INFORMATIE
BEVEILIGINGS
DIENST

VNG Realisatie

# Standaard Verwerkersovereenkomst Gemeenten

INFORMATIE
BEVEILIGINGS
DIENST

# Colofon

## Naam document
Standaard verwerkersovereenkomst gemeenten

## Versienummer
2.51

## Versiedatum
18-06-2024

## 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 |

## 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.

# Toelichting

Dit product 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.

## 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. 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.

## Maatregelen Baseline Informatiebeveiliging Overheid (BIO)

Maatregel 15.1.1.3

Met alle leveranciers die als verwerker voor of namens de organisatie persoonsgegevens verwerken, worden verwerkersovereenkomsten gesloten waarin alle wettelijk vereiste afspraken zijn vastgesteld.

# 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.

# 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, 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. 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[1]:
Aansprakelijkheid : artikel 16
Exit-strategie : artikel 24.14 en artikel 26
Audit : artikel 25[2]

## 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.

[1] Voor vragen over de GIBIT 2023 kunt u contact opnemen met info@gibit.nl
[2] 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: 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, audits en de exit-strategie 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 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.

7.1 Afspraken over de exit-strategie, audits en de 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, 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 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).

Volgens de aanbevelingen van de EDPB n.a.v. de Schrems II uitspraak van het Hof van Justitie van de EU (Recommendations 01/2020, d.d. 10 november 2020) moeten aanvullende maatregelen genomen worden als gebruik wordt gemaakt van doorgifte-instrument 3 – 6. Zo wordt nl. een aan de AVG gelijkwaardig beschermingsniveau bewerkstelligd (zie Bijlage 2 van de EDPB aanbevelingen).

Hieronder een voorbeeld :

| Naam verwerking/Welke dienst en/of product | Verwerkings-doeleinden | Categorieën van betrokkenen | (Bijzondere) persoonsgegevens | Verwerkings-locatie | Doorgifte instrument | Aanvullende maatregelen (indien van toepassing) |
|---|---|---|---|---|---|---|
| Xxxxxxsite CMS | " - identificatie binnen de applicatie - content kunnen plaatsen - registreren nieuwsbrief abonnees - reactiemogelijk op content (bv vacature)" | Gebruiker van de dienstverlening (medewerkers en inwoners) | NAW / Gebruikersnaam en wachtwoord) / emailadres / telefoonnummer / pasfoto / politieke partij | EER | | |
| Xxxform | "Benodigd om bepaalde diensten te kunnen afnemen. Bijvoorbeeld het doorgeven van een verhuizing" | Gebruiker van de dienstverlening (bezoeker website) | NAW / BSN / Overige formuliergegevens (afhankelijk van uitvraag) | EER | | |

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.
- De IBD is telefonisch 24 uur per dag bereikbaar. De mail van de IBD wordt niet 24 uur per dag gelezen.

Tabel 3: hier wordt ingevuld:

- Indien er sprake is van subverwerkers, dan vult verwerker dat hier in. Verwerker zorgt dat vanaf de start van de verwerkersovereenkomst inzichtelijk is welke subverwerkers zijn ingeschakeld en waar de gegevens worden verwerkt. Als een subverwerker de gegevens in een derde land verwerkt, moet deze aangeven wat het doorgifte instrument is en welke eventuele noodzakelijke aanvullende maatregelen zijn getroffen.

**Bijlage 2:**

Bijlage 2 is een praktische uitwerking van artikel 32 AVG. Dus verwerker geeft hier aan 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. En 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 BIO 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[3] 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.

**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] Hardcopy, dia de mail, of via een link.

# 3. 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>**
De burgemeester van <naam gemeente>

namens deze: <naam, functie>

plaats: <……>

datum: <……>

**<Naam organisatie>**

namens deze: <naam, functie>

plaats: <……>

datum: <……>

## Bijlage 1: Overzicht van te verwerken persoonsgegevens

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 kan daardoor, bijvoorbeeld als gevolg van een Update, wijzigingen.

**Versiebeheer bijlage 1**

| DATUM | WIJZIGING |
|---|---|
| 03-10-2024 | Eerste versie |

**Persoonsgegevens**
Verwerkingsverantwoordelijke verwerkt gegevens van personen die afzonderlijk of gecombineerd redelijkerwijs een natuurlijk persoon identificeren (identificerende persoonsgegevens). Verwerkingsverantwoordelijke maakt daarvoor gebruik van de ICT Prestatie Stratech Perspectief Cloud. Het betreft onderstaande (categorieën van) gegevens voor cliënten:

- Naamgegevens (zoals voornaam, achternaam);
- Adresgegevens (zoals straat, huisnummer, postcode, plaats, land);
- Contactgegevens (zoals e-mailadres, telefoonnummer);
- Geboortedatum;
- Bankgegevens (zoals IBAN, BIC);
- BSN[4].

