

**Contactgegevens Opdrachtnemer**

5.1.2.e

**Contactgegevens Hulpleveranciers mits goedgekeurd door de Politie**

&lt;bedrijfsnaam, adres en contactgegevens van de contactpersoon van Hulpleverancier&gt;

**Technische en organisatorische beveiligingsmaatregelen**

Opdrachtnemer en diens Hulpleverancier in het bezit te zijn van het omschreven in Bijlage 3, Beveiligingsaanpak.

2. De organisatorisch en en technische beveiligingsmaatregelen omvatten in ieder geval:
- a. Maatregelen om te waarborgen dat enkel bevoegd Personeel van Opdrachtnemer toegang heeft tot de Persoonsgegevens en/of Politiegegevens voor het doel dat is uiteengezet in Bijlage 1 van de Verwerkersovereenkomst;
  - b. Maatregelen waarbij Opdrachtnemer zijn Personeel en Hulpleveranciers uitsluitend toegang geeft tot Persoonsgegevens en/of Politiegegevens via op naam gestelde accounts, waarbij het gebruik van die account adequaat gelogd wordt en waarbij de betreffende account alleen toegang geven tot die Persoonsgegevens en/of Politiegegevens waartoe de toegang noodzakelijk is;
  - c. Maatregelen om de Persoonsgegevens en/of Politiegegevens te beschermen tegen onopzettelijk of onrechtmatige vernietiging, onopzettelijk verlies of wijziging, onbevoegde of onrechtmatige opslag, verwerking, toegang of openbaarmaking;
  - d. Maatregelen om zwakke plekken te identificeren ten aanzien van de verwerking van Persoonsgegevens en/of Politiegegevens in de systemen die worden ingezet voor het verlenen van de diensten aan de Politie;
  - e. Maatregelen om de tijdige beschikbaarheid van de gegevens te garanderen die benodigd zijn voor het uitvoeren van de Overeenkomst.

## 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

**Bijlage 3 Security & Privacy**

Zie paragraaf 1.4. en 3.4. in Bijlage 3 – Service Level Agreement.

5.1.2.i

A large rectangular area of the document is redacted with a solid grey fill. It starts at the level of the first '5.1.2.i' heading and extends across the width of the main content area.

5.1.2.i

A rectangular area of the document is redacted with a solid grey fill. It starts at the level of the second '5.1.2.i' heading and extends across the width of the main content area.

**Processors'**  
**Agreement**  
**ARBIT**  
Effective date:

Published by: Police, Police Services Centre - Procurement Service

Data: Procurement Management

Status: Final

Version: 1.0

Version date: 3 June 2020

# Table of Contents

|            |                                                                         |           |
|------------|-------------------------------------------------------------------------|-----------|
| <b>1.</b>  | <b>Definitions</b>                                                      | <b>5</b>  |
| <b>2.</b>  | <b>Formation, duration and termination of the Processor's agreement</b> | <b>5</b>  |
| <b>3.</b>  | <b>Object of the Processor's Agreement</b>                              | <b>5</b>  |
| <b>4.</b>  | <b>Applicable Conditions</b>                                            | <b>7</b>  |
| <b>5.</b>  | <b>Continuing obligations</b>                                           | <b>7</b>  |
| <b>6.</b>  | <b>Return of Personal Data and/or Police Data</b>                       | <b>7</b>  |
| <b>7.</b>  | <b>Intellectual property rights</b>                                     | <b>7</b>  |
| <b>8.</b>  | <b>Security</b>                                                         | <b>7</b>  |
| <b>9.</b>  | <b>Obligation to report Data Breaches and security breaches</b>         | <b>8</b>  |
| <b>10.</b> | <b>Confidentiality, availability and integrity</b>                      | <b>8</b>  |
| <b>11.</b> | <b>Audit</b>                                                            | <b>9</b>  |
| <b>12.</b> | <b>Informing Data Subjects</b>                                          | <b>9</b>  |
| <b>13.</b> | <b>Liability</b>                                                        | <b>10</b> |
| <b>14.</b> | <b>Measures of the supervisory authority</b>                            | <b>10</b> |
| <b>15.</b> | <b>Change</b>                                                           | <b>10</b> |
| <b>16.</b> | <b>Final provisions</b>                                                 | <b>10</b> |

