvuldige verwerking van onze persoonsgegevens door derden.

Compromis als oplossing voor een complex probleem

Gemeenten en leveranciers gaven aan dat er dringend behoefte is om te komen tot een oplossing van situaties waarin er geen sluitende afspraken zijn over de verwerking van persoonsgegevens namens Nederlandse gemeenten. Een oplossing voor een complex probleem als dit is per definitie een compromis. Dit compromis is gevonden in de standaardisering van de gemeentelijke verwerkersovereenkomst (standaard VWO) waar zowel gemeenten als leveranciers zich aan committeren. Gemeenten en leveranciers doen ten opzichte van elkaar op gecontroleerde wijze water bij de wijn om uit de huidige impasse te geraken. Op het niveau van een individuele overeenkomst kan het zijn dat partijen deze standaard ervaren als verbetering of verslechtering. Op het niveau van het collectief maken gemeenten en hun leveranciers een enorme stap voorwaarts: in alle gevallen waarin dat nodig is zijn er nu heldere kaders over de verwerking van persoonsgegevens.

Gemeenten hebben zichzelf op de ALV van de VNG d.d. 5 juni 2019 de verplichting opgelegd om de Standaard VWO te gebruiken. Gemeenten moeten daarom in hun jaarrapportage vastleggen in het geval zij de Standaard VWO niet gebruiken, of daarvan afwijken.

Gemeenten èn leveranciers

Bij het opstellen van deze standaard VWO is uitvoerig overleg geweest met een representatieve groep gemeenten en leveranciers. De uiteindelijke inhoud is vastgesteld door de Beheergroep VWO bestaande uit vertegenwoordigers van 14 gemeenten (CISO's, FG's en inkopers). Het IBD-model verwerkersovereenkomst diende als basis voor deze standaard. Uit dit model zijn onderdelen verwijderd die zijn geregeld in de Algemene Verordening Gegevensbescherming (definities, inbreuken), het Burgerlijk Wetboek (ingebrekestelling, beëindiging overeenkomst), of de hoofdovereenkomst (meerwerk en vergoeding daarvan, aansprakelijkheid). Daarnaast is gewerkt om het document toegankelijker te maken voor de doelgroepen die de afspraken uitvoeren of daarop toezien. Het document bevat juridische taal waar nodig en een toegankelijke omschrijving waar dat kan.

NB: Overal in de Handreiking waar 'gemeenten' staat, moet worden gelezen 'gemeentelijke organisaties'.

2. Algemeen

2.1 Is er wel een verwerkersovereenkomst nodig?

Voordat partijen afspraken maken over de verwerking van persoonsgegevens is het noodzakelijk om te weten wat de rol is van de betrokken partijen. Is er ten aanzien van de verwerking van persoonsgegevens wel sprake van een relatie verwerkingsverantwoordelijke - verwerker? Zo ja, dan maken partijen afspraken over de verwerking van persoonsgegevens. Om te bepalen wat de precieze rol is van de betrokken partijen en daarmee of het dan ook nodig is om een verwerkersovereenkomst af te sluiten, verwijzen wij u naar de Factsheet en beslismodel "Is mijn leverancier wel of geen verwerker".

2.2 Gedeelde verantwoordelijkheid en vertrouwen

Verwerkingsverantwoordelijken en verwerkers hebben op grond van de AVG gezamenlijk en individueel een verantwoordelijkheid ten aanzien van de verwerking van persoonsgegevens. Zodoende moet het echt de intentie van partijen zijn om de persoonsgegevens van betrokkenen zorgvuldig te verwerken en te beveiligen. Partijen maken in aanvulling op de hoofdovereenkomst dan ook nadere afspraken over de verwerking van persoonsgegevens. Dat kan een verwerkersovereenkomst zijn.