Naast de identificerende persoonsgegevens betreffende cliënten verwerkt Verwerkingsverantwoordelijke de navolgende aanvullende (categorieën van) persoonsgegevens die betrekking hebben op de natuurlijk persoon:

- Gebruikershistorie;
- Schulden;
- Vermogen en bezittingen;
- Cliënthistorie;
- Sociale netwerk;
- Inkomsten en uitgaven;
- Gegevens die noodzakelijk zijn voor de berekening van de afloscapaciteit (Vtlb-gegevens);
- Gegevens die noodzakelijke zijn voor het aanleveren van de WSNP-verklaring;
- Aanvullende gegevens van cliënten (zoals geslacht, geboorteland, partner en kinderen, opleidingsniveau, verblijfsstatus, et cetera);
- Gegevens die terugkomen in plan van aanpak van de VNG.

Het betreft onderstaande (categorieën van) gegevens voor Gebruikers:

- Naamgegevens (zoals voornaam, achternaam);
- Contactgegevens (zoals e-mailadres, telefoonnummer);
- Logging;
- Dienstverband (datum in dienst en datum uit dienst).

Verwerkingsverantwoordelijke legt geen andere dan de hiervoor genoemde (categorieën van)

[4] Wanneer daar een wettelijke basis voor is.

persoonsgegevens vast.

**Werkzaamheden**
Verwerker verwerkt ten behoeve van verwerkingsverantwoordelijke hierboven beschreven (categorieën van) persoonsgegevens. De werkzaamheden vloeien voort uit de tussen Leverancier en Opdrachtgever gesloten overeenkomsten en betreffen één of meerdere van de hieronder genoemde werkzaamheden:

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 werkzaamheden vanuit de SaaS omgeving van Verwerker waarbij persoonsgegevens worden uitgewisseld (ontvangen of doorgezonden) met systemen van derden.
3. Analyses
   Dit betreft geautomatiseerde werkzaamheden waarbij gegevens waaronder persoonsgegevens worden geanalyseerd.
4. 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.
5. Implementatie diensten
   Dit betreft veelal implementatie diensten of andere werkzaamheden die door (een consultant van) Verwerker op locatie van Verwerkingsverantwoordelijke of vanaf locatie 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.

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

**Contactgegevens**

| | |
|---|---|
| **Contactpersoon Verwerkingsverantwoordelijke (NB: Ook buiten kantooruren)** | Naam:<br>Contactgegevens: |
| **Contactpersoon Verwerker (NB: Ook buiten kantooruren)** | Naam:<br>Contactgegevens: privacy@stratech.nl |
| **Contactgegevens IBD** | telefoonnummer: 070-204 55 11<br>e-mailadres: privacy@vng.nl |

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

**Subverwerkers**

Naam: Microsoft Corporation
KvK: (geen)
Contactgegevens: 1 Microsoft Way, Redmond, WA 98052 USA
Verwerkingen: (beheer)werkzaamheden ten behoeve van de infrastructuur waarop de Standaardprogrammatuur Stratech Perspectief Cloud beschikbaar wordt gesteld
Toepassing: Azure diensten
Verwerkingslocatie: EER
Doorgifte-instrument: Niet van toepassing

Aanvullende maatregelen: Niet van toepassing

Naam: Interaction Next 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

**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.

De informatie heeft betrekking op de Standaardprogrammatuur Stratech-Perspectief vanaf versie 1.33.

| 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. De Standaardprogrammatuur Stratech Perspectief Cloud (hierna Perspectief Cloud) zendt de vereiste gegevens door naar de calculator. De calculator verzorgt vervolgens alles rondom de uitvoering van de berekening. De resultaten van de berekening zendt de calculator terug naar Perspectief Cloud.<br><br>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.<br><br>De calculator is een .dll bestand dat wordt ingeladen door de Perspectief Cloud. De doorzending van gegevens tussen Perspectief Cloud en de calculator vindt daardoor plaats binnen het werkgeheugen van 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.*”<br><br>De door de calculator gehanteerde beveiligingsmaatregelen worden bepaald door Bureau WSNP. |

## Bijlage 2: Aantonen passend niveau van beveiliging

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: 12 mei 2023

□ 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 afgeleid worden 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 DGT271721337 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 27001:2017+A11:2020

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 1.1 van 3 mei 2023.

