Bijlage B

Concept Verwerkersovereenkomst op basis van de ARVODI-2025

tussen

ministerie van Sociale Zaken en Werkgelegenheid

en

<Opdrachtnemer>

inzake
Wsw-statistiek

met kenmerk: 201865005.011.094_A

Contractnummer: 201865005.011.094_A

De ondergetekenden:

1. De Staat der Nederlanden, waarvan de zetel is gevestigd te Den Haag,
   te dezen vertegenwoordigd door de minister van Sociale Zaken en Werkgelegenheid
   namens deze,
   <functie>, <naam>,
   hierna te noemen: Opdrachtgever,

   en

2. <volledige naam en rechtsvorm contractant>,
   (statutair) gevestigd te <plaatsnaam>,
   te dezen vertegenwoordigd door,
   <functienaam en naam ondertekenaar>,
   hierna te noemen: Opdrachtnemer.

Hierna gezamenlijk te noemen: de Partijen.

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 verrichten 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 inzake Wsw-statistiek van <datum>, met kenmerk 201865005.011.094.

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.

2.5 Opdracthnemer verwerkt uitsluitend gegevens in opdracht en onder verantwoordelijkheid van Opdrachtgever.

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 voor zover en 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 Indien en voor zover Opdrachtgever daarom uitdrukkelijk schriftelijk verzoekt, zal Opdrachtnemer aanvullende maatregelen treffen 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 inbreuken op beveiligingsmaatregelen zoals genoemd 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 in verband met de melding aan de bevoegde Toezichthoudende autoriteit en Betrokkene te maken kosten.

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.
In geval van wissen en/of verwijderen van kopieën door Opdrachtnemer informeert hij Opdrachtgever schriftelijk zodra hij dit heeft gedaan.

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 Opdrachtnemer wist de Persoonsgegevens binnen twee maanden na afloop van de Overeenkomst, of zoveel eerder als overeengekomen.

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.

Aldus op de laatste van de twee hierna genoemde data overeengekomen en in tweevoud ondertekend,

Plaats: Den Haag Datum: ……-……-2026	Plaats: …… Datum: ……-……-2026
de minister van van Sociale Zaken en Werkgelegenheid namens deze, <functie gevolmachtigde>,	<naam Opdrachtnemer>, namens deze, <functie gevolmachtigde>,
<Naam gevolmachtigde>	<Naam gevolmachtigde>

Bijlagen:
Bijlage 1: De Verwerking van Persoonsgegevens
Bijlage 2: Passende technische en organisatorische maatregelen
Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens

Bijlage 1. De Verwerking van Persoonsgegevens

Minimale gegevensverwerking wordt nagestreefd (alleen noodzakelijke contactgegevens);

Welke gegevens moeten worden opgevraagd en geregistreerd door Opdrachtnemer staan beschreven in de bijlage behorende bij de *Regeling uitvoering Wet sociale werkvoorziening en begeleid werken 2015*. Deze gegevens vallen onder de Verwerking van Persoonsgegevens zoals bedoeld in deze verwerkersovereenkomst.

In deze bijlage moet in ieder geval het volgende worden gespecificeerd voor de in de regeling hierboven genoemde onderdelen:

Overzicht Verwerkingen

Het onderwerp/aard en doel van de Verwerking	
Het soort Persoonsgegevens	
Beschrijving categorieën Persoonsgegevens	
Beschrijving categorieën Betrokkenen	
Beschrijving categorieën Ontvangers van Persoonsgegevens	
Locatie Verwerking Persoonsgegevens	

<OPTIONEEL (indien aan de orde)***>***
Subverwerker(s)

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	

Bijlage 2. Passende technische en organisatorische maatregelen

De Verwerker voert actief risico management uit op zijn dienstverlening. Verwerker onderhoudt hiervoor een op ISO27001 gebaseerd *information security management systeem* waarmee hij passende beveiligingsmaatregelen selecteert, evalueert en verbetert.

Opdrachtgever hanteert de volgende wet- en regelgeving Op het gebied van informatieveiligheid

- Algemene Verordening Gegevensbescherming[*] (AVG, art. 32)
- Baseline Informatiebeveiliging Overheid[†] (BIO)
- Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013[‡] (VIRBI 2013)
- Beveiligingsvoorschrijf Rijksdienst 2013[§] (BVR 2013)
- Voorschrift Informatiebeveiliging Rijksdienst 2007[**] (VIR 2007)
- Rijksbreed Cloudbeleid
- Network and Information Security (NIS2) directive

Op de uitvoering van deze Verwerking is het beveiligingsniveau BBN 2 van de BIO van toepassing.