2.3 Over welke onderwerpen moeten afspraken gemaakt worden?

Het is verplicht om afspraken te maken over de omgang met persoonsgegevens tussen verantwoordelijke en verwerker. Het is echter niet verplicht om een verwerkersovereenkomst af te sluiten. Afspraken over hoe partijen omgaan met persoonsgegevens mogen bijvoorbeeld ook best in de hoofdovereenkomst worden vastgelegd. Er zijn enkele onderwerpen waarover verplicht afspraken gemaakt moeten worden. Deze onderwerpen staan ook in de standaard verwerkersovereenkomst:

Onderwerp	**Waar geregeld in verwerkersovereenkomst**
Onderwerp	Artikel 3
Duur	Artikel 2
Aard en doel	Bijlage 1, tabel 1
Soort persoonsgegevens	Bijlage 1, tabel 1
Categorieën van betrokkenen	Bijlage 1, tabel 1
Rechten en verplichtingen van de verwerkingsverantwoordelijke	Hele overeenkomst
Verwerking alleen op basis van schriftelijke instructies	Art. 3.1
Doorgifte naar derde landen	Art. 4.3
Vertrouwelijkheid	Art. 4.4
Passende technische en organisatorische maatregelen	Art. 4.1
Inschakeling subverwerkers	Art. 4.5

Verwerker verleent bijstand bij verzoeken van betrokkene	Art. 4.6
Verwerker verleent bijstand bij nakoming art. 32 t/m 36	Art. 4.1 / 5 / 4.7
Verwerker wist persoonsgegevens of geeft deze na afloop verwerking terug	Art. 2.1 en 7.1

NB: Over andere onderwerpen zoals de uitvoering van audits, aansprakelijkheid en de exit-strategie maken partijen afspraken in de hoofdovereenkomst. Als hierover geen afspraken zijn gemaakt in de hoofdovereenkomst, adviseren wij partijen om dat alsnog te doen in een addendum bij de hoofdovereenkomst. In die gevallen dat er helemaal geen hoofdovereenkomst is, kunnen partijen er voor kiezen om deze afspraken te maken in een addendum bij de Standaard VWO. En dus niet in de Standaard VWO zelf. Het vorenstaande geldt ook als bestaande afspraken niet meer passend zijn; in dat geval maken partijen in een addendum bij de hoofdovereenkomst, of in een addendum bij de Standaard VWO, nieuwe afspraken en niet in de Standaard VWO zelf.

Over de inhoud van de eventueel nader te maken afspraken verwijzen wij naar de GIBIT 2023[2]:

Aansprakelijkheid : artikel 16
Exit-strategie : artikel 24.14 en artikel 26
Audit : artikel 25[3]

2.4 Meerwerk

Het komt voor dat de verwerker bij de uitvoering van de overeenkomst t.a.v. verwerking van persoonsgegevens kosten moet maken. De vraag of dit wel of geen meerwerk en derhalve wel of niet in aanmerking komt voor vergoeding door de opdrachtgever, moet in de hoofdovereenkomst worden geregeld of in een addendum bij de hoofdovereenkomst. In die gevallen dat er helemaal geen hoofdovereenkomst is, kunnen partijen er voor kiezen om deze afspraken te maken in een addendum bij de Standaard VWO. Ook hiervoor geldt: niet regelen in de Standaard VWO zelf. Zie hiervoor artikel 11.3 van de GIBIT 2023.

2.5 Artikelsgewijze toelichting

Aanhef:

Stelregel is dat als de gemeente privaatrechtelijk handelt (bijvoorbeeld overeenkomsten sluit, gronden verkoopt), de gemeente als rechtspersoon optreedt. In het privaatrecht kunnen alleen natuurlijke personen en rechtspersonen aan het rechtsverkeer deelnemen. Voor de AVG is echter het bestuursorgaan de verwerkingsverantwoordelijke. Dit kan de burgemeester, het college of de gemeenteraad zijn. Bij het sluiten van de verwerkersovereenkomst moet wel duidelijk zijn welk gemeentelijk bestuursorgaan verwerkingsverantwoordelijke is.

Overwegingen:

De verwerkersovereenkomst maakt onderdeel uit van een hoofdovereenkomst. Vul hier de naam van hoofdovereenkomst in.

[2] Voor vragen over de GIBIT 2023 kunt u contact opnemen met info@gibit.nl
[3] Zie hiervoor Bijlage 3.