*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:
12 mei 2023

Dit certificaat is geldig tot:
12 mei 2026

Datum eerste certificaat:
12 mei 2023

Dit certificaat vervangt nr:
--

**NAMENS**

Marco Bijl
Digitrust B.V.

RvA MGMT. SYS. 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

Behorende bij het certificaat met registratienummer: DGT271721337
Het informatiebeveiligingsmanagementsysteem van: Stratech Automatisering B.V.

Werkmaatschappijen en geregistreerde activiteiten

---

Stratech Opleiding en Advies B.V.
Pantheon 15
7521PR ENSCHEDE

INFORMATIE
BEVEILIGINGS
DIENST

## Verklaring van toepasselijkheid (VVT)

ISO27001:2017 +A11:2020 Verklaring van toepasselijkheid
Stratech
Versie 1.1
Datum: 3-5-2023

| | | | Van toepassing? | Geïmplementeerd? | Wet Contract Risicoanalyse | Onderbouwing waarom niet van toepassing |
|---|---|---|---|---|---|---|
| **A.5** | **Beveiligingsbeleid** | | | | | |
| **A.5.1** | **Managementaanwijzing voor informatiebeveiliging** | Het verschaffen van directieaansturing van en -steun voor informatiebeveiliging in overeenstemming met bedrijfseisen en relevante wet- en regelgeving. | | | | |
| A.5.1.1 | **Beleidsregels voor informatiebeveiliging** | Ten behoeve van informatiebeveiliging moet een reeks beleidsregels worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen. | Ja | Ja | X | |
| A.5.1.2 | **Beoordeling van het Informatiebeveiligingsbeleid** | Het beleid voor informatiebeveiliging moet met geplande tussenpozen of als zich significante veranderingen voordoen, worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is. | Ja | Ja | X | |
| **A.6** | **Organisatie van informatiebeveiliging** | | | | | |
| **A.6.1** | **Interne organisatie** | Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen. | | | | |
| A.6.1.1 | **Rollen en verantwoordelijkheden bij informatiebeveiliging** | Alle verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen. | Ja | Ja | X | |
| A.6.1.2 | **Scheiding van taken** | Conflicterende taken en verantwoordelijkheidsgebieden moeten worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen. | Ja | Ja | X | |
| A.6.1.3 | **Contact met overheidsinstanties** | Er moeten passende contacten met relevante overheidsinstanties worden onderhouden. | Ja | Ja | X | |
| A.6.1.4 | **Contact met speciale belangengroepen** | Er moeten passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties worden onderhouden. | Ja | Ja | X | |
| A.6.1.5 | **Informatiebeveiliging in projectbeheer** | Informatiebeveiliging moet aan de orde komen in projectbeheer, ongeacht het soort project. | Ja | Ja | X | |
| **A.6.2** | **Mobiele computers en telewerken** | Het waarborgen van de veiligheid van telewerken en het gebruik van mobiele apparatuur. | | | | |
| A.6.2.1 | **Beleid voor mobiele apparatuur** | Beleid en ondersteunende beveiligingsmaatregelen moeten worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren. | Ja | Ja | X | |
| A.6.2.2 | **Telewerken** | Beleid en ondersteunende beveiligingsmaatregelen moeten worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt bereikt, verwerkt of opgeslagen. | Ja | Ja | X | |
| **A.7** | **Beveiliging personeel** | | | | | |
| **A.7.1** | **Voorafgaand aan het dienstverband** | Waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de functies waarvoor zij in aanmerking komen. | | | | |
| A.7.1.1 | **Screening** | Verificatie van de achtergrond van alle kandidaten voor een dienstverband moet worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en moet in verhouding staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's. | NEE | Ja | X | |
| A.7.1.2 | **Arbeidsvoorwaarden** | De contractuele overeenkomst met medewerkers en contractanten moet hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie vermelden. | Ja | Ja | X X | |
| **A.7.2** | **Tijdens het dienstverband** | Ervoor zorgen dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen. | | | | |
| A.7.2.1 | **Directieverantwoordelijkheden** | De directie moet van alle medewerkers en contractanten eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie. | Ja | Ja | X X | |
| A.7.2.2 | **Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging** | Alle medewerkers van de organisatie en, voor zover relevant, contractanten moeten een passende bewustzijns-opleiding en -training krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie. | Ja | Ja | X | |
| A.7.2.3 | **Disciplinaire procedure** | Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging. | Ja | Ja | X | |
| **A.7.3** | **Beëindiging en wijziging dienstverband** | Het beschermen van de belangen van de organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het dienstverband. | | | | |