## Processor's Agreement

concerning the Agreement <> <sup>5.1.2.i</sup>

a) with the additional applicability of ARBIT-2018

b) Reference number: <sup>5.1.2.i</sup>

### The signatories:

**1. Police, established in The Hague, represented by the Chief of Police, on behalf of this Mrs. P.F. Bosman, Director of the Police Services Centre, hereinafter to be referred to as: Contracting Authority**

and

**2. <sup>5.1.2.i</sup>, having its registered office at <sup>5.1.2.i</sup>  
represented by <sup>5.1.2.e</sup>,  
, hereinafter referred to as: Contractor,**

hereinafter to be referred to jointly as: "Parties";

### WHEREAS:

- the Parties have concluded the Agreement on <sup>5.1.2.i</sup> with reference <sup>5.1.2.i</sup> (hereinafter referred to as: the Agreement);
- in the context of the performance of this Agreement, Personal Data is processed within the meaning of Article 4(1) General Data Protection Regulation EU 2016/679 (hereinafter to be referred to as: GDPR) and/or Police Data within the meaning of Article 1(a) of the Police Data Act (Wet Politiegegevens, Wpg);
- in the performance of the Agreement with the Police, the Contractor processing Personal Data and/or Police Data is to be designated as a Processor within the meaning of the GDPR and/or Police Data Act (Wpg);
- as Contracting Authority, the Police is the Controller for Personal Data and Police Data;
- by means of this Processor's Agreement, Parties wish to record further agreements about the processing of the Personal Data and/or Police Data by Contractor as Processor, along with the applicable legal obligations from the GDPR and/or Police Data Act (Wpg), including the obligation to make notification of Data Breaches;

### AGREE AS FOLLOWS:

## 1. Definitions

As a supplement to the GDPR and Police Data Act (Wpg), the terms and concepts designated by a capital letter before and after in this Processor's Agreement carry the following meaning:

1. AP: Autoriteit Persoonsgegevens (<https://autoriteitpersoonsgegevens.nl>)
2. GDPR: General Data Protection Regulation EU 2016/679.
3. Data Subject: the person to whom the Personal Data relates.
4. Data Breach: a security breach within the meaning of Articles 33 and 34 GDPR resulting in a considerable risk of seriously adverse effects and/or serious adverse consequences for the protection of Personal Data and/or Police Data, including breaches of confidentiality, loss or change of data.
5. Support supplier: a party or third-party hired by the Contractor to support in the execution of the Agreement. If the Support Supplier processes Personal Data and/or Police Data on behalf of the Contractor, then the Support Supplier is also considered to be a subprocessor.
6. Agreement: the agreement on <sup>5.1.2.1</sup> [redacted] with reference <sup>5.1.2.1</sup> [redacted], in which the Police wishes to have Personal Data and/or Police Data falling under its responsibility processed by the Contractor.
7. Party: The Police or Contractor, depending on the context.
8. Processor's agreement: this agreement including considerations and associated annexes.
9. Wpg: Wet Politiegegevens (Police Data Act).

## 2. Formation, duration and termination of the Processor's agreement

- 2.1 This Processor's Agreement goes into effect after signature by both Parties and no earlier than on the date on which the Agreement goes into effect.
- 2.2 This Processor's Agreement shall be in force throughout the duration of the Agreement. If the Agreement terminates, then this Processor's Agreement legally terminates.
- 2.3 Neither of the Parties can cancel this Processor's Agreement prematurely.

## 3. Object of the Processor's Agreement

- 3.1 Contractor processes solely the category of Personal Data and/or Police Data of the Police described in **Annex 1** on behalf of the Police for the purpose stated therein.
- 3.2 Contractor shall Process the Personal Data and/or Police Data in a proper and careful manner and in accordance with the GDPR, Police Data Act (Wpg) and other applicable regulations concerning the Processing of Personal Data.
- 3.3 Contractor shall Process Personal Data and/or Police Data only on behalf of the Police to the extent necessary to provide the services described in the Agreement to the Police and shall follow all written instructions from the Police in this regard, except in instances involving deviating legal obligations.
- 3.4 Contractor has no control over the purpose and means for the Processing of Personal Data and/or Police Data. Unless stated otherwise in this Processor's Agreement, Contractor shall make no decisions about the use of the Personal Data/Police Data, its provision to third parties or about the duration of storage of Personal Data and/or Police Data. The control over the Personal Data and/or Police Data under the terms of this Processor's Agreement shall never rest with Contractor.
- 3.5. Contractor shall not hire Support Suppliers without prior written permission from the Police.

Permission given by the Police for hiring Support Suppliers shall be subject in any case to the following conditions:

- a. Contractor has concluded a written agreement with the particular Support supplier which contains at least the following:
  - an obligation that the Support supplier must act in accordance with all provisions in this Processor's Agreement;
  - an obligation that the Support Supplier follows all instructions related to the processing of Personal Data and/or Police Data given by the Police and by the Contractor, including the obligation to maintain confidentiality and to take the required security measures as described in **Annex 1**;
  - a commitment from the Support Supplier to process the Personal Data and/or Police Data solely on behalf of and according to the instructions of Contractor;
  - a commitment from the Support Supplier not to hire subcontractors itself without prior written permission from the Police;
  - an obligation that the Support Supplier enables the Contractor (and, with this, the Police) to comply with its obligations in the event of a suspected or actual Data Breach.
- b. Contractor shall provide Support Supplier access to the Personal Data and/or Police Data only after written permission from the Police; and
- c. The Police are entitled upon first request to view the agreements made between Contractor and the Support Supplier. No later than 30 days after the receipt of this request, Contractor shall provide a copy to the Police.

The permission provided by the Police is without prejudice to the responsibility and liability of Contractor for compliance with its obligations under the terms of the Processor's Agreement.

- 3.6 Contractor is expressly not permitted to provide Personal Data and/or Police Data to others, unless this is done by at the written request of the Police, or with that party's written permission. After having been granted permission, Contractor is obliged to confirm in writing that this provision has taken place, such that within 30 days exactly, the Contractor must provide documentation to the Police describing the Personal Data and/or Police Data provided, the Data Subject(s), the recipient(s) and the moment of provision.
- 3.7 If Contractor must provide information on the basis of a legal obligation, then Contractor shall verify the principle underlying the request and the identity of the requesting party and the Contractor shall inform the Police of this immediately, prior to the provision of the information if possible.
- 3.8 Contractor shall provide complete cooperation to the Police to satisfy the obligations within the legal deadlines on grounds of the GDPR and/or Police Data Act (Wpg), more particularly the rights of Data Subjects, including but not limited to a request for access to, rectification, supplementation, deletion or restriction of Personal Data and/or Police Data and the performance of a remanded defence that has been granted.
- 3.9 If Contractor notes unlawful Processing or breach of the security measures stated in article 8.1 of this Processor's Agreement, then the Contractor shall notify the Police of this immediately and shall take all reasonable and necessary efforts to terminate, prevent or limit this and any further unlawful Processing or breaches, and all this without prejudice to Contractor's obligation to compensate for any direct damages suffered in this regard by the Police in accordance with article 19.2 of the Agreement.
- 3.10 Any costs associated with articles 3.8, 3.9 and article 9 of this Processor's Agreement shall be borne by the party who incurs those costs.
- 3.11 The Police and Contractor ensure that the Data Protection Officer is properly involved in a timely manner with all occasions related to the protection of Personal Data and/or Police Data.
- 3.12 Contractor shall document all breaches described in Article 33(5) GDPR.

- 3.13 Contractor shall provide all required cooperation in the context of evaluating the effects of data protection in the context of Article 35 GDPR. The Police shall owe no (additional) compensation to Contractor for the provision of this cooperation.

## 4. Applicable Conditions

The provisions of the Agreement apply to this Processor's Agreement except in the event of deviations from this in this Processor's Agreement.

## 5. Continuing obligations

As a supplement to article 34 of the ARBIT-2018, after the termination of the Agreement and the Processor's Agreement, the Contractor's current obligation shall remain in force, including but not limited to transfer, signalling unauthorised Processing and confidentiality, in addition to any further provisions in articles 3.8, 3.9, 8, 9 and 10 of this Processor's Agreement.

## 6. Return of Personal Data and/or Police Data

- 6.1 After the termination of the Agreement and the Processor's Agreement, all Personal Data and/or Police Data, copies of this and alterations of this, along with any data media which contain or will contain Personal Data and/or Police Data, copies or alterations of this must be returned to the Police immediately upon first request or provided to the Police (or be returned to a third party to be designated by the Police), or must be destroyed – such at the discretion of the Police. As necessary, the Police can place additional requirements on the method of availability, including requirements concerning file formats, or destruction. The moment that this Processor's Agreement ends, Contractor shall also cooperate with the transfer of the work activities concerning the Processing of Personal Data and/or Police Data to the Police or to a successor contractor and, indeed, in such a way that, starting for the moment that the transfer takes place, continuity of the provision of services remains safeguarded to the maximum extent, or at least that it is not hindered by the acts or omissions of Contractor.
- 6.2 The costs associated with the Contractor's efforts as referred to in 6.1, shall be borne by the Police wherever these costs are not included in the Contractor's agreed prices and compensations pursuant to the performance of the Agreement.
- 6.3 Contractor shall guarantee the portability of data as described above in article 6.1 in such a way that there can be no loss of functionality or of (parts of) the data.

## 7. Intellectual property rights

With reference to article 8 of the ARBIT-2018, all (intellectual) property rights – including copyrights and database rights – to the collection of Personal Data and/or Police Data, copies or alterations of these are retained at all times by the Police or its licensor(s).

## 8. Security

- 8.1 Supplementary to article 18.1 of the ARBIT-2018, Contractor shall implement all technical and organisational security measures as described in Annexe 1. Taking the state of technology and the costs associated with the implementation and execution of the measures

into account, these measures shall ensure an appropriate level of protection; this shall take the risks into account that are associated with the processing of Personal Data and/or Police Data and the nature of this.

- 8.2 Contractor shall report to the Police periodically, with a frequency of once each year and no later than on 31 December, about the measures taken by the Contractor concerning the technical and organisational security measures and any focal points in these.
- 8.3 The costs associated with the reporting shall be borne by Contractor.
- 8.4 Contractor does not process Personal Data and/or Police Data outside a member state of the European Union and/or European Economic Area (Norway, Liechtenstein and Iceland).

## 9. Obligation to report Data Breaches and security breaches

- 9.1 In the event of a suspected or actual (i) Data Breach; (ii) breach of security measures; (iii) breach of the obligation of confidentiality or (iv) loss of confidential information, Contractor shall inform the Police immediately, or at least within 24 hours after the first discovery of the incident. Contractor shall take all reasonably necessary measures to prevent or to limit any (further) unauthorised access, change or provision or otherwise illegal processing and to terminate any breach of security measures or of the obligation of confidentiality and any further loss of confidential information and to prevent this in the future, without prejudice to any right on the part of the Police to compensation of damages or other measures, to the extent that the incident is attributable to Contractor or to any Support supplier it hires. This provision applies to incidents at the Contractor and any of its Support suppliers.
- 9.2 In any case, the information from the Contractor comprises the data described in **Annex 2** to the extent applicable. Contractor guarantees that the information provided is complete, correct and accurate.
- 9.3 At the request of the Police, Contractor shall cooperate with informing the competent authorities and data subject(s).

## 10. Confidentiality, availability and integrity

- 10.1 With reference to article 17.1 of the ARBIT-2018, Contractor is obliged to maintain the confidentiality, safeguarding the availability and integrity of all Personal Data and/or Police Data and information that he processes pursuant to this Processor's Agreement, except to the extent that Personal Data and/or Police Data is apparently not secret or of a confidential nature, or if it is already generally known.
- 10.2 If and to the extent the Police requests these expressly and in writing, Contractor shall take special measures with respect to the Personal Data and/or Police Data or information designated in this with regard to maintaining its confidentiality; among other things, these measures can include the destruction of the Personal Data and/or Police Data or information involved once the Police's need to access this has lapsed.
- 10.3 With reference to article 17.2 of the ARBIT-2018, Contractor shall require in its employment contracts or secondment contracts with Contractor's Personnel that those persons shall also attempt to maintain confidentiality with respect to all Personal Data and/or Police Data and information that they process in the context of their work activities in a manner corresponding with articles 10.1 and 10.2. Contractor guarantees to the Police that the intended provisions shall be adhered to by the persons involved.
- 10.4 This article 10 and the confidentiality discussed there in remain in force after the termination of the Agreement and this Processor's Agreement.

## 11. Audit

- 11.1 The Police shall audit the following (or have this be audited) at any moment it so desires:
  - a. the processing and compliance with the agreed technical and organisational security measures by Contractor or by Support Suppliers hired by Contractor, and
  - b. compliance with the information stated in **Annex 2** required to comply with the obligation of notification referred to in Article 34 GDPR.
- 11.2 Contractor shall provide a statement to the Police from an independent external expert at least once each year, no later than 31 December, in which this expert provides an assessment of the stated compliance as referred to in article 11.1 a and b.
- 11.3 Contractor shall provide all reasonable and necessary cooperation to the audit and shall ensure that the Support suppliers he has hired shall provide the reasonable and necessary cooperation for this.
- 11.4 The performance of an audit shall not result in any delay of the work activities performed by Contractor in the context of the Agreement and this Processor's Agreement. Should this nonetheless be the case, then Parties shall consult with each other for purposes of finding a solution as quickly as possible.
- 11.5 The costs associated with the audit shall be borne by the Police unless the audit reveals that Contractor evinces shortcomings in his compliance with his obligation(s) pursuant to this Processor's Agreement and/or the Agreement.
- 11.6 Contractor shall perform the recommendations for improvement indicated by the Police within a deadline to be established by the Police.

## 12. Informing Data Subjects

- 12.1 Contractor shall provide its full cooperation so that the Police can comply with its legal obligations in the event that a Party Involved exercises its rights on grounds of the GDPR, Police Data Act (Wpg) or other applicable regulations concerning the processing of Personal Data and/or Police Data.
- 12.2 Should a Party Involved contact the Contractor directly with regard to the exercise of his rights pursuant to the GDPR and/or Police Data Act (Wpg), the Contractor will proceed - unless explicitly instructed otherwise by the Police - in the first instance but shall inform the Police of this immediately with the request for further instructions.
- 12.3 If the Contractor offers its services in the context of the Agreement directly to Data Subjects, then Contractor is obliged to inform the Police in an easily accessible and permanently available manner, of the following:
  - a. the name and address of the Contractor;
  - b. the purposes for which Contractor processes the Personal Data and/or Police Data;
  - c. the categories of Personal Data and/or Police Data that the Contractor processes;
  - d. the third parties to whom access is given to the Personal Data and/or Police Data;
  - e. the countries to which the Personal Data and/or Police Data is transferred;
  - f. the right to access, correct and remove the Personal Data and/or Police Data.

The Contractor shall let the Police know where this information is published.

## 13. Liability

Notwithstanding the provision of article 26 of the ARBIT-2018 and in accordance with Article 83 GDPR, Contractor is liable for any administrative penalty charged by the AP or for damages incurred by Parties Involved or by the Police, as long as that administrative penalty or the damages suffered are the result of attributable shortcomings in Contractor's compliance with its obligations or those of its Support supplier(s).

## 14. Measures of the supervisory authority

If in the context of its task as an enforcer, the AP places a penalty or a measure on the Police and if the cause of the occurrence of the penalty or measure is attributable to non-compliance with the agreements made in the Processor's Agreement by Contractor or its Support Supplier, then the Police can recover all of the costs for this penalty or measure from Contractor. The Police are also entitled to dissolve the Agreement with immediate effect in this instance without Contractor being able to make claim to any form of compensation of damages.

As described in Annex 1 IDEMIA activities related to data processing will be under the supervision of the Police.

## 15. Change

- 15.1 Should a functional change in the Personal Data and/or Police Data to be processed or an audit such as the one referred to in article 11 of this Processor's Agreement give reason to do so, then Parties shall consult at the Police's first request to discuss any change to the agreements made within this Processor's Agreement.
- 15.2 The new agreements to be made must be recorded in writing prior to their application and must be part of this Processor's Agreement.
- 15.3 The changes may never result in the Police's being unable to comply with the GDPR, Police Data Act (Wpg) and other relevant laws and regulations related to Personal Data and/or Police Data.

## 16. Final provisions

- 16.1 Any deviations to the provisions in this Processor's Agreement are binding only if and to the extent these are expressly agreed in writing between Parties.
- 16.2 Any general conditions of delivery or other general or specific conditions of Contractor and its Support Supplier do not apply to this Processor's Agreement and are expressly rejected by the Police.
- 16.3 This Processor's Agreement is a supplement to the Agreement. In the event of contradiction between provisions in this Processor's Agreement and the Agreement, the provisions in this Processor's Agreement take precedence.
- 16.4 This Processor's Agreement is subject to Dutch law.

