5.1.2.i

Report

Regarding	5.1.2.i
On behalve of	5.1.2.e and 5.1.2.e
School/ bedrijf:	Police Academy The Netherlands
Betrokkenen extern	
Datum	May 11, 2017
by	5.1.2.e
remarks	Privay shield Restricted access

5.1.2.i

5.1.2.i

DATA PROCESSING ADDENDUM

What is the 5.1.2.i Data Processing Addendum?

5.1.2.i provides a data processing addendum to help customers meet their data protection obligations. 5.1.2.i can also add the Standard Contractual Clauses 2010/87/EU (often referred to as "Model Clauses") to a customer's data processing addendum if the customer needs this to transfer personal data from the EU to a country outside the European Economic Area.

On March 6, 2015, the 5.1.2.i data processing addendum, including the Model Clauses, was approved by the group of EU data protection authorities known as the Article 29 Working Party. This approval means that an 5.1.2.i customer who requires the Model Clauses can now rely on the 5.1.2.i data processing addendum as providing sufficient contractual commitments to enable international data flows in accordance with the Directive. For more detail on the approval from the Article 29 Working Party, please visit the Luxembourg Data Protection Authority webpage here: 5.1.2.i

Now that the EU-U.S. Safe Harbour program has been ruled invalid, can customers still use 5.1.2.i and comply with EU law?

Security of our customers' data is our number one priority, and 5.1.2.i has already obtained approval from EU data protection authorities, known as the Article 29 Working Party, of the 5.1.2.i and Model Clauses to enable transfer of data outside Europe, 5.1.2.i With our EU-approved Data Processing Addendum and Model Clauses, 5.1.2.i customers can continue to run their global operations using AWS in full compliance with EU law. The 5.1.2.i Addendum is available to al 5.1.2.i customers that are processing personal data whether they are established in Europe or a global company operating in the European Economic Area. For additional information about EU Data Protection, please visit the 5.1.2.i 5.1.2.i

How can customers enter into a Data Processing Addendum with AWS?

The 5.1.2.i with Model Clauses is available on a self-service basis for customers that are processing personal data on 5.1.2.i

5.1.2.i

Customers can obtain the 5.1.2.i with Model Clauses here.
For the 5.1.2.i to be effective, customers must following the instructions provided on the cover page of 5.1.2.i Please note that customers need to log in to their 5.1.2.i account to obtain the

Based on Customers can obtain the 5.1.2.i here.

[redacted]

[redacted]ATA PROCESSING ADDENDUM

This Data Processing Addendum (this "**Addendum**") is made and entered into by and between [redacted] Delaware corporation [redacted] and the customer specified in the table below ("**Customer**").

[redacted]	Custo[redacted]
Signature Date: December 14, 2016 **Address:** [redacted]	**By (Si[redacted]** **Your F[redacted]** **Your T[redacted]** **Signat[redacted]** **Custo[redacted]** **Attention:**

This Addendum includes the Data Processing Terms and the attached Annexes 1-2 and supplements the [redacted] Agreement available at [redacted] (as updated from time to time) between Customer and [redacted] or other agreement between Customer and [redacted] governing Customer's use of the Service Offerings (the "**Agreement**"). This Addendum will be effective as of the day AWS receives a complete and executed Addendum from Customer in accordance with the instructions under paragraphs 1 and 2 below (the "**Addendum Effective Date**").

1. **Instructions.** This Addendum (including the Standard Contractual Clauses, as defined below) has been pre-signed on behalf of [redacted] To enter into this Addendum, Customer must:

   a. Complete the table above by signing and providing the customer full legal entity name, address and signatory information; and

   b. Submit the completed and signed Addendum t[redacted]ia email t[redacted]

2. **Effectiveness.**

   a. This Addendum will be effective only if it is executed and submitted to [redacted] n accordance with paragraph 1 above and this paragraph 2, and all items identified as "Required" in the table are completed accurately and in full. If Customer makes any deletions or other revisions to this Addendum, then this Addendum will only apply to Customer's use of [redacted] accounts (including any use by agents or subcontractors (including any of its affiliates who are acting as an agent or subcontractor of Customer) performing work on behalf of Customer) that include the Customer's full legal entity name (matching the one provided in the table above) in the "Company Name" field associated with the [redacted] account. If Customer has affiliates with their own [redacted] accounts that need coverage under an [redacted] order to have coverage each affiliate must sign its own [redacted] with [redacted] n which case, the full legal entity name entered in the "Company Name" field associated with the [redacted] ccount will be the name of the affiliate.

   b. This Addendum applies only to [redacted] purchased from [redacted] and does not apply to [redacted] Customer purchases from any seller of record other than [redacted] ncluding [redacted] alue-added resellers.

   c. Customer signatory represents t[redacted] that he or she has the legal authority to bind Customer and is lawfully able to enter into contracts (e.g., is not a minor).

   d. This Addendum will terminate automatically upon termination of the Agreement, or as earlier terminated pursuant to the terms of this Addendum.

[redacted]

Data Processing Terms

1. **Definitions.** Unless otherwise defined in the Agreement, all capitalized terms used in this Addendum will have the meanings given to them below:

means the data center facilities, servers, networking equipment, and host software systems (e.g., virtual firewalls) that are within control and are used to provide the Services.

means the security standards attached to this Addendum as Annex 1.

"**Customer Data**" means the "personal data" (as defined in the Directive) that is uploaded to the Services under Customer accounts.

"**Directive**" means Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and any replacement directive or regulation imposing equivalent obligations.

"**EEA**" means the European Economic Area.

"**processing**" has the meaning given to it in the Directive and "process", "processes" and "processed" will be interpreted accordingly.

"**Standard Contractual Clauses**" means Annex 2 attached to and forming part of this Addendum pursuant to the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under the Directive.

2. **Data Processing.**

2.1 **Scope and Roles.** This Addendum applies when Customer Data is processed by AWS. In this context, Customer may act as "controller" or "processor" and AWS may act as "processor" or "sub-processor" with respect to Customer Data (as each term is defined in the Directive).

2.2 **Compliance with Laws.** Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this Addendum, including all statutory requirements relating to data protection.

2.3 **Instructions for Data Processing** will process Customer Data in accordance with Customer's instructions. The parties agree that this Addendum is Customer's complete and final instructions to AWS in relation to processing of Customer Data. ing outside the scope of this Addendum (if any) will require prior written agreement betwee and Customer on additional instructions for processing, including agreement on any additional fees Customer will pay to or carrying out such instructions. Customer may terminate this Addendum if declines to follow instructions requested by Customer that are outside the scope of this Addendum.

2.4 **Access or Use** will not access or use Customer Data, except as necessary to provide the Service Offerings initiated by Customer.

2.5 **Disclosure.** will not disclose Customer Data to any government, except as necessary to comply with the law or a valid and binding order of a law enforcement agency (such as a subpoena or court order). If a law enforcement agency sends demand for Customer Data, will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, then will give Customer reasonable Notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless s legally prohibited from doing so.

2.6 restricts its personnel from processing Customer Data without authorisation by AWS as described in the will impose appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security

2.7 **Customer Controls.** The Service Offerings provide Customer with controls to enable Customer to retrieve, correct, delete, or block Customer Data as described in the Documentation. makes available a number of security features and functionalities that Customer may elect to use. Customer is responsible for properly (a) configuring the Service Offerings, (b) using the controls available in connection with the Service Offerings (including the security controls), and (c) taking such steps as Customer considers adequate to maintain appropriate security, protection, deletion and backup of Customer Data, which may include use of encryption technology to protect Customer Data from unauthorized access and routine archiving of Customer Data.

