

12. Informeren van betrokkenen

- 12.1 Leverancier 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 Leverancier, dan gaat Leverancier 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 Leverancier zijn diensten in het kader van de Overeenkomst rechtstreeks aanbiedt aan Betrokkene, dan is Leverancier 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 Leverancier;
 - b. de doeleinden waarvoor Leverancier de persoonsgegevens en/of Politiegegevens verwerkt;
 - c. de categorieën persoonsgegevens en/of Politiegegevens die de Leverancier 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 Leverancier 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 Leverancier 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 Leverancier of zijn Hulpleverancier(s). De aansprakelijkheid van Partijen is in ieder geval beperkt tot het bedrag dat in het desbetreffende geval uit hoofde van de door betreffende partij afgesloten aansprakelijkheidsverzekering wordt uitbetaald. Indien en voor zover de aansprakelijkheidsverzekering voor schade als gevolg van de aansprakelijkheid geen aanspraak op een uitkering geeft, is iedere aansprakelijkheid beperkt tot twee maal de opdrachtwaarde van de Overeenkomst inclusief btw gedurende 12 maanden. (Polis van verzekering wordt op verzoek ter beschikking gesteld. Orca heeft een aansprakelijkheidsverzekering voor € 1.000.000 per schadegeval en € 2.000.000 per jaar)

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 Leverancier of diens Hulpleverancier, dan kan de Politie alle kosten voor deze maatregel of boete verhalen op de Verwerker met een maximum conform het gestelde bij Art. 13. gedurende 12

maanden per boete c.q. voor de kosten per maatregel. Tevens heeft de Politie het recht om de Overeenkomst in bovengenoemde situatie met onmiddellijke ingang te ontbinden zonder dat de Leverancier 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 Leverancier en diens Hulpleverancier 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,

de *Opdrachtgever*
De Politie,

5.1.2.e



de *Leverancier*

5.1.2.e



Bijlage 1 Werkprocessen, autorisaties en functiegroepen verwerking

De verwerking door Leverancier ziet toe op de volgende gegevens:

Categorieën Betrokkenen

Medewerkers Politie

De te verwerken (categorieën) persoonsgegevens en/of Politiegegevens

persoonsgegevens, inclusief door Leverancier verzamelde of verkregen (inclusief telemetriegegevens), gegevens van lokaal geïnstalleerde programmatuur.

Doel van de verwerking

Persoonsgegevens slechts voor zover proportioneel voor de volgende limitatieve doeleinden:

- a) Het leveren van de Prestatie
- b) Beveiliging van de Prestatie
- c) Het actueel houden van de Prestatie

Leverancier zal in ieder geval persoonsgegevens niet verwerken voor de volgende doeleinden:

- a) Data analyse
- b) Profilering inclusief, maar niet beperkt tot het creëren van psychometrische, psychografische of andere gebruikersprofielen.
- c) Adverteren (inclusief gerichte aanbevelingen op het scherm voor producten of diensten, aangeboden door Leverancier, maar niet ingeschreven of gebruikt door Opdrachtgever) of een vergelijkbaar commercieel doel, of
- d) Marktonderzoek gericht op het creëren van nieuwe functionaliteiten, diensten of producten of elk ander doel tenzij dit is toegestaan op basis van schriftelijke instructies van de Opdrachtgever.

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

5.1.2.1 [Redacted text block]

Bewaartermijnen

Voor de duur van de Verwerkersovereenkomst

Contactgegevens Leverancier

5.1.2.1 [Redacted text block]

Contactgegevens Hulpverleners mits goedgekeurd door de Politie

5.1.2.1 [Redacted text block]

Technische en organisatorische beveiligingsmaatregelen

Bijlage 2 Procedure en Maatregelen in verband met de meldplicht datalekken

Informatie die moet worden verstrekt bij een Datalek

Als Leverancier 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>

a) Minimaal: <vul aan>

b) 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>

a) Op <datum>

b) Tussen <begindatum periode> en <einddatum periode>

c) 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, vakbondsledenmaatschap, 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



Landelijk Crisismanagement Systeem

Instituut Fysieke Veiligheid (IFV) en Politie

**Samenwerkings
overeenkomst**

Nummer:

5.1.2.1

Ingangsdatum:

01-12-2021

Uitgegeven door: Politie, Politiedienstencentrum - Dienst Verwerving

Informatie: Inkoopmanagement

Status: Definitief

Versie: 1.1

Versie datum: 8 november 2021

© Politie, alle rechten voorbehouden.

Niets uit deze uitgave mag worden verveelvoudigd, op geautomatiseerde wijze opgeslagen of openbaar gemaakt in enige vorm of op enigerlei wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de Politie.

Inhoudsopgave

1.	Structuur overeenkomst	7
2.	Duur van de overeenkomst en beëindiging	7
3.	De samenwerking	8
4.	Voorwerp van de overeenkomst	9
5.	SaaS-dienst en service levels	9
6.	Functioneel beheer	10
7.	Vergoeding	11
8.	Verwerking persoonsgegevens en politiegegevens	11
9.	Afwijkende bepalingen ten opzichte van de “voorwaarden”	12
10.	Diversen	12
	Bijlage A: Omschrijving diensten en technische beschrijving LCMS-Politie	15
	Bijlage B: Algemene Rijksvoorwaarden bij IT-overeenkomsten 2018	18
	Bijlage C: Service Levels en Bereikbaarheid	19
	Bijlage D: Financiële afspraken en aanvullende diensten	22
	Bijlage E: Beleidskader toegangsbeveiliging LCMS	24

Samenwerkingsovereenkomst "Landelijk Crisismanagement Systeem"

Contractnummer: 5.1.2.1

Met ingangsdatum 1 december 2021

De ondergetekenden:

1. Politie, gevestigd te 's-Gravenhage, te dezen vertegenwoordigd door de korpschef de heer H.P. van Essen, namens deze, de directeur PDC, mevrouw P.F. Bosman, hierna te noemen: de Politie,

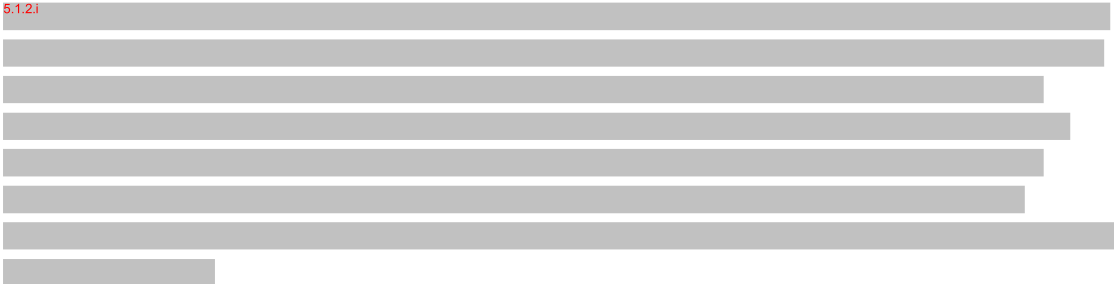
en

2. Het zelfstandig bestuursorgaan Instituut Fysieke Veiligheid, gevestigd te Arnhem (6816 RW), aan de Kemperbergerweg 783, te dezen rechtsgeldig vertegenwoordigd door 5.1.2.e, hierna te noemen: IFV,

Hierna gezamenlijk Partijen genoemd of afzonderlijk van elkaar Partij.