| A.7.3.1 | **Beëindiging of wijziging van verantwoordelijkheden van het dienstverband** | Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband moeten worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer worden gebracht. | Ja | Ja | X | |
| **A.8** | **Beheer Bedrijfsmiddelen** | | | | | |
| **A.8.1** | **Verantwoordelijkheden voor bedrijfsmiddelen** | Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren. | | | | |
| A.8.1.1 | **Inventariseren van bedrijfsmiddelen** | Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten worden geïdentificeerd, en van deze bedrijfsmiddelen moet een inventaris worden opgesteld en onderhouden. | Ja | Ja | X | |
| A.8.1.2 | **Eigendom van bedrijfsmiddelen** | Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden moeten een eigenaar hebben. | Ja | Ja | X | |
| A.8.1.3 | **Aanvaardbaar gebruik van bedrijfsmiddelen** | Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten regels worden geïdentificeerd, gedocumenteerd en geïmplementeerd. | Ja | Ja | X | |
| A.8.1.4 | **Teruggeven van bedrijfsmiddelen** | Alle medewerkers en externe gebruikers moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst teruggeven. | Ja | Ja | X | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| A.8.2.3 | Behandelen van bedrijfsmiddelen | Procedures voor het behandelen van bedrijfsmiddelen moeten worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie. | Ja | Ja | | | X | |
| A.8.3 | Behandeling media | Onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie die op media is opgeslagen voorkomen. | | | | | | |
| A.8.3.1 | Beheer van verwijderbare media | Voor het beheren van verwijderbare media moeten procedures worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld. | Ja | Ja | | | X | |
| A.8.3.2 | Verwijderen van media | Media moeten op een veilige en beveiligde manier worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures | Ja | Ja | | | X | |
| A.8.3.3 | Media fysiek overdragen | Media die informatie bevatten, moeten worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport. | Ja | Ja | | | X | |
| A.9 | Toegangscontrole | | | | | | | |
| A.9.1 | Bedrijfsvereisten voor toegangscontrole | Toegang tot informatie en informatieverwerkende faciliteiten beperken. | | | | | | |
| A.9.1.1 | Beleid voor toegangsbeveiliging | Een beleid voor toegangsbeveiliging moet worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen. | Ja | Ja | | | X | |
| A.9.1.2 | Toegang tot netwerken en netwerkdiensten | Gebruikers moeten alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. | Ja | Ja | | | X | |
| A.9.2 | Beheer van toegangsrechten van gebruikers | Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen. | | | | | | |
| A.9.2.1 | Registratie en uitschrijving van gebruikers | Een formele registratie- en uitschrijvingsprocedure moet worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken. | Ja | Ja | | | X | |
| A.9.2.2 | Gebruikers toegang verlenen | Een formele gebruikerstoegangs-verleningsprocedure moet worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken. | Ja | Ja | | | X | |
| A.9.2.3 | Beheren van speciale toegangsrechten | Het toewijzen en gebruik van bevoorrechte toegangsrechten moeten worden beperkt en gecontroleerd. | Ja | Ja | | | X | |
| A.9.2.4 | Beheer van geheime authenticatieinformatie van gebruikers | Het toewijzen van geheime authenticatie-informatie moet worden beheerst via een formeel beheersproces. | Ja | Ja | | | X | |
| A.9.2.5 | Beoordeling van toegangsrechten van gebruikers | Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig beoordelen. | Ja | Ja | | | X | |
| A.9.2.6 | Toegangsrechten intrekken of aanpassen | De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten moeten bij beëindiging van hun dienstverband, contract of overeenkomst worden verwijderd, en bij wijzigingen moeten ze worden aangepast. | Ja | Ja | | | X | |
| A.9.3 | Verantwoordelijkheden van gebruikers | Gebruikers verantwoordelijk maken voor het beschermen van hun authenticatie-informatie. | | | | | | |
| A.9.3.1 | Geheime authenticatie-informatie gebruiken | Van gebruikers moet worden verlangd dat zij zich bij het gebruiken van geheime authenticatieinformatie houden aan de praktijk van de organisatie. | Ja | Ja | | | X | |
| A.9.4 | Systeem en applicatie toegangscontrole | Onbevoegde toegang tot systemen en toepassingen voorkomen. | | | | | | |
| A.9.4.1 | Beperking toegang tot informatie | Toegang tot informatie en systeemfuncties van applicaties moet worden beperkt in overeenstemming met het beleid voor toegangscontrole. | Ja | Ja | | | X | |
| A.9.4.2 | Beveiligde inlogprocedures | Indien het beleid voor toegangsbeveiliging dit vereist, moet toegang tot systemen en toepassingen worden beheerst door een beveiligde inlogprocedure. | Ja | Ja | | | X | |
