

een audit te laten voeren. Het is 5.1.2.1 toegestaan, na in hiertoe toestemming te hebben gevraagd en gekregen van Politie, deze audit-rapportage te gebruiken voor haar andere klanten. Het recht om een audit te doen verrichten bij 5.1.2.1 blijft bestaan tot twaalf maanden na ontvangst van de in artikel 13.1 genoemde schriftelijke verklaring.

7. Inbreuk in verband met persoonsgegevens (datalek)

- 7.1 Indien er sprake is van een Datalek waarbij de Persoonsgegevens die 5.1.2.1 of de door haar ingeschakelde Subverwerkers Verwerken zijn betrokken, dan stelt 5.1.2.1 Politie zonder vertraging, en in ieder geval binnen 36 uur, na kennisneming daarvan op de hoogte. 5.1.2.1 voorziet Politie daarbij van alle, redelijkerwijs benodigde informatie, waaronder in ieder geval begrepen de informatie als bedoeld in artikel 33 lid 3 AVG, om Politie in staat te stellen zulks - indien vereist op grond van artikel 33 en 34 AVG - tijdig, juist en volledig te melden aan de Autoriteit Persoonsgegevens en de relevante Betrokkenen.
- 7.2 Bij het aanleveren van de informatie zoals bedoeld in artikel 7.1 levert 5.1.2.1 de informatie aan zoals deze door de Autoriteit Persoonsgegevens wordt opgevraagd middels de door haar vastgestelde standaardformulieren. Daarnaast is de functionaris gegevensbescherming van 5.1.2.1 beschikbaar voor eventuele vervolgvragen van Politie.
- 7.3 5.1.2.1 documenteert alle Datalekken, inclusief de feiten omtrent een Datalek, de gevolgen daarvan en de genomen corrigerende maatregelen. 5.1.2.1 houdt documentatie beschikbaar voor Politie voor zover dit betrekking heeft op Politie.
- 7.4 Indien zich na de melding aan Politie, als bedoeld in artikel 7.1, eventuele nieuwe, relevante ontwikkelingen voordoen, dan stelt 5.1.2.1 Politie daarvan onverwijld op de hoogte.
- 7.5 5.1.2.1 zal alle redelijkerwijs te nemen maatregelen treffen die nodig zijn om nadelige gevolgen te beperken of te voorkomen. Deze maatregelen worden in beginsel pas getroffen na overleg met Politie, tenzij door de aard van het Datalek dergelijk overleg niet kan worden afgewacht, in welk geval 5.1.2.1 Politie onverwijld op de hoogte stelt van de getroffen maatregelen.
- 7.6 5.1.2.1 verleent bijstand aan Politie bij het verrichten van meldingen aan toezichthoudende autoriteit(en) en betrokkenen in verband met een Datalek waarbij 5.1.2.1 betrokken is.
- 7.7 Indien Persoonsgegevens door een Datalek beschadigd of anderszins onbruikbaar zijn geworden, dan zal de 5.1.2.1 zich inspannen om die onverwijld en kosteloos te herstellen op basis van de gehanteerde backup en/of disaster recovery-procedures.

8. Aansprakelijkheid

- 8.1 5.1.2.1 is jegens Politie als gevolg van of verband houdende met deze Verwerkersovereenkomst of uit enige andere hoofde aansprakelijk voor zover en tot zover partijen dit zijn overeengekomen in de Hoofdovereenkomst. De in de Hoofdovereenkomst overeengekomen beperking van de aansprakelijkheid is onverminderd van kracht op de verplichtingen zoals opgenomen in deze Verwerkersovereenkomst, met dien verstande dat eenzelfde gebeurtenis nooit tot meerdere schadevorderingen kan leiden.
- 8.2 Onverminderd artikel 8.1 kan 5.1.2.1 geen beroep doen op de aansprakelijkheidsbeperking en uitsluiting van aansprakelijkheid opgenomen in de Hoofdovereenkomst in geval van schade waarvoor 5.1.2.1 conform artikel 82 AVG aansprakelijk is. 5.1.2.1 vrijwaart Politie ter zake van alle kosten, schade, aanspraken, claims en handhaving jegens Politie voor zover er sprake is van een tekortkoming die of handelen dat toerekenbaar is aan 5.1.2.1. In geval van aanspraken of

claims van derden zal Politie onverwijld melding doen aan ^{5.1.2.1} de verdediging, schikkingsonderhandelingen en de processtrategie laten bepalen door ^{5.1.2.1} en in dat kader alle redelijke instructies van ^{5.1.2.1} opvolgen, waaronder – zo nodig – het verstrekken van een procesvolmacht. In het geval van handhaving jegens Politie zal Politie ^{5.1.2.1} hierover zo spoedig mogelijk informeren en ^{5.1.2.1} in de gelegenheid stellen haar visie te geven.

9. Overmacht

- 9.1 Indien ^{5.1.2.1} als gevolg van overmacht haar verplichtingen uit hoofde van deze Verwerkersovereenkomst geheel of gedeeltelijk niet kan of kon nakomen, dient ^{5.1.2.1} Politie hiervan onverwijld melding te doen.

10. Looptijd

- 10.1 Deze Verwerkersovereenkomst treedt in werking op 1 januari 2018 en loopt qua duur gelijk aan de Hoofdovereenkomst.

11. Aanvullingen en wijzigen van deze Verwerkersovereenkomst

- 11.1 Aanvullingen van en wijzigingen in deze Verwerkersovereenkomst en de daarbij behorende bijlagen zijn slechts geldig indien deze schriftelijk zijn opgemaakt en door beide partijen zijn ondertekend. Dit houdt - ter verduidelijking - tevens in dat handgeschreven wijzigingen op deze Verwerkersovereenkomst niet akkoord zijn, tenzij door beide partijen geparafeerd.

12. Overdraagbaarheid

- 12.1 Partijen zijn niet gerechtigd zonder voorafgaande schriftelijke toestemming van de andere Partij de rechten en/of plichten voortvloeiende uit deze Verwerkersovereenkomst aan een derde over te dragen.

13. Teruggave / Vernietiging Persoonsgegevens

- 13.1 Na afloop of tussentijdse beëindiging van de Verwerkersovereenkomst zal ^{5.1.2.1} alle Persoonsgegevens zo spoedig mogelijk, in ieder geval binnen vier (4) weken, terug overdragen aan Politie en/of op verzoek van Politie alle achterblijvende Persoonsgegevens vernietigen, wissen of verwijderen, inclusief alle (kopieën van) elektronisch vastgelegde Persoonsgegevens uit/van alle documenten, computerdisks en andere gegevensdragers waarop of waarin deze Persoonsgegevens zich bevinden, met inbegrip van alle (archief)kopieën daarvan met uitzondering van de centrale off-site back-up tape. ^{5.1.2.1} zal schriftelijk bevestigen aan Politie dat alle Persoonsgegevens terug aan haar zijn overgedragen dan wel zijn vernietigd of verwijderd. De centrale off-site back-up tape is een secundaire back-up die door ^{5.1.2.1} alleen in geval van ernstige calamiteiten wordt gebruikt. De data op deze back-up is met behulp van hardware versleuteling offline en fysiek opgeslagen in een beveiligde omgeving en kan alleen door ^{5.1.2.1} met behulp van unieke hardware gebruikt worden. Na afloop of tussentijdse beëindiging van de Verwerkersovereenkomst worden de Persoonsgegevens overeenkomstig best practice procedureel uitgesloten van gebruik door ze te kenmerken als 'niet meer beschikbaar voor restoredoeleinden'.
- 13.2 Indien op ^{5.1.2.1} de wettelijke plicht rust om te blijven Verwerken, dan zal zij aan het verzoek van Politie voldoen voor zover zulks is toegestaan op grond van toepasselijke wet- en regelgeving. Zodra naleving van de verplichting uit artikel 13.1 niet langer wordt verhinderd door de betreffende regelgeving, zal ^{5.1.2.1} alsnog overgaan tot over hetgeen dat daar is bepaald.

14. Slotbepalingen

- 14.1 Op deze Verwerkersovereenkomst is Nederlands recht van toepassing. Geschillen zullen ter beslechting worden voorgelegd aan de bevoegde rechter te Amsterdam.
- 14.2 De nietigheid van enige bepaling van deze Verwerkersovereenkomst tast de geldigheid van de overige bepalingen niet aan.
- 14.3 Voorwaarden van deze Verwerkersovereenkomst die naar hun aard bedoeld zijn om voort te duren, blijven van kracht na beëindiging ervan.
- 14.4 In geval van strijdigheid tussen bepalingen van de Verwerkersovereenkomst en de Hoofdovereenkomst, prevaleert de bepaling van de Verwerkersovereenkomst, tenzij expliciet anders overeengekomen.
- 14.5 In geval van strijdigheid tussen bepalingen van de Verwerkersovereenkomst en de Bijlagen bij deze Verwerkersovereenkomst, prevaleert de bepaling van de Verwerkersovereenkomst, tenzij expliciet anders overeengekomen.
- 14.6 In geval ^{5.1.2.1} een informatie- of notificatieplicht heeft jegens Politie op basis van deze Verwerkersovereenkomst zal de communicatie schriftelijk plaatsvinden tussen ^{5.1.2.1} en de desbetreffende accountmanager van Politie.
- 14.7 Een verandering van een bijlage bij deze overeenkomst is alleen mogelijk met wederzijdse schriftelijke instemming van partijen. Partijen zijn gezamenlijk verantwoordelijk voor het actueel houden van de bijlagen bij deze Verwerkersovereenkomst. Partijen zullen dit binnen de bestaande governance op de agenda zetten van het maandelijks Service Lijn Overleg ("SLO") dat wordt gehouden met de accountteams van beide Partijen.

[TEKENPAGINA VOLGT]

ALDUS OVEREENGEKOMEN EN GETEKEND:

5.1.2.e



Functie: Directeur, Politiedienstencentrum

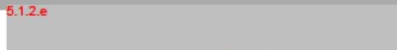
Datum:

21/2/2019

5.1.2.e



5.1.2.e



Datum:

28/2/2019

Bijlagen:

1. Overzicht van Verwerkingen
2. Goedgekeurde Subverwerkers
3. Beveiligingsmaatregelen en toegang

Bijlage 1 – Overzicht van Verwerkingen

1.1 Beaufort (HR Core)

1.1.1 Overzicht Verwerking

Algemeen doeleinde van de verwerkingen: uitvoeren van de personeels- en salarisadministratie.

	Betrokkenen (per categorie)	Persoonsgegevens (per categorie)	Doeleinde van Verwerking
(1)	- NP medewerkers - Externe medewerkers - Ketenpartners	Persoons- en arbeidsrelatie.	- Onderhouden statussen - Onderhoudt historie
(2)	Idem	Personeelsgegevens, adresgegevens en BSN.	- Identificatie - Rapportages - Uitvoeren CAO - Correspondentie - Calamiteiten
(3)	Idem	Aanstelling / dienstverband	- Aanstellings- en contractgegevens
(4)	NP medewerkers	Verzuim	- Uitvoering regelgeving
(5)	Idem	Werktijd	- Management informatie - Planning
(6)	Idem	Salarisgegevens	- Uitvoering salarisberekening en -afrekening - Uitbetaling salaris per CAO-soort en functiegroep - Loonbeslagen
(7)	Idem	Bankrelaties	- Overmaking betalingen naar medewerker d.m.v. opgegeven betalingswijze
(8)	Idem	Externe overschrijvingen	- betaalbaar stellen/overschrijven naar derde organisaties
(9)	Idem	Loonheffing	- randvoorwaarden uitvoering fiscale regelgeving
(10)	Idem	Sociale verzekeringen	- Registratie van SV-gegevens t.b.v. uitvoering - Bruto/netto salarisverwerking.

1.1.2 Locaties

In het kader van HR Core worden de Persoonsgegevens op de volgende locaties Verwerkt:

- (1) Politielocatie; 5.1.2.1 levert de software die door de politie lokaal wordt geïnstalleerd en gebruikt.

1.2 Gemal (payroll)

1.2.1 Overzicht Verwerkingen

Algemeen doeleinde van de verwerkingen: uitvoeren van de Salarisadministratie.

	Betrokkenen (per categorie)	Persoonsgegevens (per categorie)	Doeleinde van Verwerking
(1)	NP medewerkers	Salarisgegevens	- Uitvoering salarisberekening en -afrekening - Uitbetalen salaris per CAO-soort en functie - Loonbeslagen - Verzorgen van afdrachten - Genereren van loonstroken en jaaropgaven

1.2.2 Locaties

5.1.2.i

5.1.2.i

1.3.1 Overzicht Verwerkingen

Algemeen doeleinde van de verwerkingen: voor de persoonlijke ontwikkeling van medewerkers en tevens management informatie voor leidinggevende.