Partijen overwegen als volgt:

- a. IFV en de Politie willen met elkaar samenwerken door onder andere het ontwikkelen en ter beschikking stellen van expertise op het gebied van brandweezorg, rampenbestrijding, crisisbeheersing en geneeskundige hulpverlening. Onderdeel hiervan is het verwerven, beheren en ter beschikking stellen van een Landelijk Crisismanagement systeem.
- b. Partijen wensen in dit document nadere afspraken over te maken in deze Samenwerkingsovereenkomst.
- c. Het IFV is de landelijke ondersteuningsorganisatie voor de vijftientig veiligheidsregio's in Nederland, ingesteld bij de Wet veiligheidsregio's.
- d. De veiligheidsregio's zijn openbare lichamen die belast zijn met diverse taken van algemeen belang, waaronder (i) het voorbereiden op de bestrijding van branden en het organiseren van rampenbestrijding en crisisbeheersing en (ii) het inrichten en in stand houden van de informatievoorziening binnen de diensten van de veiligheidsregio, alsmede tussen deze diensten en de andere diensten en organisaties die betrokken (kunnen) zijn bij rampenbestrijding en crisisbeheersing.
- e. Op grond van de Wet veiligheidsregio's heeft het IFV een aantal wettelijke taken op het gebied van brandweezorg, rampenbestrijding, crisisbeheersing en geneeskundige hulpverlening. Het IFV ondersteunt de veiligheidsregio's door onder andere (i) het ontwikkelen en ter beschikking stellen van expertise op voornoemde gebieden en (ii) het verwerven, beheren en aan de veiligheidsregio's ter beschikking stellen van materieel, uitrusting en telecommunicatievoorzieningen.
- f. De Koninklijke marechaussee en de Politie voeren politietaken uit zoals omschreven in de Politiewet 2012 en waken hiermee over de veiligheid van Nederland en het Caribisch gedeelte van het koninkrijk der Nederlanden. De Koninklijke marechaussee en de Politie zijn verantwoordelijk voor de politieprocessen tijdens een crisis als bedoeld in het Referentiekader Regionaal Crisisplan 2016. Zij hebben deze verantwoordelijkheid op basis van een bepaald grondgebied, in samenwerkingsverbanden of bij wederzijdse bijstandverlening.
- g. Het "Referentiekader Netcentrische Crisisbeheersing", zoals vastgesteld door het Veiligheidsberaad, is de basis voor netcentrisch werken in Nederland. De regie op de doorontwikkeling en het uniforme gebruik van de netcentrische werkwijze is belegd bij het Programma Netcentrisch Werken van het Veiligheidsberaad. De netcentrische werkwijze is geïmplementeerd bij alle veiligheidsregio's.

- h. Eén van de door het IFV geleverde telecommunicatievoorzieningen is het Landelijk Crisismanagement Systeem ("LCMS"). Het LCMS is een IT-systeem dat de netcentrische werkwijze ondersteunt. Het LCMS wordt gebruikt door alle veiligheidsregio's en het Nationaal CrisisCentrum (NCC), het Landelijk Operationeel Coördinatie Centrum (LOCC), diverse waterschappen en diverse acute zorgnetwerken.
- i. Teneinde haar interne coördinatie- en crisisbeheersingsprocessen te optimaliseren en gelet op de noodzaak om in het geval van een crisis of een ramp, op eenduidige en geautomatiseerde wijze informatie te kunnen uitwisselen tussen de Politie en haar crisispartners zoals de veiligheidsregio's, heeft de Politie besloten om de netcentrische werkwijze in te voeren.
- j. Als onderdeel van hun samenwerking treffen de veiligheidsregio's en de Politie gezamenlijke voorbereidingen zodat rampen of crises gecoördineerd kunnen worden aangepakt. Afstemming en samenwerking tussen Veiligheidsregio's, Politie en overige crisispartners zijn van cruciaal belang om te komen tot een adequate crisispreparatie, respons en nazorg in relatie tot de politiezorg taken zoals beschreven in het Referentiekader Regionaal Crisisplan 2016 (RRCP2016). Tijdens incidenten, calamiteiten en crises is het delen van informatie cruciaal. Het middel LCMS wordt hierbij gezien als een basisfunctionaliteit met de uitstraling van een basisinformatievoorziening voor de gehele crisisbeheersing in Nederland.
- k. 5.1.2.i 
- l. 5.1.2.i 
- m. 5.1.2.i 
- n. 5.1.2.i 
- o. In het kader van deze samenwerkingsovereenkomst werken de Politie en IFV actief aan verdere samenwerking op het gebied van de informatievoorziening rondom crisisbeheersingsprocessen, breder dan enkel rondom het LCMS-Politie.
- p. Het IFV verklaart dat zij alle dienstverlening van derden, die wordt ingezet rondom LCMS, heeft aanbesteed conform EU-aanbestedingsregels.
- q. Gelet op de hiervoor genoemde overwegingen wenst de Politie gebruik te maken van het LCMS-Politie.
- r. Het IFV is bereid om het LCMS-Politie aan de Politie ter beschikking te stellen in de vorm van een webapplicatie onder de hierna genoemde voorwaarden.
- s. De Politie heeft vastgesteld dat er maar één leverancier is die de diensten rondom LCMS kan aanbieden en verstrekt derhalve de Opdracht op grond van technische redenen aan het IFV.



KOMEN HET VOLGENDE OVEREEN:

1. Structuur overeenkomst

- 1.1. Deze samenwerkingsovereenkomst LCMS-Politie ("**Overeenkomst**") bestaat uit het onderhavige document en de volgende bijlagen:
- a. Bijlage A: Omschrijving diensten en Technische beschrijving van het LCMS-Politie.
 - b. Bijlage B: Algemene Rijksvoorwaarden bij IT-overeenkomsten 2018 (ARBIT-2018) ("**Voorwaarden**").
 - c. Bijlage C: Service Levels en Bereikbaarheid ("**SLA**").
 - d. Bijlage D: Financiële afspraken en aanvullende diensten.
 - e. Bijlage E: Beleidskader Toegangsbeveiliging LCMS.
- 1.2. In geval van strijdigheid tussen hetgeen is bepaald in het onderhavige document enerzijds en de bijlagen anderzijds, prevaleert het onderhavige document. In geval van strijdigheid tussen hetgeen is bepaald in de bijlagen onderling, geldt de rangorde genoemd in artikel 1.1, waarbij het hoger genoemde document prevaleert boven het lager genoemde.
- 1.3. In de Overeenkomst hebben de met een hoofdletter geschreven begrippen de betekenis als beschreven in de Voorwaarden of in één van de overige documenten van de Overeenkomst.