2.8 **Transfers of Personal Data.**

2.8.1 **Regions.** Customer may specify egion(s) where Customer Data will be processed within including the EU (Dublin) Region, the EU (Frankfurt) Region and the EU (London) Region (each a "**Region**"). Once Customer has made its choice, will not transfer Customer Data from Customer's selected Region(s) except as necessary to comply with the law or a valid and binding order of a law enforcement agency (such as a subpoena or court order) as described in Section 2.5.

2.8.2 **Application of Standard Contractual Clauses.** The Standard Contractual Clauses will apply to Customer Data that is transferred outside the EEA, either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the Directive). The Standard Contractual Clauses will not apply to Customer Data that is not transferred, either directly or via onward transfer, outside the EEA. Notwithstanding the foregoing, the Standard Contractual Clauses will not apply: (a) if s acting as a sub-processor (as defined in the Standard Contractual Clauses) with respect to Customer Data, or (b) if has adopte or an alternative recognized compliance standard for the lawful transfer of personal data (as defined in the Directive) outside the EEA.

3. Security Responsibilities of AWS

3.1 is responsible for implementing and maintaining the technical and organisational measures for the as described in the Security Standards and this Section of this Addendum designed to help Customer secure Customer Data against unauthorized processing and accidental or unlawful loss, access or disclosure.

3.2 The technical and organisational measures include the following:

(i) AWS has implemented and will maintain measures to maintain the physical security of the Facilities as set out in Section 1.2 of the Security Standards;

(ii) has implemented and will maintain measures to maintain the security of the as set out in Section 1.1 of the ecurity Standards;

(iii) has implemented and will maintain measures to control access rights fo employees and contractors in relation to the AWS Network as set out in Section 1.1 of the Security Standards. Customer has implemented and will maintain measures to control access rights to Customer Data; and

(iv) will process Customer Data in accordance with Customer's instructions as described in Section 2.3 of this Addendum.

4. Certifications.

4.1 As of the Addendum Effective Date, is certified under ISO 27001 and agrees to maintain an information security program for the Services that complies with the ISO 27001 standards or such other alternative standards as are substantially equivalent to ISO 27001 for the establishment, implementation, control, and improvement of the ecurity Standards.

4.2 Customer is solely responsible for reviewing the information made available by relating to data security and making an independent determination as to whether the Services meet Customer's requirements, and for ensuring that Customer's personnel and consultants follow the guidelines they are provided regarding data security.

5. Audit of Technical and Organisational Measures.

5.1 uses external auditors to verify the adequacy of its security measures, including the security of the physical data centers from which provides the Services. This audit: (a) will be performed at least annually; (b) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001; (c) will be performed by independent third party security professionals a selection and expense; and (d) will result in the generation of an audit report ("**Report**"), which will be Confidential Information. If Customer's Agreement does not include a provision protecting Confidential Information, then Reports will be made available to Customer subject to a mutually agreed upon non-disclosure agreement covering the Report (an "**NDA**").

5.2 At Customer's written request, will provide Customer with a confidential Report so that Customer can reasonably verify compliance with the security obligations under this Addendum. The Summary Report will constitute Confidential Information under the confidentiality provisions of the Agreement or the NDA, as applicable.

5.3 If the Standard Contractual Clauses apply, then Customer agrees to exercise its audit right by instructing to execute the audit as described in this Section of the Addendum. If Customer has not opted out of the Standard Contractual Clauses and desires to change this instruction regarding exercising this audit right, then Customer has the right to change this instruction, as mentioned in the Standard Contractual Clauses, which shall be requested in writing. If the Standard Contractual Clauses apply, then nothing in this Section of the Addendum varies or modifies the Standard Contractual Clauses nor affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses.

6. Security Breach Notification.

6.1 If becomes aware of either (a) any unlawful access to any Customer Data stored on equipment or in facilities; or (b) any unauthorized access to such equipment or facilities, where in either case such access results in loss, disclosure, or alteration of Customer Data (each a "**Security Incident**"), will promptly: (a) notify Customer of the Security Incident; and (b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

6.2 Customer agrees that:

(i) an unsuccessful Security Incident will not be subject to this Section. An unsuccessful Security Incident is one that results in no unauthorized access to Customer Data or to any of equipment or facilities storing Customer Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond IP addresses or headers) or similar incidents; and

(ii) obligation to report or respond to a Security Incident under this Section is not and will not be construed as an acknowledgement by of any fault or liability of with respect to the Security Incident.

6.3 Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's administrators by any means selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on the management console at all times.

7. Subcontracting.

7.1 **Authorised Subcontractors.** Customer agrees that AWS may use subcontractors to fulfil its contractual obligations under this Addendum or to provide certain services on its behalf, such as providing support services. The 5.1.2.i website lists subcontractors that are currently authorized by 5.1.2.i to access Customer Data. At least 30 days before 5.1.2.i authorizes and permits any new subcontractor to access Customer Data 5.1.2.i will update the applicable website. If Customer does not approve of a new subcontractor, then without prejudice to any termination rights Customer has under the Agreement and subject to the applicable terms and conditions, Customer may move the Customer Data to another 5.1.2.i where the new subcontractor who is not approved by Customer is not an authorized subcontractor. Customer hereby consents to 5.1.2.i use of subcontractors as described in this Section 7. Except as set forth in this Section 7, or as Customer may otherwise authorize, 5.1.2.i will not permit any subcontractor to access Customer Data.

7.2 **Subcontractor Obligations.** Where 5.1.2.i authorises any subcontractor as described in this Section 7:

(i) 5.1.2.i will restrict the subcontractor's access to Customer Data only to what is necessary to maintain the Service Offerings or to provide the Service Offerings to Customer and any End Users in accordance with the Documentation and 5.1.2.i will prohibit the subcontractor from accessing Customer Data for any other purpose;

(ii) 5.1.2.i will impose appropriate contractual obligations in writing upon the subcontractor that are no less protective than this Addendum, including relevant contractual obligations regarding confidentiality, data protection, data security and audit rights; and

(iii) 5.1.2.i will remain responsible for its compliance with the obligations of this Addendum and for any acts or omissions of the subcontractor that cause 5.1.2.i to breach any of 5.1.2.i obligations under this Addendum.

8. Duties to Inform. Where Customer Data becomes subject to confiscation during bankruptcy or insolvency proceedings, or similar measures by third parties while being processed by 5.1.2.i will inform Customer without undue delay. 5.1.2.i will, without undue delay, notify all relevant parties in such action (e.g. creditors, bankruptcy trustee) that any Customer Data subjected to those proceedings is Customer's property and area of responsibility and that Customer Data is at Customer's sole disposition.

9. Nondisclosure. Customer agrees that the details of this Addendum are not publicly known and constitute 5.1.2.i Confidential Information under the confidentiality provisions of the Agreement or NDA. If the Agreement does not include a confidentiality provision protecting 5.1.2.i Confidential Information and Customer and 5.1.2.i or its affiliates do not have an NDA in place covering this Addendum, then Customer will not disclose the contents of this Addendum to any third party except as required by law.

10. Entire Agreement; Conflict. Except as amended by this Addendum, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this Addendum, the terms of this Addendum will control.