Artikelen:

1.1: De definities van art. 4 AVG hebben in deze verwerkersovereenkomst dezelfde betekenis.

2.1: Het uitgangspunt is dat de verwerkersovereenkomst ingaat op het moment dat de hoofdovereenkomst tot stand is gekomen. Partijen kunnen daar echter van afwijken. Zij moeten dat dan wel expliciet aangeven

2.2: Dit artikel moet in samenhang met artikel 7.1 worden gelezen.

2.3 Wanneer Partijen ervoor kiezen om de nieuwe versie van de Standaard VWO af te sluiten, betekent dat dat de vorige overeengekomen verwerkersovereenkomst niet meer geldig is.

3.1: Voor iedere verdere verwerking van persoonsgegevens die buiten de opdrachtverlening valt zoals genoemd in tabel 1 van Bijlage 1, moet de verwerker vooraf uitdrukkelijk toestemming vragen aan de verwerkingsverantwoordelijke. Dit geldt ook voor de verwerking van persoonsgegevens als op enige wijze kunstmatige intelligentie wordt toegepast, waaronder testen en trainen.
Verwerker zal de verwerkingsverantwoordelijke zonder onredelijke vertraging informeren, indien een schriftelijke instructie van de verwerkingsverantwoordelijke naar het oordeel van de verwerker in strijd is met de AVG of de UAVG.

3.2: De verwerker mag alleen de in Bijlage 1, tabel 1 vermelde verwerkingen uitvoeren.

4.1: Een uit artikel 4.1 volgend passend beveiligingsniveau kan betekenen dat de verwerker zelf het initiatief neemt om aanvullende maatregelen te nemen. Daarnaast kan ook de verwerkingsverantwoordelijke aan de verwerker opdragen om het beveiligingsniveau te verbeteren. Als objectief is vastgesteld dat de verwerker geen passend beveiligingsniveau heeft en de verwerkingsverantwoordelijke daarom uitdrukkelijk schriftelijk verzoekt, zullen partijen in onderling overleg bepalen welke aanvullende beveiligingsmaatregelen de verwerker zal treffen.

4.2: De verwerker is op grond van de AVG verplicht om mee te werken aan de uitvoering van een audit. Partijen maken vooraf afspraken over de frequentie van de uit te voeren audits. Als de verwerker op basis van een certificering kan aantonen dat het beveiligingsniveau voldoende is, kan een audit achterwege blijven. Hiervoor dienen de scope en de verklaring van toepasselijkheid van de certificering wel de verwerking volledig dekken. Partijen treden daarover in overleg. Mocht uit het auditverslag blijken dat de verwerker bepaalde werkzaamheden moet verrichten om het beveiligingsniveau aan te passen, dan zal de verwerker deze werkzaamheden binnen een redelijke termijn uitvoeren. T.a.v. de kosten van de audit wordt aangesloten bij art. 25.6 van de GIBIT 2023.
Bij twijfel over de uitkomsten van de audit gaat de verwerkingsverantwoordelijke daarover in gesprek met de verwerker. Eventueel kan de verwerkingsverantwoordelijke zich wenden tot de auditor.
Als DigiD wordt gebruikt bij de verwerking, moet de verwerker jaarlijks een TPM overleggen aan de verwerkingsverantwoordelijke.
NB: De kosten van de certificering zelf zijn voor rekening van de verwerker.

4.3: De verwerker moet de verwerkingsverantwoordelijke altijd vooraf op de hoogte brengen van een doorgifte aan een derde land of een internationale organisatie. Als de Europese Commissie een adequaatheidsbesluit heeft genomen t.a.v. de doorgifte aan een derde land, of een internationale organisatie, is hiervoor geen toestemming nodig van de verwerkingsverantwoordelijke (art. 45 AVG).
Als er geen adequaatheidsbesluit is afgegeven voor een doorgifte aan een derde land of een internationale organisatie, dan mag de verwerking van persoonsgegevens daar toch plaatsvinden, als er wordt voldaan aan de in artikel 46 AVG genoemde instrumenten. De verwerker maakt dan een analyse van de passende waarborgen en de voor de betrokkenen afdwingbare rechten en doeltreffende rechtsmiddelen die het derde land of internationale organisatie heeft getroffen en de eventueel noodzakelijke aanvullende maatregelen. De verwerker legt deze analyse ter beoordeling voor aan de verwerkingsverantwoordelijke.