As agreed in 16 articles and two annexes on the later of the two dates stated below and signed in duplicate,

*the Contracting Authority*  
The Police,

On behalf of this party,

15 oktober 2020

5.1.2.e

P.F. Bosman, directeur PDC

*the Contractor*  
On behalf of

5.1.2.i

On behalf of this party,

5.1.2.i

5.1.2.e

5.1.2.e

## Annex 1 Work processes, authorisations and functional groups for processing

The processing by the Contractor concerns the following information:

### Categories of Data Subjects

- Suspects, convicts, former suspects
- Deceased victims of crime
- Foreign nationals
- Employees
- Users

### The (categories of) Personal Data and/or Police Data to be processed

- Biographical data on suspects, convicts, former suspects, deceased victims of crime and foreign nationals
- Biometric data (dactyloscopic and face) of suspects, convicts, former suspects, traces of unknown suspects, deceased victims of crime and foreign nationals (photo only)
- Contact details of employees and users
- User logging of users

### Purpose of the processing

1. <sup>5.1.2.i</sup> [REDACTED]

### Functional roles and/or functional groups of Contractor's Personnel and their processing activities;

- <sup>5.1.2.i</sup> [REDACTED]

### Periods of retention

For the duration of the Processor's Agreement.

### Contact details of the Contractor

<sup>5.1.2.e</sup> [REDACTED], program manager, <sup>5.1.2.e</sup> [REDACTED]

### Support Suppliers contact information - presuming approval by the Police

No support supplier

### Technical and organisational security measures

1. Contractor and his Support supplier possess\*:

\* place a checkmark next to whatever applies

☐ a written security policy in accordance with ISO 27001 concerning Information Security Management

\* ☐ a written quality policy in accordance with ISO 9001 concerning Quality Management

X different, viz.

<sup>5.1.2.i</sup> [REDACTED].

5.1.2.i

[REDACTED]

2. The organisational and technical security measures comprise in any case:

5.1  
.2.i

[REDACTED]

## Annex 2 Procedure and Measures in connection with the obligation to report data breaches

### Information that must be provided in the event of a Data Breach

In the event that the Contractor must notify the Police's Information Security Coordinator on grounds of article 5 of the Processor's Agreement, Contractor must provide the following information:

#### Contact information of the notifier

<Name, position, e-mail address, telephone number>

#### Information about the Data Breach

- Summary of the incident involving a security breach of Personal Data and/or Police Data:

<summary>

- How many Data Subjects were affected by the data breach of Personal Data and/or Police Data?

<Enter the numbers>

a) At least: <add info>

b) At most: <add info>

- Description of the group of people whose Personal Data and/or Police Data is involved in the incident

<description>

- When did the breach take place?

<Select one of the following options and supplement as necessary>

a) On <date>

b) Between <start date of the period> and <end date of the period>

c) Not yet known

- What is the nature of the breach?

<check multiple possibilities>

☐ a) Reading (confidentiality)

☐ b) Copying

☐ c) Changing (integrity)

☐ d) Deletion or destruction (availability)

☐ e) Theft

☐ f) Not yet known

- What type of Personal Data and/or Police Data is involved?

<check multiple possibilities>

☐ a) Name, address and residence information

☐ b) Telephone numbers

☐ c) E-mail addresses or other addresses for electronic communication

☐ d) Access or identification information (e.g. login name/password or client number)

☐ e) Financial information (e.g. account number, credit card number)

☐ f) Social Security number (BSN) or taxpayer ID

☐ g) Copies of passport or copies of other proofs of identification

☐ h) Gender, birth date and/or age

- ☐ i) Special Personal Data (e.g. data revealing racial or ethnic origin, criminal information, political conviction, union membership, religion, sex life, medical history): [<indicate which special Personal Data>](#)
- ☐ j) Other Data, namely [<add info>](#)

- Which consequences can the breach have for the personal lives of those involved?

[<check multiple possibilities>](#)

- ☐ a) Stigmatisation or exclusion
- ☐ b) Damage to health
- ☐ c) Exposure to (identity) fraud
- ☐ d) Exposure to spam or phishing
- ☐ e) Other, namely [<add info>](#)

#### **Follow-up actions resulting from the Data Breach**

- The following technical and organisational measures have been taken to address the breach and to prevent further breaches:

[<description>](#)

#### **Technical protective measures**

- Is the Personal Data and/or Police Data encrypted, hashed or otherwise made incomprehensible

inaccessible to unauthorised parties in another manner?

[<Select one of the following options and supplement as necessary>](#)

- ☐ a) Yes
- ☐ b) No
- ☐ c) Partially, namely: [<add info>](#)

- If the Police Data is made either entirely or partially incomprehensible or inaccessible, in what way was this done?

[<Answer this question if you chose option a or c for the previous question. If you used encryption, then explain the method of encryption.>](#)

#### **International aspects**

- Does the breach involve persons in other EU countries?

[<Select one of the following options>](#)

- ☐ a) Yes
- ☐ b) No
- ☐ c) Not yet known