| A.9.4.3 | Systeem voor wachtwoordbeheer | Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen. | Ja | Ja | | | X | |
| A.9.4.4 | Speciale systeemhulpmiddelen gebruiken | Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen moet worden beperkt en nauwkeurig worden gecontroleerd. | Ja | Ja | | | X | |
| A.9.4.5 | Toegangsbeveiliging op programmabroncode | Toegang tot de programmabroncode moet worden beperkt. | Ja | Ja | | | X | |
| A.10 | Cryptografie | | | | | | | |
| A.10.1 | Cryptografische beheersmaatregelen | Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen. | | | | | | |
| A.10.1.1 | Beleid inzake het gebruik van cryptografische beheersmaatregelen | Ter bescherming van informatie moet een beleid voor het gebruik van cryptografische beheersmaatregelen worden ontwikkeld en geïmplementeerd. | Ja | Ja | | | X | |
| A.10.1.2 | Sleutelbeheer | Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels moet tijdens hun gehele levenscyclus een beleid worden ontwikkeld en geïmplementeerd. | Ja | Ja | | | X | |
| A.11 | Fysieke en omgevingsbeveiliging | | | | | | | |
| A.11.1 | Beveiligde gebieden | Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatieverwerkende faciliteiten van de organisatie voorkomen. | | | | | | |
| A.11.1.1 | Fysieke beveiligingszone | Beveiligingszones moeten worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten. | Ja | Ja | | | X | |
| A.11.1.2 | Fysieke toegangsbeveiliging | Beveiligde gebieden moeten worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt. | Ja | Ja | | | X | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| A.11.1.3 | Kantoren, ruimten en faciliteiten beveiligen | Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en toegepast. | Ja | Ja | | | X | |
| A.11.1.4 | Beschermen tegen bedreigingen van buitenaf | Tegen natuurrampen, kwaadwillige aanvallen of ongelukken moet fysieke bescherming worden ontworpen en toegepast. | Ja | Ja | | | X | |
| A.11.1.5 | Werken in beveiligde gebieden | Voor het werken in beveiligde gebieden moeten procedures worden ontwikkeld en toegepast. | Ja | Ja | | | X | |
| A.11.1.6 | Laad- en loslocatie | Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, moeten worden beheerst, en zo mogelijk worden afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden. | Ja | Ja | | | X | |
| A.11.2 | Beveiliging van apparatuur | Verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie voorkomen. | | | | | | |
| A.11.2.1 | Plaatsing en bescherming van apparatuur | Apparatuur moet zo worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind. | Ja | Ja | | | X | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| A.11.2.2 | Nutsvoorzieningen | Apparatuur moet worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen. | Ja | Ja | | | X | |
| A.11.2.3 | Beveiliging van bekabeling | Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen interceptie, verstoring of schade. | Ja | Ja | | | X | |
| A.11.2.4 | Onderhoud van apparatuur | Apparatuur moet correct worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen. | Ja | Ja | | | X | |
| A.11.2.5 | Verwijdering van bedrijfsmiddelen | Apparatuur, informatie en software mogen niet van de locatie worden meegenomen zonder voorafgaande goedkeuring. | Ja | Ja | | | X | |
| A.11.2.6 | Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein | Bedrijfsmiddelen die zich buiten het terrein bevinden, moeten worden beveiligd, waarbij rekening moet worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie. | Ja | Ja | | | X | |
| A.11.2.7 | Veilig verwijderen of hergebruiken van apparatuur | Alle onderdelen van de apparatuur die opslagmedia bevatten, moeten worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of veilig zijn overschreven. | Ja | Ja | | | X | |
| A.11.2.8 | Onbeheerde gebruikersapparatuur | Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is. | Ja | Ja | | | X | |
| A.11.2.9 | 'Clear desk'- en 'clear screen'beleid | Er moet een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten worden ingesteld. | Ja | Ja | | | X | |
| A.12 | Beveiliging operatie | | | | | | | |
| A.12.1 | Bedieningsprocedures en verantwoordelijkheden | Correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen. | | | | | | |
| A.12.1.1 | Gedocumenteerde bedieningsprocedures | Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben. | Ja | Ja | | | X | |
| A.12.1.2 | Wijzigingsbeheer | Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging moeten worden beheerst. | Ja | Ja | | | X | |
| A.12.1.3 | Capaciteitsbeheer | Het gebruik van middelen moet worden gemonitord en afgestemd, en er moeten verwachtingen worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen. | Ja | Ja | | | X | |
| A.12.1.4 | Scheiding van ontwikkel-, test- en productieomgevingen | Ontwikkel-, test- en productieomgevingen moeten worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen. | Ja | Ja | | | X | |
