

Verwerkersovereenkomst ARVODI-2025

Behorende bij: Aanbesteding Uitbesteden DT-KOT met Kenmerk: IUC24-734

De ondergetekenden:

1. De Staat der Nederlanden, waarvan de zetel is gevestigd te Den Haag, te dezen vertegenwoordigd door de Minister van Financiën, namens deze, Directeur Generaal drs. C.H.L.M. van de Louw, hierna te noemen: Opdrachtgever,

en

2. [volledige naam en rechtsvorm Opdrachtnemer], (statutair) gevestigd te [...], hierbij vertegenwoordigd door [naam ondertekenaar] hierna te noemen: Opdrachtnemer,

OVERWEGENDE DAT:

- voor zover Opdrachtnemer Persoonsgegevens Verwerkt ten behoeve van Opdrachtgever in het kader van de Overeenkomst, kwalificeert Opdrachtgever als Verwerkingsverantwoordelijke voor de Verwerking van Persoonsgegevens en Opdrachtnemer als Verwerker;
- Partijen in deze Verwerkersovereenkomst, zoals bedoeld in artikel 28, derde lid, van de Verordening, hun afspraken over de Verwerking van Persoonsgegevens door Opdrachtnemer wensen vast te leggen.

KOMEN OVEREEN:

Artikel 1. Begrippen

In deze Verwerkersovereenkomst wordt een aantal begrippen met een beginhoofdletter gebruikt. Aan deze begrippen komt de betekenis toe die hieraan wordt gegeven in de ARVODI-2025 of de Verordening, met dien verstande dat een aantal begrippen op de Verwerkersovereenkomst zijn toegespitst. Aldus en in aanvulling daarop wordt onder de volgende begrippen, ongeacht of ze in meervoud of enkelvoud, of als werkwoord of zelfstandig naamwoord worden gebruikt, in deze Verwerkersovereenkomst verstaan:

- 1.1 ARVODI-2025: Algemene Rijksvoorwaarden voor het verstrekken van opdrachten tot het uitvoeren van Diensten 2025.
- 1.2 Betrokkene: degene op wie een Persoonsgegeven betrekking heeft.
- 1.3 EER: Europese Economische Ruimte, zijnde alle EU-landen plus Liechtenstein, Noorwegen en IJsland.
- 1.4 Inbreuk in verband met Persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de

ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins Verwerkte gegevens.

- 1.5 Ontvanger: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de Persoonsgegevens worden verstrekt. Overheidsinstanties die mogelijk Persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig het Unierecht of het lidstatelijke recht gelden echter niet als Ontvangers; de Verwerking van die gegevens door die overheidsinstanties strookt met de gegevensbeschermingsregels die op het betreffende verwerkingsdoel van toepassing zijn.
- 1.6 Overeenkomst: de overeenkomst tussen Opdrachtgever en Opdrachtnemer [titel] van [datum], met kenmerk [kenmerk].
- 1.7 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, die Opdrachtnemer in het kader van de Overeenkomst ten behoeve van Opdrachtgever Verwerkt.
- 1.8 Toezichthoudende autoriteit: een door een lidstaat ingevolge artikel 51 van de Verordening ingestelde onafhankelijke overheidsinstantie.
- 1.9 Verordening: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van de Richtlijn 95/46/EG (algemene verordening gegevensbescherming).
- 1.10 Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de Verwerkingsverantwoordelijke Persoonsgegevens Verwerkt.
- 1.11 Verwerkersovereenkomst: deze overeenkomst inclusief overwegingen en bijbehorende bijlagen.
- 1.12 Verwerking: een bewerking of een geheel van bewerkingen in het kader van de Overeenkomst met betrekking tot Persoonsgegevens, of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.
- 1.13 Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de Verwerking van Persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze Verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de Verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.

Artikel 2. Voorwerp van deze Verwerkersovereenkomst

- 2.1 Deze Verwerkersovereenkomst regelt de Verwerking door Opdrachtnemer in het kader van de Overeenkomst en is onlosmakelijk verbonden met de Overeenkomst.
- 2.2 De aard en het doel van de Verwerking, het soort Persoonsgegevens en de categorieën van Persoonsgegevens, Betrokkenen en Ontvangers zijn in Bijlage 1 omschreven.
- 2.3 Opdrachtnemer garandeert de toepassing van passende technische en organisatorische maatregelen, opdat de Verwerking aan de vereisten van de Verordening voldoet en de bescherming van de rechten van de Betrokkene is gewaarborgd.
- 2.4 Opdrachtnemer garandeert te voldoen aan de vereisten van de toepasselijke wet- en regelgeving betreffende de Verwerking.

Artikel 3. Inwerkingtreding en duur

- 3.1 Deze Verwerkersovereenkomst treedt in werking op het moment waarop deze door Partijen is ondertekend.
- 3.2 Deze Verwerkersovereenkomst eindigt nadat Opdrachtnemer alle Persoonsgegevens heeft gewist, terugbezorgd en bestaande kopieën heeft verwijderd met inachtneming van artikel 10 van deze Verwerkersovereenkomst.
- 3.3 Deze Verwerkersovereenkomst is niet tussentijds opzegbaar.

Artikel 4. Omvang verwerkingsbevoegdheid Opdrachtnemer

- 4.1 Opdrachtnemer Verwerkt de Persoonsgegevens uitsluitend in opdracht en op basis van schriftelijke instructies van Opdrachtgever, tenzij een op Opdrachtnemer van toepassing zijnde wettelijk voorschrift hem tot Verwerking verplicht. In dat geval stelt Opdrachtnemer Opdrachtgever voorafgaand aan de Verwerking in kennis van dat wettelijk voorschrift, tenzij dat wettelijk voorschrift deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.
- 4.2 Opdrachtnemer heeft geen zeggenschap over het doel van en de middelen voor de Verwerking als bedoeld in de Verordening.

Artikel 5. Beveiliging van de Verwerking

- 5.1 Onverminderd artikel 2.3 van deze Verwerkersovereenkomst treft Opdrachtnemer de technische en organisatorische beveiligingsmaatregelen zoals beschreven in Bijlage 2.
- 5.2 Partijen erkennen dat het waarborgen van een passend beveiligingsniveau voortdurend kan dwingen tot het treffen van aanvullende beveiligingsmaatregelen. Opdrachtnemer waarborgt een op het risico afgestemd beveiligingsniveau.
- 5.3 Voor zover Opdrachtgever daarom uitdrukkelijk schriftelijk verzoekt, treft Opdrachtnemer aanvullende maatregelen met het oog op de beveiliging van de Persoonsgegevens.
- 5.4 Opdrachtnemer Verwerkt Persoonsgegevens niet buiten de EER, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming, zo nodig voorzien van nadere voorwaarden, heeft verkregen van Opdrachtgever en behoudens afwijkende wettelijke verplichtingen.
- 5.5 Opdrachtnemer informeert Opdrachtgever zonder onredelijke vertraging zodra hij kennis heeft genomen van onrechtmatige Verwerkingen van Persoonsgegevens of tekortschieten (in de naleving van) technische en organisatorische beveiligingsmaatregelen zoals bedoeld in het eerste en tweede lid.
- 5.6 Opdrachtnemer verleent Opdrachtgever bijstand bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36 van de Verordening.

Artikel 6. Geheimhouding door Personeel van Opdrachtnemer

- 6.1 De Persoonsgegevens hebben een vertrouwelijk karakter als bedoeld in artikel 11.1 van de ARVODI-2025.
- 6.2 Opdrachtnemer waarborgt dat zijn Personeel zich ertoe heeft verbonden vertrouwelijkheid in acht te nemen als bedoeld in artikel 11.2 van de ARVODI-2025.

Artikel 7. Subverwerker

Wanneer Opdrachtnemer, met inachtneming van het bepaalde in artikel 6 van de ARVODI-2025, een andere Verwerker inschakelt om ten behoeve van Opdrachtgever verwerkingsactiviteiten te verrichten, worden aan deze andere Verwerker bij een overeenkomst dezelfde verplichtingen inzake gegevensbescherming opgelegd als die welke in deze Verwerkersovereenkomst zijn opgenomen.

Artikel 8. Bijstand vanwege rechten van Betrokkene

- 8.1 Voor zover mogelijk en rekening houdend met de aard van de Verwerking door middel van passende technische en organisatorische maatregelen, verleent Opdrachtnemer Opdrachtgever bijstand bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III van de Verordening vastgelegde rechten van de Betrokkene te beantwoorden.
- 8.2 Partijen dragen elk de door henzelf in verband met de in het eerste lid te maken kosten.
- 8.3 Opdrachtnemer stuurt een verzoek vanuit een Betrokkene zo spoedig mogelijk aan Opdrachtgever.

Artikel 9. Inbreuk in verband met Persoonsgegevens

- 9.1 Opdrachtnemer informeert Opdrachtgever zonder onredelijke vertraging, zodra hij kennis heeft genomen van een Inbreuk in verband met Persoonsgegevens, overeenkomstig de afspraken zoals vastgelegd in Bijlage 3.
- 9.2 Opdrachtnemer informeert Opdrachtgever ook na een melding op grond van het eerste lid over ontwikkelingen betreffende de Inbreuk in verband met Persoonsgegevens.
- 9.3 Partijen dragen elk de door henzelf te maken kosten gerelateerd aan de Inbreuk in verband met Persoonsgegevens.

Artikel 10. Terugbezorgen of wissen Persoonsgegevens

- 10.1 Na afloop van de Overeenkomst, of zoveel eerder als overeengekomen, draagt Opdrachtnemer er zorg voor dat hij, naar gelang de keuze van Opdrachtgever, alle Persoonsgegevens wist of terugbezorgt aan Opdrachtgever en bestaande kopieën verwijdert, tenzij opslag van de Persoonsgegevens op basis van een wettelijk voorschrift verplicht is.
- 10.2 Partijen kunnen voor afzonderlijke of categorieën Persoonsgegevens bewaartermijnen overeenkomen. Na afloop van de overeengekomen bewaartermijn draagt Opdrachtnemer zorg voor het wissen of terugbezorgen en het verwijderen van kopieën van de betreffende Persoonsgegevens, tenzij opslag van deze Persoonsgegevens op basis van een wettelijk voorschrift verplicht is.
- 10.3 Persoonsgegevens worden in de door Opdrachtgever aangegeven vorm en op de door Opdrachtgever aangegeven wijze terugbezorgd.

Artikel 11. Informatieverplichting en audit

- 11.1 Opdrachtnemer stelt alle informatie ter beschikking die nodig is om aan te tonen dat de verplichtingen uit deze Verwerkersovereenkomst zijn en worden nagekomen.
- 11.2 Opdrachtgever kan een audit van de onder deze Verwerkersovereenkomst vallende verwerkingsactiviteiten (laten) uitvoeren als concrete omstandigheden daartoe aanleiding geven. Opdrachtnemer verleent alle medewerking aan audits, waaronder begrepen audits bij Personeel van Opdrachtnemer, tenzij dit redelijkerwijs niet van hem kan worden verwacht.
- 11.3 Opdrachtnemer stelt Opdrachtgever onmiddellijk in kennis indien naar zijn mening een instructie van Opdrachtgever in het kader van artikel 11 eerste en/of tweede lid van deze Verwerkersovereenkomst, inbreuk oplevert met een wettelijk voorschrift inzake gegevensbescherming.

- 11.4 Partijen dragen zelf de kosten die zij maken in verband met de in dit artikel bedoelde informatieverstrekking en audits, waaronder begrepen de kosten van door hen ingeschakelde derden.
- 11.5 Opdrachtgever is te allen tijde bevoegd om naar aanleiding van de op grond van dit artikel verkregen informatie nadere maatregelen voor te stellen. Opdrachtnemer is gehouden aan die maatregelen in redelijkheid uitvoering te geven.

Plaats:
Datum:-.....-.....

De Minister van Financiën,
namens deze,
Directeur Generaal,

Plaats:
Datum:-.....-.....

Externe partij
namens deze,
Functie bevoegde,

Drs. C.H.L.M. van de Louw

Naam bevoegde externe partij

Bijlage 1. De Verwerking van Persoonsgegevens

Overzicht Verwerkingen

Het onderwerp, aard en doel van de Verwerking	Deze opdracht betreft het uitbesteden van een deel van het handmatige proces voor de definitieve toekenning van de kinderopvangtoeslag (DT KOT). Het doel is het kwalitatief, tijdig en conform wet- en regelgeving verwerken van circa 16.000 handmatige behandelposten binnen het DT KOT-proces. Dit is exclusief de eventuele extra 2.500 posten. Deze handmatige behandeling is nodig wanneer geautomatiseerde verwerking op basis van opvanggegevens niet mogelijk is vanwege onvolledige of onbetrouwbare informatie.
Beschrijving categorieën Betrokkenen	Aanvragers KOT (Av), toeslagpartner (Tp), medebewonder, kinderen, medewerker, kinderopvangorganisaties (in het geval als het om natuurlijke personen gaat)
Beschrijving categorieën Ontvangers van Persoonsgegevens	Aanvrager, gemachtigde. Via TVS: kerndepartementen, SZW en W&I, belastingdienst
Locatie Verwerking Persoonsgegevens	Nederland (in systemen van Toeslagen)

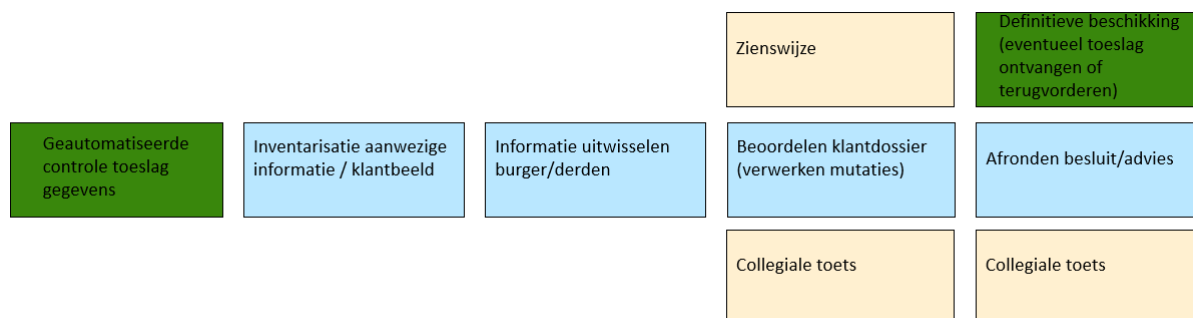
Soort persoonsgegevens gewoon	Bron*	Betrekking op
Naam (achternaam, voorletters, tussenvoegsels)	BVR	Av, Tp, en kinderen
Woonadres	BVR	Av, Tp, en kinderen
Geboortedatum	BVR	Av, Tp, en kinderen
Huishouden	BVR	Av, Tp, kinderen
Rekeningnummer	BRG	Av
Vermogen en wereldvermogen	IND, TVS	Av, Tp en MB
Opvanggegevens: • LRK-nummer	DUO	Av en kinderen
Afgenomen uren	KOO	Av en kinderen
(Gemiddeld) uurtarief	KOO	Av en kinderen
Ingangs- en einddatum opvang	KOO	Av en kinderen
LRK en Register Buitenlandse Kinderopvang (RBK)	DUO	Av, tp en kinderen

Soort persoonsgegevens gevoelig	Bron	Betrekking op
IP-adres (wordt gelogd op het moment dat de medewerker de "DT-run" start)		Toeslagen medewerker

Soort persoonsgegevens gevoelig wettelijke identificerend	Bron	Betrekking op
BSN	BVR	Av, Tp, en kinderen,

* De gegevens wordt d.m.v. TVS geleverd.

Gegevensverwerking:



De gegevensverwerking heeft betrekking op de blauwe vlakken van bovenstaande afbeelding.[†]

- Opdrachtgever geeft handwerkposten aan opdrachtnemer;
- Opdrachtnemer verwerkt de gegevens op de systemen van opdrachtgever. De opdrachtgever stelt laptops en opladers en overige benodigde accessoires ter beschikking aan de opdrachtnemer voor het uitvoeren van de opdracht. Dit materiaal mag uitsluitend worden gebruikt voor de werkzaamheden die direct verband houden met de uitvoering van de opdracht;
- In de handwerkpost staat een omschrijving wat de reden is voor het aanbieden van handmatige behandeling. Dit is het startpunt voor de opdrachtnemer;
- De medewerker van opdrachtnemer controleert op basis van de aanwezige gegevens de opvanglasten in TVS en past deze waar nodig in TVS aan.
- Als er nog vragen op gegevens nodig zijn neemt de medewerker (telefonisch) contact op met de kinderopvangorganisatie of aanvrager als er nog niet geautomatiseerd een vraagbrief is verstuurd.
- Alle communicatie met kinderopvangorganisaties verloopt uitsluitend via telefoon of het Belastingdienst FileTransfer systeem. Andere communicatiemiddelen zijn niet toegestaan.
- Alle communicatie met burgers verloopt uitsluitend via telefoon, brief of de uploadfunctie van TVS. Andere communicatiemiddelen zijn niet toegestaan.
- Bij vermoedens van valsheid in geschriften, misbruik of oneigenlijk gebruik dient de opdrachtnemer dit direct voor te leggen bij de opdrachtgever.
- De opdrachtnemer verstuurt een beoordelingsbrief als de lasten correct in TVS staan.
- Bij einde van de opdracht levert de opdrachtnemer de gegevens terug. In het geval gegevens moeten worden vernietigd levert opdrachtnemer bewijs van de concrete en onherstelbare vernietiging van de gegevens.

<OPTIONEEL indien aan de orde>

Subverwerker(s) (denk ook aan clouddiensten)

Naam en contactgegevens subverwerker	
Nummer handelsregister van subverwerker	
Het onderwerp, aard en doel van de Verwerking	
Het soort Persoonsgegevens	
Beschrijving categorieën van Persoonsgegevens	
Beschrijving categorieën Betrokkenen	
Beschrijving categorieën Ontvangers van Persoonsgegevens	
Locatie Verwerking Persoonsgegevens	
.....	

[†] Zie bijlagen 1, 2 en 8 voor een uitgebreidere omschrijving van de gegevensverwerkingen.

Bijlage 2. Passende technische en organisatorische maatregelen

De Opdrachtnemer is ISO 27001 (informatiebeveiliging) en 27701 gecertificeerd en voldoet daarmee aan de door Opdrachtgever gestelde normen op het gebied van informatiebeveiliging en/of het servicemanagementsysteem. Zie hieronder de "Eisen aan Informatiebeveiliging en Privacy". Opdrachtnemer kan aan de hand van geldige certificering aantonen dat hij hieraan voldoet (zie ook programma van eisen (bijlage1)).

	Eisen aan Informatiebeveiliging en Privacy*
1.	Opdrachtnemer voldoet aan de vigerende wet- en regelgeving met betrekking tot wettelijke bewaartermijnen, signaleringen, archivering, anonimisering, vernietiging van persoonsgegevens.
2.	Normen privacy & Informatiebeveiliging De opdrachtnemer beschikt bij aanvang van de uitvoer van de opdracht over onderstaande geldige certificaten betreft privacy en informatiebeveiliging. a) ISO 27701 uitbreiding op ISO 27001, specifiek gericht op de inrichting, implementatie, het onderhoud en de continue verbetering van een Privacy Informatie Management Systeem (PIMS) of gelijkwaardig. b) ISO 27001 eisen en richtlijnen voor een Information Security Management System (ISMS) of gelijkwaardig. Training en bewustwording vertrouwelijk omgaan met overheidsinformatie De opdrachtnemer is verplicht om alle door haar in te zetten medewerkers te trainen in het vertrouwelijk omgaan met overheidsinformatie. De opdrachtgever zal de opdrachtnemer van informatie voorzien om het eigen personeel te kunnen trainen. Hierbij dient er gekeken te worden naar de Privacy Awareness van de medewerker (kennis, praktijk en doorontwikkeling). Dit kan opgesplitst worden in: a) Kennis bij de opdrachtnemer in relatie tot AVG en missie, beleidsuitgangspunten van opdrachtgever. b) Vaardigheden, toepassen van de kennis: bewezen trackrecord van de opdrachtnemer c) Verankering van de Privacy awareness: dus onderdeel van beoordelings- en functioneringsgesprekken zowel bij opdrachtgever intern als wel bij de organisatie/bedrijf welke wordt ingehuurd door opdrachtgever. d) Digitale geletterdheid: kunnen aantonen. e) Verslagen van de beoordelingen op het punt van privacy awareness worden gearchiveerd en gedeeld met de opdrachtgever. De opdrachtgever kan op basis van deze verslagen en beoordelingen de afweging maken welke ingehuurde medewerkers groei laten zien met betrekking tot privacy-awareness. Zo kunnen werkzaamheden hierop aangesloten kunnen worden. f) Werken overeenkomstig de gedragsregeling voor de digitale werkomgeving: Eventuele beveiligingsincidenten of problemen dienen door de opdrachtnemer direct gemeld te worden bij de opdrachtgever.
3.	Wet Open Overheid (Woo) verzoeken & AVG a) De opdrachtnemer dient binnen 48 uur medewerking te verlenen bij het verwerken van informatieverzoeken op grond van de Wet Open Overheid (Woo). De opdrachtnemer dient kennis te hebben van en in directe communicatie met de opdrachtgever te staan indien het ingeroepen rechten van betrokkenen (AVG) betreft. Indien opdrachtgever hier niet adequaat op kan reageren dan heeft de burger het recht om direct melding te maken en een klacht in te dienen bij de AP.
4.	Informatiebeveiligingsinvalshoek m.b.t logging en monitoring

	De opdrachtnemer dient indien van toepassing logging en monitoring in te richten voor alle werkzaamheden buiten de systemen van de opdrachtgever met als doel het identificeren en onderzoeken van beveiligingsinbreuken en risico's. Logging en monitoring op het gebied van informatiebeveiliging moeten voldoen aan de relevante ISO-normen (ISO 27001) of gelijkwaardig. Bij de uitvoering van de werkzaamheden is het voor de opdrachtnemer uitsluitend toegestaan de informatie van de burger te gebruiken voor de uitvoering van de opdracht van de opdrachtgever. De opdrachtnemer dient gedetailleerde informatie te registreren over systeem- en gebruikersactiviteiten om beveiligingsincidenten te kunnen detecteren en onderzoeken. De geregistreerde loggegevens moeten veilig worden bewaard en beschermd tegen ongeautoriseerde toegang of wijziging.
--	---

Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens (waaronder datalekken)

Incidentenrapportages

De opdrachtnemer dient snel en tijdig incidenten te melden bij de opdrachtgever door incidentenrapportages voor beveiligingsincidenten op te stellen, conform de geldende ISO-normen of vergelijkbaar voor informatiebeveiliging en de verwerkersovereenkomst. Incidentenrapportages dienen te bestaan uit de volgende onderdelen:

- 1) Beschrijving van het incident: Gedetailleerde beschrijving van wat er is gebeurd.
- 2) Datum en tijd van het incident: Specifieke tijdstippen van het begin en einde van het incident.
- 3) Betrokken systemen en gegevens: Overzicht van de systemen en data die door het incident zijn getroffen.
- 4) Oorzaak en impact van het incident: Analyse van de oorzaak en de impact op de organisatie.
- 5) Acties die zijn ondernomen om het incident te mitigeren: Overzicht van de genomen maatregelen om het incident te beperken.
- 6) Aanbevelingen voor toekomstige preventie: Suggesties en plannen om soortgelijke incidenten in de toekomst te voorkomen.

De opdrachtnemer registreert en classificeert alle beveiligingsincidenten, inclusief de aard en impact van het incident. Incidenten dienen te worden geanalyseerd en voorzien van een risicobeoordeling.

De opdrachtnemer meldt datalekken/incidenten direct aan de opdrachtgever, zodat de opdrachtgever aan de verplichtingen volgens de AVG kan voldoen.

Deze melding zal conform het datalek & incidentenproces verlopen. Deze zullen bij gunning aan de opdrachtnemer kenbaar gemaakt worden.

De opdrachtnemer dient een beleid en proces te hanteren voor het signaleren, registreren en afhandelen van datalekken en beveiligingsincidenten. Bij een datalek of beveiligingsincident heeft de opdrachtnemer maximaal 24 uur de tijd om dit te melden aan de opdrachtgever zo ook omschreven in de verwerkersovereenkomst.

Verbetercyclus

De opdrachtnemer dient een continue verbetercyclus toe te passen op het gebied van informatiebeveiliging. Dit zal in overleg tussen de opdrachtnemer en opdrachtgever afgesproken worden.

Baseline Informatiebeveiliging Overheid (BIO)

Opdrachtnemer moet aan opdrachtgever, bij aanvang opdracht, aantonen hoe zij waarborgen dat de eisen betreft de informatiebeveiliging zijn geborgd, doormiddel van zelfbeoordeling (eigen format) op basis van de Baseline Informatiebeveiliging Overheid (BIO).

Deze eis kan deze ook aangetoond worden door het volgende aan te tonen:

- Eventuele verklaring van informatiebeveiliging ISAE3402/SOC 2 (indien aanwezig);
- Beveiligingsbeheer op basis van het NIST Cybersecurity Framework ;
- Risicobeheer op basis van COBIT (Control Objectives for Information and Related Technologies);
- Zelf gedefinieerd Beveiligingsbeleid met Verantwoording;
- Schaalbare en flexibele Beveiligingsmaatregelen;
- Externe audits door een Onafhankelijke Partij.