	Betrokkenen (per categorie)	Persoonsgegevens (per categorie)	Doeleinde van Verwerking
(1)	(Interne) medewerkers NP	- Personeelsnummer - Eenheidscode - OE code en afdelingsnaam - Voor- en achternaam - Functie - E-mailadres (werk) - Arbeidsrelatie (vast dienst of tijdelijk)	Om de aanvraag te kunnen koppelen aan de persoon die het betreft. Het functieprofiel wordt gekoppeld aan het aanbod van onderwijs Om de gevolgde opleidingen per medewerker te kunnen vasthouden (wie heeft welke trainingen gevolgd (skills). En om het resultaat van de gevolgde opleiding te kunnen beschouwen.
(2)	Trainer (in dienst van NP)	- Naam of inloggegevens	Wie de training heeft verzorgd/ het examen heeft afgenomen

1.3.2 Locaties

5.1.2.i

1.4 YouForce Performance Management

1.4.1 Overzicht Verwerkingen

Algemeen doeleinde van de verwerkingen: deze tool dient als digitale ondersteuning van de Resultaat- en Ontwikkelcyclus (R&O cyclus) bestaande uit resultaatgesprek, voortgangsgesprek, functioneringsgesprek (evaluatie) en ontwikkelgesprek over ontwikkelplan.

	Betrokkenen (per categorie)	Persoonsgegevens (per categorie)	Doeleinde van Verwerking
(1)	Medewerkers NP	- Voor- en achternaam - Personeelsnummer - Datum indiensttreding - Functie - Eenheid - Afdeling - Team - Geboortedatum - Competenties - Kennis - Vaardigheden - Beoordeling (per target) - Portfolio	Ondersteuning van de Resultaat- en Ontwikkelcyclus (R&O cyclus). Deze cyclus bestaat uit regelmatige gesprekken tussen medewerker en leidinggevende of medewerker met organisatorische coördinatie.
(2)	(Plaatsvervangend) leidinggevenden	- Voor- en achternaam	Wie de afspraken met de medewerker heeft gemaakt

1.4.2 Locaties

5.1.2.i

Bijlage 2 – Goedgekeurde Subverwerkers

In deze bijlage wordt een onderscheid gemaakt tussen de Subverwerkers voor diensten met een algemene toestemming en de Subverwerkers waarvoor ^{5.1.2.i} een specifieke toestemming heeft gegeven.

2.1 Algemene toestemming

Politie stemt ermee in dat ^{5.1.2.i} – met in acht name van hetgeen opgemerkt in artikel 4 van deze Verwerkersovereenkomst – de volgende partijen als Subverwerker inschakelt, waarvoor Politie een algemene toestemming geeft:

^{5.1.2.h}



Locaties van dienstverlening en datacentra buiten de EEA, waarbij er sprake is van een Verwerking van Persoonsgegevens buiten de EEA of toegang vanuit buiten de EEA:

- (1) N.v.t.

2.2 Specifieke toestemming

Politie stemt ermee in dat ^{5.1.2.i} – met in acht name van hetgeen opgemerkt in artikel 4 van deze Verwerkersovereenkomst – de volgende partijen als Subverwerker inschakelt, waarvoor Politie een specifieke toestemming geeft:

- (1) N.v.t.
- Soort dienstverlening: n.v.t.

Locaties van dienstverlening en datacentra buiten de EEA, waarbij er sprake is van een Verwerking van Persoonsgegevens buiten de EEA of toegang vanuit buiten de EEA:

- (1) N.v.t.

Bijlage 3 – Beveiligingsmaatregelen en toegang

In het kader van de dienstverlening van 5.1.2.1 aan Politie treft 5.1.2.1 passende technische en organisatorische maatregelen ter beveiliging van de Persoonsgegevens zoals nader gespecificeerd in deze bijlage. 5.1.2.1 draagt zorg voor het actualiseren van haar beveiligingsmaatregelen bij mogelijke veranderingen in de toekomst.

3.1 Beveiligingsmaatregelen

Met betrekking tot de Verwerkingen die plaatsvinden in het kader van de dienstverlening worden ten tijde van het sluiten van de Verwerkersovereenkomst de volgende beveiligingsmaatregelen getroffen door 5.1.2.1

- momentopname 5.1.2.1
- de huidige 5.1.2.1 'in control'-statement bijgevoegd als **Annex 1** bij deze Bijlage.
- de huidige 'Statement of Applicability ISO27001' bijgevoegd als **Annex 2** bij deze Bijlage.

3.2 Doorgifte buiten de EEA

Niet van toepassing: er is geen sprake van doorgifte van Persoonsgegevens door 5.1.2.1 naar een land buiten de EEA of naar een internationale organisatie in het kader van de dienstverlening aan Politie.

Bijlage 3 – Annex 1: ^{5.1.2.1} in control statement

Bijlage 3 – Annex 2: Statement of Applicability ISO27001

Inhoudsopgave

Inhoud

Artikel 1. Begrippen	2
Artikel 2. Voorwerp van deze Verwerkersovereenkomst	3
Artikel 3. Inwerkingtreding en duur	3
Artikel 4. Omvang Verwerkingsbevoegdheid Wederpartij	3
Artikel 5. Beveiliging van de Verwerking	4
Artikel 6. Geheimhouding door Personeel van Wederpartij	4
Artikel 7. Subverwerker	4
Artikel 8. Bijstand vanwege rechten van Betrokkene	4
Artikel 9. Inbreuk in verband met Persoonsgegevens	5
Artikel 10. Teruggave Persoonsgegevens	5
Artikel 11. Informatieverplichting en audit	5
Artikel 12. Overige Voorwaarden	5
Bijlage 1. De Verwerking van Persoonsgegevens	7
Bijlage 2. Passende technische en organisatorische maatregelen	8
Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens	9

Verwerkersovereenkomst ^{5.1.2.i}

Contractnummer: ^{5.1.2.i}

De ondergetekenden:

1. De Staat der Nederlanden, waarvan de zetel is gevestigd te Den Haag, te dezen vertegenwoordigd door de Minister van Justitie en Veiligheid, namens deze,

^{5.1.2.e}

hierna te noemen: Opdrachtgever,

en

2. ^{5.1.2.i}

(statutair) gevestigd te ^{5.1.2.i}

te dezen vertegenwoordigd door

^{5.1.2.e}

hierna te noemen: Wederpartij,

hierna gezamenlijk te noemen: Partijen;

OVERWEGENDE DAT:

- Voor zover Wederpartij Persoonsgegevens verwerkt ten behoeve van Opdrachtgever in het kader van de Overeenkomst kwalificeert Opdrachtgever krachtens artikel 4, onderdeel 7 en onderdeel 8, van de Verordening als verwerkingsverantwoordelijke voor de Verwerking van Persoonsgegevens en Wederpartij als verwerker;
- Partijen in deze Verwerkersovereenkomst, zoals bedoeld in artikel 28, derde lid, van de Verordening, hun afspraken over de Verwerking van Persoonsgegevens door Wederpartij 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 artikel 1 van de Algemene Rijksvoorwaarden bij IT-overeenkomsten 2016 (ARBIT-2016) en de Overeenkomst tussen Opdrachtgever en Wederpartij Overeenkomst ^{5.1.2.i}, met kenmerk ^{5.1.2.i}. In afwijking daarvan of aanvulling daarop wordt onder de volgende begrippen in deze Verwerkersovereenkomst verstaan:

1.1 Betrokkene: degene op wie een Persoonsgegeven betrekking heeft.

1.2 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.

1.3 Opdrachtgever: Ministerie van Justitie en veiligheid

1.4 Overeenkomst: de overeenkomst tussen Opdrachtgever en Wederpartij Overeenkomst ^{5.1.2.i}, met kenmerk ^{5.1.2.i}

1.5 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, die Wederpartij in het kader van de Overeenkomst ten behoeve van Opdrachtgever verwerkt.

1.6 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).

1.7 Verwerkersovereenkomst: deze overeenkomst inclusief overwegingen en bijbehorende bijlagen.

1.8 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.

1.9 Wederpartij ^{5.1.2.i}

Artikel 2. Voorwerp van deze Verwerkersovereenkomst

2.1 Deze Verwerkersovereenkomst regelt de Verwerking van Persoonsgegevens door Wederpartij in het kader van de Overeenkomst.

2.2 De aard en het doel van de Verwerking, het soort Persoonsgegevens en de categorieën van Betrokkenen zijn in Bijlage 1 omschreven.

2.3 Wederpartij 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 Wederpartij garandeert te voldoen aan de vereisten van de toepasselijke wet- en regelgeving betreffende de verwerking van Persoonsgegevens.

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 en voor zover Wederpartij alle Persoonsgegevens overeenkomstig artikel 10 heeft gewist of terugbezorgd.

3.3 Geen van Partijen kan deze Verwerkersovereenkomst tussentijds opzeggen.

Artikel 4. Omvang Verwerkingsbevoegdheid Wederpartij

4.1 Wederpartij Verwerkt de Persoonsgegevens uitsluitend in opdracht van en op basis van schriftelijke instructies van Opdrachtgever behoudens afwijkende wettelijke voorschriften die op Wederpartij van toepassing zijn.

4.2 Indien een instructie als bedoeld in het eerste lid naar het oordeel van Wederpartij in strijd is met een wettelijk voorschrift inzake gegevensbescherming, stelt hij Opdrachtgever daarvan

voorafgaand aan de verwerking in kennis, tenzij een wettelijk voorschrift deze kennisgeving verbiedt.

4.3 Indien Wederpartij op grond van een wettelijke verplichting Persoonsgegevens dient te verstrekken, informeert hij Opdrachtgever onmiddellijk, en zo mogelijk voorafgaand aan de verstrekking.

4.4 Wederpartij heeft geen zeggenschap over het doel van en de middelen voor de Verwerking van Persoonsgegevens.

Artikel 5. Beveiliging van de Verwerking

5.1 In aanvulling op artikel 29 van de Overeenkomst en onverminderd artikel 2.3 treft Wederpartij 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. Wederpartij waarborgt een op het risico afgestemd beveiligingsniveau.

5.3 Indien en voor zover Opdrachtgever daarom uitdrukkelijk schriftelijk verzoekt, zal Wederpartij aanvullende maatregelen treffen met het oog op de beveiliging van de Persoonsgegevens.

5.4 Wederpartij Verwerkt Persoonsgegevens niet buiten de Europese Unie, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming heeft verkregen van Opdrachtgever en behoudens afwijkende wettelijke verplichtingen.

5.5 Wederpartij 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 Wederpartij 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 Wederpartij

6.1 De Persoonsgegevens hebben een vertrouwelijk karakter als bedoeld in artikel 30 van de Overeenkomst.

6.2 Wederpartij toont op verzoek van Opdrachtgever aan dat zijn Personeel zich ertoe heeft verbonden vertrouwelijkheid in acht te nemen als bedoeld in artikel 30 van de Overeenkomst.

Artikel 7. Subverwerker

7.1 Bij het uitvoeren van de Overeenkomst mag Wederpartij alleen met voorafgaande toestemming van Opdrachtgever gebruik maken van de diensten van derden. Deze toestemming, waaraan door Opdrachtgever nadere voorwaarden kunnen worden verbonden, wordt niet zonder redelijke grond geweigerd.

7.2 Toestemming van Opdrachtgever laat de eigen verantwoordelijkheid en aansprakelijkheid van Wederpartij 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 Wederpartij, met inachtneming van het bepaalde in artikel 7.1 en 7.2, 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

Wederpartij verleent Opdrachtgever bijstand bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III van de Verordening vastgestelde rechten van de Betrokkene te beantwoorden.

Artikel 9. Inbreuk in verband met Persoonsgegevens

9.1 Wederpartij 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 Wederpartij 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 de door henzelf in verband met de melding aan de bevoegde toezichthoudende autoriteit en Betrokkene te maken kosten.

9.4 In aanvulling op artikel 23.4 van de Overeenkomst komt de in artikel 23.3 van de Overeenkomst opgenomen beperking van aansprakelijkheid ook te vervallen ten aanzien van aanspraken op schadevergoeding, waaronder mede begrepen de door de toezichthoudende autoriteit opgelegde boetes, in verband met tekortschieten in de nakoming van de Verwerkersovereenkomst.

Artikel 10. Teruggave Persoonsgegevens

10.1 Na afloop van de Overeenkomst draagt Wederpartij, naar gelang de keuze van Opdrachtgever, zorg voor het terugbezorgen aan Opdrachtgever of het wissen van alle Persoonsgegevens. Wederpartij verwijdt kopieën, behoudens afwijkende wettelijke voorschriften.

10.2 Wederpartij wist de Persoonsgegevens binnen 5 dagen na afloop van de Overeenkomst, bij gebreke waarvan Wederpartij een boete verschuldigd is van €1.000 per dag, met een maximum van €10.000.

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

11.2 Wederpartij verleent alle benodigde medewerking aan audits.

11.3 Om aan de door Opdrachtgever gestelde eisen te voldoen heeft Wederpartij ervoor gekozen om zich te laten certificeren voor de ISO27000 standaard. In het kader van die certificering laat Wederpartij zich eenmaal per jaar auditen. Opdrachtgever accepteert dit als de jaarlijks uit te

voeren audit indien Wederpartij de Verklaring van toepasselijkheid en het rapport van bevindingen van die audit aan Opdrachtgever overlegt.