2. Duur van de overeenkomst en beëindiging

- 2.1. De Overeenkomst treedt in werking op de bovenvermelde ingangsdatum en heeft een initiële looptijd van drie jaar ("Initiële Looptijd"). Uiterlijk drie maanden voor afloop van de Initiële Looptijd vindt een evaluatie plaats van de Overeenkomst, op basis waarvan een verlenging kan worden overeengekomen, telkens voor de duur van één jaar, tenzij één van de Partijen de Overeenkomst schriftelijk beëindigt met inachtneming van een opzegtermijn van drie maanden voor het einde van de desbetreffende periode.
- 2.2. Tussentijdse beëindiging van de Overeenkomst - voor afloop van de initiële looptijd - is voor de Politie mogelijk wanneer zij dit schriftelijk aan IFV kenbaar maakt met een opzegtermijn van 3 maanden. In overleg met de Politie zal door IFV vervolgens een exit-procedure worden afgesproken. Bij tussentijdse opzegging door de Politie zal een éénmalig een bedrag betaald worden aan IFV als tegemoetkoming in de gemaakte opstartkosten en kosten voor de exit-procedure door IFV. Dit houdt concreet in:
- Bij opzegging in het eerste jaar zal door de Politie - naast de tot en met beëindiging van de Overeenkomst in dat jaar verschuldigde vergoeding en éénmalige opstartkosten - een bedrag van 50% van de jaarlijkse kosten inclusief BTW aan uittredekosten betaald worden aan IFV;
 - Bij opzegging in het tweede jaar zal door de Politie - naast de tot en met beëindiging van de overeenkomst verschuldigde vergoeding - een bedrag van 25% van de jaarlijkse contractkosten inclusief BTW aan uittredekosten betaald worden aan IFV;
 - Bij opzegging in of na het derde jaar zullen er geen uittredekosten verrekend worden aan de Politie.

Onderdeel van de exit-procedure na afloop van het contract is dat IFV alle bij de Politie berustende operationele data uit LCMS-Politie aan de Politie digitaal overdraagt en gelijktijdig al deze bij de Politie berustende operationele data uit LCMS-Politie verwijdt.

- 2.3. De bestaande overeenkomstvorm gaat uit van hosting van LCMS door het IFV. De Politie heeft aangegeven - op termijn - te overwegen LCMS-Politie zelf te willen hosten. In het geval de Politie aangeeft dat hij deze Overeenkomst wenst te beëindigen – en daarbij een aansluitende overeenkomst aangaat met het IFV ten aanzien van het gebruiksrecht van LCMS waarbij de Politie zelf de uitvoering van de hosting voor LCMS-Politie voor haar rekening neemt – dan vervallen de in artikel 2.2 genoemde uittreetskosten volledig.
- Afspraken over een dergelijke overgang van de uitvoering van de hosting van LCMS-Politie kunnen jaarlijks worden gemaakt, als onderdeel van het evalueren van de overeenkomst.
 - Het feitelijke moment van overdracht van de hosting kan vanaf het 2^e jaar van de Overeenkomst op ieder nader overeen te komen moment plaatsvinden, waarbij de Politie het IFV in deze een redelijke termijn biedt om deze overdracht te kunnen faciliteren.
- 2.4. De Overeenkomst kan door Partijen slechts worden beëindigd overeenkomstig artikel 30 van de **Voorwaarden**, dan wel op grond van het bepaalde in artikelen 2.1, 2.2 en 2.3 hierboven.

3. De samenwerking

- 3.1. Rol IFV: Het IFV ondersteunt de veiligheidsregio's door onder andere het ontwikkelen en ter beschikking stellen van expertise op voornoemde gebieden en het verwerven, beheren en aan de veiligheidsregio's ter beschikking stellen van materieel, uitrusting en telecommunicatievoorzieningen.

Eén van de door het IFV geleverde telecommunicatievoorzieningen is het Landelijk Crisismanagement Systeem (LCMS). Het LCMS is een IT-systeem dat een netcentrische werkwijze ondersteunt. Afstemming en samenwerking tussen veiligheidsregio's, Politie en overige crisispartners zijn van cruciaal belang om te komen tot een adequate crisispreparatie, respons en nazorg in relatie tot de politietaken zoals genoemd in de Politiewet 2012 en het RRCP2016. Tijdens incidenten, calamiteiten en crisis is het delen van informatie cruciaal. Het middel LCMS wordt hierbij gezien als een basisfunctionaliteit met de uitstraling van een basisinformatievoorziening voor de gehele crisisbeheersing in Nederland.

- 3.2. Rol Politie: De taken van de Politie zijn vastgelegd in de Politiewet 2012 en heeft daarmee ook een rol in de Hoofdstructuur van de Rampenbestrijding en Crisisbeheersing als bedoeld in de Wet veiligheidsregio's. Deze Politiezorgtaken zijn nader uitgewerkt in het RRCP2016. In de Wet en het Besluit Veiligheidsregio's is opgenomen dat bij crisissituaties relevante informatie op een netcentrische werkwijze door betrokken organisaties gedeeld dient te worden voor beheersing van de crisis. Er zijn diverse evaluaties waaruit blijkt dat deze wederzijdse informatiedeling van en door politie verbeterd dient te worden om te komen tot een betere afstemming, informatie-uitwisseling en samenwerking met partners in de veiligheidsregio's.

Het LCMS-Politie (PCMS) ondersteunt de behoefte om op basis van een actueel gemeenschappelijk situatiebeeld te komen tot een verbetering in de samenwerking tussen de partners in de veiligheidsketen en tot een snellere/betere beeldvorming, oordeelsvorming en besluitvorming in de crisisbeheersingsprocessen. Vanuit politie zijn met alle Veiligheidsregio's convenanten afgesloten om onder andere de informatiedeling te verbeteren. Met behulp van de technische applicaties kan dit proces verder worden doorontwikkeld.

De Politie heeft een rol en verantwoordelijkheid binnen de samenwerking met crisispartners als het gaat om informatie-uitwisseling tijdens een crisis, informatiedeling tijdens een incident, tijdens een evenement of bijzondere gebeurtenis. Binnen de samenwerking tijdens een crisissituatie is o.a. maar niet uitsluitend beoogd: bereidheid van Partijen om informatie te delen en hiermee een data netwerk op te bouwen.

De Politie neemt actief deel aan de Governance en de werkgroepen voor het beheer, de gebruikskaders, prioriteiten, financiële keuzes, de ontwikkeling van het LCMS als systeem en de verdere doctrine.