Het vorenstaande geldt ook als een subverwerker persoonsgegevens doorgeeft aan een derde land of een internationale organisatie.

4.4: De verwerker zorgt dat de personen die onder zijn verantwoordelijkheid werkzaam zijn en toegang hebben tot de persoonsgegevens op een of andere schriftelijke manier zijn gehouden aan de geheimhoudingsplicht.

4.5: Verwerker mag een andere verwerker inschakelen: een subverwerker. Een subverwerker is een andere zelfstandige partij die in opdracht van de 1e verwerker (een deel) van de persoonsgegevens verwerkt. Deze subverwerker opereert zelfstandig, maar moet de persoonsgegevens wel verwerken volgens de schriftelijke instructies van de verwerkingsverantwoordelijke, net als de 1e verwerker. De subverwerker heeft t.a.v. de gegevensbescherming dezelfde verplichtingen die de 1e verwerker heeft. Als de subverwerker zijn verplichtingen niet nakomt, blijft de 1e verwerker t.a.v. de gegevensbescherming volledig aansprakelijk voor het niet nakomen van de verplichtingen door de subverwerker. In het geval het niet (direct) mogelijk is om dezelfde afspraken te maken met een subverwerker (bv. In geval van multinationals als Microsoft/Google), dan moet de subverwerker in ieder geval voldoen aan de verplichtingen van de AVG. Ook na de ingangsdatum van de verwerkersovereenkomst moet de verwerker de verwerkingsverantwoordelijke informeren over de inschakeling van nieuwe subverwerkers. Verwerkingsverantwoordelijke heeft overeenkomstig artikel 28.2 AVG het recht om bezwaar te maken tegen een subverwerker. Als een verwerkingsverantwoordelijke daadwerkelijk bezwaar heeft tegen een subverwerker, gaan partijen hierover in overleg.
NB: Als de verwerker een persoon inhuurt voor bepaalde werkzaamheden, hoeft dat niet automatisch te betekenen dat er sprake is van een subverwerker.

4.6: Als een betrokkene een beroep doet op zijn rechten, dan helpt de verwerker de verwerkingsverantwoordelijke om hier binnen de wettelijke termijn op te kunnen beslissen. Mocht een betrokkene bij de uitoefening van zijn rechten zich rechtstreeks richten tot de verwerker, dan neemt laatstgenoemde hierover direct contact op met de verwerkingsverantwoordelijke.
Voor wat betreft eventuele kosten die hiermee gepaard gaan: zie § 2.4.

4.7: Partijen zullen in onderling overleg afspraken maken over de uitvoering, de termijn van uitvoering van de DPIA en de kosten die daarmee zijn gemoeid. Als partijen hier vooraf concrete afspraken over maken, nemen ze deze op in de hoofdovereenkomst, dan wel een addendum bij de hoofdovereenkomst. Als er helemaal geen hoofdovereenkomst is, kunnen partijen het opnemen in het addendum bij de Standaard VWO. En dus niet in de Standaard VWO zelf.