| A.12.2 | Bescherming Malware | Waarborgen dat informatie en informatieverwerkende faciliteiten beschermd zijn tegen malware. | | | | | | |
| A.12.2.1 | Beheersmaatregelen tegen malware | Ter bescherming tegen malware moeten beheersmaatregelen voor detectie, preventie en herstel worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers. | Ja | Ja | | | X | |
| A.12.3 | Back-up | Beschermen tegen het verlies van gegevens. | | | | | | |
| A.12.3.1 | Back-up van informatie | Regelmatig moeten back-upkopieën van informatie, software en systeemafbeeldingen worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid. | Ja | Ja | | | X | |
| A.12.4 | Logging en bewaking | Gebeurtenissen vastleggen en bewijs verzamelen. | | | | | | |
| A.12.4.1 | Gebeurtenissen registreren | Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligings-gebeurtenissen registreren, moeten worden gemaakt, bewaard en regelmatig worden beoordeeld. | Ja | Ja | | | X | |
| A.12.4.2 | Beschermen van informatie in logbestanden | Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang. | Ja | Ja | | | X | |
| A.12.4.3 | Logbestanden van beheerders en operators | Activiteiten van systeembeheerders en -operators moeten worden vastgelegd en de logbestanden moeten worden beschermd en regelmatig worden beoordeeld. | Ja | Ja | | | X | |
| A.12.4.4 | Kloksynchronisatie | De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein moeten worden gesynchroniseerd met één referentietijdbron. | Ja | Ja | | | X | |
| A.12.5 | Beheersing van operationele programmatuur | De integriteit van operationele systemen waarborgen. | | | | | | |
| A.12.5.1 | Software installeren op operationele systemen | Om het op operationele systemen installeren van software te beheersen moeten procedures worden geïmplementeerd. | Ja | Ja | | | X | |
| A.12.6 | Beheer van technische kwetsbaarheden | Benutting van technische kwetsbaarheden voorkomen. | | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| A.12.6.1 | Beheersing van technische kwetsbaarheden | Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt moet tijdig worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en passende maatregelen moeten worden genomen om het risico dat ermee samenhangt aan te pakken. | Ja | Ja | | | X | |
| A.12.6.2 | Beperkingen voor het installeren van software | Voor het door gebruikers installeren van software moeten regels worden vastgesteld en geïmplementeerd. | Ja | Ja | | | X | |
| A.12.7 | Overwegingen bij audits van informatiesystemen | De impact van auditactiviteiten op uitvoeringssystemen zo gering mogelijk maken. | | | | | | |
| A.12.7.1 | Beheersmaatregelen betreffende audits van informatiesystemen | Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, moeten zorgvuldig worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren. | Ja | Ja | | | X | |
| A.13 | Beveiliging van verbindingen | | | | | | | |
| A.13.1 | Beheer van netwerkbeveiliging | De bescherming van informatie in netwerken en de ondersteunende informatieverwerkende faciliteiten waarborgen. | | | | | | |
| A.13.1.1 | Beheersmaatregelen voor netwerken | Netwerken moeten worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen. | Ja | Ja | | | X | |
| A.13.1.2 | Beveiliging van netwerkdiensten | Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten moeten worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede | Ja | Ja | | | X | |
| A.13.1.3 | Scheiding in netwerken | diensten.<br>Groepen van informatiediensten, -gebruikers en -systemen moeten in netwerken worden gescheiden. | Ja | Ja | | | X | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| A.13.2 | Informatie-uitwisseling | Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe entiteit. | | | | | | |
| A.13.2.1 | Beleid en procedures voor informatietransport | Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, moeten formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht zijn. | Ja | Ja | | | X | |
| A.13.2.2 | Overeenkomsten over informatietransport | Overeenkomsten moeten betrekking hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen. | Ja | Ja | | X | X | |
| A.13.2.3 | Elektronische berichten | Informatie die is opgenomen in elektronische berichten moet passend beschermd zijn. | Ja | Ja | | | X | |
| A.13.2.4 | Vertrouwelijkheids- of geheimhoudingsovereenkomst | Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen moeten worden vastgesteld, regelmatig worden beoordeeld en gedocumenteerd. | Ja | Ja | | | X | |
| A.14 | Verwerving, ontwikkeling en onderhoud van informatiesystemen | | | | | | | |
| A.14.1 | Beveiligingseisen voor informatiesystemen | Waarborgen dat informatiebeveiliging integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus. Hiertoe behoren ook de eisen voor informatiesystemen die diensten verlenen via openbare netwerken. | | | | | | |