- 3.3. In het kader van deze samenwerkingsovereenkomst werken de Politie en IFV actief aan verdere samenwerking op het gebied van de informatievoorziening rondom crisisbeheersingsprocessen, breder dan enkel rondom het LCMS-Politie.
- 3.4. De hiervoor staande openbare diensten worden verleend met het oog op de verwezenlijking van het algemeen belang en de gemeenschappelijke doelstellingen van de Politie en het IFV. Dit algemeen belang en gemeenschappelijke doelstellingen: het verhogen van het kennisniveau binnen een crisissituatie, het verbeteren van de informatiepositie, en digitale transformatie bij de Politie waarmee alle betrokken partijen streven naar het verbeteren van de veiligheid binnen de maatschappij.
- 3.5. Het IFV en de Politie begeven zich niet of maximaal tot 20% van hun gezamenlijke activiteiten t.a.v. LCMS op de (commerciële) markt en houden zich dus voor minimaal 80% bezig met het verstrekken van gebruiksrechten in het kader van rampenbestrijding en crisisbeheersing voor de publieke afnemers in het kader van de samenwerking.

4. Voorwerp van de overeenkomst

- 4.1. De Politie verleent het IFV hierbij opdracht tot het verlenen van de diensten, welke opdracht het IFV hierbij aanvaardt. De diensten zijn nader omschreven in Bijlage A en omvatten:
- a. het ter beschikking stellen van het LCMS-Politie in de vorm van een webapplicatie ("SaaS-dienst"); en
 - b. het verzorgen van het landelijk functioneel beheer van het LCMS-Politie; en
 - c. het ter beschikking stellen van een Servicedesk ter ondersteuning van de functioneel beheerders van de Politie.
- 4.2. Additionele afspraken buiten de huidige overeengekomen dienstverlening en service levels worden nader vastgelegd in de Omschrijving van de diensten (Bijlage A) en de SLA (Bijlage C). Hiervoor geldt dat het IFV zich zal inspannen deze diensten op vakbekwame wijze te verrichten.

5. SaaS-dienst en service levels

- 5.1. Het IFV verleent de Politie het niet-exclusieve recht om de SaaS-dienst gedurende de looptijd van de Overeenkomst te gebruiken ten behoeve van de uitvoering van zijn eigen wettelijke taken. Het is de Politie niet toegestaan om derden buiten dit kader gebruik te laten maken van de SaaS-dienst. De Politie erkent dat het karakter van de SaaS-dienst met zich meebrengt dat hij niet de beschikking krijgt over een exemplaar van de programmatuur.
- 5.2. De SaaS-dienst is gebaseerd op een standaard webapplicatie die wordt geleverd aan alle veiligheidsregio's, de waterschappen en andere crisispartners van de veiligheidsregio's. Door middel van parametrisering kan de Politie de SaaS-dienst aanpassen.
- 5.3. De doorontwikkeling van de netcentrische werkwijze en het LCMS vindt plaats onder regie van het Veiligheidsberaad. Van tijd tot tijd leidt dit tot een nieuwe versie van het LCMS die, na implementatie daarvan, ook wordt aangeboden aan de Politie en daarmee dus onderdeel wordt van de SaaS-dienst. Wanneer het IFV, al dan niet in opdracht van het Veiligheidsberaad, een nieuwe versie van het LCMS uitbrengt, zal IFV onverwijld de Politie daaromtrent inlichten. IFV stelt de Politie tijdig, maar tenminste 8 weken vooraf op de hoogte van wijzigingen die redelijkerwijs gevolgen kunnen hebben voor de werkwijze van de Politie en het tijdstip van implementatie. Kosten die samenhangen met de implementatie van die wijzigingen binnen de organisatie van de Politie komen voor rekening van de Politie.

- 5.4. Het IFV zal zich ervoor inspannen dat de SaaS-dienst zonder technische storingen functioneert maar garandeert niet dat de SaaS-dienst zonder onderbrekingen beschikbaar is of dat de programmatuur die hij inzet ten behoeve van de SaaS-dienst foutloos is. Het IFV neemt bij de levering van de SaaS-dienst de service levels in acht die zijn vastgelegd in Bijlage C (SLA).
- 5.5. Het IFV is gerechtigd de SaaS-dienst geheel of gedeeltelijk tijdelijk buiten gebruik te stellen in verband met onderhouds- of beheerwerkzaamheden na voorafgaand overleg met de Politie. Het IFV zal de onderbreking niet langer laten duren dan noodzakelijk en deze zo mogelijk buiten kantooruren laten plaatsvinden. Voorafgaand aan de geplande werkzaamheden wordt door het IFV gecontroleerd of er een crisissituatie is waarbij, op dat moment het gebruik van LCMS cruciaal is. Als dit het geval is, worden de geplande werkzaamheden in overleg uitgesteld. Het proces met betrekking tot de uitvoering van deze onderhouds- of beheerwerkzaamheden wordt nader vastgelegd in een Dossier Afspraken en Procedures.
- 5.6. Partijen nemen de administratie en de logs van het IFV als uitgangspunt voor het meten van de service levels. De Politie is gerechtigd tegenbewijs te leveren. Bij het meten van de service levels laten Partijen de vooraf door het IFV aangekondigde onderbrekingen van (de beschikbaarheid) de SaaS-dienst, alsmede omstandigheden die buiten de invloedssfeer liggen van het IFV, buiten beschouwing.
- 5.7. De dienstverlening wordt jaarlijks door IFV en de Politie geëvalueerd. Van deze tussenevaluatie wordt een verslag opgesteld. Beide Partijen zullen zich naar beste vermogen inspannen om eventuele nadere afspraken of acties die voortvloeien uit deze evaluatie te realiseren voor zover deze niet strijdig zijn met hetgeen in de voorliggende samenwerkingsovereenkomst is overeengekomen.
- 5.8. De Politie zal zich houden aan het Beleidskader Toegangsbeveiliging LCMS, zoals door het IFV aan de Politie beschikbaar wordt gesteld (zie Bijlage E), daar waar er sprake is van gegevensuitwisseling met andere (crisis)partners. In het LCMS-Politie worden politiegegevens verwerkt tot en met het niveau als bedoeld in artikel 9 van de Wet Politiegegevens. De Politie stelt hiertoe een eigen Beleidskader Toegangsbeveiliging op die aanvullend is aan het Beleidskader Toegangsbeveiliging LCMS.
- 5.9. Het IFV neemt de specifieke technische beveiligingsmaatregelen die nodig zijn voor het verwerken van politiegegevens als bedoeld in artikel 5.8, zoals omschreven in Bijlage A of conform deze bijlage nader worden uitgewerkt.

6. Functioneel beheer

- 6.1. De Politie zal het IFV voor de start van de uitvoering van de diensten schriftelijk informeren welke medewerker(s) zijn aangesteld als functioneel beheerder(s) binnen haar organisatie. Indien de aangestelde medewerker(s) nog niet bekend zijn bij de start van de uitvoering van de diensten, worden deze zo snel als mogelijk bekend gemaakt aan het IFV.
- 6.2. De Politie is verantwoordelijk voor het functioneel beheer van het LCMS-Politie. Landelijk functioneel beheer van het IFV biedt ondersteuning aan de door de Politie aangestelde beheerder(s). Deze beheerders (van de Politie) zijn verantwoordelijk voor de inrichting van de applicatie en bieden ondersteuning aan de eindgebruikers binnen de organisatie van de Politie. Het IFV voorziet in een initiële opleiding/training voor deze beheerders.