Artikel 12. Overige Voorwaarden

Artikel 28.1 van de Overeenkomst vervalt. De inhoud van dit artikel is vastgelegd in deze Verwerkersovereenkomst.

Artikel 28.2 van de Overeenkomst blijft van toepassing. De verwijzing in artikel 28.2 van de Overeenkomst naar artikel 28.1 van de Overeenkomst moet worden gelezen als een verwijzing naar deze Verwerkersovereenkomst.

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

5.1.2.e

5.1.2.e

5.1.2.e

Bijlage 1. De Verwerking van Persoonsgegevens

Voor de verwerking is door de politie een Gegevensbeschermingseffectbeoordeling (GEB) uitgevoerd.

Doel van de verwerking

Primaire doelstelling is

- snelle en ongestoorde toegangsverlening tot C2000 opstelpunten voor daartoe geautoriseerde personen,
- voorkomen en detecteren van ongeautoriseerde toegang tot C2000 opstelpunten;
- verificatie van alarmen van sensoren ter bewaking van bovenstaande doelen of de omgevingscondities van de C2000 apparatuur.

Secondaire doelstellingen

- Ondersteuning in onderzoek naar verdachte beheer- en onderhoudshandelingen in het C2000 opstelpunt indien daartoe een vermoeden bestaat.

Persoonsgegevens

De volgende persoonsgegevens worden verwerkt binnen het 5.1.2.1 systeem.

Betrokkene	Categorie persoonsgegevens	Persoonsgegevens
Houder van een toegangspas en/of mechatronische sleutel	Algemeen	5.1.2.1
	Gevoelig	
	Bijzonder	
	Strafrechtelijk	
	Wettelijke identificatienummers	
Houder van een mechatronische sleutel die het terrein van het opstelpunt betreedt	Algemeen	
	Gevoelig	
	Bijzonder	
	Strafrechtelijk	
	Wettelijke identificatienummers	
Houder van een toegangspas en mechatronische sleutel die een apparatuuruimte betreedt	Algemeen	
	Gevoelig	
	Bijzonder	
	Strafrechtelijk	
	Wettelijke identificatienummers	

Verwerkersovereenkomst 5.1.2.1

PAC operators en functioneel beheerders	Algemeen
	Gevoelig
	Bijzonder
	Strafrechtelijk
ICT beheerders	Wettelijke identificatienummers
	Algemeen
	Gevoelig
	Bijzonder
	Strafrechtelijk
	Wettelijke identificatienummers

(*) Conform Cameratoezicht Beleidsregels voor de toepassing van bepalingen uit de Wvets bescherming persoonsgegevens en de Wvets politiegegevens – Autoriteit Persoonsgegevens paragraaf 2.11 worden de bijzondere persoonsgegevens niet als zodanig beschouwd gezien het doel van de verwerking, maar wel als strafrechtelijke gegevens wanneer het cameratoezicht ertoe zal leiden dat er onderscheid wordt gemaakt ten aanzien van een betrokkene die een strafbaar feit begaat. Het verbod om strafrechtelijke gegevens te verwerken is echter niet van toepassing op de verantwoordelijke die deze gegevens verwerkt ter bescherming van zijn belangen voor zover het gaat om strafbare feiten die zijn of op grond van feiten en omstandigheden naar verwachting zullen worden gepleegd jegens hem of jegens personen die in zijn dienst zijn. Conform AVG artikel 10 zijn strafrechtelijke gegevens: persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen 5.1.2.1 camerabeelden en/of loggegevens waaruit strafbare handelingen blijken vallen buiten deze definitie. Er worden dus geen bijzondere persoonsgegevens verwerkt.

Verstrekkers en ontvangers

Verstrekker	Medewerker van beheer- of onderhoudspartij die toegang nodig heeft tot C2000 opstelpunt.
Ontvanger	Politie (intern belegd bij MDC) De van verstrekker ontvangen gegevens
Verstrekker	5.1.2.1 namens MinJenV Logging en camerabeelden indien gerechtelijke vervolging wordt ingesteld tegen een pashouder
Ontvanger	Politie/Openbaar ministerie Logging en camerabeelden indien gerechtelijke vervolging wordt ingesteld tegen een pashouder

Bijlage 2. Passende technische en organisatorische maatregelen

De eisen aan de Wederpartij zijn gesteld in hoofdstuk 7 van Bijlage 3 Programma van Eisen, Niet-openbare Europese aanbesteding Site Toegangs- en Alarmeringssysteem C2000 2017- 2027 (versie 1.0, kenmerk 805210, d.d 13 juli 2017) en in de Overeenkomst EA Site Toegangs- en Alarmeringssysteem C2000 v3.0 in de artikelen 28, 29 en 30.

Wederpartij heeft zijn technische en organisatorische maatregelen ingericht conform deze eisen. De maatregelen zijn door Wederpartij beschreven in:

Plan	Versie	Goedgekeurd	Datum
5.1.2.i			5.1.2.i
	J		
	J		
	J		
	J		
	J		
	J		
	J		

Als onderdeel van de organisatorische maatregelen worden deze documenten periodiek beoordeeld en zo nodig aangepast.

De technische inrichting van het 5.1.2.i is door Wederpartij beschreven in:

Plan	Versie	Goedgekeurd	Datum
5.1.2.i			5.1.2.i
	J		
	J		
	J		
	J		
	J		
	J		

Bewaartermijnen

De autorisatiegegevens worden bewaard tot 12 maanden na inlevering van de toegangsmiddelen.

De loggegevens worden tot 24 maanden na de logdatum bewaard.

De centraal opgeslagen (low quality) camerabeelden worden opgeslagen en automatisch gewist / overschreven na 28 dagen.

De lokaal (in de camera's zelf) opgeslagen camerabeelden (high quality) worden automatisch overschreven zodra de SD opslagkaart vol is. Bewaartermijn is dus afhankelijk van aantal en lengte van bezoeken aan de betreffende ruimte.

Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens

In deze bijlage moeten de afspraken over hoe Wederpartij Opdrachtgever over Inbreuken in verband met Persoonsgegevens gaat informeren nader worden gespecificeerd.

Inbreuken in verband met Persoonsgegevens worden door Wederpartij gemeld aan Opdrachtgever conform paragraaf 3.2.5 Informatiebeveiligingsincidenten van Appendix 4 – Dossier Afspraken en Procedures, Niet - openbare Europese aanbesteding Site Toegangs- en Alarmeringssysteem C2000 2017- 2027 (5.1.2.1 of een geldende nieuwere versie)

Informatie die ten minste door Wederpartij moet worden verstrekt

Aard van de Inbreuk in verband met Persoonsgegevens
De Persoonsgegevens en Betrokkene
Waarschijnlijke gevolgen van de Inbreuk in verband met Persoonsgegevens
Maatregelen die Wederpartij 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

ADDENDUM

Documentgegevens

Publicatiegegevens

Titel	Verwerkersovereenkomst
Versie	1.0
Datum	11 juni 2019
Auteur	5.1.2.e ;
Afdeling	5.1.2.i ;
Bedrijfsnaam	5.1.2.i

Contact

Contactpersoon	5.1.2.e
Telefoon	
E-mail	5.1.2.e
Webpagina	5.1.2.i

Copyright 2019, 5.1.2.i

Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder schriftelijke toestemming van 5.1.2.i

Inhoudsopgave

Artikel 1. Definities	4
Artikel 2. Ingangsdatum en duur	5
Artikel 3. Onderwerp van deze overeenkomst.....	5
Artikel 4. Naleving wet- en regelgeving	5
Artikel 5. Inbreuk in verband met Persoonsgegevens	6
Artikel 6. Geheimhoudingsplicht.....	6
Artikel 7. Beveiligingsmaatregelen	6
Artikel 8. Inschakeling derden	7
Artikel 9. Wijziging overeenkomst	7
Artikel 10. Aansprakelijkheid	7
Artikel 11. Toepasselijk recht	7

Verwerkersovereenkomst van Ministerie van Justitie en Veiligheid met de Verwerker

De ondergetekenden:

De Staat der Nederlanden, de Minister van Justitie en Veiligheid, ten deze rechtsgeldig vertegenwoordigd door de heer P.Th. Gelton, directeur Veiligheidsregio's, Crisisbeheersing en Meldkamer, hierna te noemen: de "Verwerkingsverantwoordelijke";

en

^{5.1.2.i} [redacted], gevestigd te ^{5.1.2.i} [redacted],
rechtsgeldig vertegenwoordigd door ^{5.1.2.e} [redacted],
hierna te noemen: ^{5.1.2.i} [redacted] of "Verwerker";

Komen overeen:

Artikel 1. Definities

- 1.1 "**Verwerking**": een bewerking of een geheel van bewerkingen 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, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;
- 1.2 "**Verwerkingsverantwoordelijke**": Het Ministerie van Justitie en Veiligheid, die alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.
- 1.3 "**Verwerker**": ^{5.1.2.i} [redacted] die ten behoeve van de Verwerkingsverantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.
- 1.4 "**Betrokkene**": degene op wie een persoonsgegeven betrekking heeft.
(Identificeerbaar natuurlijk persoon)
- 1.5 "**Derde**": een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de Verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de Verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken.
- 1.6 "**Privacywetgeving**": De Algemene Verordening Gegevensbescherming, indien en voor zover sprake is van geldend recht dat binnen de Nederlandse rechtsorde rechtstreeks van toepassing is op de uitvoering van de Hoofdovereenkomst.
- 1.7 "**Hoofdovereenkomst**": 2009-08-20 d.d. 29 januari 2010.

Artikel 2. Ingangsdatum en duur

- 2.1 Deze Verwerkersovereenkomst gaat in op het moment van ondertekening en duurt voort zolang de Verwerker als Verwerker van persoonsgegevens optreedt in het kader van de door de Verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens.

Artikel 3. Onderwerp van deze overeenkomst

- 3.1 De Verwerker verwerkt persoonsgegevens uitsluitend op basis van schriftelijke instructies van de Verwerkingsverantwoordelijke in het kader van de uitvoering van de Hoofdovereenkomst.
- 3.2 De Verwerker verbindt zich om in het kader van die werkzaamheden de door de Verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens zorgvuldig te verwerken.
- 3.3 Dat de Privacywetgeving aan de Verwerkingsverantwoordelijke de plicht oplegt om ervoor zorg te dragen dat de Verwerker voldoende waarborgen biedt ten aanzien van de technische- en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen.

Artikel 4. Naleving wet- en regelgeving

- 4.1 De Verwerker heeft geen zeggenschap over de ter beschikking gestelde persoonsgegevens.
- 4.2 De Verwerker zal bij de verwerking van persoonsgegevens in het kader van de in artikel 3 genoemde werkzaamheden, handelen in overeenstemming met de toepasselijke wet- en regelgeving betreffende de bescherming van persoonsgegevens. De Verwerker verwerkt persoonsgegevens slechts in schriftelijke opdracht van de Verwerkingsverantwoordelijke, behoudens afwijkende wettelijke verplichtingen.
- 4.3 De Verwerker informeert de Verwerkingsverantwoordelijke onmiddellijk zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens.
- 4.4 De Verwerker zal te allen tijde op eerste verzoek van de Verwerkingsverantwoordelijke afkomstige persoonsgegevens met betrekking tot deze Verwerkersovereenkomst ter hand stellen.
- 4.5 De Verwerker zal alle van de Verwerkingsverantwoordelijke afkomstige persoonsgegevens met betrekking tot deze Verwerkersovereenkomst op een nader te bepalen wijze vernietigen op het moment van beëindigen van deze overeenkomst, dan wel op uitdrukkelijk verzoek van de Verwerkingsverantwoordelijke de gegevens te vernietigen op een nader te bepalen wijze, tenzij opslag van de persoonsgegevens Unierechtelijk of lidstaatrechtelijk is verplicht.
- 4.6 De Verwerker stelt, indien dit redelijkerwijs binnen zijn invloedssfeer ligt, de Verwerkingsverantwoordelijke te allen tijde in staat om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de Privacywetgeving, meer in het bijzonder de rechten van betrokkenen, zoals, maar niet beperkt tot een

- 4.7 verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens en het uitvoeren van een gehonoreerd aangetekend verzet. Partijen garanderen dat zij in hun hoedanigheid als Verwerker en Verwerkingsverantwoordelijke niet in strijd zullen handelen met de bij of krachtens de Privacywetgeving gegeven voorschriften.

Artikel 5. Inbreuk in verband met Persoonsgegevens

- 5.1 Verwerker zal Verwerkingsverantwoordelijke onmiddellijk 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 zo snel mogelijk alle maatregelen om de Inbreuk te herstellen, de gevolgen daarvan te beperken en verdere Inbreuken te voorkomen.
- 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.