5.1: Het is belangrijk dat de verwerker de verwerkingsverantwoordelijke zo snel mogelijk op de hoogte brengt van een (vermoedelijke) inbreuk. Het gaat er daarbij om dat de verwerker de verwerkingsverantwoordelijke direct informeert zodra er voldoende redenen zijn om aan te nemen dat er sprake is van een inbreuk. Als er sprake is van verdachte activiteiten, hoeft er geen sprake te zijn van een inbreuk. Verwerker moet daar wel een adequaat onderzoek naar doen. Partijen vertrouwen er daarbij op dat de verwerker professioneel genoeg is om een inschatting te maken van het incident dat moet worden gemeld. Mocht verwerker desondanks niet een goede inschatting kunnen maken van het incident, dan kan deze een second opinion vragen bij de IBD. Daarbij blijft de verantwoordelijkheid om het incident wel of niet te melden aan de verwerkingsverantwoordelijke altijd bij de verwerker. Zolang een onderzoek naar een vermoedelijke inbreuk loopt, kan de verwerker niet worden geacht "kennis" te hebben genomen van een inbreuk. De meldingstermijn van 24 uur begint op dat moment dan ook niet te lopen. Zodra de verwerker wel kennis heeft van de inbreuk, moet hij die binnen 24 uur melden bij de verwerkingsverantwoordelijke. De termijn van 24 uur is een maximale termijn.
De termijn van 72 uur die de verwerkingsverantwoordelijke heeft om de inbreuk te melden bij de toezichthoudende autoriteit begint te lopen, zodra de verwerkingsverantwoordelijke kennis heeft genomen van de inbreuk. Zie hiervoor opinie 250 van de EDPB:

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 (en dan vooral onderaan pagina 15). Dus als de inbreuk heeft plaatsgevonden bij de verwerker en deze meldt het aan de verwerkingsverantwoordelijke, heeft laatstgenoemde pas op dat moment kennis genomen van de inbreuk en begint de meldingstermijn van 72 uur te lopen.
Ten behoeve van de uiteindelijke melding aan de toezichthoudende autoriteit verstrekt de verwerker alle hem beschikbare informatie aan de Verwerkingsverantwoordelijke zoals vermeld op het formulier van Meldloket van de Autoriteit Persoonsgegevens (hierna: AP).
Let op: De verwerker doet nooit zelf een melding bij de AP.
Verwerkingsverantwoordelijke moet zorgen voor een 24/7 bereikbaarheid om zo een melding via het afgesproken kanaal in ontvangst te kunnen nemen. Als een verwerker is aangesloten bij de IBD, kan verwerker ervoor kiezen om een inbreuk ook te melden via IBD. De IBD is een CERT en is erop ingericht om in geval van een inbreuk direct alle betrokken gemeenten te informeren.

5.3 Een verwerkingsverantwoordelijke heeft alleen toegang heeft tot het logboek van de verwerker voor zover dat betrekking heeft op de verwerkingen die worden gedaan in opdracht van de verwerkingsverantwoordelijke.

5.4: De beslissing om de inbreuk te melden bij de toezichthoudende autoriteit en/of de betrokkene ligt bij de verwerkingsverantwoordelijke en niet bij de verwerker.

6.1: Afspraken over aansprakelijkheid t.a.v. de verwerking van persoonsgegevens horen thuis in de hoofdovereenkomst. Als hierover geen afspraken zijn gemaakt, adviseren wij partijen om dat alsnog te doen in een addendum bij de hoofdovereenkomst. In die gevallen dat er helemaal geen hoofdovereenkomst is, kunnen partijen ervoor kiezen om deze afspraken te maken in een addendum bij de Standaard VWO. En dus niet in de Standaard VWO zelf. Zie ook § 2.3.
Let op: Als er (in de hoofdovereenkomst, een addendum bij de hoofdovereenkomst of een addendum bij de Standaard VWO) t.a.v. de verwerking van persoonsgegevens geen aparte afspraken zijn gemaakt over aansprakelijkheid, dan geldt de aansprakelijkheidsregeling in de toepasselijke inkoopvoorwaarden, te weten de GIBIT 2023, of de van de van het VNG Model Inkoopvoorwaarden diensten en leveringen afgeleide gemeentelijke inkoopvoorwaarden, of een eventuele afwijkende aansprakelijkheidsregeling in de hoofdovereenkomst. Als in de hoofdovereenkomst of in de inkoopvoorwaarden een beperking van de aansprakelijkheid is opgenomen, adviseren wij partijen om te verifieren of deze beperking ook van toepassing is op de aansprakelijkheid t.a.v. de verwerking van persoonsgegevens en of deze beperking passend is.