- 6.3. Als uitvloeisel van deze overeenkomst worden door landelijk functioneel beheer van het IFV en functioneel beheer van LCMS-Politie nadere afspraken over de initiële opleiding van de beheerders, onderlinge samenwerking, escalatieprocedures en rapportage ten aanzien van het LCMS-Politie vastgelegd in een Dossier Afspraken en Procedures LCMS-Politie ("DAP LCMS-Politie").
- 6.4. De contactgegevens van de Dienst/Sector van de beheerders van de Politie en van het landelijk functioneel beheer van het IFV worden vastgelegd in het DAP LCMS-Politie.

7. Vergoeding

- 7.1. De vergoedingen voor de geleverde diensten zijn gespecificeerd in Bijlage D. Alle vergoedingen zijn vastgesteld in euro's, exclusief btw.
- 7.2. De vergoedingen per kalenderjaar wordt omstreeks 1 juli van dat jaar gefactureerd.
- 7.3. Het IFV is gerechtigd de vergoedingen jaarlijks per 1 januari te indexeren op basis van de loon-/prijsindexatie volgens opgave van de VNG in haar meicirculaire.

8. Verwerking persoonsgegevens en politiegegevens

- 8.1. Voor zover het IFV in het kader van de uitvoering van de Overeenkomst persoonsgegevens voor de Politie verwerkt wordt het IFV als verwerker in de zin van de algemene verordening gegevensbescherming (AVG) aangemerkt, en de Politie als verwerkingsverantwoordelijke. Deze paragraaf geldt tevens als verwerkersovereenkomst in de zin van artikel 28, 3e lid van de AVG.
- 8.2. Voor zover het IFV in het kader van de uitvoering van de Overeenkomst politiegegevens voor de Politie verwerkt wordt het IFV als verwerker in de zin van de Wet politiegegevens (Wpg) aangemerkt. Deze paragraaf geldt tevens als verwerkersovereenkomst in de zin van artikel 6c, van de Wpg.
- 8.3. Het IFV verwerkt persoonsgegevens uitsluitend in opdracht en volgens de instructies van de Politie en voor zover dit noodzakelijk is voor de uitvoering van de Overeenkomst en het in stand houden van LCMS-Politie. IFV gebruikt de persoonsgegevens niet voor eigen doeleinden of doeleinden van derden. Het IFV zal de persoonsgegevens behoorlijk en zorgvuldig verwerken en in overeenstemming met de op haar rustende verplichtingen uit de AVG.
- 8.4. IFV zal passende technische en organisatorische maatregelen treffen om persoonsgegevens die zij verwerkt in het kader van deze Overeenkomst te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen zullen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau garanderen, gelet op de risico's die de verwerking en de aard van de te beschermen persoonsgegevens met zich brengen. De beveiligingsmaatregelen zijn beschreven in Bijlage A.
- 8.5. Het IFV zal de Politie in staat stellen toe te zien op de naleving van het in artikel 8.3 bepaalde, bijvoorbeeld door middel van het inschakelen van een onafhankelijke derde. De kosten daarvan komen voor rekening van de Politie. De Politie kan het onderzoek slechts laten uitvoeren na voorafgaand overleg met het IFV over onder meer de scope, timing en doorlooptijden.

- 8.6. Het IFV zal de Politie onverwijld informeren nadat hij bekend is geworden met een beveiligingsinbreuk of datalek die/dat ernstige nadelige gevolgen heeft of kan hebben voor de werking van LCMS en/of de bescherming van persoonsgegevens. De Politie is vervolgens zelf verantwoordelijk voor het onverwijld informeren van de Autoriteit Persoonsgegevens in deze. Bij beveiligingsinbreuken of datalekken treft het IFV de nodige maatregelen om de schade te beperken en herhaling te voorkomen.
- 8.7. Personen in dienst van of werkzaam voor het IFV, evenals het IFV zelf, zijn verplicht tot geheimhouding met betrekking tot alle gegevens in het LCMS, waaronder maar niet beperkt tot de persoonsgegevens, en werkwijzen waarop de Politie haar crisismanagement heeft ingericht.
- 8.8. Het IFV zal alle van de Politie afkomstige persoonsgegevens die worden verwerkt in het kader van deze Overeenkomst aantoonbaar vernietigen, op het moment dat de Overeenkomst wordt beëindigd ongeacht de gronden voor beëindiging, tenzij het IFV wettelijk verplicht is om de persoonsgegevens te bewaren.
- 8.9. Indien het IFV voor de uitvoering van de diensten gebruik maakt van derden, is het IFV gehouden deze derden in kennis te stellen van de inhoud van dit artikel 8 en de in Bijlage A beschreven beveiligingsmaatregelen. Het IFV staat er jegens de Politie voor in dat deze derden bij de uitvoering van de diensten handelen conform dit artikel 7 en de in Bijlage A beschreven beveiligingsmaatregelen.
- 8.10. IFV en de Politie sluiten zo spoedig mogelijk een nadere verwerkersovereenkomst af, welke na inwerkingtreding artikel 8 uit deze Overeenkomst vervangt. Wanneer er strijdige bepalingen zijn tussen de samenwerkingsovereenkomst en de nadere verwerkersovereenkomst, prevaleert de verwerkersovereenkomst omtrent de specifieke onderwerpen “verwerking persoonsgegevens” en “verwerking politiegegevens”.

9. Afwijkende bepalingen ten opzichte van de “voorwaarden”

- 9.1. In plaats van artikel 43 van de Voorwaarden (“Aard en inhoud van het Gebruiksrecht”), met betrekking tot het Gebruiksrecht is, Artikel 5.1 van deze overeenkomst van toepassing.
- 9.2. Artikel 45 van de Voorwaarden (“Verstrekken van een Installatiekopie”) is in het kader van deze overeenkomst niet relevant en wordt als zijnde niet van toepassing verklaard.

10. Diversen

- 10.1. Alle intellectuele eigendomsrechten die kunnen worden uitgeoefend ten aanzien van LCMS, waaronder het LCMS-Politie en de diensten berusten uitsluitend bij het IFV of haar licentiegevers.
- 10.2. Het IFV maakt bij de uitvoering van de diensten gebruik van derden, waaronder derden die de technische infrastructuur, hardware, hosting en het technisch beheer van het LCMS-Politie verzorgen. Bij de inzet van derden bij voorgenoemde dienstverlening door derden is tevens de ARBIT van toepassing, waarbij voor de inzet van derden eerst toestemming moet worden gevraagd aan de Politie, dit in het kader van een mogelijke integriteitstoetsing.
- 10.3. Het IFV verklaart dat zij ter verkrijging van de Opdracht Personeel van de Politie generlei voordeel heeft geboden, gegeven, doen of aanbieden of doen geven. Hij zal dat ook niet alsnog doen teneinde personen in dienst van de Politie te bewegen enige handeling te verrichten of na te laten. De Politie verklaart niets te hebben aangenomen.