Artikel 6. Geheimhoudingsplicht

- 6.1 Personen in dienst van, dan wel werkzaam ten behoeve van de Verwerker, evenals de Verwerker zelf, zijn verplicht tot geheimhouding met betrekking tot de persoonsgegevens waarvan zij kennis kunnen nemen, behoudens voor zover een bij, of krachtens de wet gegeven voorschrift tot verstrekking verplicht of zijn taak daartoe noodzaakt.

Artikel 7. Beveiligingsmaatregelen

- 7.1 Partijen nemen in hun rol als Verwerker en Verwerkingsverantwoordelijke alle passende technische en organisatorische maatregelen om de persoonsgegevens welke worden verwerkt te beveiligen en beveiligd te houden.
- 7.2 De Verwerkingsverantwoordelijke is te allen tijde gerechtigd de verwerking van persoonsgegevens te doen controleren. De Verwerker is verplicht medewerking te verlenen zodat de controle daadwerkelijk uitgevoerd kan worden tegen haar standaard (uur) tarieven. De Verwerkingsverantwoordelijke, of de door de Verwerkingsverantwoordelijke ingeschakelde derde, is gehouden alle informatie betreffende deze controles vertrouwelijk te behandelen.

Artikel 8. Inschakeling derden

- 8.1 De Verwerker is verantwoordelijk voor de correcte naleving van de bepalingen van deze verwerkingsovereenkomst door eventueel door haar ingeschakelde derden.

Artikel 9. Wijziging overeenkomst

- 9.1 Wijziging van deze Verwerkersovereenkomst kan slechts schriftelijk plaatsvinden.
9.2 Elk van de partijen is gerechtigd de overeenkomst met onmiddellijke ingang te beëindigen in geval van overmacht, waaronder mede begrepen een zodanige wijziging van wettelijke regels dat een verdere voortzetting van de overeenkomst niet kan worden verlangd.
9.3 Bij het beëindigen van deze Verwerkersovereenkomst met onmiddellijke ingang, wordt in de brief aan de andere Partij de reden van beëindiging vermeld.

Artikel 10. Aansprakelijkheid

- 10.1 Indien de Verwerker tekortschiet in de nakoming van de verplichting uit deze overeenkomst kan Verwerkingsverantwoordelijke hem in gebreke stellen. Ingebrekestelling geschiedt schriftelijk, waarbij aan de Verwerker een redelijke termijn wordt gegund om alsnog haar verplichtingen na te komen. Deze termijn is een fatale termijn. Indien nakoming binnen deze termijn uitblijft, is Verwerker in verzuim.
10.2 De uitsluitingen en beperkingen van aansprakelijkheid als opgenomen in de Hoofdovereenkomst hebben mede betrekking op iedere aansprakelijkheid van Verwerker (voor schade, boetes dwangsommen en/of anderszins) die voortvloeit of verband houdt met het niet-nakomen van, of in strijd handelen met de bij of krachtens de Privacywetgeving gegeven voorschriften en/of het niet-nakomen van, of in strijd handelen met het in deze Verwerkersovereenkomst bepaalde.
10.3 Indien Verwerker door enige derde wordt aangesproken met betrekking tot dwangsommen, boetes en/of de vergoeding van schade en deze aanspraak vloeit voort uit het in strijd handelen met de bij of krachtens de Privacywetgeving gegeven voorschriften en/of het niet-nakomen van, of in strijd handelen met het in deze Verwerkersovereenkomst bepaalde door Verwerkingsverantwoordelijke, zal Verwerkingsverantwoordelijke Verwerker volledig vrijwaren en schadeloos stellen.

Artikel 11. Toepasselijk recht

- 11.1 Op deze overeenkomst en op alle geschillen die daaruit mogen voortvloeien of daarmee mogen samenhangen, is het Nederlands recht van toepassing.

Ondertekening

Aldus overeengekomen op 11 juni 2019, vastgelegd op 8 pagina's tekst en in tweevoud ondertekend te Den Haag / 5.1.2.i .

Namens de Staat der Nederlanden,
de Minister van Justitie en Veiligheid,
voor deze,

P.Th. Gelton, directeur Veiligheidsregio's, Crisisbeheersing en Meldkamer

5.1.2.e





Verwerkersovereenkomst

**support- en
onderhoudsdiensten
Landelijk Contact Center
Politie**

5.1.2.1

**Verwerkers-
Overeenkomst
ARBIT**

Nummer: 5.1.2.1

Ingangsdatum: 01-07-201

Uitgegeven door: Politie, Politiedienstencentrum - Dienst Verwerving

Informatie: Inkoopmanagement

Status:Definitief

Versie: 1.0

Versie datum: 9 juli 2019

Inhoudsopgave

1.	Begrippen	5
2.	Totstandkoming, duur en einde van de Verwerkersovereenkomst	5
3.	Voorwerp van de Verwerkersovereenkomst	5
4.	Van toepassing zijnde Voorwaarden	7
5.	Voortdurende verplichtingen	7
6.	Teruggave Persoonsgegevens en/of Politiegegevens	7
7.	Intellectuele eigendomsrechten	8
8.	Beveiliging	8
9.	Meldplicht Datalekken en beveiligingsinbreuken	8
10.	Geheimhouding, beschikbaarheid en integriteit	8
11.	Controle	9
12.	Informereren van betrokkenen	9
13.	Aansprakelijkheid	10
14.	Maatregelen toezichthouder	10
15.	Wijziging	10
16.	Slotbepalingen	11

Verwerkersovereenkomst

inzake de **Overeenkomst** support- en onderhoudsdiensten Landelijk Contact Center Politie

a) met daarop aanvullend van toepassing de ARBIT-2018

b) Referentienummer: 5.1.2.i

De ondergetekenden:

1. Politie, (statutair) gevestigd te 's-Gravenhage, te dezen vertegenwoordigd door haar korpschef de heer E.S.M. Akerboom, namens deze dhr. G.Th. den Uyl MPA (Directeur PDC), hierna te noemen: Opdrachtgever,

en

2. 5.1.2.i (statutair) gevestigd te 5.1.2.i, te 5.1.2.e dezen vertegenwoordigd door haar 5.1.2.e hierna te noemen: Opdrachtnemer

hierna gezamenlijk te noemen: 'Partijen;

OVERWEGENDE DAT:

Partijen de Overeenkomst inzake "support- en onderhoudsdiensten Landelijk Contact Center Politie"

- met kenmerk 5.1.2.i (hierna te noemen: de Overeenkomst) hebben gesloten;
- in het kader van de uitvoering daarvan Persoonsgegevens in de zin van artikel 4 sub 1 van de Algemene Verordening Gegevensbescherming EU 2016/679 (hierna te noemen: AVG) worden verwerkt en/of Politiegegevens in de zin van artikel 1 onder a van de Wet Politiegegevens (Wpg);
- Opdrachtnemer die in het kader van de uitvoering van de Overeenkomst met de Politie Persoonsgegevens en/of Politiegegevens verwerkt is aan te merken als Verwerker in de zin van de AVG en/of Wpg;
- De Politie als Opdrachtgever Verwerkingsverantwoordelijk is voor de Persoonsgegevens en Politiegegevens;
- Partijen middels deze Verwerkersovereenkomst nadere afspraken over het verwerken van de Persoonsgegevens en/of Politiegegevens door Opdrachtnemer als Verwerker en de geldende wettelijke verplichtingen uit de AVG en/of Wpg waaronder meldplicht Datalek wensen vast te leggen;

KOMEN OVEREEN:

1. Begrippen

Aanvullend op de AVG en Wpg geldt dat de hierna en hiervoor in deze Verwerkersovereenkomst vermelde, met een hoofdletter geschreven begrippen, de volgende betekenis hebben:

1. AP: Autoriteit Persoonsgegevens (<https://autoriteitpersoonsgegevens.nl>)
2. AVG: Algemene Verordening Gegevensbescherming EU 2016/679.
3. Betrokkene: degene op wie de Persoonsgegevens betrekking hebben.
4. Datalek: een inbreuk op de beveiliging, in de zin van artikel 33 en 34 AVG, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van Persoonsgegevens en/of Politiegegevens waaronder een inbreuk op vertrouwelijkheid, verlies, wijziging van gegevens.
5. Hulpleverancier: een partij of derde die door Opdrachtnemer is ingeschakeld om te ondersteunen bij het uitvoeren van de Overeenkomst. Indien de Hulpleverancier in opdracht van Opdrachtnemer Persoonsgegevens en/of Politiegegevens verwerkt, is Hulpleverancier tevens aan te merken als sub-verwerker.
Overeenkomst: de overeenkomst inzake support- en onderhoudsdiensten Landelijk Contact Center Politie
6. met kenmerk ^{5.1.2.1} [REDACTED] waarin de Politie onder zijn verantwoordelijkheid vallende Persoonsgegevens en/of Politiegegevens door Opdrachtnemer wil laten bewerken.
7. Partij: De Politie of Opdrachtnemer, afhankelijk van de context.
8. Verwerkersovereenkomst: deze overeenkomst inclusief overwegingen en bijbehorende bijlagen.
9. Wpg: Wet Politiegegevens.

2. Totstandkoming, duur en einde van de Verwerkersovereenkomst

- 2.1 Deze Verwerkersovereenkomst treedt in werking na ondertekening door beide Partijen en niet eerder dan op de datum waarop de Overeenkomst in werking treedt.
- 2.2 Deze Verwerkersovereenkomst zal van kracht zijn gedurende de looptijd van de Overeenkomst. Indien de Overeenkomst eindigt, eindigt deze Verwerkersovereenkomst van rechtswege.
- 2.3 Geen van beide Partijen kan deze Verwerkersovereenkomst tussentijds opzeggen.

3. Voorwerp van de Verwerkersovereenkomst

- 3.1 Opdrachtnemer Verwerkt in opdracht van de Politie uitsluitend de in **Bijlage 1** beschreven categorieën Persoonsgegevens en/of Politiegegevens van de Politie voor het daarin genoemde doel.
- 3.2 Opdrachtnemer zal de Persoonsgegevens en/of Politiegegevens op behoorlijke en zorgvuldige wijze en in overeenstemming met de AVG, Wpg en andere toepasselijke regelgeving betreffende de Verwerking van Persoonsgegevens verwerken.
- 3.3 Opdrachtnemer Verwerkt Persoonsgegevens en/of Politiegegevens slechts in opdracht van de Politie voor zover noodzakelijk om de diensten zoals omschreven in de Overeenkomst aan de Politie te verlenen en volgt alle instructies van de Politie dienaangaande op, behoudens afwijkende wettelijke verplichtingen.
- 3.4 Opdrachtnemer heeft geen zeggenschap over het doel en de middelen voor de Verwerking van Persoonsgegevens en/of Politiegegevens. Voor zover niet anders is bepaald in deze Verwerkersovereenkomst, neemt Opdrachtnemer geen beslissingen over het gebruik van de Persoonsgegevens en/of Politiegegevens, de verstrekking aan derden en de duur van de opslag van Persoonsgegevens en/of Politiegegevens. De zeggenschap over de

Persoonsgegevens en/of Politiegegevens verstrekt onder deze Verwerkersovereenkomst komt nimmer bij Opdrachtnemer te berusten.

- 3.5. Opdrachtnemer schakelt geen Hulpverleners in zonder schriftelijke voorafgaande toestemming van de Politie.

Aan toestemming van de Politie voor de inschakeling van Hulpverleners zullen in ieder geval de volgende voorwaarden worden verbonden:

- a. Opdrachtnemer heeft een schriftelijke overeenkomst met de desbetreffende Hulpverlener waarin in ieder geval het volgende is opgenomen:
 - een verplichting dat de Hulpverlener dient te handelen in overeenstemming met alle bepalingen uit deze Verwerkersovereenkomst;
 - een verplichting dat de Hulpverlener alle aanwijzingen met betrekking tot de verwerking van Persoonsgegevens en/of Politiegegevens van de Politie en Opdrachtnemer opvolgt inclusief de verplichting tot geheimhouding en het nemen van de nodige beveiligingsmaatregelen als beschreven in **Bijlage 1**;
 - een verplichting van de Hulpverlener om de Persoonsgegevens en/of Politiegegevens uitsluitend in opdracht en volgens de instructies van Opdrachtnemer te verwerken;
 - een verplichting van de Hulpverlener om zelf geen sub-opdrachtnemers in te schakelen, zonder de voorafgaande schriftelijke toestemming van de Politie;
 - een verplichting dat de Hulpverlener de Opdrachtnemer (en daarmee de Politie) in staat stelt zijn verplichtingen in het geval van een vermoedelijk of daadwerkelijk Datalek na te komen.
- b. Opdrachtnemer geeft de Hulpverlener pas toegang tot de Persoonsgegevens en/of Politiegegevens na de schriftelijke toestemming van de Politie; en
- c. De Politie is gerechtigd om op eerste verzoek de gemaakte afspraken tussen Opdrachtnemer en de Hulpverlener in te zien. Opdrachtnemer zal uiterlijk 30 dagen na ontvangst van dit verzoek een afschrift aan de Politie verstrekken.