7.1 Afspraken over de exit-strategie t.a.v. de verwerking van persoonsgegevens horen thuis in de hoofdovereenkomst. Als hierover geen afspraken zijn gemaakt adviseren wij partijen om dat alsnog te doen, hetzij in de hoofdovereenkomst, of in een addendum bij de hoofdovereenkomst. In die gevallen dat er helemaal geen hoofdovereenkomst is, kunnen partijen er voor kiezen om deze afspraken te maken in een addendum bij de Standaard VWO. En dus niet in de Standaard VWO zelf. Zie ook § 2.3.
Er zijn verschillende manieren waarop partijen de exit-strategie vorm kunnen geven. Artikel 26 van de GIBIT 2023 is onder andere een voorbeeld van een exit-strategie die aan de minimumvoorwaarden voldoet.

2.6 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/Welke dienst en/of product	**Verwerkings-doeleinden**	**Categorieën van betrokkenen**	**(Bijzondere) persoonsgegevens**	**Verwerkings-locatie**	**Doorgifte instrument (indien van toepassing)**	**Aanvullende maatregelen (indien van toepassing)**
Xxxxxxsite CMS	• Identificatie binnen de applicatie • Content kunnen plaatsen op website Optioneel: • Registreren nieuwsbrief abonnees (module Nieuwsbrief) • Reactiemogelijk op vacature (module Vacature)	• Aanvragers/Indieners • Belanghebbenden • Websitebezoekers • Medewerkers organisatie	• Persoonlijke gegevens: Naam, geboortedatum, geslacht • Contactgegevens: e-mailadres, telefoonnummer, adres • Inloggegevens: Gebruikersnaam, wachtwoord • Internetgegevens: IP-adres, online surfgedrag, cookies • Arbeidsgegevens: Functie, werktijden	EER	Niet van toepassing	Niet van toepassing
Xxxform (formulieren-generator)	"Benodigd om bepaalde diensten te kunnen afnemen. Bijvoorbeeld het doorgeven van een verhuizing"	• Aanvragers/Indieners • Belanghebbenden • Websitebezoekers Medewerkers organisatie	• Persoonlijke gegevens: Naam, geboortedatum, geslacht • Contactgegevens: e-mailadres, telefoonnummer, adres • Inloggegevens: Gebruikersnaam, wachtwoord • Internetgegevens: IP-adres, online surfgedrag, cookies	EER	Niet van toepassing	Niet van toepassing

			Optioneel: • BSN (bij gebruik DigiD) • Overige formuliergegevens afhankelijk van de uitvraag.			

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

1. Ingeschakelde subverwerkers

Naam en contactgegevens subverwerker	KvK-nummer	Uitbestede verwerkingen	Toepassing (geautomatiseerd systeem)	Verwerkings-locatie	Doorgifte instrument	Aanvullende maatregelen (indien van toepassing)
HostingXXX	KvK XXX	• Opslaan en hosten van persoonsgegevens • Beschikbaar stellen van persoonsgegevens ten behoeve van uitvoering van diensten • Technisch beheer met mogelijke toegang tot persoonsgegevens • Back-ups, herstel en continuïteitsvoorzieningen • Verwijderen en vernietigen van persoonsgegevens	Xxxxxxsite CMS	Duitsland - Europese Economische Ruimte (EER)	N.v.t. of gekozen instrument	Encryptie, toegangsbeperking, logging, etc.

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 verstrekt[4] 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.

[4] Hardcopy, via de mail, of via een link.

Bijlage 3:
Bijlage 3 is géén onderdeel van de Standaard VWO.

Partijen hebben niet altijd afspraken gemaakt over de aansprakelijkheid, de exit-strategie en/of de uitvoering van audits. Soms willen zij hierover alsnog afspraken maken. In de GIBIT 2023 zijn de aansprakelijkheid, de exit-strategie en de uitvoering van audits wel geregeld. In Bijlage 3 staan de artikelen uit de GIBIT 2023 over deze onderwerpen. Partijen kunnen er voor kiezen om deze artikelen over te nemen in een bijlage bij de hoofdovereenkomst of een bijlage bij de Standaard VWO (en dus niet in de Standaard VWO zelf!).