- 10.4. Deze Overeenkomst bevat al hetgeen Partijen in verband met het onderwerp daarvan zijn overeengekomen. Met ingang van het tijdstip waarop deze Overeenkomst in werking treedt, eindigen alle overeenkomsten en afspraken die de Partijen daarover eerder mochten hebben gesloten respectievelijk gemaakt.

Aldus overeengekomen en in tweevoud ondertekend,

[datum] 09-11-2021

De korpschef van politie, namens deze,

5.1.2.e

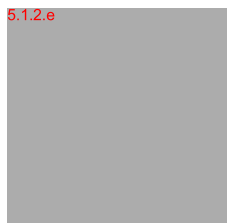


Mevrouw P.F. Bosman
Directeur PDC

[datum] 16 november 2021

Het zelfstandig bestuursorgaan Instituut
Fysieke Veiligheid, namens deze,

5.1.2.e



5.1.2.e

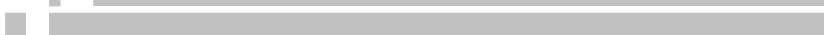


Bijlage A: Omschrijving diensten en technische beschrijving

LCMS-Politie

Omschrijving diensten

De diensten die IFV aan de Politie levert zijn:

- a. 5.1.2.i 
 - 
 - 
- 
 - 
 - 
- 
 - 
 - 

Niveau van dienstverlening

Het niveau van de dienstverlening is beschreven in Bijlage C: Service Levels en Bereikbaarheid.

Deze bijlage beschrijft de afspraken waaronder het LCMS-Politie wordt aangeboden, incident- en probleembeheer, rapportages en hoe het IFV kan worden bereikt voor ondersteuning.

Technische beschrijving van het LCMS-Politie

LCMS-Politie wordt door het IFV als SaaS-dienst (Software as a Service) aangeboden aan de Politie. Door het LCMS-Politie als een SaaS-dienst aan te bieden, wordt een maximale ontzorging nagestreefd.

5.1.2.i 




.

5.1.2.i 


.

Daarnaast zijn extra eisen gesteld aan de datacenters waar de hosting van het LCMS-Politie in wordt uitgevoerd:

- > 5.1.2.i 



5.1.2.h



Afspraken met betrekking tot de beschikbaarheid en toepassing van de Back-up- en Recovery procedures zullen in het DAP LCMS-Politie worden overeengekomen.

Version	Number of Publications
5.1.21	950
5.1.20	250
5.1.19	650
5.1.18	950
5.1.17	150
5.1.16	900
5.1.15	450
5.1.14	800
5.1.13	650
5.1.12	980
5.1.11	150
5.1.10	850
5.1.9	750
5.1.8	1000
5.1.7	950
5.1.6	980
5.1.5	950
5.1.4	800

Pagina 17 van 25

Bijlage B: Algemene Rijksvoorwaarden bij IT-overeenkomsten 2018

Zie ARBIT2018.

Bijlage C: Service Levels en Bereikbaarheid

Definities

“Probleem”: een structurele fout in de Dienst of de dienstverlening met betrekking tot de Dienst.

“Incident”: een (dreigende) verstoring van het LCMS-Politie.

“Melding”: een ingediende vraag of informatieverzoek.

“Prioriteit 1 - Zeer hoog”:

Incident betreft zowel de operationele- als de oefenomgeving van het LCMS waardoor geen uitwijk mogelijk is naar een andere omgeving van het LCMS-Politie. Het LCMS-Politie is onbruikbaar voor alle gebruikers.

“Prioriteit 2 - Hoog”:

Incident betreft de operationele omgeving van het LCMS-Politie, uitwijk naar de oefenomgeving is mogelijk.

“Prioriteit 3 - Midden”:

Incident betreft de operationele omgeving of de oefenomgeving van het LCMS-Politie. Het LCMS-Politie is bruikbaar maar met verminderde functionaliteit.

“Prioriteit 4 - Laag”:

Geldt voor meldingen.

De afspraken ten aanzien van Reactietijden en Oplostijden van Incidenten en Meldingen per prioriteit zijn:

Reactie/ Oplossing	Prioriteit 1 zeer hoog	Prioriteit 2 hoog	Prioriteit 3 midden	Prioriteit 4 laag
Reactietijd	15 minuten	15 minuten	120 minuten	120 minuten
Oplostijd	60 minuten *	4 uur *	24 uur *	Eerstvolgende release

* De gegeven oplostijd moet in 90% van de meldingen binnen de gestelde oplostijd worden gehaald.

Reactietijd is de tijdsduur tussen een correcte melding door de Politie en de aanvang van de werkzaamheden verband houdende met de oplossing daarvan.

Incidenten met prioriteit 1 en 2 moeten altijd eerst telefonisch worden aangemeld. Aanmelder krijgt ook telefonisch een terugkoppeling van de status. Incidenten met prioriteit 1 moeten 24/7 kunnen worden opgelost.

Bij incidenten met prioriteit 3 of 4 heeft de reactietijd betrekking op tijd binnen het standaard servicevenster. Bij incidenten met prioriteit 2, 3 of 4, heeft de oplostijd betrekking op tijd binnen het standaard servicevenster.

Het standaard servicevenster is gedefinieerd als:

- werkdagen van 09:00 - 17:00 uur;
- buiten het standaard servicecenter vallen niet werkdagen, aangemerkt zaterdagen, zondagen en de in Nederland wettelijk erkende feestdagen.

Beschikbaarheid van LCMS-Politie

5.1.2.1

Usability en performance van LCMS

Usability is een belangrijk onderwerp bij de doorontwikkeling van LCMS. Naast de traditionele test methodes wordt er ook getest op usability. Eén van de eisen die is opgesteld in het kader van de usability test is dat wanneer een gebruiker een actie uitvoert, deze binnen 3,5 seconden (de gemeten tijden zijn binnen het hosting netwerk) response krijgt in een situatie waarbij concurrent 1100 gebruikers ingelogd zijn op het LCMS. Naarmate er minder concurrent gebruikers ingelogd zijn, zal de response tijd van 3,5 seconden lager uitvallen (voor exacte responsetijden moet er een usability test uitgevoerd worden op het lokale netwerk van de Politie).

Incidenten- en Meldingenbeheer

Incidenten kunnen door de daartoe in de DAP LCMS-Politie gedefinieerde medewerkers van de Politie, zoals bedoeld in Artikel 6.1, 7 dagen per week, 24 uur per dag telefonisch of per mail worden gemeld. In het DAP LCMS-Politie is dit proces nader beschreven.

Incidenten met prioriteit 1 en 2 moeten altijd eerst telefonisch worden aangemeld.

Probleembeheer

Probleembeheer betreft het analyseren en oplossen van structurele fouten in de Dienst of de dienstverlening met betrekking tot de Dienst. Problemen kunnen afkomstig zijn uit de analyse van incidentmeldingen, testbevindingen en release-evaluaties. Een probleemanalyse wordt door IFV op eigen initiatief uitgevoerd, of na verzoek of opdrachtverstrekking door de Politie. In het laatste geval wordt het probleem volgens het wijzigingenproces behandeld en kan aan de Politie gevraagd worden, eventuele kosten te vergoeden. Indien het oplossen van een probleem door IFV uitgevoerd dient te worden zal de Politie hier opdracht toe verlenen volgens het wijzigingenproces.