De door de Politie gegeven toestemming laat onverlet de verantwoordelijkheid en aansprakelijkheid van Opdrachtnemer voor de nakoming van zijn verplichtingen onder de Verwerkersovereenkomst.

- 3.6 Het is Opdrachtnemer uitdrukkelijk niet toegestaan Persoonsgegevens en/of Politiegegevens aan anderen dan de Politie te verstrekken, tenzij op schriftelijk verzoek van de Politie, of met diens schriftelijke toestemming. Opdrachtnemer is na verleende toestemming verplicht schriftelijk te bevestigen dat een verstrekking heeft plaatsgevonden, waarbij hij binnen 30 dagen exact de verstrekte Persoonsgegevens en/of Politiegegevens, de Betrokkene(n), de ontvanger(s) en het moment van verstrekking gedocumenteerd aan de Politie dient te beschrijven.
- 3.7 Indien Opdrachtnemer op grond van een wettelijke verplichting gegevens dient te verstrekken, verifieert Opdrachtnemer de grondslag van het verzoek en de identiteit van de verzoeker en informeert hij onmiddellijk, zo mogelijk voorafgaand aan de verstrekking, de Politie ter zake.
- 3.8 Opdrachtnemer verleent de Politie volledige medewerking om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de AVG en/of Wpg, meer in het bijzonder de rechten van Betrokkenen, zoals, maar niet beperkt tot, een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van Persoonsgegevens en/of Politiegegevens en het uitvoeren van een gehonoreerd aangetekend verzet.
- 3.9 Indien Opdrachtnemer onrechtmatige Verwerkingen of inbreuken op de in artikel 8.1 van deze Verwerkersovereenkomst genoemde beveiligingsmaatregelen signaleert, zal hij de Politie hierover onmiddellijk inlichten en alle redelijkerwijs benodigde maatregelen treffen om deze en verdere onrechtmatige Verwerkingen of inbreuken te beëindigen, te voorkomen of te beperken en ander onverminderd de verplichting van Opdrachtnemer om de eventueel door de Politie daardoor geleden schade te vergoeden.

- 3.10 De eventuele met de in de artikelen 3.8, artikel 3.9 en artikel 9 van deze Verwerkersovereenkomst gemoeide kosten komen voor rekening van degene die die kosten maakt.
- 3.11 De Politie en Opdrachtnemer zorgen ervoor dat de Functionaris voor de gegevensbescherming naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van Persoonsgegevens en/of Politiegegevens.
- 3.12 Opdrachtnemer documenteert alle inbreuken die in artikel 33 lid 5 AVG zijn beschreven.
- 3.13 Opdrachtnemer verleent alle benodigde medewerking in het kader van een gegevensbeschermingseffectbeoordeling in het kader van artikel 35 AVG. Voor het verlenen van deze medewerking is de Politie geen (aanvullende) vergoeding aan Opdrachtnemer verschuldigd.

4. Van toepassing zijnde Voorwaarden

Op deze Verwerkersovereenkomst zijn de bepalingen van de Overeenkomst van toepassing voor zover daarvan in deze Verwerkersovereenkomst niet wordt afgeweken.

5. Voortdurende verplichtingen

In aanvulling op artikel 34 van de ARBIT-2018 geldt dat na afloop van de Overeenkomst en de Verwerkersovereenkomst de lopende verplichtingen van Opdrachtnemer in stand blijven, zoals, doch niet beperkt tot overdracht, signalering van ongeautoriseerde Verwerkingen en geheimhouding, als ook nader bepaald in de artikelen 3.8, 3.9, 8, 9 en 10 van deze Verwerkersovereenkomst.

6. Teruggave Persoonsgegevens en/of Politiegegevens

- 6.1 Na afloop van de Overeenkomst en de Verwerkersovereenkomst dienen alle Persoonsgegevens en/of Politiegegevens, kopieën en bewerkingen daarvan, alsmede alle gegevensdragers waarop de Persoonsgegevens en/of Politiegegevens, kopieën of bewerkingen daarvan zijn of zullen worden vastgelegd, onmiddellijk op eerste verzoek van Politie te worden geretourneerd c.q. verstrekt aan de Politie (of een door de Politie aan te wijzen derde), dan wel te worden vernietigd, een en ander naar de keuze van de Politie. De Politie kan zo nodig nadere eisen stellen aan de wijze van beschikbaarstelling, waaronder eisen aan het bestandsformaat, dan wel vernietiging. Op het moment dat deze Verwerkersovereenkomst eindigt, zal Opdrachtnemer bovendien al zijn medewerking verlenen ter zake van de overdracht van de werkzaamheden inzake de Verwerking van de Persoonsgegevens en/of Politiegegevens aan de Politie of een opvolgende opdrachtnemer en wel op een zodanige wijze dat vanaf het moment dat de overdracht plaatsvindt de continuïteit van de dienstverlening maximaal gewaarborgd blijft, althans niet door handelen of nalaten van Opdrachtnemer wordt belemmerd.
- 6.2 De kosten gemoeid met de inspanningen van Opdrachtnemer als genoemd in 6.1, komen voor rekening van de Politie voor zover deze kosten niet inbegrepen zijn in de overeengekomen prijzen en vergoedingen van Opdrachtnemer voortvloeiende uit de uitvoering van de Overeenkomst.
- 6.3 Opdrachtnemer zal te allen tijde de hiervoor in artikel 6.1 beschreven dataportabiliteit waarborgen zodanig dat er geen sprake is van verlies van functionaliteit of (delen van) de gegevens.

7. Intellectuele eigendomsrechten

Onder verwijzing naar artikel 8 van de ARBIT-2018 blijven alle (intellectuele) eigendomsrechten – daaronder begrepen auteursrechten en databankenrechten – op de verzameling van Persoonsgegevens en/of Politiegegevens, kopieën of bewerkingen daarvan, blijven te allen tijde berusten bij de Politie of haar licentiegever(s).

8. Beveiliging

- 8.1 In aanvulling op artikel 18.1 van de ARBIT-2018 zal Opdrachtnemer alle technische en organisatorische beveiligingsmaatregelen implementeren zoals beschreven in Bijlage 1. Deze maatregelen zullen, met inachtneming van de stand der techniek en de kosten gemoeid met de implementatie en de uitvoering van de maatregelen, een passend beschermingsniveau verzekeren, zulks met inachtneming van de risico's die het verwerken van de Persoonsgegevens en/of Politiegegevens, en de aard daarvan, meebrengen.
- 8.2 Opdrachtnemer rapporteert periodiek met een frequentie van 1 maal per jaar, uiterlijk op 31 december aan de Politie over de door Opdrachtnemer genomen maatregelen aangaande de getroffen technische en organisatorische beveiligingsmaatregelen en eventuele aandachtspunten daarin.
- 8.3 De met de rapportage gemoeide kosten zijn voor rekening van Opdrachtnemer.
- 8.4 Opdrachtnemer Verwerkt geen Persoonsgegevens en/of Politiegegevens buiten een lidstaat van de Europese Unie en/of Europese Economische Ruimte (Noorwegen, Liechtenstein en IJsland).

9. Meldplicht Datalekken en beveiligingsinbreuken

- 9.1 In het geval van een daadwerkelijk(e) (i) Datalek; (ii) schending van de beveiligingsmaatregelen; (iii) schending van de geheimhoudingsplicht of (iv) verlies van vertrouwelijke gegevens zal Opdrachtnemer de Politie direct, doch uiterlijk binnen 24 uur na de eerste ontdekking van het incident, informeren. De Opdrachtnemer zal alle redelijkerwijs benodigde maatregelen treffen om (verdere) onbevoegde kennisneming, wijziging, en verstrekking dan wel anderszins onrechtmatige verwerking te voorkomen of te beperken en een schending van beveiligingsmaatregelen, schending van de geheimhoudingsplicht of verder verlies van vertrouwelijke gegevens te beëindigen en in de toekomst te voorkomen, onverminderd enig recht van de Politie op schadevergoeding of andere maatregelen voor zover het incident toerekenbaar is aan Opdrachtnemer of de door haar in te zetten Hulpleverancier. Deze bepaling is van toepassing op incidenten bij de Opdrachtnemer en haar eventuele Hulpleveranciers.
- 9.2 De informatie van de Opdrachtnemer behelst in ieder geval de in de **Bijlage 2** beschreven gegevens voor zover toepasselijk. Opdrachtnemer garandeert dat de verstrekte informatie volledig, correct en accuraat is.
- 9.3 Opdrachtnemer zal op verzoek van de Politie meewerken aan het informeren van de bevoegde autoriteiten en betrokkene(n).

10. Geheimhouding, beschikbaarheid en integriteit

- 10.1 Onder verwijzing naar artikel 17.1 van de ARBIT-2018 is Opdrachtnemer gehouden tot geheimhouding, en borging van de beschikbaarheid en integriteit van alle Persoonsgegevens en/of Politiegegevens en informatie die zij als uitvloeisel van deze Verwerkersovereenkomst

- verwerkt, behoudens in zoverre die Persoonsgegevens of informatie klaarblijkelijk geen geheim of vertrouwelijk karakter hebben, dan wel reeds algemeen bekend zijn.
- 10.2 Indien en voor zover de Politie daarom uitdrukkelijk schriftelijk verzoekt, zal Opdrachtnemer ten aanzien van de daarbij aangeduide Persoonsgegevens en/of Politiegegevens of informatie bijzondere maatregelen treffen met het oog op de geheimhouding daarvan, welke maatregelen onder meer kunnen inhouden de vernietiging van betrokken Persoonsgegevens en/of Politiegegevens of informatie zodra de noodzaak voor Opdrachtnemer om daarvan nog langer kennis te nemen, is komen te vervallen.
- 10.3 Onder verwijzing naar artikel 17.2 van de ARBIT-2018 zal Opdrachtnemer in haar arbeids- of inhuurovereenkomsten met het Personeel van Opdrachtnemer bedingen dat door die personen op overeenkomstige wijze als in artikel 10.1 en 10.2 bepaald geheimhouding zal worden betracht ten aanzien van alle Persoonsgegevens en/of Politiegegevens en informatie die zij in het kader van hun werkzaamheden verwerken. Opdrachtnemer staat er jegens de Politie voor in dat de bedoelde bedingen door de betrokken personen zullen worden nageleefd.
- 10.4 Na afloop van de Overeenkomst en deze Verwerkersovereenkomst blijft dit artikel 10 en de hierin besproken geheimhouding van kracht.

11. Controle

- 11.1 De Politie controleert op elk door haar gewenst moment dan wel laat op elk door haar gewenst moment:
- de verwerkingen en de naleving van de overeengekomen technische en organisatorische beveiligingsmaatregelen van Opdrachtnemer dan wel die van door Opdrachtnemer ingeschakelde Hulpleveranciers controleren, en
 - de naleving van de in **Bijlage 2** genoemde gegevens, die nodig zijn om aan de meldplicht, bedoeld in artikel 34 AVG, te voldoen controleren.
- 11.2 Opdrachtnemer verstrekt met een frequentie van 1 maal per jaar, uiterlijk op 31 december aan de Politie een verklaring van een onafhankelijke externe deskundige, waarin deze een oordeel geeft over de genoemde naleving als bedoeld in artikel 11.1 a en b.
- 11.3 Opdrachtnemer zal alle redelijkerwijs benodigde medewerking verlenen aan de controle en er voor zorg dragen ook de door hem ingeschakelde Hulpleveranciers hiertoe de redelijkerwijs benodigde medewerking zullen verlenen.
- 11.4 Het uitvoeren van een controle zal niet tot een vertraging van de door Opdrachtnemer in het kader van de Overeenkomst en deze Verwerkersovereenkomst te verrichten werkzaamheden mogen leiden. Indien dat onverhoopt toch het geval is, zullen Partijen in overleg treden teneinde daarvoor zo snel mogelijk een oplossing te vinden.
- 11.5 De met de controle gemoeide kosten zijn voor rekening van de Politie tenzij uit de controle blijkt dat Opdrachtnemer is tekortgeschoten in de nakoming van zijn verplichting(en) uit deze Verwerkersovereenkomst en/of de Overeenkomst.
- 11.6 Opdrachtnemer voert de door de Politie aangegeven aanbevelingen ter verbetering uit binnen de daartoe door de Politie te bepalen termijn.

12. Informeren van betrokkenen

- 12.1 Opdrachtnemer zal haar volledige medewerking verlenen opdat de Politie kan voldoen aan zijn wettelijke verplichtingen in het geval dat een Betrokkene zijn rechten uitoefent op grond van de AVG, Wpg of andere toepasselijke regelgeving betreffende de verwerking van Persoonsgegevens en/of Politiegegevens.
- 12.2 Indien een Betrokkene met betrekking tot de uitvoering van zijn rechten onder de

AVG en/of Wpg direct contact opneemt met Opdrachtnemer, dan gaat Opdrachtnemer hierbehoudens uitdrukkelijke andersluidende instructie van de Politie - in eerste instantie niet (inhoudelijk) op in, maar bericht hij dit onverwijld aan de Politie met een verzoek om nadere instructies.