NB: Deze artikelsgewijze toelichting maakt onderdeel uit van de Standaard Verwerkersovereenkomst.

3. Colofon

Naam document
Standaard verwerkersovereenkomst gemeenten

Versienummer
2.53

Versiedatum
15-12 2025

Versiebeheer
Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).

Rechten en vrijwaring
De IBD is zich bewust van haar verantwoordelijkheid een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kan de IBD geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. De IBD aanvaardt ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

Met dank aan

De gemeenten, leveranciers en derden die hebben bijgedragen aan de totstandkoming van dit document. In het bijzonder de toetsgroep, de klankbordgroep en Beheergroep VWO die hebben bijgedragen aan het verwerken van de feedback.

Wijzigingshistorie:

Versie	Datum	Wijziging / Actie
0.1	20-05-2018	Opzet
		Bespreking met leveranciers en gemeenten.
0.2	17-06-2018	Commentaar bespreking verwerkt.
		Voorgelegd aan alle contactpersonen van gemeenten en leveranciers.
0.99	30-07-2018	Commentaar Leveranciers en Gemeenten verwerkt.
1.00	01-08-2018	Voorpublicatie IBD website – Ter vaststelling aangeboden aan het College van Dienstverlening.
1.09	07-11-2018	Versie aangepast na consultatie gemeenten en leveranciers. Deze versie wordt voorgelegd aan toetsgroep.
1.10	15-11-2018	Versie aangepast op basis van beslissing toetsgroep d.d. 12-11-2018
1.11	30-11-2018	Versie aangepast op basis van consultatie Beheergroep VWO (toetsgroep gemeenten en klankbordgroep leveranciers).
2.0	28-03-2019	Versie aangepast conform input Landsadvocaat en besluitvorming Beheergroep VWO.
2.1	11-11-2019	Versie 2.0 aangepast n.a.v. bijeenkomst Beheergroep VWO d.d. 10-10-2019.
2.2	08-04-2020	Versie 2.1 aangepast conform besluit Beheergroep VWO.
2.3	19-11-2020	Versie 2.2 aangepast conform besluit beheergroep VWO
2.3-3	19-01-2021	Versie 2.3-3 aangepast o.b.v. EDPB advies n.a.v. Schrems II
2.4	12-04-2021	Versie 2.3-3 aangepast conform besluit Beheergroep VWO
2.41	15-12-2021	Versie 2.4 aangepast conform besluit Beheergroep VWO
2.42	15-08-2023	Versie 2.42 aangepast conform besluit Beheergroep VWO
2.5	15-02-2024	Versie 2.42 aangepast conform besluit Beheergroep VWO
2.51	18-06-2024	Versie 2.5 aangepast conform besluit Beheergroep VWO
2.51a	03-10-2024	Versie 2.51 ingevuld voor ICT Prestatie Stratech Perspectief Cloud.
2.51b	12-03-2025	Subverwerkers van Interaction Next B.V. toegevoegd.
2.51c	26-03-2025	Nieuw certificaat en update VVT wegens transitie naar nieuwe norm voor ISO 27001.
2.52	01-04-2025	Versie 2.51c aangepast conform besluit Beheergroep VWO.
2.52a	08-05-2025	Bijlage 1 en 2 verder ingevuld.
2.52b	14-10-2025	Wijziging naam subverwerker Interaction Next BV naar Xential BV
2.52c	11-11-2025	Verwerking ‘Analyses’ verwijderd
2.53	15-12-2025	Versie 2.52 aangepast conform besluit Beheergroep VWO
2.53a	15-04-2026	Bijlage 1 en 2 ingevuld en aangevuld.

Over de IBD

De IBD is een gezamenlijk initiatief van alle Nederlandse Gemeenten. De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en richt zich op (incident)ondersteuning op het gebied van

informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD ondersteunt gemeenten bij hun inspanningen op het gebied van informatiebeveiliging en privacy / gegevensbescherming en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. Alle Nederlandse gemeenten kunnen gebruikmaken van de producten en de generieke dienstverlening van de IBD. De IBD is ondergebracht bij VNG Realisatie.