Wijzigingen- en releasebeheer

Het Changemanagement proces valt onder de verantwoordelijkheid van het Instituut Fysieke Veiligheid. Binnen IFV bestaat een Themagroep functioneel beheer (Change Control Board) waarin vertegenwoordigers van de verschillende disciplines en aangesloten partners of LCMS gebruikersorganisaties zitting hebben, waaronder de Politie. Binnen dit overleg (driemaandelijks) worden wijzigingen geëvalueerd, geprioriteerd en goed- of afgekeurd.

Goedgekeurde wijzigingen worden via een online ticketsysteem als RfC doorgeleid naar het Ontwikkelteam via de Applicatie Manager van IFV. Binnen de themagroep functioneel beheer wordt bepaald wanneer een wijziging doorgevoerd wordt in een release.

Wanneer een organisatie voor haar wens te weinig draagvlak of prioriteit krijgt (maar de wens niet is uitgesloten i.c. op termijn in principe wel kan worden gerealiseerd) kan men door middel van eigen financiering onder voorwaarden de RfC als "bijzonder verzoek" toch gerealiseerd krijgen. Deze manier van werken maakt de weg vrij voor de Politie om laag geprioriteerde verbeteringen sneller te laten ontwikkelen, zodra de Politie daar zelf de financiering voor over heeft.

Een belangrijke voorwaarde is dat versnelde realisering van een bijzonder verzoek geen verstoring van het reguliere release proces betekent, met andere woorden de planning voor realisatie van door het netwerk vastgestelde eisen en wensen niet verstoort.

Realisatie van een bijzonder verzoek kan nooit leiden niet tot een beperking in het ontwikkelbudget of aanpassing van de opleverplanning van door het netwerk geaccordeerde RfC's voor de andere gebruikers.

De releaseplanning wordt vastgesteld door het directeurenoverleg LVCb, waarin de Politie vertegenwoordigd is. Uitgangspunt is dat er twee (2) releases per jaar worden uitgevoerd. Onder release wordt verstaan een bepaalde versie van het systeem dat als geheel is (of zal worden) geaccepteerd. Een release bestaat uit programmatuur, data definities en data (inhoud database).

Service level rapportage en service-overleg

Na afloop van iedere kalendermaand ontvangt de Politie een service level rapportage. Eénmaal per kalenderkwartaal vindt er service level overleg plaats tussen functioneel beheer van de Politie en Landelijk Functioneel Beheer LCMS van het IFV. In het DAP LCMS-Politie is de governance nader beschreven.

Bijlage D: Financiële afspraken en aanvullende diensten

Vergoeding LCMS-Politie

De Vergoeding voor LCMS-politie wordt vastgesteld conform het lange termijn financieringsmodel voor LCMS en netcentrisch werken welke door het bestuurlijk overleg LVCb is vastgesteld in het kader van de financiële en governance afspraken voor de landelijke voorziening crisisbeheersing (LVCb). De LVCb omvat alle activiteiten door het programma netcentrisch werken ten aanzien van het beheer van LCMS en de netcentrisch werkwijze.

Alle genoemde bedragen zijn vastgesteld in euro's, exclusief btw en kunnen jaarlijks geïndexeerd worden op basis van artikel 7.2.

De jaarlijkse kosten worden ieder kalenderjaar omstreeks 1 juli gefactureerd. In geval van een start van de overeenkomst gedurende het jaar wordt de vergoeding van de jaarlijkse kosten voor het desbetreffende kalenderjaar bepaald naar rato van het aantal dagen vanaf ingangsdatum contract tot en met 31 december.

De éénmalige opstartkosten worden bij oplevering van de LCMS-Politie omgeving aan de Politie gefactureerd.

Specificatie van de jaarlijkse vergoeding voor LCMS-Politie (prijspeil 2021)

LCMS-Politie	
5.1.2.b	

5.1.2.b	
---------	--

Alle genoemde bedragen zijn op basis van hosting door het IFV van een eigen LCMS-Politie-omgeving (PCMS).

Overige dienstverlening

Overige diensten door het IFV kan door de Politie worden afgenomen op basis van de dan geldende tarieven van het IFV. IFV verstrekt desgevraagd jaarlijks een opgave aan de Politie van de voor dat kalenderjaar voor IFV geldende tarieven. Deze tariefstelling van IFV wordt door het Veiligheidsberaad ten behoeve van IFV jaarlijks vastgesteld.

Het gebruik van een e-learning is onderdeel van het geheel aan dienstverlening rondom LCMS-Politie. Voor het aanpassen van deze e-learning worden éénmalig kosten gerekend. De kosten hiervoor bedragen 5.12,1. Voor het gebruik van de e-learning worden geen aanvullende (jaarlijkse) vergoedingen gevraagd. Om de look-and-feel van de e-learning identiek te krijgen aan de LCMS-Politie kan de e-learning pas worden afgerond en opgeleverd na de installatie van LCMS-Politie. Voor de oplevering van de e-learning is een bijdrage door de Politie vereist ten aanzien van inhoudelijke (crisis)scenario's, die de kern vormen van de e-learning. Onderdeel hiervan is o.a. het in de e-learning verwerken van specifieke Politie terminologie en semantiek.

Bijlage E: Beleidskader toegangsbeveiliging LCMS

Zie Beleidskader Toegangsbeveiliging - Versie 1.0, 21 oktober 2014.





5.1.2.1

5.1.2.1

Verwerkers- Overeenkomst ARBIT

Nummer:

**Ingangsdatum: 1
december 2021**

Uitgegeven door: Politie, Politiedienstencentrum - Dienst Verwerving

Status: Concept

Versie: 0.1

Versie datum: 13 juni 2022

© Politie, alle rechten voorbehouden

Niets uit deze uitgave mag worden verveelvoudigd, op geautomatiseerde wijze opgeslagen of openbaar gemaakt in enige vorm of op enigerlei wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de Politie.

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 ^{5.1.2.i} [redacted]

- a) met daarop aanvullend van toepassing de ARBIT-2018
- b) Referentienummer: ^{5.1.2.i} [redacted]

De ondergetekenden:

1. De Politie, gevestigd te Den Haag,
te dezen rechtsgeldig vertegenwoordigd door de korpschef van politie de heer H.P. van
Essen, te dezen rechtsgeldig vertegenwoordigd door mevrouw G. Woudenberg, Directeur
Dienst ICT, hierna te noemen: 'de Politie',

en

2 ^{5.1.2.i} [redacted] te dezen vertegenwoordigd door ^{5.1.2.i} [redacted] hierna te
noemen: 'Opdrachtnemer',

hierna gezamenlijk te noemen: 'Partijen;

OVERWEGENDE DAT:

- Partijen de Overeenkomst inzake ^{5.1.2.i} [redacted] met kenmerk ^{5.1.2.i} [redacted] (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.
6. Overeenkomst: de overeenkomst inzake ^{5.1.2.1} met kenmerk ^{5.1.2.1}, 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 Hulpleveranciers in zonder schriftelijke voorafgaande toestemming van de Politie.