- 12.3 Als Opdrachtnemer zijn diensten in het kader van de Overeenkomst rechtstreeks aanbiedt aan Betrokkene, dan is Opdrachtnemer verplicht om op een makkelijk toegankelijke en permanent beschikbare manier de Politie te informeren over het volgende:
- a. de naam en het adres van de Opdrachtnemer;
 - b. de doeleinden waarvoor Opdrachtnemer de Persoonsgegevens en/of Politiegegevens verwerkt;
 - c. de categorieën Persoonsgegevens en/of Politiegegevens die de Opdrachtnemer verwerkt;
 - d. de derden aan wie de Persoonsgegevens en/of Politiegegevens toegankelijk worden gemaakt;
 - e. de landen waarnaar de Persoonsgegevens en/of Politiegegevens worden overgedragen;
 - f. het recht op inzage, correctie en verwijdering van de Persoonsgegevens en/of Politiegegevens.

De Opdrachtnemer zal de Politie laten weten waar deze informatie gepubliceerd is.

13. Aansprakelijkheid

Onverminderd het bepaalde in artikel 26 van de ARBIT-2018 en artikel 83 AVG, is Opdrachtnemer aansprakelijk voor een door de AP opgelegde bestuurlijke boete dan wel door Betrokkene(n) of de Politie geleden schade, voor zover die bestuurlijke boete respectievelijk die geleden schade het gevolg is van toerekenbaar tekortschieten in de nakoming van haar verplichtingen door Opdrachtnemer of zijn Hulpverlener(s).

14. Maatregelen toezichthouder

Indien de AP in het kader van haar taak als handhaver een maatregel of boete oplegt aan de Politie en indien de oorzaak voor het opleggen van de maatregel of boete te wijten is aan het niet nakomen van de in de Verwerkersovereenkomst gemaakte afspraken door Opdrachtnemer of diens Hulpverlener, dan kan de Politie alle kosten voor deze maatregel of boete verhalen op de Opdrachtnemer. Tevens heeft de Politie het recht om de Overeenkomst in bovengenoemde situatie met onmiddellijke ingang te ontbinden zonder dat de Opdrachtnemer aanspraak kan maken op enige vorm van schadevergoeding.

15. Wijziging

- 15.1 Indien een functionele wijziging in de te verwerken Persoonsgegevens en/of Politiegegevens of een controle als bedoeld in artikel 11 van deze Verwerkersovereenkomst daartoe aanleiding geeft treden Partijen op eerste verzoek van de Politie in overleg over het aanpassen van de gemaakte afspraken binnen deze Verwerkersovereenkomst.
- 15.2 De nieuw te maken afspraken dienen voorafgaand aan de toepassing daarvan schriftelijk te zijn vastgelegd en deel uit te maken van deze Verwerkersovereenkomst.
- 15.3 De wijzigingen kunnen nooit tot gevolg hebben dat de Politie niet kan voldoen aan de AVG, Wpg en overige relevante wet- en regelgeving met betrekking tot Persoonsgegevens en/of Politiegegevens.

16. Slotbepalingen

- 16.1 Afwijkingen van deze Verwerkersovereenkomst zijn slechts bindend voor zover zij uitdrukkelijk tussen Partijen schriftelijk zijn overeengekomen.
- 16.2 Algemene leveringsvoorwaarden dan wel andere algemene of bijzondere voorwaarden van Opdrachtnemer en diens Hulpverancier zijn niet van toepassing op deze Verwerkersovereenkomst en worden door de Politie uitdrukkelijk van de hand gewezen.
- 16.3 Deze Verwerkersovereenkomst vormt een aanvulling op de Overeenkomst. Bij strijdigheid tussen bepalingen uit deze Verwerkersovereenkomst en de Overeenkomst prevaleren de bepalingen uit deze Verwerkersovereenkomst.
- 16.4 Op deze Verwerkersovereenkomst is het Nederlands recht van toepassing.

Aldus op de laatste van de twee hierna genoemde data overeengekomen in 16 artikelen en twee bijlagen en in tweevoud ondertekend,

5.1.2.e



G. M. den Ouden A
Directeur Politiedienstencentrum

de Opdrachtnemer

5.1.2.f

5.1.2.e



Bijlage 1 Werkprocessen, autorisaties en functiegroepen verwerking

De verwerking door Opdrachtnemer ziet toe op de volgende gegevens:

Categorieën Betrokkenen

5.1.2.1

De te verwerken (categorieën) Persoonsgegevens en/of Politiegegevens

Alle gegevens waarmee ^{5.1.2.1} in het kader van de uitvoering van de opdracht in aanraking komt.

Doel van de verwerking

5.1.2.1

Functierollen en/of functiegroepen van Personeel van Opdrachtnemer en hun verwerkingen;

Servicedesk medewerkers
Lead Engineers
Developers
Business Consultants

Bewaartermijnen

Voor de duur van de Verwerkersovereenkomst.

Contactgegevens Opdrachtnemer

5.1.2.1

Contactgegevens Hulpverleners mits goedgekeurd door de Politie

5.1.2.1

Technische en organisatorische beveiligingsmaatregelen

1. Opdrachtnemer en diens Hulpverlener in het bezit te zijn* van:

**aankruisen wat van toepassing is*

V een geschreven beveiligingsbeleid conform ISO 27001 inzake Information Security Management

V een geschreven kwaliteitsbeleid conform ISO 9001 inzake Quality Management

5.1.2.1

5.1.2.3



Bijlage 2 Procedure en Maatregelen in verband met de meldplicht datalekken

Informatie die moet worden verstrekt bij een Datalek

Als Opdrachtnemer de Coördinator Informatiebeveiliging van de Politie moet informeren op grond van artikel 5 van de Verwerkersovereenkomst, zal zij de volgende gegevens moeten verschaffen:

Contactgegevens melder

<Naam, functie, emailadres, telefoonnummer>

Gegevens over het Datalek

- Samenvatting van het incident waarbij de inbreuk op de beveiliging van Persoonsgegevens en/of Politiegegevens zich heeft voorgedaan:

<samenvatting>

- Van hoeveel personen zijn Persoonsgegevens en/of Politiegegevens betrokken bij de inbreuk?

<Vul de aantallen in>

- Minimaal: <vul aan>
- Maximaal: <vul aan>

- Omschrijving van de groep mensen van wie Persoonsgegevens en/of Politiegegevens zijn betrokken bij het incident

<omschrijving>

- Wanneer vond de inbreuk plaats?

<Kies een van de volgende opties en vul waar nodig aan>

- Op <datum>
- Tussen <begindatum periode> en <einddatum periode>
- Nog niet bekend

- Wat is de aard van de inbreuk ?

<meerdere mogelijkheden aankruisen>

- ☐ a) Lezen (vertrouwelijkheid)
- ☐ b) Kopiëren
- ☐ c) Veranderen (integriteit)
- ☐ d) Verwijderen of vernietigen (beschikbaarheid)
- ☐ e) Diefstal
- ☐ f) Nog niet bekend

- Om welk type Persoonsgegevens en/of Politiegegevens gaat het?

< meerdere mogelijkheden aankruisen>

- ☐ a) Naam -, adres - en woonplaatsgegevens
- ☐ b) Telefoonnummers
- ☐ c) E - mailadressen of andere adressen voor elektronische communicatie
- ☐ d) Toegangs - of identificatiegegevens (bijvoorbeeld inlognaam/wachtwoord of klantnummer)
- ☐ e) Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)
- ☐ f) Burgerservicenummer (BSN) of sofinummer
- ☐ g) Paspoortkopieën of kopieën van andere legitimatiebewijzen

- ☐ h) Geslacht, geboortedatum en/of leeftijd
- ☐ i) Bijzondere Persoonsgegevens (bijvoorbeeld ras, etniciteit, criminele gegevens, politieke overtuiging, vakbondslidmaatschap, religie, seksuele leven, medische gegevens): <geef aan welke bijzondere persoonsgegevens>
- ☐ j) Overige gegevens, namelijk <vul aan>

- Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen?

<meerdere mogelijkheden aankruisen>

- ☐ a) Stigmatisering of uitsluiting
- ☐ b) Schade aan de gezondheid
- ☐ c) Blootstelling aan (identiteits)fraude
- ☐ d) Blootstelling aan spam of phishing
- ☐ e) Anders, namelijk <vul aan>

Vervolgacties naar aanleiding van het Datalek

- De volgende technische en organisatorische maatregelen zijn getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen:

<beschrijving>

Technische beschermingsmaatregelen

- Zijn de Persoonsgegevens en/of Politiegegevens versleuteld, gehasht of op een andere manier

onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

<Kies een van de volgende opties en vul waar nodig aan>

- ☐ a) Ja
- ☐ b) Nee
- ☐ c) Deels, namelijk: <vul aan>

- Als de Persoonsgegevens en/of Politiegegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd?

<Beantwoord deze vraag als u bij de vorige vraag gekozen heeft voor optie a of optie c. Als u gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen toe.>

Internationale aspecten

- Heeft de inbreuk betrekking op personen in andere EU-landen?

< Kies een van de volgende opties>

- ☐ a) Ja
- ☐ b) Nee
- ☐ c) Nog niet bekend





Justitiële Informatiedienst
Ministerie van Justitie en Veiligheid

DEP. VERTROUWELIJK

**Dienstenniveau- en
verwerkersovereenkomst Politie,
Afdeling Vreemdelingen, Identificatie
en Mensenhandel en Justitiële
Informatiedienst**

Betreft: Centraal Digitaal Depot

Datum	24 maart 2020
Status	Definitief

Colofon

Afzendgegevens	Justitiële Informatiedienst Burg. Ravenslootsingel 2 7607 GK Almelo Postbus 337 7600 AH Almelo www.justid.nl
Contactpersoon	5.1.2.e / 5.1.2.e <i>Service delivery managers</i>
	T 088 5.1.2.i
	5.1.2.e
Ons kenmerk	Contract: 5.1.2.i
Politie dienst ICT	Contract: 5.1.2.i E nummer: 5.1.2.i
Auteurs	Deliverymanagement Privacy Officer

Inhoud

Colofon 3
Versiegeschiedenis 7

1 Algemeen 9

- 1.1 Partijen 9
- 1.2 Looptijd 9
- 1.3 Wijzigen van het document 10
- 1.4 Gerelateerde documenten 10
- 1.5 Beëindiging 10

2 Dienstverlening CDD+ 11

- 2.1 Algemene beschrijving van de dienstverlening 11
- 2.2 Niveau van dienstverlening 11
 - 2.2.1 Change en release management 11
 - 2.2.2 Continuity management 11
- 2.3 Communicatie 12
 - 2.3.1 Rapportages 12
 - 2.3.2 Overlegvormen 12

3 Verwerkersafspraken 15

- 3.1 Definities 15
- 3.2 Voorwerp van deze Verwerkersafspraken 15
- 3.3 Omvang verwerkingsbevoegdheid Verwerker 15
- 3.4 Geheimhouding door Personeel van Verwerker 16
- 3.5 Locatie van de verwerkingen 16
- 3.6 Subverwerkers 16
- 3.7 Rechten van betrokkene 16
- 3.8 Beveiliging van de Verwerking 16
- 3.9 Inbreuk in verband met Persoonsgegevens (datalek) 16
- 3.10 Bewaartermijn 17
- 3.11 Terugbezorgen of wissen Persoonsgegevens 17
- 3.12 Informatieverplichting en audit 17
- 3.13 Geschil 17

- Tekenblad 19
- Bijlage 1 De verwerking van persoonsgegevens 21
- Bijlage 2 Passende technische en organisatorische maatregelen 23
- Bijlage 3 Meldingsformulier Datalekken (artikel 8) 25

Versiegeschiedenis

Versie	Datum	Auteur	Omschrijving
0.1	25 september 2018	5.1.2.e	Initieel concept
0.2	28 september 2018	5.1.2.e	Tekstuele wijzigingen na interne afstemming
0.3	5 december 2018	5.1.2.e	Review AVIM verwerkt
0.4	22 maart 2019	5.1.2.e	Review AVIM/Justid
0.5	01 juli 2019	5.1.2.e	Review Privacy/Justid
0.9	11 juli 2019	5.1.2.e	Finale check EDDA
0.99	11 februari 2020	5.1.2.e	Wijzigingen PO verwerkt Voor akkoord AVIM
0.991	19 maart 2020	5.1.2.e	Finaal concept voor akkoord P. Steneker
1.0	24 maart 2020	5.1.2.e	Definitief na akkoord AVIM en G. van Zuthem manager EDDA

1 Algemeen

Het doel van dit document is tweeledig. Enerzijds beschrijft het de dienstverlening van de Justitiële Informatiedienst aan de afnemer in het kader van het beheer van een dienst en anderzijds zijn er bepalingen opgenomen ter voldoening aan wet- en regelgeving op het gebied van privacy en fungeert het als verwerkersafspraken.