| A.14.1.1 | Analyse en specificatie van informatiebeveiligings-eisen | De eisen die verband houden met informatiebeveiliging moeten worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen. | Ja | Ja | | | X | |
| A.14.1.2 | Toepassingsdiensten op openbare netwerken beveiligen | Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, moet worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging. | Ja | Ja | | | X | |
| A.14.1.3 | Transacties van toepassingsdiensten beschermen | Informatie die deel uitmaakt van transacties van toepassingsdiensten moet worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen. | ja | Ja | | | X | |
| A.14.2 | Beveiliging bij ontwikkelings- en ondersteuningsprocessen | Bewerkstelligen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen. | | | | | | |
| A.14.2.1 | Beleid voor beveiligd ontwikkelen | Voor het ontwikkelen van software en systemen moeten regels worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie worden toegepast. | Ja | Ja | | | X | |
| A.14.2.2 | Procedures voor wijzigingsbeheer met betrekking tot systemen | Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling moeten worden beheerst door het gebruik van formele controleprocedures voor wijzigingsbeheer. | Ja | Ja | | | X | |
| A.14.2.3 | Technische beoordeling van toepassingen na wijzigingen bedieningsplatform | Als bedieningsplatforms zijn veranderd, moeten bedrijfskritische toepassingen worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie. | Ja | Ja | | | X | |
| A.14.2.4 | Beperkingen op wijzigingen aan softwarepakketten | Wijzigingen aan softwarepakketten moeten worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen moeten strikt worden gecontroleerd. | Ja | Ja | | | X | |
| A.14.2.5 | Principes voor engineering van beveiligde systemen | Principes voor de engineering van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen. | Ja | Ja | | | X | |
| A.14.2.6 | Beveiligde ontwikkelingsomgeving | Organisaties moeten beveiligde ontwikkelomgevingen vaststellen en passend beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling. | Ja | Ja | | | X | |
| A.14.2.7 | Uitbestede software- ontwikkeling | Uitbestede systeemontwikkeling moet onder supervisie staan van en worden gemonitord door de organisatie. | Nee | Nee | | | | We besteden geen software ontwikkeling uit. |
| A.14.2.8 | Testen van systeembeveiliging | Tijdens ontwikkelactiviteiten moet de beveiligingsfunctionaliteit worden getest. | Ja | Ja | | | X | |
| A.14.2.9 | Systeemacceptatietests | Voor nieuwe informatiesystemen, upgrades en nieuwe versies moeten programma's voor het uitvoeren van acceptatietests en gerelateerde criteria worden vastgesteld. | Ja | Ja | | | X | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| A.14.3 | Testgegevens | Bescherming waarborgen van gegevens die voor het testen zijn gebruikt. | | | | | | |
| A.14.3.1 | Bescherming van testgegevens | Testgegevens moeten zorgvuldig worden gekozen, beschermd en gecontroleerd. | Ja | Ja | | | X | |
| A.15 | Relaties leveranciers | | | | | | | |
| A.15.1 | Informatiebeveiliging in leveranciersrelaties | De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers. | | | | | | |
| A.15.1.1 | Informatiebeveiligings-beleid voor leveranciersrelaties | Met de leverancier moeten de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, worden overeengekomen en gedocumenteerd. | Ja | Ja | | | X | |
| A.15.1.2 | Opnemen van beveiligingsaspecten in leveranciers-overeenkomsten | Alle relevante informatiebeveiligings-eisen moeten worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuur-elementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt. | Ja | Ja | X | X | X | |
| A.15.1.3 | Toeleveringsketen van informatieen communicatie-technologie | Overeenkomsten met leveranciers moeten eisen bevatten die betrekking hebben op de informatiebeveiligings-risico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie. | Ja | Ja | | | X | |
| A.15.2 | Beheersing van leveranciersdiensten | Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven. | | | | | | |
| A.15.2.1 | Monitoring en beoordeling van dienstverlening van leveranciers | Organisaties moeten regelmatig de dienstverlening van leveranciers monitoren, beoordelen en auditen. | Ja | Ja | | | X | |
| A.15.2.2 | Beheer van veranderingen in dienstverlening van leveranciers | Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, moeten worden beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's. | Ja | Ja | | | X | |
| A.16 | Beheer van informatiebeveiligingsincidenten | | | | | | | |
| A.16.1 | Rapportage van informatiebeveiligingsgebeurtenissen en verbeteringen | Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging. | | | | | | |
| A.16.1.1 | Verantwoordelijkheden en procedures | Directieverantwoordelijkheden en -procedures moeten worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatie-beveiligingsincidenten te bewerkstelligen. | Ja | Ja | | | X | |
| A.16.1.2 | Rapportage van informatiebeveiligingsgebeurtenissen | Informatiebeveiligingsgebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd. | Ja | Ja | | | X | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| A.16.1.3 | Rapportage van zwakke plekken in de informatiebeveiliging | Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie moet worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren. | Ja | Ja | | | X | |
| A.16.1.4 | Beoordeling van en besluitvorming over informatiebeveiligings- | Informatiebeveiligingsgebeurtenissen moeten worden beoordeeld en er moet worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten. | Ja | Ja | | | X | |
| A.16.1.5 | Respons op informatiebeveiligingsincidenten | Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures. | Ja | Ja | | | X | |
| A.16.1.6 | Lering uit informatiebeveiligingsincidenten | Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen moet worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen. | Ja | Ja | | | X | |
| A.16.1.7 | Verzamelen van bewijsmateriaal | De organisatie moet procedures definiëren en toepassen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen. | Ja | Ja | | | X | |
| A.17 | Informatiebeveiligings-aspecten van bedrijfscontinuïteitsbeheer | | | | | | | |
| A.17.1 | informatiebeveiliging in het proces van bedrijfscontinuïteitsbeheer | Informatiebeveiligingscontinuïteit moet worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie. | | | | | | |
| A.17.1.1 | Informatiebeveiligingscontinuïteit plannen | De organisatie moet haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vaststellen. | Ja | Ja | | | X | |
| A.17.1.2 | Informatiebeveiligingscontinuïteit implementeren | De organisatie moet processen, procedures en beheersmaatregelen vaststellen, documenteren, implementeren en handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen. | Ja | Ja | | | X | |
| A.17.1.3 | Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren | De organisatie moet de ten behoeve van informatiebeveiligings-continuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties. | Ja | Ja | | | X | |
| A.17.2 | Redundancies | Beschikbaarheid van informatieverwerkende faciliteiten bewerkstelligen. | | | | | | |
| A.17.2.1 | Beschikbaarheid van informatieverwerkende faciliteiten | Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen. | Ja | Ja | | X | X | |
| A.18 | Naleving | | | | | | | |
| A.18.1 | Naleving van wettelijke en contractuele verplichtingen | Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen. | | | | | | |
| A.18.1.1 | Vaststellen van toepasselijke wetgeving en contractuele eisen | Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen moeten voor elk informatiesysteem en de organisatie expliciet worden | Ja | Ja | X | X | X | |
| A.18.1.2 | Intellectuele eigendomsrechten | vastgesteld, gedocumenteerd en actueel gehouden.<br>Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectuele-eigendomsrechten en het gebruik van eigendomssoftwareproducten te waarborgen moeten passende procedures worden geïmplementeerd. | Ja | Ja | X | | X | |
| A.18.1.3 | Beschermen van registraties | Registraties moeten in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave. | Ja | Ja | X | | X | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| A.18.1.4 | Privacy en bescherming van persoonsgegevens | Privacy en bescherming van persoonsgegevens moeten, voor zover van toepassing, worden gewaarborgd in overeenstemming met relevante wet- en regelgeving. | Ja | Ja | X | | X | |
| A.18.1.5 | Voorschriften voor het gebruik van cryptografische beheersmaatregelen | Cryptografische beheersmaatregelen moeten worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving. | Ja | Ja | X | | X | |
| A.18.2 | Herbeoordelingen van informatiebeveiliging | Verzekeren dat informatiebeveiliging wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie. | | | | | | |
| A.18.2.1 | Onafhankelijk beoordeling van informatiebeveiliging | De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheersdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen worden beoordeeld. | Ja | Ja | | | X | |
| A.18.2.2 | Naleving van beveiligingsbeleid en -normen | Leidinggevenden moeten regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging. | Ja | Ja | X | X | X | |
| A.18.2.3 | Beoordeling van technische naleving | Informatiesystemen moeten regelmatig worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging. | Ja | Ja | X | X | X | |