[Remainder of Page Intentionally Left Blank]

5.1.2.i

Annex 1

5.1.2.i

1. **Information Security Program.** 5.1.2.i will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help Customer secure Customer Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the 5.1.2.i and (c) minimize security risks, including through risk assessment and regular testing. 5.1.2.i will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:

   1.1 **Network Security.** The 5.1.2.i will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. 5.1.2.i will maintain access controls and policies to manage what access is allowed to the 5.1.2.i from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls 5.1.2.i will maintain corrective action and incident response plans to respond to potential security threats.

   1.2 **Physical Security**

      1.2.1 **Physical Access Controls.** Physical components of th 5.1.2.i are housed in nondescript facilities (the "**Facilities**"). Physical barrier controls are used to prevent unauthorized entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor is at any of the Facilities, and are continually escorted by authorized employees or contractors while visiting the Facilities.

      1.2.2 **Limited Employee and Contractor Access.** 5.1.2.i provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of 5.1.2.i or its affiliates.

      1.2.3 **Physical Security Protections.** All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. 5.1.2.i also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.

2. **Continued Evaluation.** 5.1.2.i will conduct periodic reviews of the security of it 5.1.2.i and adequacy of its information security program as measured against industry security standards and its policies and procedures. 5.1.2.i will continually evaluate the security of its 5.1.2.i and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

[Remainder of Page Intentionally Left Blank]

5.1.2.i [redacted]

Annex 2

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

The entity identified as "Customer" in the Addendum
(the "**data exporter**")

and

5.1.2.i [redacted]

(the "**data importer**")

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

5.1.2.i [redacted]

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) *'the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

5.1.2.i [redacted]

5.1.2.i [redacted]

5.1.2.i [redacted]

5.1.2.i [redacted]

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

5.1.2.i

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

***Obligations of the data importer*[1]**

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

---

1 Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

5.1.2.i

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the

data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

5.1.2.i [redacted]

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

5.1.2.i [redacted]

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

Data exporter

The data exporter is the entity identified as "Customer" in the Addendum

Data importer

The data importer is 5.1.2.i [redacted] Inc., a provider of web services.

Data subjects

Data subjects include the data exporter's customers and end-users.

Categories of data

The personal data relating to individuals which is uploaded onto 5.1.2.i [redacted] Services by the data exporter.

Processing operations

The personal data transferred will be subject to the following basic processing activities (as applicable):

Compute, Storage and Content Delivery on the 5.1.2.i [redacted] Network

5.1.2.i [redacted]

5.1.2.i [redacted]

5.1.2.i [redacted]

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties. By signing the signature page on page 1 of this Addendum, the parties will be deemed to have signed this Appendix 2.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The technical and organisational security measures implemented by the data importer are as described in the Addendum.

Vewerkersovereenkomst [redacted]

1Verwerkersovereenkomst Politie - 2017
Contractnummer: [redacted]

De ondergetekenden:

1. De Politie, gevestigd te Den Haag,
te dezen vertegenwoordigd door de korpschef van politie,
namens deze, De directeur PDC,
Namens deze,
Hoofd bedrijfsvoering ODPA, [redacted]
hierna te noemen: Opdrachtgever,

en

2. [redacted]
(statutair) gevestigd [redacted]
te dezen vertegenwoordigd door [redacted]
hierna te noemen: Opdrachtnemer,

hierna gezamenlijk te noemen: Partijen;

OVERWEGENDE DAT:

- Opdrachtgever met Opdrachtnemer op 9 februari 2017 een Overeenkomst tot het leveren en implementeren van [redacted] ten behoeve van de Politieacademie (hierna te noemen: de Overeenkomst) heeft gesloten;
- in het kader van de uitvoering daarvan Persoonsgegevens in de zin van artikel 1, onder a, van de Wet bescherming persoonsgegevens (hierna te noemen: Wbp) worden verwerkt;
- krachtens het bepaalde in artikel 1 van de Wbp is de Opdrachtgever verwerkingsverantwoordelijke voor de Persoonsgegevens en is de opdrachtnemer verwerker;
- Partijen in overeenstemming met de Wbp in deze Verwerkersovereenkomst hun afspraken over het verwerken van de Persoonsgegevens door opdrachtnemer als Verwerker wensen vast te leggen;
- deze Verwerkersovereenkomst is aan te merken als een Verwerkersovereenkomst in de zin van artikel 14, tweede lid, van de Wbp;

KOMEN OVEREEN:

1. Begrippen

De hierna en hiervoor in deze Verwerkersovereenkomst vermelde, met een hoofdletter geschreven begrippen, hebben de volgende betekenis:

1.1 Persoonsgegevens: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

1.2 Verwerking: elke handeling of elk geheel van handelingen met betrekking tot Persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen, of vernietigen van gegevens.

Paraaf Op[redacted]r: Paraaf Opdrachtnemer: [redacted]

1.3 Overeenkomst: de Overeenkomst tussen de Politie en 5.1.2.i van 9 februari 2017 inzake het leveren en implementeren van 5.1.2.i 5.1.2.i

1.4 Verwerkersovereenkomst: deze overeenkomst inclusief overwegingen en bijbehorende bijlagen.

1.5 Betrokkene: degene op wie een Persoonsgegeven betrekking heeft.

1.6 Datalek: een inbreuk op de beveiliging, in de zin van artikel 13 van de Wbp, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.

2. Totstandkoming, duur en einde van de Verwerkersovereenkomst

2.1 Deze Verwerkersovereenkomst treedt niet eerder in werking dan op de datum waarop Partijen de Overeenkomst hebben ondertekend.

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 Opdrachtgever de in Bijlage 1 beschreven Persoonsgegevens van Opdrachtgever.

3.2 Opdrachtnemer zal de Persoonsgegevens op behoorlijke en zorgvuldige wijze en in overeenstemming met de Wbp en andere toepasselijke regelgeving betreffende de Verwerking van Persoonsgegevens Verwerken.

3.3 Opdrachtnemer Verwerkt Persoonsgegevens slechts in opdracht van Opdrachtgever en volgt alle instructies van Opdrachtgever dienaangaande op, behoudens afwijkende wettelijke verplichtingen.

3.4 Opdrachtnemer heeft geen zeggenschap over het doel en de middelen voor de Verwerking van Persoonsgegevens. Voor zover niet anders is bepaald in deze Verwerkersovereenkomst, neemt Opdrachtnemer geen beslissingen over het gebruik van de Persoonsgegevens, de verstrekking aan derden en de duur van de opslag van Persoonsgegevens. De zeggenschap over de Persoonsgegevens verstrekt onder deze Verwerkersovereenkomst komt nimmer bij Opdrachtnemer te berusten.

3.5 Opdrachtnemer schakelt geen derden in zonder voorafgaande toestemming van Opdrachtgever. Opdrachtgever kan de toestemming om derden in te schakelen aan nadere voorwaarden binden.
Opdrachtnemer verzekert in ieder geval dat de derde zich richt naar de instructies van Opdrachtgever, tot geheimhouding verplicht is en de nodige beveiligingsmaatregelen ten opzichte van de gegevensverwerking neemt. Alle relevante verplichtingen uit deze Verwerkersovereenkomst voor de bescherming en beveiliging van de Persoonsgegevens worden overgenomen in de overeenkomst met de derde.

3.6 Het is Opdrachtnemer, onverminderd het bepaalde in artikel 3.7, niet toegestaan Persoonsgegevens aan anderen dan Opdrachtgever te verstrekken, tenzij op schriftelijk verzoek van Opdrachtgever, of met diens schriftelijke toestemming. Opdrachtnemer is verplicht schriftelijk te bevestigen dat een verstrekking heeft plaatsgevonden, waarbij hij exact de verstrekte Persoonsgegevens, de Betrokkene(n), de ontvanger(s) en het moment van verstrekking 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, Opdrachtgever ter zake.

3.8 Opdrachtnemer verleent Opdrachtgever volledige medewerking om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de Wbp, 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 het uitvoeren van een gehonoreerd aangetekend verzet.

3.9 Indien Opdrachtnemer onrechtmatige Verwerkingen of inbreuken op de in artikel 8.1 genoemde beveiligingsmaatregelen signaleert, zal hij Opdrachtgever hierover onverwijld 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 Opdrachtgever daardoor geleden schade te vergoeden.

3.10 Opdrachtnemer informeert Opdrachtgever onverwijld en adequaat over een Datalek. Hierna houdt Opdrachtnemer Opdrachtgever op de hoogte van nieuwe ontwikkelingen rond het Datalek, en van de maatregelen die Opdrachtnemer treft om de gevolgen van het Datalek te beperken en herhaling te voorkomen. Tevens verleent Opdrachtnemer Opdrachtgever volledige medewerking aan het voldoen aan de meldplicht van artikel 34a van de Wbp aan de Autoriteit Persoonsgegevens en de Betrokkenen. Afspraken over hoe Opdrachtnemer Opdrachtgever gaat informeren zijn opgenomen in Bijlage 3.

3.11 De eventuele met de in de artikelen 3.8 tot en met 3.10 gemoeide kosten komen voor rekening van degene die die kosten maakt.

3.12 Onverminderd het bepaalde in de Overeenkomst en artikel 49, derde lid, van de Wbp, is Opdrachtnemer aansprakelijk voor een door de Autoriteit Persoonsgegevens opgelegde bestuurlijke boete dan wel door Betrokkene(n) of Opdrachtgever 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.

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

Na afloop van de Overeenkomst en de Verwerkersovereenkomst blijven de lopende verplichtingen van Opdrachtnemer in stand, zoals, doch niet beperkt tot overdracht, signalering van ongeautoriseerde Verwerkingen en geheimhouding, als ook nader bepaald in de artikelen 3.8, 3.9, 3.10 en 9.4.

6. Teruggave Persoonsgegevens

Na afloop van de Overeenkomst en de Verwerkersovereenkomst worden alle Persoonsgegevens, kopieën en bewerkingen daarvan, alsmede alle gegevensdragers waarop de Persoonsgegevens, kopieën of bewerkingen daarvan zijn of zullen worden vastgelegd, onmiddellijk op eerste verzoek van Opdrachtgever geretourneerd c.q. verstrekt aan Opdrachtgever (of een door Opdrachtgever aan te wijzen derde), dan wel te worden vernietigd, een en ander naar keuze van Opdrachtgever. 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 aan Opdrachtgever of een opvolgende Opdrachtnemer en wel op zo een 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. De kosten gemoeid met deze inspanningen van Opdrachtnemer, komen voor rekening van Opdrachtgever voor zover deze kosten niet

inbegrepen zijn in de overeengekomen prijzen en vergoedingen van Opdrachtnemer voortvloeiende uit de uitvoering van de Overeenkomst.

7. Intellectuele eigendomsrechten

Alle (intellectuele) eigendomsrechten – daaronder begrepen auteursrechten en databankenrechten – blijven op de verzameling van Persoonsgegevens, kopieën of bewerkingen daarvan, te allen tijde berusten bij Opdrachtgever of haar licentiegever(s).

8. Beveiliging

8.1 Opdrachtnemer zal de technische en organisatorische beveiligingsmaatregelen implementeren zoals beschreven in Bijlage 2. 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 de aard daarvan, meebrengen.

8.2 Opdrachtnemer rapporteert periodiek met een frequentie van één maal per jaar, uiterlijk op 1 juli aan Opdrachtgever over de door Opdrachtnemer genomen maatregelen aangaande de getroffen technische en organisatorische beveiligingsmaatregelen en eventuele aandachtspunten daarin.
Daarnaast toont Opdrachtnemer aan dat hij voldoet aan normen op het gebied van informatiebeveiliging en/of het servicemanagementsysteem, zoals opgenomen in ISO 27001, of gelijkwaardig. Opdrachtnemer kan aan de hand van geldige certificering of een gelijkwaardig bewijsmiddel aantonen dat hij hieraan voldoet.

8.3 De met de rapportage gemoeide kosten zijn voor rekening van Opdrachtnemer.

8.4 Opdrachtnemer Verwerkt geen Persoonsgegevens buiten een lidstaat van de Europese Unie, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming heeft verkregen van Opdrachtgever.

9. Geheimhouding

9.1 Opdrachtnemer is gehouden tot geheimhouding van alle Persoonsgegevens 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.
Opdrachtnemer is bij schending van de geheimhoudingsverplichting die ingevolge deze Verwerkersovereenkomst op hem en zijn personeel rusten, aan Opdrachtgever een boete verschuldigd van € 1.250.00 per gebeurtenis.

9.2 Indien en voor zover Opdrachtgever daarom uitdrukkelijk schriftelijk verzoekt, zal Opdrachtnemer ten aanzien van de daarbij aangeduide Persoonsgegevens of informatie bijzondere maatregelen treffen met het oog op de geheimhouding daarvan, welke maatregelen onder meer kunnen inhouden de vernietiging van betrokken Persoonsgegevens of informatie zodra de noodzaak voor Opdrachtnemer om daarvan nog langer kennis te nemen, is komen te vervallen.

9.3 Opdrachtnemer zal in haar overeenkomsten met het personeel van Opdrachtnemer bedingen dat door die personen op overeenkomstige wijze als in artikel 9.1 en 9.2 bepaald geheimhouding zal worden betracht ten aanzien van alle Persoonsgegevens en informatie die zij in het kader van hun werkzaamheden voor Opdrachtnemer Verwerken.
Opdrachtnemer staat er jegens Opdrachtgever voor in dat de bedoelde bedingen door de betrokken personen zullen worden nageleefd.

9.4 Na afloop van de Overeenkomst en deze Verwerkersovereenkomst blijft dit artikel 9 en de hierin besproken geheimhouding van kracht.

10. Controle

10.1 Opdrachtgever controleert op elk door haar gewenst moment dan wel laat op elk door haar gewenst moment de Verwerkingen en de naleving van de overeengekomen technische en organisatorische beveiligingsmaatregelen van Opdrachtnemer controleren, dan wel die van door Opdrachtnemer ingeschakelde derden, en de naleving van de in bijlage 3 genoemde maatregelen, die nodig zijn om aan de meldplicht, bedoeld in artikel 34a van de Wbp, te voldoen. In ieder geval vinden de volgende controle(s) plaats:

Opdrachtnemer verstrekt met een frequentie van één maal per 2 jaar, uiterlijk op 1 juli aan Opdrachtgever een verklaring van een onafhankelijke externe deskundige (audit), waarin deze een oordeel geeft over de genoemde naleving.

10.2 Opdrachtnemer zal alle redelijkerwijs benodigde medewerking verlenen aan de controle en er voor zorg dragen ook de door hem ingeschakelde derden hiertoe de redelijkerwijs benodigde medewerking zullen verlenen.

10.3 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.

10.4 De met de controle gemoeide kosten zijn voor rekening van Opdrachtgever tenzij uit de controle blijkt dat Opdrachtnemer is tekortgeschoten in de nakoming van zijn verplichting(en) uit deze Verwerkersovereenkomst en/of de Overeenkomst.

10.5 Opdrachtnemer voert de door Opdrachtgever aangegeven aanbevelingen ter verbetering uit binnen de daartoe door Opdrachtgever te bepalen termijn.

11. Slotbepalingen

11.1 Afwijkingen van deze Verwerkersovereenkomst zijn slechts bindend voor zover zij uitdrukkelijk tussen Partijen schriftelijk zijn overeengekomen.

11.2 Algemene leveringsvoorwaarden dan wel andere algemene of bijzondere voorwaarden van Opdrachtnemer zijn niet van toepassing op deze Verwerkersovereenkomst en worden door Opdrachtgever uitdrukkelijk van de hand gewezen.

11.3 Deze Verwerkersovereenkomst vormt een aanvulling op de Overeenkomst. Bij strijdigheid tussen bepalingen uit deze Verwerkersovereenkomst en de Overeenkomst prevaleren de bepalingen uit deze Verwerkersovereenkomst.

11.4 Op deze Overeenkomst is het Nederlands recht van toepassing.

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

[redacted]]

VAN POLITIE
e directeur PDC,

ering ODPA.

[redacted], 8 december 2017

Algemeen directeur
[redacted]

Bijlagen: 3

Paraaf [redacted]ever:

Paraaf Opdrachtnemer:

Bijlage 1. De Verwerking van Persoonsgegevens (artikel 3.1)

De persoonsgegevens worden verwerkt in het kader van de verzorging van onderwijs en aanbieden van kennis vanuit Politieacademie. Hiertoe heeft de Opdrachtgever met de Opdrachtnemer de overeenkomst "Tot het leveren en implementeren van een 5.1.2.i gesloten. Er wordt gebruik gemaakt van een Elektronische Leeromgeving. Het primaire doel van de verwerking is de verzorging en de ondersteuning bij de verzorging, van het onderwijs.

5.1.2.i

5.1.2.i

Deze persoonsgegevens worden alleen gebruikt voor het ondersteunen van het onderwijsproces, er vinden met de gegevens geen verdere verwerkingen plaats.

Bijlage 2. Passende technische en organisatorische maatregelen (artikel 8.1)

5.1.2.i

5.1.2.i De leverancier dient te voldoen aan ISO 27001 certificering of gelijkwaardig, met de leverancier wordt tevens een non-disclosure agreement overeen gekomen. Medewerkers van de leverancier die met politiegegevens en persoonsgegevens in aanraking komen hebben een screening op minimaal niveau van BGO-lang gehad. Voor de niet Nederlandse medewerkers van de Leverancier en de onderaannemers wordt het 4-ogen principe gehanteerd. Dit principe houdt in dat de werkzaamheden (al dan niet op afstand) worden uitgevoerd terwijl een (gescreende) medewerker (van de Politieacademie) meekijkt. Met alle onderaannemers van 5.1.2.i wordt tevens een verwerkersovereenkomt overeengekomen. 5.1.2.i

5.1.2.i

5.1.2.i

5.1.2.i

5.1.2.i

Bijlage 3: Maatregelen in verband met de meldplicht datalekken (artikel 3.9)

Opdrachtnemer verplicht zich om aan de Opdrachtgever te melden als er zich een datalek voordoet. Deze meldplicht houdt in dat opdrachtnemer onverwijld een melding moeten doen bij de opdrachtgever zodra zij een ernstig datalek hebben. De verwerker verleent de opdrachtgever bijstand bij het doen nakomen van de wettelijke verplichtingen uit hoofde van onder andere de melding inbreuk in verband met persoonsgegevens rekening houdend met de aard van de verwerking en de hem ter beschikking staande informatie.
Opdrachtnemer legt vast welke maatregelen zijn genomen om herhaling te voorkomen.

Namen van contactpersonen bij de opdrachtgever die geinformeerd moeten worden zijn vastgelegd in een Dossier Afspraken en Procedures.

5.1.2.i [redacted]

Verwerkersovereenkomst

5.1.2.i [redacted]

t.b.v.

Politieacademie

Datum: 21 augustus 2018

5.1.2.e [redacted]

5.1.2.i

Verwerkersovereenkomst 5.1.2.i

DE ONDERGETEKENDEN:

Politieacademie, gevestigd aan de Arnhemseweg 348 te Apeldoorn, rechtsgeldig vertegenwoordigd door 5.1.2.e **staf de** 5.1.2.e **namens de directie van de ZBO Politieacademie** (hierna: "**Verwerkingsverantwoordelijke**");

en

5.1.2.i gevestigd aan 5.1.2.i , rechtsgeldig vertegenwoordigd door de heer 5.1.2.e (hierna: "**Verwerker**");

Hierna gezamenlijk te noemen: "**Partijen**" en individueel te noemen "**Partij**";

NEMEN HET VOLGENDE IN AANMERKING:

- Partijen hebben een overeenkomst gesloten met betrekking to 5.1.2.i Ter uitvoering van de Overeenkomst (hierna te noemen Hoofdovereenkomst) verwerkt Verwerker ten behoeve van Verwerkingsverantwoordelijke Persoonsgegevens;
- In het kader van het uitvoeren van de Overeenkomst is 5.1.2.i an te merken als Verwerker in de zin van de AVG en is Politieacademie aan te merken als Verwerkingsverantwoordelijke in de zin van de AVG;
- Partijen wensen zorgvuldig en in overeenstemming met de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens om te gaan met de Persoonsgegevens die ter uitvoering van de Overeenkomst verwerkt (zullen) worden;
- Partijen wensen in overeenstemming met de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens hun rechten en plichten ten aanzien van de Verwerking van Persoonsgegevens van Betrokkenen Schriftelijk vast te leggen in deze Verwerkersovereenkomst.

EN ZIJN ALS VOLGT OVEREENGEKOMEN:

5.1.2.e

5.1.2.i

Verwerkersovereenkomst 5.1.2.i

ARTIKEL 1. DEFINITIES

In deze Verwerkersovereenkomst hebben de met hoofdletter geschreven begrippen de in dit artikel opgenomen betekenis. Waar de definitie in dit artikel in het enkelvoud is opgenomen, wordt ook het meervoud daaronder begrepen en vice versa, tenzij uitdrukkelijk anders vermeld of uit de context anders blijkt.

1.1 AVG: de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de Verwerking van Persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

1.2 Betrokkene: de geïdentificeerde of identificeerbare natuurlijke persoon op wie de Persoonsgegevens betrekking hebben, zoals bedoeld in artikel 4 onder 1) AVG.

1.3 Bijlage: een bijlage bij deze Verwerkersovereenkomst, die een integraal onderdeel vormt van deze Verwerkersovereenkomst.

1.4 Bijzondere categorieën Persoonsgegevens: Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid, zoals bedoeld in artikel 9 AVG.

1.5 Derde: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de Betrokkene, noch de Verwerkingsverantwoordelijke, noch de Verwerker, noch de personen die onder rechtstreeks gezag van de Verwerkingsverantwoordelijke of de Verwerker gemachtigd zijn om Persoonsgegevens te verwerken, zoals bedoeld in artikel 4 onder 10) AVG.

1.6 Dienst: de op grond van de Overeenkomst te leveren dienst(en) door Verwerker aan Verwerkingsverantwoordelijke.

1.7 Inbreuk in verband met Persoonsgegevens: een (vermoeden van een) inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte Persoonsgegevens, zoals bedoeld in artikel 4 onder 12) AVG.

1.8 Medewerker: de door Verwerker ingeschakelde werknemers en andere personen waarvan de werkzaamheden onder zijn verantwoordelijkheid vallen en die worden ingeschakeld door Verwerker ter uitvoering van de Overeenkomst.

1.9 Ontvanger: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een Derde, aan wie/waaraan de Persoonsgegevens worden verstrekt, zoals bedoeld in artikel 4 onder 9) AVG.

1.10 Overeenkomst: de overeenkomst die tussen Verwerkingsverantwoordelijke en Verwerker is gesloten en op grond waarvan Verwerker Persoonsgegevens ten behoeve van de uitvoering van deze overeenkomst voor Verwerkingsverantwoordelijke verwerkt.

5.1.2.e

1.11 Persoonsgegeven: alle informatie over een Betrokkene; als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon, zoals bedoeld in artikel 4 onder 1) AVG.

1.12 DPIA: de gegevensbeschermingseffectbeoordeling (Data Protection Impact Assessment) die vóór de Verwerking ten aanzien van het effect van de beoogde verwerkingsactiviteiten op de bescherming van Persoonsgegevens wordt uitgevoerd, zoals bedoeld in artikel 35 AVG.

1.13 Schriftelijk: op schrift gesteld of langs de elektronische weg, zoals bedoeld in artikel 6:227a van het Burgerlijk Wetboek.

1.14 Sub-verwerker: een andere verwerker, waaronder maar niet beperkt tot groepsmaatschappijen, zustermaatschappijen, dochtermaatschappijen en hulpleveranciers, die Verwerker inschakelt om voor rekening van de Verwerkingsverantwoordelijke specifieke verwerkingsactiviteiten te verrichten.

1.15 Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens: de toepasselijke wet- en regelgeving en/of (nadere) verdragen, verordeningen, richtlijnen, besluiten, beleidsregels, instructies en/of aanbevelingen van een bevoegde overheidsinstantie betreffende de Verwerking van Persoonsgegevens, tevens omvattende toekomstige wijziging hiervan en/of aanvulling hierop, inclusief lidstaatrechtelijke uitvoeringswetten van de AVG en de Telecommunicatiewet.

1.16 Toezichthoudende autoriteit: één of meer onafhankelijke overheidsinstanties die verantwoordelijk is of zijn voor het toezicht op de toepassing van de AVG, teneinde de grondrechten en fundamentele vrijheden van natuurlijke personen in verband met de Verwerking van hun Persoonsgegevens te beschermen en het vrije verkeer van Persoonsgegevens binnen de Unie te vergemakkelijken, zoals bedoeld in artikel 4 onder 21) en artikel 51 AVG. In Nederland is dit de Autoriteit Persoonsgegevens.

1.17 Verwerkersovereenkomst: de onderhavige overeenkomst inclusief Bijlagen, zoals bedoeld in artikel 28 lid 3 AVG.

1.18 Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot Persoonsgegevens of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens, zoals bedoeld in artikel 4 onder 2) AVG.

ARTIKEL 2. VOORWERP VAN DE VERWERKERSOVEREENKOMST

2.1 De Verwerkersovereenkomst vormt een aanvulling op de Overeenkomst en vervangt eventuele eerder gemaakte afspraken tussen Partijen ten aanzien van de Verwerking van Persoonsgegevens. Bij

tegenstrijdigheid tussen de bepalingen uit de Verwerkersovereenkomst en de Overeenkomst, prevaleren de bepalingen uit de Verwerkersovereenkomst.

2.2 De bepalingen uit de Verwerkersovereenkomst gelden voor alle Verwerkingen die plaatsvinden ter uitvoering van de Overeenkomst. Verwerker brengt Verwerkingsverantwoordelijke onverwijld op de hoogte indien Verwerker reden heeft om aan te nemen dat Verwerker niet langer aan de Verwerkersovereenkomst kan voldoen.

2.3 Verwerkingsverantwoordelijke geeft Verwerker opdracht en instructies om de Persoonsgegevens te verwerken namens de Verwerkingsverantwoordelijke. De instructies van Verwerkingsverantwoordelijke zijn nader omschreven in de Verwerkersovereenkomst en de Overeenkomst. Verwerkingsverantwoordelijke kan naar redelijkheid Schriftelijk aanvullende of afwijkende instructies geven.

2.4 Verwerker verwerkt de Persoonsgegevens uitsluitend in opdracht van Verwerkingsverantwoordelijke en op basis van de instructies van Verwerkingsverantwoordelijke. Verwerker verwerkt de Persoonsgegevens uitsluitend voor zover de Verwerking noodzakelijk is ter uitvoering van de Overeenkomst, nimmer ten eigen nutte, ten nutte van Derden en/of voor reclamedoeleinden c.q. andere doeleinden, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling Verwerker tot Verwerking verplicht. In dat geval stelt Verwerker Verwerkingsverantwoordelijke voorafgaand aan de Verwerking Schriftelijk op de hoogte van deze bepaling, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

2.5 Verwerker en Verwerkingsverantwoordelijke leven de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens na. Verwerker stelt de Verwerkingsverantwoordelijke onmiddellijk in kennis indien naar mening van Verwerker een instructie van Verwerkingsverantwoordelijke inbreuk oplevert op de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

2.6 Indien Verwerker in strijd met de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens het doel en de middelen van de Verwerking van Persoonsgegevens bepaalt, wordt Verwerker voor die Verwerkingen als Verwerkingsverantwoordelijke beschouwd.

ARTIKEL 3. VERWERKING VAN PERSOONSGEGEVENS

3.1 Voorafgaand aan het sluiten van de Verwerkersovereenkomst informeert Verwerker Verwerkingsverantwoordelijke in Bijlage A volledig en naar waarheid over de Verwerkingen die Verwerker ter uitvoering van de Overeenkomst uitvoert, tenzij in Bijlage A is opgenomen dat Verwerkingsverantwoordelijke de betreffende informatie in deze Bijlage opneemt. Verwerker is uitsluitend tot de in Bijlage A gespecificeerde Verwerkingen gerechtigd.

ARTIKEL 4. VERLENEN VAN BIJSTAND EN MEDEWERKING

4.1 Verwerker verleent Verwerkingsverantwoordelijke alle benodigde bijstand en medewerking bij het doen nakomen van de op Partijen rustende verplichtingen op grond van de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens. Verwerker verleent Verwerkingsverantwoordelijke in ieder geval bijstand met betrekking tot:

(i) De beveiliging van Persoonsgegevens;

(ii) Het uitvoeren van controles en audits;

(iii) Het uitvoeren van DPIA's;

(iv) Voorafgaande raadpleging van de Toezichthoudende autoriteit;

(v) Het voldoen aan verzoeken van de Toezichthoudende autoriteit of een andere overheidsinstantie;

(vi) Het voldoen aan verzoeken van Betrokkenen;

(vii) Het melden van Inbreuken in verband met Persoonsgegevens.

4.2 Onder het verlenen van bijstand en medewerking met betrekking tot het voldoen aan verzoeken van Betrokkenen, worden in ieder geval de volgende verplichtingen voor Verwerker verstaan:

4.2.1 Verwerker neemt alle redelijke maatregelen om ervoor te zorgen dat Betrokkene zijn rechten kan uitoefenen.

4.2.2 Indien een Betrokkene met betrekking tot de uitvoering van zijn rechten direct contact opneemt met Verwerker, dan gaat Verwerker hier – behoudens uitdrukkelijke andersluidende instructie van Verwerkingsverantwoordelijke – niet (inhoudelijk) op in, maar bericht Verwerker dit onverwijld aan Verwerkingsverantwoordelijke met een verzoek om nadere instructies.

4.2.3 Indien Verwerker de Dienst rechtstreeks aanbiedt aan Betrokkene, is Verwerker verplicht om Betrokkene namens de Verwerkingsverantwoordelijke te informeren over de Verwerking van de Persoonsgegevens van Betrokkene op een wijze die in overeenstemming is met de rechten van Betrokkene.

4.3 Onder het verlenen van bijstand en medewerking met betrekking tot het voldoen aan verzoeken van de Toezichthoudende autoriteit of een andere overheidsinstantie, worden in ieder geval de volgende verplichtingen voor Verwerker verstaan:

4.3.1 Indien Verwerker een verzoek of een bevel van een Nederlandse en/of buitenlandse overheidsinstantie ontvangt met betrekking tot Persoonsgegevens, waaronder maar niet beperkt tot een verzoek van de Toezichthoudende autoriteit, informeert Verwerker Verwerkingsverantwoordelijke onverwijld, voor zover dat wettelijk is toegestaan. Bij de behandeling van het verzoek of bevel neemt Verwerker alle instructies van

Verwerkingsverantwoordelijke in acht en verleent Verwerker alle redelijkerwijs benodigde medewerking aan Verwerkingsverantwoordelijke.

4.3.2 Indien het Verwerker wettelijk is verboden om te voldoen aan zijn verplichtingen op grond van artikel 4.3.1, behartigt Verwerker de redelijke belangen van Verwerkingsverantwoordelijke. Hieronder wordt in ieder geval verstaan:

4.3.2.1 Verwerker laat juridisch toetsen in hoeverre: (i) Verwerker wettelijk verplicht is om aan het verzoek of bevel te voldoen; en (ii) het Verwerker daadwerkelijk is verboden om aan zijn verplichtingen jegens Verwerkingsverantwoordelijke op grond van artikel 4.3.1 te voldoen.

4.3.2.2 Verwerker werkt alleen mee aan het verzoek of bevel indien Verwerker hiertoe wettelijk verplicht is en waar mogelijk maakt Verwerker (in rechte) bezwaar tegen het verzoek of bevel of het verbod om Verwerkingsverantwoordelijke hierover te informeren of de instructies van Verwerkingsverantwoordelijke op te volgen.

4.3.2.3 Verwerker verstrekt niet meer Persoonsgegevens dan strikt noodzakelijk om aan het verzoek of bevel te voldoen.

4.3.2.4 Verwerker onderzoekt indien sprake is van doorgifte in de zin van artikel 9 de mogelijkheden om te voldoen aan de artikelen 44 tot en met 46 AVG.

ARTIKEL 5. TOEGANG TOT PERSOONSGEGEVENS

5.1 Verwerker beperkt de toegang tot Persoonsgegevens aan Medewerkers, Derden en andere Ontvangers van Persoonsgegevens tot een noodzakelijk minimum.

5.2 Verwerker verschaft uitsluitend toegang aan die Medewerkers voor wie ter uitvoering van de Overeenkomst deze toegang tot Persoonsgegevens noodzakelijk is. De categorieën Medewerkers zijn in Bijlage A gespecificeerd.

5.7 Verwerker legt de in de Verwerkersovereenkomst opgenomen verplichtingen op aan de door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers. Verwerker draagt er zorg voor dat de door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers, de in de Verwerkersovereenkomst opgenomen verplichtingen naleven door middel van een Schriftelijke overeenkomst.

5.8 Verwerker brengt Verwerkingsverantwoordelijke onverwijld op de hoogte indien Verwerker en/of door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers, in strijd handelen met de Verwerkersovereenkomst en/of de met Verwerker gesloten Schriftelijke overeenkomst zoals bedoeld in artikel 5.7.

5.9 Verwerker verstrekt op verzoek van Verwerkingsverantwoordelijke een afschrift van de Schriftelijke overeenkomst tussen Verwerker en de door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers.

5.10 Verwerker blijft ten aanzien van de Verwerkingsverantwoordelijke volledig verantwoordelijk en volledig aansprakelijk voor het nakomen van de verplichtingen door de door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers, voortvloeiende uit de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens en de verplichtingen voortvloeiende uit de Overeenkomst en de Verwerkersovereenkomst.

ARTIKEL 6. BEVEILIGING

6.1 Verwerker treft passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, opdat de Verwerking aan de vereisten van de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet en de bescherming van de rechten van Betrokkenen is gewaarborgd. Verwerker treft hiertoe tenminste de technische en organisatorische maatregelen die zijn opgenomen in Bijlage B.

6.2 Bij de beoordeling van het passende beveiligingsniveau houdt Verwerker rekening met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

6.3 Verwerker legt zijn beveiligingsbeleid Schriftelijk vast. Op verzoek van Verwerkingsverantwoordelijke verschaft Verwerker inzage in het beveiligingsbeleid van Verwerker.

6.4 Het aansluiten bij een goedgekeurde gedragscode als bedoeld in artikel 40 AVG of een goedgekeurd certificeringsmechanisme als bedoeld in artikel 42 AVG kan worden gebruikt als element om aan te tonen dat de in dit artikel bedoelde vereisten worden nageleefd.

ARTIKEL 7. AUDIT

7.1 Verwerker is verplicht periodiek een onafhankelijke, externe deskundige een audit te laten uitvoeren ten aanzien van de organisatie van Verwerker, teneinde aan te tonen dat Verwerker aan het bepaalde in de Overeenkomst, de Verwerkersovereenkomst, de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet.

7.2 Verwerker verricht tenminste een keer per twee jaar een periodieke audit, zoals bedoeld in artikel 7.1. Indien Bijzondere categorieën Persoonsgegevens worden verwerkt, verricht Verwerker tenminste eenmaal per jaar een periodieke audit zoals bedoeld in artikel 7.1.

7.3 Verwerker is enkel niet gehouden tot het verrichten van een periodieke audit zoals bedoeld in artikel 7.1, indien Verwerker uitsluitend Persoonsgegevens verwerkt met een laag risico en uitdrukkelijk in Bijlage A is opgenomen dat Verwerker niet gehouden is tot het verrichten van een periodieke audit. Verwerkingsverantwoordelijke stelt vast of er sprake is van een laag risico.

7.4 Verwerkingsverantwoordelijke heeft het recht om op zijn verzoek een audit te laten uitvoeren door een door Verwerkingsverantwoordelijke gemachtigde (rechts)persoon, ten aanzien van de

5.1.2.e

organisatie van Verwerker, teneinde aan te tonen dat Verwerker aan het bepaalde in de Overeenkomst, de Verwerkersovereenkomst, de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet.

7.5 De kosten van de periodieke audit komen voor rekening van Verwerker. De kosten van de audit op verzoek van Verwerkingsverantwoordelijke komen voor rekening van Verwerkingsverantwoordelijke, tenzij uit de bevindingen van de audit blijkt dat Verwerker de bepalingen uit de Overeenkomst en/of de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens niet is nagekomen. Deze bepaling laat de overige rechten van Verwerkingsverantwoordelijke, waaronder het recht op schadevergoeding, onverlet.

7.6 Indien tijdens een audit wordt vastgesteld dat Verwerker niet aan het bepaalde in de Overeenkomst en/of de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet, neemt Verwerker onverwijld alle redelijkerwijs noodzakelijke maatregelen om te zorgen dat Verwerker hieraan alsnog voldoet. De bijbehorende kosten komen voor rekening van Verwerker.

ARTIKEL 8. INBREUK IN VERBAND MET PERSOONSGEGEVENS

8.1 Verwerker informeert Verwerkingsverantwoordelijke zonder onredelijke vertraging en uiterlijk binnen 24 uur na kennisneming, over een Inbreuk in verband met Persoonsgegevens of een redelijk vermoeden van een Inbreuk in verband met Persoonsgegevens. Verwerker informeert Verwerkingsverantwoordelijke via de contactpersoon en de contactgegevens van Verwerkingsverantwoordelijke zoals opgenomen in Bijlage A en ten minste ten aanzien van hetgeen is opgenomen in Bijlage C. Verwerker garandeert dat de verstrekte informatie volledig, correct en accuraat is.

8.2 Indien en voor zover het voor Verwerker niet mogelijk is om alle informatie uit Bijlage C gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging en uiterlijk binnen 24 uur na het ontdekken, in stappen worden verstrekt aan Verwerkingsverantwoordelijke.

8.3 Verwerker heeft adequaat beleid en adequate procedures ingericht om Inbreuken in verband met Persoonsgegevens in een zo vroeg mogelijk stadium te detecteren, Verwerkingsverantwoordelijke hierover uiterlijk binnen 24 uur te informeren, hierop adequaat en onmiddellijk te reageren, (verdere) onbevoegde kennisneming, wijziging, en verstrekking dan wel anderszins onrechtmatige Verwerking te voorkomen of te beperken en herhaling hiervan te voorkomen. Op verzoek van Verwerkingsverantwoordelijke verschaft Verwerker informatie over en inzage in dit door Verwerker ingerichte beleid en deze door Verwerker ingerichte procedures.

8.4 Verwerker houdt Schriftelijk een register bij van alle Inbreuken in verband met Persoonsgegevens die betrekking hebben op of verband houden met de (uitvoering van de) Overeenkomst, met inbegrip van de feiten omtrent de Inbreuk in verband met Persoonsgegevens, de gevolgen daarvan en de getroffen corrigerende maatregelen. Op verzoek van Verwerkingsverantwoordelijke verschaft Verwerker Verwerkingsverantwoordelijke een afschrift van dit register.

ARTIKEL 9. DOORGIFTE VAN PERSOONSGEGEVENS

9.1 Persoonsgegevens mogen enkel worden doorgegeven aan derde landen of internationale organisaties indien sprake is van een passend beschermingsniveau en Verwerkingsverantwoordelijke hiervoor specifieke Schriftelijke toestemming heeft verleend. Deze specifieke Schriftelijke toestemming is slechts verleend indien dit is opgenomen in Bijlage A. Verwerker is uitsluitend gerechtigd tot deze in Bijlage A gespecificeerde doorgiften aan derde landen of internationale organisaties, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling Verwerker tot Verwerking verplicht. In dat geval stelt Verwerker Verwerkingsverantwoordelijke voorafgaand aan de Verwerking Schriftelijk op de hoogte van deze bepaling, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

9.2 Verwerkingsverantwoordelijke kan aan de Schriftelijke toestemming, zoals bedoeld in artikel 9.1, nadere voorwaarden verbinden, waaronder maar niet beperkt tot het aantonen dat aan de vereisten zoals opgenomen in artikel 9.3 is voldaan.

9.3 Verwerkingsverantwoordelijke kan Verwerker slechts toestemming verlenen voor een doorgifte van Persoonsgegevens aan derde landen of internationale organisaties indien, ofwel:

(i) Een adequaatheidsbesluit overeenkomstig artikel 45 lid 3 AVG is genomen ten aanzien van het betreffende derde land of de betreffende internationale organisatie; ofwel

(ii) Passende waarborgen overeenkomstig artikel 46 AVG met inbegrip van bindende voorschriften zoals bedoeld in artikel 47 AVG, zijn getroffen ten aanzien van het betreffende derde land of de betreffende internationale organisatie; ofwel

(iii) Aan één van de specifieke voorwaarden uit artikel 49 lid 1 AVG is voldaan ten aanzien van het betreffende derde land of de betreffende internationale organisatie.

ARTIKEL 10. VERTROUWELIJKHEID VAN PERSOONSGEGEVENS

10.1 Alle Persoonsgegevens worden als vertrouwelijke gegevens gekwalificeerd en dienen als zodanig te worden behandeld.

10.2 Partijen houden alle Persoonsgegevens geheim en maken deze op geen enkele wijze verder intern of extern bekend, behalve voor zover:

(i) Bekendmaking en/of verstrekking van de Persoonsgegevens in het kader van de uitvoering van de Overeenkomst of Verwerkersovereenkomst noodzakelijk is;

(ii) Enig dwingendrechtelijk wettelijk voorschrift of rechterlijke uitspraak Partijen tot bekendmaking en/of verstrekking van die Persoonsgegevens verplicht, waarbij Partijen eerst de andere Partij hiervan op de hoogte stellen;

(iii) Bekendmaking en/of verstrekking van die Persoonsgegevens geschiedt met voorafgaande Schriftelijke toestemming van de andere Partij.

5.1.2.e

10.3 Overtreding van artikel 10.1 en/of artikel 10.2 wordt beschouwd als een Inbreuk in verband met Persoonsgegevens.

ARTIKEL 11. AANSPRAKELIJKHEID EN VRIJWARING

11.1 Verwerker is jegens Verwerkingsverantwoordelijke als gevolg van of verband houdende met deze Verwerkersovereenkomst of uit enige andere hoofde aansprakelijk voor zover en tot zover partijen dit zijn overeengekomen in de Hoofdovereenkomst. De in de Hoofdovereenkomst overeengekomen beperking van de aansprakelijkheid is onverminderd van kracht op de verplichtingen zoals opgenomen in deze Verwerkersovereenkomst, met dien verstande dat eenzelfde gebeurtenis nooit tot meerdere schadevorderingen kan leiden.

ARTIKEL 12. WIJZIGING

12.1 Verwerker is verplicht Verwerkingsverantwoordelijke onmiddellijk te informeren over voorgenomen wijzigingen in de Dienst, de uitvoering van de Overeenkomst en de uitvoering van de Verwerkersovereenkomst die betrekking hebben op de Verwerking van Persoonsgegevens. Hieronder wordt in ieder geval verstaan:

(i) Wijzigingen die invloed (kunnen) hebben op de te verwerken (categorieën) Persoonsgegevens;

(ii) Wijziging van de middelen waarmee de Persoonsgegevens worden verwerkt;

(iii) Wijziging in de doorgifte van Persoonsgegevens aan derde landen en/of internationale organisaties.

12.2 Indien een wijziging met betrekking tot de Verwerking van Persoonsgegevens of een audit daartoe aanleiding geeft, treden Partijen op eerste verzoek van Verwerkingsverantwoordelijke in overleg over het wijzigen van de Verwerkersovereenkomst.

12.3 Verwerker is pas gerechtigd tot het uitvoeren van een wijziging in de Dienst, een wijziging in de uitvoering van de Overeenkomst, een wijziging in de uitvoering van de Verwerkersovereenkomst en/of een wijziging die aanpassing van Bijlage A tot gevolg heeft, indien Verwerkingsverantwoordelijke daaraan voorafgaand Schriftelijk toestemming voor deze wijziging(en) heeft gegeven.

12.4 Wijzigingen die betrekking hebben op de Verwerking van Persoonsgegevens mogen nooit tot gevolg hebben dat Verwerkingsverantwoordelijke niet kan voldoen aan de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

12.5 In geval van nietigheid of vernietigbaarheid van één of meer bepalingen van de Verwerkersovereenkomst, blijven de overige bepalingen onverkort van kracht.