Dienstverlening

Het doel van de dienstverlening is de uitwisseling van digitaal ondertekende formulieren en dossiers met de partners in de vreemdelingenketen mogelijk maken door middel van het uitwisselmechanisme in het Centraal Digitaal Depot. Hiermee wordt uitvoering gegeven aan de wens om gegevens te delen met en op te halen bij:

- Directoraat-Generaal Migratie
- Immigratie- en Naturalisatiedienst
- Dienst Justitiële Inrichtingen
- Dienst Terugkeer en Vertrek
- Koninklijke Marechaussee
- Centraal Orgaan opvang asielzoekers

Deze dienstenniveau overeenkomst (DNO) is bedoeld om de dienstverlening en de daarbij behorende dienstenniveaus vast te leggen tussen afnemer en dienstverlener. Het gaat om afspraken aanvullend op het basisniveau dienstverlening (BND). De hoofdstukken 1 en 2 zien op de dienstverlening.

Afspraken op het gebied van Privacy

De privacy wetgeving gebiedt om afspraken te maken op het gebied van privacy tussen verwerkingsverantwoordelijke en verwerker. Tussen (rijks)overheidspartijen kan echter geen overeenkomst gesloten worden. Niettemin is het van belang de wederzijdse verantwoordelijkheden en afspraken op dat gebied vast te leggen. In deze gebeurt dat door een verwerkersafspraken op te nemen in hoofdstuk 3 van dit document.

1.1 Partijen

Politie, Afdeling Vreemdelingen, Identificatie en Mensenhandel (AVIM), hierna te noemen **afnemer** en **verwerkingsverantwoordelijke**,
en

Justitiële Informatiedienst (Justid)
hierna te noemen **dienstverlener** en **verwerker**,

hierna gezamenlijk te noemen: **Partijen**.

1.2 Looptijd

Deze overeenkomst treedt in werking op 1 januari 2019 en heeft een looptijd van 1 jaar. Na deze looptijd wordt de overeenkomst stilzwijgend verlengd voor de periode van telkens één jaar.

1.3 Wijzigen van het document

Het beheer van deze overeenkomst is belegd bij deliverymanagement van dienstverlener.

Bij partijen kan de wens ontstaan om deze overeenkomst te wijzigen. De wens tot een wijziging wordt door afnemer bij deliverymanagement van dienstverlener 5.1.2.I@justid.nl) neergelegd. In een gezamenlijk overleg wordt de wijziging bepaald.

- Overeengekomen wijzigingen worden vastgelegd in een wijzigingsblad;
- Dit wijzigingsblad wordt door beide partijen formeel ondertekend en als addendum toegevoegd;
- De in het addendum opgenomen afspraken worden in de eerstvolgende geactualiseerde versie van de overeenkomst opgenomen;
- De bijlagen in dit document kunnen na en in onderling overleg tussentijds worden geactualiseerd. Het tast de rechtmatigheid van de afspraken in dit document niet aan.

1.4 Gerelateerde documenten

De volgende documenten maken deel uit van deze DNO:

- Basisniveau dienstverlening Justid (BND), beschrijft de standaard dienstverlening die van toepassing is op de geleverde dienst;
- Dossier financiële afspraken (DFA), beschrijft de jaarlijkse vaste kosten, afspraken over indexatie van de vaste kosten en eventuele variabele kosten en waarop deze zijn gebaseerd;
- Dossier afspraken en procedures (DAP), beschrijft de verschillende operationele aspecten van de dienstverlening.

In de producten en dienstencatalogus Justid (PDC) staan alle ketenvoorzieningen met de daaraan gerelateerde diensten gedetailleerd beschreven.

1.5 Beëindiging

Het verzoek van een van de partijen om de overeenkomst te beëindigen vindt schriftelijk plaats met opgave van de reden. De opzegtermijn van deze DNO bedraagt voor beide partijen 6 kalendermaanden voorafgaand aan de einde looptijd. Partijen treden met elkaar in overleg over de wijze van beëindiging.

Beëindiging van de dienstverlening brengt mogelijk kosten met zich mee. Voor deze kosten wordt dan een separate offerte opgesteld

2 Dienstverlening CDD+

2.1 Algemene beschrijving van de dienstverlening

In lijn met de doelarchitectuur Digitaal Werken in de Vreemdelingenketen wil de politie gebruik maken van een Document Management Systeem voor de uitwisseling van ongestructureerde informatie. Met de inzet van het Centraal Digitaal Depot (CDD+) heeft dienstverlener voor afnemer de mogelijkheid gecreëerd om digitaal ondertekende formulieren en dossiers uit te wisselen met de partners in de vreemdelingenketen.

CDD+ is de gemeenschappelijke voorziening voor de opslag en uitwisseling van digitale objecten die voldoet aan de geldende wet- en regelgeving. Afnemer is eigenaar van de data in zijn archief in CDD+, beheert zelf zijn archief in CDD+ en bepaalt ook zelf wie welke informatie mag inzien.

2.2 Niveau van dienstverlening

Op de dienstverlening is het BND van toepassing. Paragraaf 2.2 en 2.3 beschrijven de specifieke afspraken die afwijken van het BND. Operationele consequenties zijn opgenomen in de DAP.

2.2.1 *Change en release management* *Aanvulling op paragraaf 3.6 BND*

Dienstverlener werkt volgens de scrummethodiek en levert in principe 3-wekelijkse sprint wijzigingen op, op productie.
Buiten het scrumproces kunnen (security)patches naar productie worden gebracht.

2.2.2 *Continuity management* *Vervanging van paragraaf 3.7 BND*

Continuity management is het proces dat zorgt voor afdoende technische, financiële en organisatorische voorzieningen ten behoeve van het waarborgen van de continuïteit van de dienstverlening.

Onderwerp	Toelichting	Norm
Back-up venster	De periode dat de back-up gemaakt wordt	Dagelijks tussen 24:00 en 04:00
Back-up	Het veiligstellen van software en data (full back-up) op de productieomgeving	Maximaal 1 werkdag verlies van gegevens

Bewaar termijn	Periode dat de veiliggestelde gegevens worden bewaard	Periode standaard: • Dagtapes: 1 week • Weektape: 4 weken • Maandtape: 1 jaar
Restore bestanden	Aangevraagd en geaccordeerd verzoek om restore	90% van de restores is afgerond binnen maximaal 48 ¹ uur na ontvangst verzoek afnemer
Uitwijk	De mogelijkheid om, na een calamiteit, dienstverlening te hervatten op een andere wijze of andere locatie	Het datacentrum is dubbel uitgevoerd. Dit betekent dat de onderliggende infrastructuur van CDD ⁺ redundant uitgevoerd is.

2.3 Communicatie

2.3.1 Rapportages

Vervanging van paragraaf 6.1 BND

Dienstverlener rapporteert afnemer over onderstaande zaken:

Element van dienstverlening	Rapportage	Frequentie
Beschikbaarheid	Overzicht geplande en niet geplande uitval t.o.v. de norm	Per kalenderkwartaal
Incidentmanagement	Overzicht van (afgehandelde) incidenten t.o.v. de norm	Per kalenderkwartaal
Change- en releasemanagement	Overzicht van (afgehandelde) wijzigingen en (afgehandelde) releases t.o.v. de norm	Per kalenderkwartaal
Autorisatiebeheer en logische toegangsbeveiliging	Account informatie	Per kalenderkwartaal
Productiegegevens	Informatie over het gebruik van CDD ⁺ door afnemer (denk aan aantallen documenten, dossiers, verbruikte opslagcapaciteit en aantal raadplegingen)	Per kalenderkwartaal

Overzicht periodieke rapportage

2.3.2 Overlegvormen

Aanvulling op paragraaf 6.2 BND

In deze paragraaf zijn achtereenvolgens het strategisch, tactisch en operationeel overleg beschreven. Van ieder overleg wordt verslag gemaakt door dienstverlener.

Tactisch

Functioneel beheer PSH-V en Dienstenmanager ICT van afnemer en de manager EDDA van dienstverlener overleggen 2 maal per jaar. Tijdens het overleg worden onder meer de verschillen besproken tussen het geleverde en het overeengekomen niveau van dienstverlening gedurende de afgelopen periode. Tijdens het overleg zullen zowel de functionele als technische aspecten van de dienstverlening aan de orde komen.

¹ De restore tijd is afhankelijk van de omvang van het archief.

Het overleg is bedoeld om de wederzijdse verwachtingen ten aanzien van de korte en middellange termijn op elkaar af te stemmen. Het overleg levert input om de daadwerkelijk geleverde dienstverlening goed bij de in de DNO vastgelegde dienstverlening aan te laten sluiten.

Operationeel

Op operationeel niveau vindt er naar wederzijdse behoefte overleg plaats. Uiteraard is sprake van reguliere, "dagelijkse" contacten ten behoeve van de reguliere taakuitvoering. Deze vinden voornamelijk plaats tussen Servicedesk en/of Functioneel Beheer PSH-V van de afnemer en de Frontoffice van de dienstverlener.

Gebruikersraad

De gebruikersraad draagt zorg voor een intensief contact tussen de gebruikersorganisaties en Justid, om archivering en uitwisseling van digitale documenten met behulp van CDD+ zo goed mogelijk aan te laten sluiten op de (keten)werkprocessen. Voor meer informatie wordt verwezen naar het Statuut gebruikersraad CDD.

De frequentie van de gebruikersraad CDD+ is 4 keer per jaar.

3 Verwerkersafspraken

Overwegende dat:

- Partijen onderdeel zijn van dezelfde rechtspersoon, zijnde de Staat der Nederlanden, en derhalve geen overeenkomst in de zin van art. 6:213 BW kunnen sluiten;
- Partijen evenwel hun afspraken over het Verwerken van de Persoonsgegevens door Verwerker wensen vast te leggen;
- Partijen in dit hoofdstuk, in plaats van in een afzonderlijke verwerkersafpraak, hun afspraken over de Verwerking van Persoonsgegevens wensen vast te leggen.
- Justid in deze optreedt als Verwerker voor Verwerkingsverantwoordelijke;
- Verwerker verantwoordelijk is voor het namens Verwerkingsverantwoordelijke voorzien in het duurzaam opslaan, beheren en ontsluiten van persoonsgegevens in documenten en dossiers ten behoeve van de vreemdelingenketen;
- De opgenomen Persoonsgegevens in voornoemde documenten vallen onder het regime van de Algemene Verordening Gegevensbescherming (AVG) in samenhang met het gestelde in het vreemdelingenrecht (o.a. Vreemdelingenwet 2000 en Vreemdelingenbesluit).

3.1 Definities

In deze Verwerkersafpraak wordt een aantal begrippen met een beginhoofdletter gebruikt. Met deze begrippen worden de definities uit artikel 4 van de AVG bedoeld, waarnaar gemakshalve wordt verwezen.

3.2 Voorwerp van deze Verwerkersafpraak

Deze Verwerkersafpraak regelt de Verwerking van Persoonsgegevens door Verwerker binnen deze afspraak.

De aard en het doel van de Verwerking, de categorie en een opsomming van de Persoonsgegevens en de ontvangers van de gegevens, zijn in Bijlage 1 opgenomen.

Verwerker draagt zorg voor de toepassing van passende technische en organisatorische (beveiligings)maatregelen, opdat de Verwerking aan de vereisten van de Verordening voldoet en de bescherming van de rechten van de Betrokkene is gewaarborgd.

3.3 Omvang verwerkingsbevoegdheid Verwerker

Verwerker verwerkt Persoonsgegevens ten behoeve van Verwerkingsverantwoordelijke, overeenkomstig diens instructies en onder diens verantwoordelijkheid, op de wijze zoals bepaald in deze afspraak. Verwerker heeft geen zeggenschap over het doel en de middelen voor de verwerking van gegevens. Zo worden geen beslissingen genomen over het gebruik van de gegevens, de verstrekking aan derden en de duur van de opslag van de gegevens.

Indien Verwerker op grond van een wettelijk voorschrift Persoonsgegevens dient te verstrekken aan een derde niet door Verwerkingsverantwoordelijke genoemde partij, informeert hij Verwerkingsverantwoordelijke onmiddellijk, en zo mogelijk voorafgaand aan de verstrekking.

Verwerker ondersteunt Verwerkingsverantwoordelijke op diens verzoek bij het voldoen aan de verplichtingen welke voortvloeien uit de geldende wet- en

regelgeving, zoals de bescherming van Persoonsgegevens, de rechten van Betrokkene, de uitvoering van Gegevensbeschermingseffectbeoordelingen en het opstellen van Verwerkersafspraken.

3.4 Geheimhouding door Personeel van Verwerker

Verwerker is gehouden tot geheimhouding van alle gegevens en informatie die zij op basis van deze DNO verwerkt. Na de beëindiging van deze DNO zal de geheimhoudingsplicht blijven bestaan.

3.5 Locatie van de verwerkingen

Verwerker verwerkt Persoonsgegevens uitsluitend binnen Nederland, tenzij Verwerker daarvoor uitdrukkelijk schriftelijk toestemming heeft verkregen van de Verwerkingsverantwoordelijke.

3.6 Subverwerkers

Verwerker maakt bij de uitvoering van zijn dienstverlening geen gebruik van de diensten van een subverwerker, anders dan na schriftelijke toestemming van de Verwerkingsverantwoordelijke.

3.7 Rechten van betrokkene

Verwerker onthoudt zich van communicatie in de richting van Betrokkenen. Verzoeken van Betrokkenen binnen de rechten van betrokkenen zoals genoemd in de wet zijn een verantwoordelijkheid voor Verwerkingsverantwoordelijke.

Verzoeken van betrokkenen gericht aan Verwerker zullen terstond worden doorgezonden aan Verwerkingsverantwoordelijke.

3.8 Beveiliging van de Verwerking

Verwerker treft de technische en organisatorische beveiligingsmaatregelen zoals beschreven in Bijlage 2.

Partijen erkennen dat het waarborgen van een passend beveiligingsniveau voortdurend kan dwingen tot het treffen van aanvullende beveiligingsmaatregelen. Verwerker waarborgt een op het risico afgestemd beveiligingsniveau.

Als Verwerkingsverantwoordelijke de wens uit dat aanvullende maatregelen met het oog op de beveiliging van de Persoonsgegevens, getroffen moeten worden, zal de noodzaak daarvan in overleg met de eigenaar besproken worden. Aan het nemen van de gewenste maatregelen kunnen extra kosten verbonden zijn.

Verwerker informeert Verwerkingsverantwoordelijke binnen 24 uur nadat hij kennis heeft genomen van inbreuken in verband met de beveiliging.

3.9 Inbreuk in verband met Persoonsgegevens (datalek)

Verwerker informeert Verwerkingsverantwoordelijke binnen 24 uur, zodra zij kennis heeft genomen van een Inbreuk die te maken heeft met Persoonsgegevens.

Hiervoor wordt het door de Autoriteit Persoonsgegevens beschikbaar gestelde template gebuikt, zoals opgenomen in Bijlage 3.

Verwerker informeert Verwerkingsverantwoordelijke ook over het onderzoek en de te nemen maatregelen betreffende deze Inbreuk die te maken heeft met Persoonsgegevens.

3.10 Bewaartermijn

Verwerker bewaart de gegevens overeenkomstig het gestelde door en in opdracht van Verwerkingsverantwoordelijke.

3.11 Terugbezorgen of wissen Persoonsgegevens

Voorafgaande aan beëindiging van de Overeenkomst (zie ook artikel 1.4 draagt Verwerker zorg voor het terugbezorgen van de gegevens aan Verwerkingsverantwoordelijke of het vernietigen daarvan. Verwerker stelt hiertoe een vernietigingsverklaring op.

3.12 Informatieverplichting en audit

Verwerker stelt alle informatie ter beschikking aan Verwerkingsverantwoordelijke die nodig is om de werking van de afspraken te toetsen, dit betreft ook auditdoeleinden.

3.13 Geschil

Een partij die meent dat een geschil bestaat, deelt dat mee aan de andere partij en treedt daarmee in overleg om tot een oplossing van het (vermeende) geschil te komen.

Indien het overleg tussen partijen op operationeel of tactisch niveau, niet tot overeenstemming leidt, wordt het geschil voorgelegd aan de directies c.q. lijnverantwoordelijken van beide partijen. Deze nemen, gehoord de standpunten, een besluit over het geschil.

Tekenblad

Hierbij verklaren, als vertegenwoordiger van hun organisatie en bevoegd om namens hun organisatie te tekenen, dat overeenstemming is over de in dit document vastgelegde afspraken:

Voor akkoord	
Politie Dienst ICT	Justitiële Informatiedienst
Dhr. J. Jansen. Diensthofd ICT	5.1.2.e 
Datum: 30 maart 2020	Datum: 25 maart 2020
Handtekening: 5.1.2.e 	Handtekening: 5.1.2.e 

Bijlage 1 De verwerking van persoonsgegevens

De in deze bijlage behorende gegevens worden uiterlijk 1 oktober door afnemer aangeleverd en hierin opgenomen.

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

Het onderwerp/aard en doel van de Verwerking	
Ontvangers	
Beschrijving categorieën Persoonsgegevens	
Opsomming van de Persoonsgegevens	

Bijlage 2 Passende technische en organisatorische maatregelen

In onderstaand overzicht worden beknopt de beveiligingsmaatregelen gespecificeerd die tussen Partijen gelden.

5.1.2.i



Bijlage 3 Meldingsformulier Datalekken (artikel 8)

Rapportageformulier datalek

Dit formulier² bevat de gegevens die moeten worden opgegeven bij het rapporteren van een mogelijk datalek in de zin van de AVG dan wel Wpg of Wjsg aan de verwerkingsverantwoordelijke en eigenaar van Justid (pSG). Naast dit formulier zal de verwerkingsverantwoordelijke ook nog een advies krijgen inzake het meldingswaardig zijn van het datalek.

0. Over deze melding	
1. Is dit een vervolg op een eerdere melding? Kies één van de volgende opties. ☐ Ja ☐ Nee	
2. Wat is het nummer van de oorspronkelijke melding? Beantwoord deze vraag als u vraag 1 met ja hebt beantwoord. Antwoord:	
3. Wat is de strekking van de vervolgmelding? Beantwoord deze vraag als u vraag 1 met ja hebt beantwoord. Kies één van de volgende opties. ☐ Toevoegen of wijzigen van informatie betreffende de eerdere melding ☐ Intrekking van de eerste melding	
4. Wat is de reden van intrekking? Beantwoord deze vraag als u bij vraag 3 gekozen heeft voor optie [Intrekking van de eerdere melding]. Antwoord:	
Op grond van welke wettelijke bepaling doet u deze melding?	AVG, Algemene Verordening Gegevensbescherming
1. Contactgegevens en overige algemene informatie	
1.1 Contactgegevens	
Over welke organisatie of welk bedrijf gaat het?	
Registratienummer bij de Kamer van Koophandel	
Naam van het bedrijf of de organisatie	
Adres	
Postcode	
Plaats	
In welke sector is de organisatie of het bedrijf actief?	Vreemdelingenwetgeving
Wie meldt het datalek	
Naam	

² Gebaseerd op het formulier van de Autoriteit Persoonsgegevens, juli 2018

Functie	
E-mailadres	
Telefoonnummer	
Tweede telefoonnummer	088-511.211
Met wie kan de Autoriteit Persoonsgegevens contact opnemen voor nadere informatie over de melding?	
De melder is contactpersoon	Kies een item.
Naam	
Functie	
E-mailadres	
Telefoonnummer	
Tweede telefoonnummer	088-511.211
1.2 Betrokkenheid andere organisatie	
Was er een andere organisatie betrokken bij de inbreuk?	Kies een item.
Naam van de andere organisatie die betrokken was bij de inbreuk.	
In welke hoedanigheid was de andere organisatie betrokken bij de inbreuk?	
Antwoord:	
2. Tijdslijn	
Exacte datum waarop de inbreuk was, indien bekend	Klik hier als u een datum wilt invoeren.
Startdatum van de periode waarbinnen de inbreuk was	Klik hier als u een datum wilt invoeren.
Einddatum van de periode waarbinnen de inbreuk was	Klik hier als u een datum wilt invoeren.
Duurt de inbreuk op dit moment nog voort?	☐ Ja ☐ Nee
Wanneer werd de inbreuk ontdekt?	Klik hier als u een datum wilt invoeren.
Als u de inbreuk later meldt dan 72 uur na de ontdekking, wat is daarvan de reden?	
Antwoord:	Intern onderzoek om vast te stellen of het hier een datalek betreft.
3. Gegevens over het datalek	
3.1 Aard van de inbreuk	
Inbreuk op de vertrouwelijkheid van de gegevens	☐ Ja ☐ Nee
Inbreuk op de integriteit van de gegevens	☐ Ja ☐ Nee
Inbreuk op de beschikbaarheid van de gegevens	☐ Ja ☐ Nee
3.1 Aard van het incident	
Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van de persoonsgegevens is geweest?	Kies een item.

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest:	
Samenvatting:	
4. Persoonsgegevens die betrokken zijn bij het datalek	
4.1 Persoonsgegevens in het algemeen	
Naam	☐ Ja ☐ Nee
Geslacht, geboortedatum en/of leeftijd	☐ Ja ☐ Nee
Burgerservicenummer (BSN)	☐ Ja ☐ Nee
Contactgegevens	☐ Ja ☐ Nee
Toegangs- of identificatiegegevens	☐ Ja ☐ Nee
Financiële gegevens	☐ Ja ☐ Nee
(Kopieën van) paspoorten of andere legitimatiebewijzen	☐ Ja ☐ Nee
Locatiegegevens	☐ Ja ☐ Nee
Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen	☐ Ja ☐ Nee
Onbekend / anders namelijk:	
4.2 Bijzondere categorieën van persoonsgegevens	
Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt	☐ Ja ☐ Nee
Persoonsgegevens waaruit iemands politieke opvattingen blijken	☐ Ja ☐ Nee
Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken	☐ Ja ☐ Nee
Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt	☐ Ja ☐ Nee
Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid	☐ Ja ☐ Nee
Gegevens over iemands gezondheid	☐ Ja ☐ Nee
Genetische gegevens	☐ Ja ☐ Nee
Biometrische gegevens	☐ Ja ☐ Nee
4.3 Hoeveelheid persoonsgegevens	

Geef (eventueel bij benadering) aan hoeveel gegevensrecords ("gegevensregisters") zijn getroffen door de inbreuk		
5. De groep mensen van wie persoonsgegevens betrekken zijn bij het datalek		
Werknemers	☐ Ja ☐ Nee	
Klanten (huidig en potentieel)	☐ Ja ☐ Nee	
Leerlingen of studenten	☐ Ja ☐ Nee	
Patiënten	☐ Ja ☐ Nee	
Minderjarigen	☐ Ja ☐ Nee	
Personen uit kwetsbare groepen	☐ Ja ☐ Nee	
Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk:		
Omschrijving:		
Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk		
Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk		
6. Maatregelen die zijn getroffen voordat het datalek plaatsvond		
Waren de persoonsgegevens op het moment dat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk voor onbevoegden?	☐ Deels, namelijk ☐ Ja ☐ Nee	
Als de persoonsgegevens deels onbegrijpelijk of ontoegankelijk waren, om wel deel gaat het dan?		
Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk waren gemaakt, op welke manier is dit dan gebeurd?		
Antwoord:		
7. Gevolgen van het datalek		
7.1 Gevolgen van de inbreuk op de vertrouwelijkheid, de integriteit en/of de beschikbaarheid van de gegevens		
Onbevoegden hebben kennis kunnen nemen van de gegevens	☐ Ja ☐ Nee	
De gegevens kunnen op een onbehoorlijke of onrechtmatig manier worden misbruikt	☐ Ja ☐ Nee	
Er worden binnen uw eigen organisatie mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt	☐ Ja ☐ Nee	
Er worden mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens hergebruikt voor andere doeleinden of doorgegeven aan andere organisaties	☐ Ja ☐ Nee	

Een essentiële dienst kan tijdelijk niet meer worden verleend aan de betrokkenen	☐ Ja ☐ Nee
Een essentiële dienst kan permanent niet meer worden verleend aan de betrokkenen	☐ Ja ☐ Nee
Anders, namelijk:	
7.2 Lichamelijke, materiële en immateriële schade voor de betrokkenen	
Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkene?	
Discriminatie	☐ Ja ☐ Nee
Identiteitsdiefstal of –fraude	☐ Ja ☐ Nee
Financiële verliezen	☐ Ja ☐ Nee
Reputatieschade	☐ Ja ☐ Nee
Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens	☐ Ja ☐ Nee
Ongoorloofde ongedaanmaking van pseudonimisering	☐ Ja ☐ Nee
Betrokkene kunnen hun rechten en vrijheden niet uitoefenen	☐ Ja ☐ Nee
Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen	☐ Ja ☐ Nee
Andere gevolgen namelijk:	
Antwoord:	
Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkenen.	Kies een item.
8. Vervolgacties naar aanleiding van het datalek	
8.1 Informeren van de betrokkenen	
Heeft u het datalek gemeld aan de betrokkene of bent u van plan dat te gaan doen?	Kies een item.
Wanneer heeft u het datalek gemeld aan de betrokkene?	Klik hier als u een datum wilt invoeren.
Wanneer gaat u het datalek melden aan de betrokkene?	Klik hier als u een datum wilt invoeren.
Wat is de inhoud van de melding aan de betrokkene?	
Inhoud:	
Hoeveel betrokkenen heeft u geïnformeerd of gaat u informeren?	
Welk communicatiemiddel of welke communicatiemiddelen gaat u	