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

- a. Opdrachtnemer heeft een schriftelijke overeenkomst met de desbetreffende Hulpleverancier waarin in ieder geval het volgende is opgenomen:
 - een verplichting dat de Hulpleverancier dient te handelen in overeenstemming met alle bepalingen uit deze Verwerkersovereenkomst;
 - een verplichting dat de Hulpleverancier 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 Hulpleverancier om de Persoonsgegevens en/of Politiegegevens uitsluitend in opdracht en volgens de instructies van Opdrachtnemer te verwerken;
 - een verplichting van de Hulpleverancier om zelf geen sub-opdrachtnemers in te schakelen, zonder de voorafgaande schriftelijke toestemming van de Politie;
 - een verplichting dat de Hulpleverancier 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 Hulpleverancier 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 Hulpleverancier 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 een 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:
- a. de verwerkingen en de naleving van de overeengekomen technische en organisatorische beveiligingsmaatregelen van Opdrachtnemer dan wel die van door Opdrachtnemer ingeschakelde Hulpleveranciers controleren,
 - en
 - b. 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 Hulpleverancier(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 Hulpleverancier, 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 Hulpleverancier 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,

de Opdrachtgever

De korpschef van politie,
namens deze,
de directeur PDC,
namens deze,

5.1.2.e



G. Woudenberg
Directeur Dienst ICT

de Opdrachtnemer

5.1.2.i



namens deze,

5.1.2.e



5.1.2.i



Bijlage 1 Werkprocessen, autorisaties en functiegroepen verwerking

De verwerking door Opdrachtnemer ziet toe op de volgende gegevens:

Categorieën Betrokkenen

Medewerkers van de politie

Externe partijen

De te verwerken (categorieën) Persoonsgegevens en/of Politiegegevens

Naam, e-mail, organisatie

Naam, e-mail, organisatie

Medewerkers van gecontracteerde leveranciers van de politie dienen over een geldig VOG+GHVK te beschikken.

Bij de autorisatie van medewerkers van externe partijen wordt dit expliciet gevraagd.

Doel van de verwerking

Om een gebruikersnaam en toegangscode aan te kunnen maken, voor zowel de gehele politieomgeving als voor de specifieke projecten waar betreffend persoon in werkt.

Tevens voor communicatie vanuit de software naar de gebruiker en het delen van informatie met de externe partijen die aan een huisvestings-ontwikkel-project samenwerken.

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

Externe organisatie	Waarom ontvangt de externe organisatie die gegevens?	Wat doet de externe organisatie met die gegevens?	<u>Door privacy adviseur in te vullen:</u> Rol van deze organisatie • Verwerkingsverantwoordelijk • Verwerker • Gezamenlijke verwerkingsverantwoordelijke
5.1.2.i	5.1.2.i is een SAAS-software-applicatie.	Wordt opgeslagen in de software. 5.1.2.i doet zelf niets met deze inloggegevens, maar heeft wel toegang.	Technisch beheerder van de leverancier/verwerker 5.1.2.i heeft toegang tot de autorisatiegegevens.
Externe partijen	Persoonlijke inloggegevens voor het gebruik van 5.1.2.i in een huisvestingsproject	Niets.	Verwerker 5.1.2.i

Bewaartermijnen

Voor de duur van de Verwerkersovereenkomst

Contactgegevens Opdrachtnemer

5.1.2.e

Contactgegevens Hulpverleners mits goedgekeurd door de Politie

<bedrijfsnaam, adres en contactgegevens van de contactpersoon van Hulpverancier>

Technische en organisatorische beveiligingsmaatregelen

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

**aankruisen wat van toepassing is*

☒ een geschreven beveiligingsbeleid conform ISO 27001 inzake Information Security Management

5.1.2.1

☐ een geschreven kwaliteitsbeleid conform ISO 9001 inzake Quality Management

☐ anders, nl.

2. De organisatorisch en en technische beveiligingsmaatregelen omvatten in ieder geval:

5.1.2.1

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>

a) Minimaal: <vul aan>

b) 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>

a) Op <datum>

b) Tussen <begindatum periode> en <einddatum periode>

c) 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





Raamovereenkomst

5.1.2.i

5.1.2.i

**Verwerkers-
Overeenkomst
ARBIT**

Nummer:

Ingangsdatum: 01-12-2021

Uitgegeven door: Politie, Politiedienstencentrum - Dienst Verwerving

Status:Definitief

Versie: 1.0

Versie datum: 16 december 2021

2021© Politie, alle rechten voorbehouden

Niets uit deze uitgave mag worden verveelvoudigd, op geautomatiseerde wijze opgeslagen of openbaar gemaakt in enige vorm of op enigerlei wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de Politie.

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^{5.1.2.i}

- a) met daarop aanvullend van toepassing de ARBIT-2018
- b) Referentienummer^{5.1.2.i}

De ondergetekenden:

1. De Politie, gevestigd te Den Haag,
te dezen rechtsgeldig vertegenwoordigd door de korpschef van politie,
te dezen rechtsgeldig vertegenwoordigd door Directeur PDC, Petra Bosman
hierna te noemen: 'de Politie',

en

2. ^{5.1.2.i} (statutair) gevestigd te ^{5.1.2.i} te dezen
vertegenwoordigd door ^{5.1.2.e} er ^{5.1.2.e}
^{5.1.2.e} hierna te noemen: Opdrachtnemer,

hierna gezamenlijk te noemen: 'Partijen;

OVERWEGENDE DAT:

- Partijen een overeenkomst voor de levering van ^{5.1.2.i} of ^{5.1.2.i}, met kenmerk ^{5.1.2.i} (hierna te noemen: de Overeenkomst) hebben gesloten;
- Als onderdeel van de Overeenkomst de Klant ook de ^{5.1.2.i} (hierna: de ^{5.1.2.i} van Opdrachtnemer aanneemt;
- Voor wat betreft de ^{5.1.2.i} pdrachtnemer is aan te merken als verwerkingsverantwoordelijke;
- Voor wat betreft ^{5.1.2.i} voor een beperkt gedeelte sprake van een verantwoordelijke tot verwerker relatie – namelijk voor de verwerking van door de Opdrachtgever aan de portal toegevoegde persoonsgegevens van eindgebruikers - waarbij de Oprachtgever doel en middelen aanwijst en daarmee optreedt als verwerkingsverantwoordelijke, en door Opdrachtnemer in het kader van de uitvoering van de Portaldienst persoonsgegevens worden verwerkt in de zin van artikel 4 sub 1 van de Algemene Verordening Gegevensbescherming EU 2016/679 (hierna te noemen: AVG) , en zij daarmee optreedt als verwerker;
- 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: