Bijlage C – concept 2.0
Verwerkersovereenkomst op basis van de ARIV-2026

tussen

het ministerie van Sociale Zaken en Werkgelegenheid

de directie Bestuursondersteuning

en

<Leverancier>

inzake

Eindejaarsgeschenken

met kenmerk
20186505.011.098_A

Verwerkersovereenkomst ARIV-2026

Contractnummer: 201865005.011.098_A

De ondergetekenden:

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

en

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

Hierna gezamenlijk te noemen: de Partijen.

OVERWEGENDE DAT:

- voor zover Leverancier Persoonsgegevens Verwerkt ten behoeve van Koper in het kader van de Overeenkomst, Koper krachtens artikel 4, onderdeel 7 en onderdeel 8, van de Verordening kwalificeert als verwerkingsverantwoordelijke voor de Verwerking van Persoonsgegevens en Leverancier als verwerker;
- Partijen in deze Verwerkersovereenkomst, zoals bedoeld in artikel 28, derde lid, van de Verordening, hun afspraken over de Verwerking van Persoonsgegevens door Leverancier wensen vast te leggen.

KOMEN OVEREEN:

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 ARIV-2026 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. ARIV-2026: Algemene Rijksinkoopvoorwaarden 2026.

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 Koper en Leverancier aangaande Eindejaarsgeschenken van <datum>, met kenmerk 201865005.011.098.

1.7. Persoonsgegevens: Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, die Leverancier in het kader van de Overeenkomst ten behoeve van Koper 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.

2. Voorwerp van deze Verwerkersovereenkomst

2.1. Deze Verwerkersovereenkomst regelt de Verwerking door Leverancier 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. Leverancier 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. Leverancier garandeert te voldoen aan de vereisten van de toepasselijke wet- en regelgeving betreffende de Verwerking.

3. Inwerktreding 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 Leverancier 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.

4. Omvang verwerkingsbevoegdheid Leverancier

4.1. Leverancier Verwerkt de Persoonsgegevens uitsluitend in opdracht en op basis van schriftelijke instructies van Koper, tenzij een op Leverancier van toepassing zijnde wettelijk voorschrift hem tot Verwerking verplicht. In dat geval stelt Leverancier Koper 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. Leveranciers heeft geen zeggenschap over het doel van en de middelen voor de Verwerking als bedoeld in de Verordening.

5. Beveiliging van de Verwerking

5.1. Onverminderd artikel 2.3 van deze Verwerkersovereenkomst treft Leverancier 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. Leverancier waarborgt een op het risico afgestemd beveiligingsniveau.

5.3. Voor zover Koper daarom uitdrukkelijk schriftelijk verzoekt, treft Leverancier aanvullende maatregelen met het oog op de beveiliging van de Persoonsgegevens.

Voor zover Koper aanvullende technische of organisatorische beveiligingsmaatregelen verlangt die uitstijgen boven de in deze Verwerkersovereenkomst, Bijlage 2, Bijlage B –

Programma van Eisen, of toepasselijke wetgeving opgenomen vereisten, zullen Partijen vooraf overleg voeren over de technische haalbaarheid, planning en de daarmee gemoeide kosten. Leverancier is uitsluitend gehouden dergelijke aanvullende maatregelen te treffen voor zover deze redelijk, proportioneel en technisch uitvoerbaar zijn.

5.4. Leverancier Verwerkt Persoonsgegevens niet buiten de EER, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming, zo nodig voorzien van nadere voorwaarden, heeft verkregen van Koper en behoudens afwijkende wettelijke verplichtingen.

5.5. Leverancier informeert Koper 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. Leverancier verleent Koper bijstand bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36 van de Verordening.

6. Geheimhouding door Personeel van Leverancier

6.1. De Persoonsgegevens hebben een vertrouwelijk karakter als bedoeld in artikel 8.1 van de ARIV-2026.

6.2. Leverancier waarborgt dat zijn Personeel zich ertoe heeft verbonden vertrouwelijkheid in acht te nemen als bedoeld in artikel 8.2 van de ARIV-2026.

7. Subverwerker

7.1. Bij het uitvoeren van de Overeenkomst mag Leverancier alleen met voorafgaande schriftelijke toestemming van Koper een andere verwerker inschakelen. Deze toestemming, waaraan door Koper nadere voorwaarden kunnen worden verbonden, wordt niet zonder redelijke grond geweigerd.

Leverancier houdt een actueel overzicht van subverwerkers beschikbaar voor Koper. Leverancier informeert Koper vooraf over voorgenomen wijzigingen in de door hem ingeschakelde subverwerkers. Koper kan binnen dertig (30) dagen na kennisgeving gemotiveerd bezwaar maken op redelijke privacy- of beveiligingsgronde.

7.2. Toestemming van Koper laat de eigen verantwoordelijkheid en aansprakelijkheid van Leverancier voor de nakoming van de krachtens de Overeenkomst op hem rustende verplichtingen en de krachtens de belasting-, zorgverzekerings- en sociale verzekeringswetgeving op hem als werkgever rustende verplichtingen, onverlet.

7.3. Wanneer Leverancier met inachtneming van het bepaalde in dit artikel een andere verwerker inschakelt om ten behoeve van Koper verwerkingsactiviteiten te verrichten, worden aan deze andere verwerker bij een overeenkomst dezelfde verplichtingen inzake gegevensbescherming opgelegd als die welke in deze Verwerkersovereenkomst zijn opgenomen.

8. Bijstand vanwege rechten van Betrokkene

8.1. Leverancier verleent Koper 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. Leverancier stuurt een verzoek vanuit een Betrokkene zo spoedig mogelijk aan Koper.

9. Inbreuk in verband met Persoonsgegevens

9.1. Leverancier informeert Koper 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. Leverancier informeert Koper 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.

10. Terugbezorgen of wissen Persoonsgegevens

10.1. Na afloop van de Overeenkomst, of zoveel eerder als overeengekomen, draagt Leverancier er zorg voor dat hij, naar gelang de keuze van Koper, alle Persoonsgegevens wist of terugbezorgt aan Koper 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 Leverancier informeert hij Koper zodra hij dit heeft gedaan.

10.2. Partijen kunnen voor afzonderlijke of categorieën Persoonsgegevens bewaartermijnen overeenkomen. Na afloop van de overeengekomen bewaartermijn draagt Leverancier 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. Leverancier wist de Persoonsgegevens binnen 30 dagen na afloop van de Overeenkomst, of zoveel eerder als overeengekomen.

10.4. Persoonsgegevens worden in de door Koper aangegeven vorm en op de door Koper aangegeven wijze terugbezorgd.

11. Informatieverplichting en audit

11.1. Leverancier stelt alle informatie ter beschikking die nodig is om aan te tonen dat de verplichtingen uit deze Verwerkersovereenkomst zijn en worden nagekomen.

11.2. Koper kan een audit van de onder deze Verwerkersovereenkomst vallende verwerkingsactiviteiten (laten) uitvoeren als concrete omstandigheden daartoe aanleiding

geven. Leverancier verleent alle medewerking aan audits, waaronder begrepen audits bij Personeel van Leverancier, tenzij dit redelijkerwijs niet van hem kan worden verwacht.

11.3. Leverancier stelt Koper onmiddellijk in kennis indien naar zijn mening een instructie van Koper 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. Koper is te allen tijde bevoegd om naar aanleiding van de op grond van dit artikel verkregen informatie nadere maatregelen voor te stellen. Leverancier 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: ……	Plaats: ……
Datum: ……-……-……	Datum: ……-……-……
de minister van Sociale Zaken en Werkgelegenheid,	<naam Leverancier>,
namens deze,	namens deze,
<functie gevolmachtigde>,	<functie gevolmachtigde>,
<Naam gevolmachtigde>	<Naam gevolmachtigde>

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

Bijlage 1. De Verwerking van Persoonsgegevens

Instructie:
Voor de inhoud van deze bijlage kan onder meer gebruik worden gemaakt van de registratie die de Verwerkingsverantwoordelijke op grond van artikel 30 van de Verordening dient aan te houden.

In deze bijlage moet in ieder geval het volgende worden gespecificeerd:

Overzicht Verwerkingen

Het onderwerp, aard en doel van de Verwerking	Het verstrekken van digitale en fysieke vouchers en het leveren van eindejaarsgeschenken voor de medewerkers van het ministerie van SZW.
Het soort Persoonsgegevens	Voornaam, achternaam, adres, huisnummer, postcode, woonplaats, emailadres
Beschrijving categorieën Persoonsgegevens	Gewoon
Beschrijving categorieën Betrokkenen	Medewerkers
Beschrijving categorieën Ontvangers van Persoonsgegevens	Verwerker
Locatie Verwerking Persoonsgegevens	Nederland

<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

In deze bijlage worden de normen en maatregelen gespecificeerd die Leverancier in het kader van de beveiliging van de Verwerking dient te hanteren respectievelijk te treffen. Hierbij kan worden verwezen naar documenten waarin normen en maatregelen zijn vastgelegd, zoals het Programma van Eisen en het Beschrijvend document.

De Verwerker voert actief risicomanagement uit op zijn dienstverlening. Verwerker onderhoudt hiervoor een op ISO 27001 gebaseerd information security management system waarmee passende beveiligingsmaatregelen worden geselecteerd, geëvalueerd en verbeterd.

Opdrachtgever hanteert de volgende wet- en regelgeving en kaders op het gebied van informatiebeveiliging, voor zover van toepassing op de Verwerking

- Algemene Verordening Gegevensbescherming[*] (AVG, art. 32)
- Baseline Informatiebeveiliging Overheid 2 (BIO2), versie 1.3
- Cyberbeveiligingswet (Cbw), voor zover relevant voor de beveiliging van de dienstverlening en de toeleveringsketen;
- Rijksbreed Cloudbeleid, indien Verwerker gebruikmaakt van een clouddienst voor de Verwerking.

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

Alle onderstaande eisen zijn van toepassing op de gehele leverancierskeken.

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

Normen, standaarden, richtlijnen	**Toelichting opdrachtnemer toepassing maatregelen**
Indien Verwerker gebruik maakt van een clouddienst voor de verwerking van gegevens, dienen gepaste maatregelen te zijn getroffen, conform het vigerende Rijksbreed Cloudbeleid[†].	
Beleid	
Verwerker dient ten behoeve van informatiebeveiliging een informatiebeveiligingsbeleid te hebben vastgesteld dat met geplande tussenpozen en bij significante wijzigingen wordt beoordeeld.	
Er dient aantoonbaar aandacht te zijn voor het bevorderen van bewustzijn ten aanzien van informatiebeveiliging en privacy onder medewerkers.	
Toegangsbeveiliging	
Een beleid voor toegangsbeveiliging dient te zijn vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	

[*] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving
[†] https://open.overheid.nl/documenten/ronl-a79331dc7c088f2cb6259f591c3b4f2fbcc9b5f1/pdf

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 meervoudige authenticatie (MFA).	
Opdrachtnemer heeft een wachtwoordbeleid vastgesteld en gedocumenteerd, gebaseerd op de toepasselijke beheersmaatregelen uit NEN-EN-ISO/IEC 27002:2022.	
Voor gebruikers die toegang hebben tot systemen waarin gegevens van Opdrachtgever worden verwerkt, wordt gebruikgemaakt van persoonsgebonden gebruikersaccounts. Niet-persoonsgebonden accounts worden uitsluitend gebruikt indien dit technisch noodzakelijk is en worden passend beheerst.	
Autorisaties worden bepaald, toegewezen en beheerd op basis van Role Based Access Control (RBAC).	
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 eenmaal 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 de actuele toepasselijke standaarden en richtlijnen van 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	
Opdrachtnemer 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 Opdrachtnemer inzet bij deze opdracht maakt deel uit van het patchmanagement- en hardeningbeleid.	
Indien mobiele apparatuur wordt gebruikt voor de verwerking of toegang tot persoonsgegevens in het kader van de Opdracht, zijn passende beveiligingsmaatregelen getroffen om ongewenste lokale opslag van deze gegevens te voorkomen. Indien persoonsgegevens lokaal worden opgeslagen, zijn deze passend versleuteld en is, waar mogelijk, wissen op afstand mogelijk.	
Ter bescherming tegen malware dienen aantoonbare beheersmaatregelen voor detectie, preventie en herstel te zijn geïmplementeerd, in combinatie met passend bewustzijn van gebruikers. Deze beheersmaatregelen zijn van toepassing op endpoint devices, servers, netwerkinfrastructuur en dataopslagapparatuur, zowel fysiek als gevirtualiseerd en zowel in eigen beheer als bij clouddiensten. De beheersmaatregelen zijn van toepassing op de ICT-middelen die voor de uitvoering van de Opdracht worden ingezet, waaronder de relevante ICT-middelen van eventuele toeleveranciers en onderaannemers. Opdrachtnemer beschikt over een beleid voor patchmanagement waarmee beveiligingspatches zo spoedig mogelijk en proactief worden geïnstalleerd.	
Leveranciersrelatie	
Op Opdrachtnemer moet haar relevante keten van toeleveranciers bekendmaken en transparant zijn over de maatregelen die zij heeft genomen om de aan haar opgelegde informatiebeveiligingseisen,	

voor zover relevant, door te vertalen naar haar relevante toeleveranciers en onderaannemers.	
Bij beëindiging van de Opdracht behandelt Verwerker de persoonsgegevens overeenkomstig de afspraken in artikel 10 van de Verwerkersovereenkomst.	
Op verzoek van Opdrachtgever verstrekt Verwerker een verklaring waaruit blijkt dat de persoonsgegevens overeenkomstig de gemaakte afspraken zijn verwijderd of vernietigd.	
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 Opdrachtnemer 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 die betrekking hebben op de Verwerking of de uitvoering van de Opdracht dienen zo spoedig mogelijk, in ieder geval binnen 24 uur na constatering, aan Opdrachtgever te worden gemeld.	
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 verwerkersafspraken voordat de verwerking van de persoonsgegevens aanvangt.	
Pseudonimisering wordt toegepast indien dit, gelet op de aard en het doel van de Verwerking, passend en mogelijk is.	

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

In deze bijlage moeten de afspraken over hoe Leverancier Koper over Inbreuken in verband met Persoonsgegevens gaat informeren worden gespecificeerd.

Informatie die ten minste door Leverancier moet worden verstrekt:

Datum en tijdstip van de constatering van de (vermoedelijke) Inbreuk in verband met Persoonsgegevens
Aard van de Inbreuk in verband met Persoonsgegevens
De soort, categorieën en het aantal Persoonsgegevens en Betrokkene
Waarschijnlijke gevolgen van de Inbreuk in verband met Persoonsgegevens
Maatregelen die Leverancier heeft voorgesteld of genomen om de Inbreuk in verband met Persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan

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 Opdrachtgever per e-mail te rapporteren. Het centrale meldpunt hiervoor is :

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

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).