Wanneer er sprake is van een Verwerking in een publieke cloudomgeving, waardoor er (gevoelige) Persoonsgegevens in het kader van deze Overeenkomst in de cloud worden opgeslagen, mag dit alleen na uitdrukkelijk toestemming van Opdrachtgever. Voor het gebruik van een cloudomgeving dient een aanvullende risico analyse te worden uitgevoerd. Daarnaast worden er dan extra eisen door de Opdrachtgever aan de cloudomgeving opgelegd.

Verwerker geeft van onderstaande minimale maatregelen aan hoe deze zijn ingevuld.

Alle onderstaande eisen zijn van toepassing op de gehele leverancierskеten.

Tabel 1. Concretisering van minimale set aan maatregelen vanuit de baseline informatiebeveiliging overheid

Normen, standaarden, richtlijnen	**Toelichting Verwerker toepassing maatregelen**
Verwerker dient aan één van de hieronder genoemde voorwaarde te voldoen, om aan te tonen dat hij op het gebied van informatiebeveiliging en de veilige omgang met data in control is: a) Verwerker is ISO27001 gecertificeerd of soortgelijk en overlegt vóór gunning een kopie van het certificaat en de bijbehorende verklaring van toepasselijkheid (Vvt). **Of**,	

[*] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving
[†] https://bio-overheid.nl/
[‡] https://wetten.overheid.nl/BWBR0033507/2013-06-01
[§] wetten.nl - Regeling - Beveiligingsvoorschrift Rijksdienst 2013 - BWBR0033512 (overheid.nl)
[**] https://wetten.overheid.nl/BWBR0022141/2007-07-01

b) Verwerker levert vóór gunning een derdenverklaring op, ook wel een Third Party Memorandum of Thrid Party Mededeling (TPM) genoemd. **Of**, c) Verwerker voert een Gap-analyse BIO[††] (Baseline Informatiebeveiliging Overheid) uit en overlegt deze vóór gunning. **Of**, d) Verwerker overlegt vóór gunning een beschrijvend document (In-Control-Statement) waarin minimaal de volgende zaken **voor de gehele toeleveringsketen** zijn beschreven: • De wijze waarop aan de informatiebeveiligingsmaatregelen uit de Baseline Informatiebeveiliging Overheid (BIO)[‡‡] wordt voldaan; • Hoe de processen en procedures op het gebied van informatiebeveiliging zijn ingericht, om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie die wordt verwerkt in het kader van het onderzoek te waarborgen; • De procesbeschrijving voor de behandeling van informatiebeveiligingsincidenten; • Op welke wijze de continuïteit van het onderzoek met de daarin verwerkte gegevens (back-up en recovery beleid) wordt gewaarborgd; • Hoe Multi Factor Authentication voor het beschermen van de toegang tot (gevoelige) gegevens in het kader van het onderzoek wordt toegepast; • Op welke wijze logging en monitoren voor het waarborgen van de integriteit en vertrouwelijkheid van het onderzoek is geïmplementeerd.	
Indien Verwerker gebruik maakt van een clouddienst voor de Verwerking van gegevens, dienen gepaste maatregelen te zijn getroffen, conform het vigerende Rijksbreed Cloudbeleid[§§].	

[††] https://www.informatiebeveiligingsdienst.nl/product/gap-analyse-1-2-alle-sheets/
[‡‡] https://bio-overheid.nl/media/13kduqsi/bio-versie-104zv_def.pdf
[§§] https://open.overheid.nl/documenten/ronl-a79331dc7c088f2cb6259f591c3b4f2fbcc9b5f1/pdf

Beleid	
Verwerker dient ten behoeve van informatiebeveiliging een informatiebeveiligingsbeleid te hebben vastgesteld dat met geplande tussenpozen en als zich significante wijzigingen voordoen, dient te worden beoordeeld.	
Er dient aantoonbaar aandacht te zijn voor het bevorderen van bewustzijn ten aanzien van informatiebeveiliging en privacy onder medewerkers. De Verwerker toont aan op welke wijze bewustzijn voor privacy en informatiebeveiliging onder medewerkers wordt bevorderd.	
Toegangsbeveiliging	
Een beleid voor toegangsbeveiliging dient te zijn vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	
Er is een strikt toegangsbeheer dat bepaalt wie toegang heeft tot bijzondere Persoonsgegevens.	
Voor telewerken dienen aantoonbaar adequate beveiligingsmaatregelen te zijn genomen.	
Als vanuit een onvertrouwde zone toegang wordt verleend tot een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie.	
Verwerker heeft een wachtwoordbeleid vastgesteld en gedocumenteerd dat is gebaseerd op ISO27002:2022 beheersmaatregelen.	
Voor de toegang tot het informatiesysteem waarin de gegevens van Opdrachtgever worden verwerkt, wordt gebruik gemaakt van persoonsgebonden loginnamen. Het gebruik van niet- persoonsgebonden loginnamen zoals groupaccounts of functionele accounts is niet toegestaan, tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar.	
Autorisaties worden bepaald, toegewezen en beheerd op basis van rollen.	

Toegang tot gegevens, informatiesystemen en systeemfuncties wordt beperkt, op basis van 'need to know' en 'Least Privilege'. Deze toegang (wie heeft toegang met welke autorisatie) dient 1x per kwartaal te worden gecontroleerd en waar nodig gecorrigeerd.	
De gegevens, in het kader van de Opdracht, van Opdrachtgever dienen waterdicht te zijn afgeschermd van de gegevens van andere klanten van de Verwerker.	
Cryptografie	
Cryptografische toepassingen voldoen aan passende standaarden van het Forum Standaardisatie.	
De sterkte van de cryptografie wordt gebaseerd op de actuele adviezen van het NCSC.	
Ter bescherming van gegevens dient de Verwerker een beleid voor het gebruik van cryptografische beheersmaatregelen te hebben geïmplementeerd.	
De gegevens in het kader van de Opdracht dienen zowel in rust als tijdens transport te zijn versleuteld.	
Mobiele apparatuur	
Verwerker heeft beleid en ondersteunende beveiligingsmaatregelen vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	
De mobiele apparatuur die Verwerker ingezet bij deze opdracht maakt deel uit van patchmanagement en hardening.	
Mobiele apparatuur is zo ingericht dat de gegevens in het kader van het Onderzoek niet onbewust worden opgeslagen ('zero footprint'). Als zero footprint (nog) niet realiseerbaar is, biedt een mobiel apparaat (zoals een laptop, tablet en smartphone) de mogelijkheid om de toegang te beschermen door middel van een toegangsbeveiligingsmechanisme en, indien vertrouwelijke gegevens worden opgeslagen, versleuteling van die	

gegevens. In het geval van opslag van vertrouwelijke gegevens moet op deze mobiele apparatuur 'wissen op afstand' mogelijk zijn.	
Ter bescherming tegen malware dienen aantoonbaar beheersmaatregelen voor detectie, preventie en herstel te zijn geïmplementeerd in combinatie met een passend bewustzijn van gebruikers. De beheersmaatregelen zijn van toepassing op Endpoint devices, servers, netwerkinfrastructuur en dataopslagapparatuur zowel fysiek als gevirtualiseerd, zowel in eigen beheer als bij clouddiensten. Met andere woorden is van toepassing op de gehele leveranciersketen van ingezette ICT apparatuur.	
Er dient een beleid opgesteld te zijn voor patchmanagement waarmee zo spoedig mogelijk en proactief patches worden geïnstalleerd.	
Leveranciersrelatie	
Verwerker moeten haar keten van toeleveranciers bekendmaken en transparant zijn over de maatregelen die zij genomen heeft om de aan haar opgelegde eisen ook door te vertalen naar haar toeleveranciers.	
Bij beëindiging van de opdracht behandelt de Verwerker de Persoonsgegevens in het kader van de Opdracht conform de vastgelegde afspraken in de Overeenkomst (overdragen en vernietigen of vernietigen).	
Verwerker levert een verklaring van vernietiging van de Persoonsgegevens aan Opdrachtgever bij het beëindigen van de opdracht.	
Bedrijfscontinuïteit	
De ICT-gereedheid dient te worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoelstellingen en ICT-continuïteitseisen. *Toelichting:* Verwerker *heeft aantoonbaar adequate maatregelen genomen, zodat de bedrijfsactiviteiten die nodig zijn om de continuïteit van* de Opdracht *en de*	

daarbij verwerkte gegevens te waarborgen, zelfs bij een ernstige verstoring. Hierbij wordt in eerste instantie gedacht aan back-up en recovery (incl. offline/offsite back-up), maar ook indirecte maatregelen als malware/ransomware protection en file encryption, zijn hierbij een preventieve maatregel.	
Er dient een back-up en recovery beleid te zijn geïmplementeerd dat in ieder geval ondersteunend is aan de uitvoering van de Overeenkomst. Het back-upbeleid van Verwerker ondersteunt minimaal de volgende eisen van Opdrachtgever: - Dataverlies bedraagt maximaal 24 uur; - Hersteltijd in geval van incidenten is maximaal 16 werkuren (2 dagen van 8 uur)	
Logging	
Logging is geïmplementeerd om gebruikersactiviteiten te registreren en adequate afhandeling van informatiebeveiligingsincidenten zoals onbevoegde toegang en mutatie van gegevens mogelijk te maken.	
Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	
Ten behoeve van de loganalyse is de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd door de Verwerker.	
Scheiding in netwerken	
Groepen van informatiediensten, -gebruikers en -systemen dienen in netwerken te worden gescheiden.	
Informatiebeveiligingsincidenten	
Informatiebeveiligingsincidenten dienen zo spoedig mogelijk, in ieder geval binnen 24 uur na constatering, gemeld te worden aan de Opdrachtgever.	

Privacy	
Verwerker neemt bij de verwerking van Persoonsgegevens de beginselen van de AVG in acht.	
Verwerker dient medewerking te verlenen aan de tijdige uitvoering van een DPIA indien van toepassing, voordat de verwerking van Persoonsgegevens aanvangt.	
Verwerker ondertekent de verwerkersovereenkomst voordat de verwerking van de Persoonsgegevens aanvangt.	
Pseudonimisering en/of anonimisering van (zeer) bedrijfs- en privacygevoelige informatie dient op een passend niveau te worden toegepast.	

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

Opdrachtnemer is gehouden beveiligingsincidenten en datalekken in de zin van artikel 33 en 34 van de Verordening **zo snel mogelijk, doch in ieder geval binnen 24 uur**, nadat deze geconstateerd zijn, aan de Opdrachtgever per e-mail te rapporteren. Het centrale meldpunt hiervoor is :

E-mailadres: PostbusIBenPSGpSG@minszw.nl
Met een CC naar: incidenten@minszw.nl

Stap 1:
Zodra Opdrachtnemer een Inbreuk in verband met Persoonsgegevens ontdekt of anderszins hiervan op de hoogte raakt zal Opdrachtnemer:

a. onmiddellijk alle maatregelen nemen om de tekortkomingen in de beveiliging die hebben geleid tot de Inbreuk in verband met Persoonsgegevens te corrigeren en de gevolgen daarvan te beperken;
b. Opdrachtgever zo snel als redelijkerwijs mogelijk is, maar niet later dan 24 uur na de ontdekking van de Inbreuk in verband met Persoonsgegevens, de in artikel 33, tweede lid van de Verordening bedoelde informatie toekomen, waaronder:
    - de aard van de Inbreuk in verband met Persoonsgegevens, waar mogelijk onder vermelding van de **categorieën** van Betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering het **aantal** Betrokkenen en persoonsgegevensregisters in kwestie;
    - de mogelijke impact, c.q. waarschijnlijke gevolgen van de Inbreuk in verband met Persoonsgegevens;
    - de maatregelen die Opdrachtnemer heeft genomen of zal nemen om de beveiliging te corrigeren en/of de gevolgen te beperken.
c. samenwerken met Opdrachtgever om de oorzaak van de Inbreuk Persoonsgegevens te onderzoeken en alle maatregelen nemen die Opdrachtgever nodig acht om een vergelijkbaar incident te voorkomen.

Stap 2:
Opdrachtnemer draagt er zorg voor dat eventuele ingeschakelde subverwerker(s) bij hen geconstateerde Inbreuken in verband met Persoonsgegevens op de beveiliging op zodanige wijze aan Opdrachtnemer te melden, dat deze in staat is de hierboven beschreven verplichtingen jegens Opdrachtgever na te kunnen komen.

Stap 3:
Nadat een melding over een Inbreuk in verband met Persoonsgegevens heeft plaatsgevonden rapporteert Opdrachtnemer over eventuele relevante nieuwe ontwikkelingen rond het incident en informeert aan Opdrachtgever over de maatregelen die Opdrachtnemer treft om de gevolgen van het incident te beperken en herhaling te voorkomen.

Stap 4:
In onderling overleg kunnen Partijen besluiten dat over een melding geen rapportage meer nodig is. Dit besluit wordt schriftelijk vastgelegd.

Stap 5:
Opdrachtgever draagt zorg in overeenstemming met artikel 34 van de Verordening voor de afhandeling van de voorgevallen Inbreuk in verband met Persoonsgegevens richting de Autoriteit Persoonsgegevens alsmede Betrokkene(n).