

## Data Protection and Privacy Exhibit for Juniper Services

This data processing agreement based on the unmodified standard contractual clauses as per Commission Decision 2010/87/EU as of February 5, 2010 including Appendices 1 (Details of the Transfer), 2 (Technical and Organizational Measures), and 3 (Additional Provisions) (“**DPA**”) covering the services (“**Juniper Services**”) rendered under a respective end user services agreement (“**Main Agreement**”) between the contracting party receiving Juniper Services and Juniper Networks (as defined in the Main Agreement), as sold by Juniper Networks or an authorized reseller, is entered into by and between the contracting party receiving Juniper Services under the Main Agreement (“**Data Exporter**”) and the data importers as specified in Appendix 1 (each a “**Data Importer**”).

### 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 sub-processor” means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor 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.

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 sub-processor 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 sub-processor 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;

(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 sub-processor 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 sub-processor 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

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;

(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 sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor 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 sub-processor 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 sub-processor 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 or 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 sub-processor 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 sub-processor 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 sub-processor agrees that the data subject may issue a claim against the data sub-processor 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 sub-processor 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 sub-processor, 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 sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, 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 Clauses.

#### **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 sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor 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 sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor 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 sub-processor 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.

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 sub-processor 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 sub-processor 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.

**SIGNATURES**

**On behalf of the Data Exporter:**

Name (written out in full):

Position:

Address:

**Signature.....**

**On behalf of Data Importer 1 (as defined below):**

Name (written out in full):

Position:

Address:

**Signature.....**

**On behalf of Data Importer 2 (complete only if Juniper Networks, Inc. has not already signed this DPA as Data Importer 1 above):**

Name (written out in full):

Position:

Address:

**Signature.....**

**APPENDIX 1**  
**Details of the Transfer**

*This Appendix forms part of the Clauses and must be completed by the parties.*

**Data Exporter:** The Data Exporter is the contracting party of the Main Agreement receiving Juniper Services.

**Data Importer:** The Data Importers are:

- Data Importer 1: Juniper Networks, Inc., or if contracting party purchases Juniper Services directly from Juniper Networks, then Juniper Networks as defined in the Main Agreement
- Data Importer 2: Juniper Networks, Inc. (only if Juniper Networks, Inc. is not the entity covered as Data Importer 1 above)

**Data subjects:** The personal data transferred concern the following categories of data subjects:  
Personnel of Data Exporter or of its end users.

**Categories of data:** The personal data transferred concern the following categories of data:

Typically only business contact information of personnel involved in requesting and coordinating customer support from the Data Importer is required for Data Importer to provide support. Occasionally, Data Exporter or its end users' IP addresses, and less frequently, core dump files or network traffic snippets from a network device, may also be provided when requesting support and could be deemed to contain personal data to the extent it can be associated with an individual data subject although only information about the state of a network device and not the personal data itself is required for Data Importer to provide support. No sensitive or special categories of personal data are expected or shall be received by the Data Importer without prior written notice to and consent from the Data Importer.

**Special categories of data (if appropriate):** The personal data transferred concern the following special categories of data:  
None

**Processing operations:** The personal data transferred will be subject to the following basic processing activities:

Providing Juniper Services that entail accessing and reviewing the information provided by Data Exporter which relates to the technical problem encountered by the Data Exporter.

**APPENDIX 2**  
**Technical and Organisational Measures**

This Appendix forms part of the Clauses and must be completed by the parties. Data Exporter agrees that the terms set forth in this Appendix 2 are appropriate Technical and Organizational Measures to protect Data Exporter's personal data.

Description of the technical and organisational security measures implemented by the Data Importer in accordance with Clauses 4(d) and 5(c):

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall implement the following technical and organizational measures to ensure a level of security appropriate to the risks for the rights and freedoms of natural persons. In assessing the appropriate level of security the Controller and the Processor took account in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

**1. Information Security Governance**

- The information security function within Processor reports directly to a company executive.
- A Security and Privacy Steering Committee made up of representatives from the business, meets regularly to discuss and review information security policies, projects, and practices.
- A comprehensive set of information security policies and standards are documented, approved and regularly maintained.
- Personnel with access to personal data are subject to confidentiality obligations.

**2. Network Security**

- Network security is maintained using industry standard techniques, including firewalls, intrusion detection systems, access control lists, and routing protocols.
- Network, application and server authentication passwords are required to meet minimum complexity guidelines (at least 12 characters with at least 3 of the following four classes: upper case, lower case, numeral, special character) and be changed at least every 180 days.

**3. Encryption**

- Full disk encryption is configured on all laptops.
- Sensitive personal data is encrypted in transit.

**4. Confidentiality of the processing systems and of the services**

- Data processing systems and personal data are prevented from being accessed or used without authorization.
- Personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport.
- All employees or contractors with access to personal data are assigned unique IDs.
- Only authorized staff may grant, modify or revoke access.
- Access rights are assigned using a least privilege approach.
- Access is revoked upon termination of the employee or contract.

**5. Physical Security**

- Physical access to Processor buildings is restricted to personnel on a need to have basis.
- Physical access controls, such as surveillance cameras and identification badges, are implemented for all data centers.

**6. Integrity and availability of the processing systems and of the services**

- Anti-malware software is installed and updated on end user systems.
- Logging of who, what, and when is in place for access to personal data.
- Personal data is protected from accidental destruction or loss.

**7. Ability to restore the availability and access to the personal data in a timely manner in the event of a physical or technical incident**

- Emergency and contingency plans are available and maintained to restore personal data.
- Business continuity plans are tested and updated on a periodic basis.
- Backups of data are maintained for business continuity purposes.

**8. Process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures**

- Third party penetration tests are conducted on an annual basis.
- External vulnerability scans are performed on a monthly basis.
- Any severe vulnerability is remediated in a timely manner, depending on the associated risk.

**9. Training and Information Security Review**

- Background checks are required on personnel with network or facilities access.
- Employees are required to undergo privacy and information security training.
- Subprocessors that must have need to know access to personal data undergo a comprehensive vendor information security review.

**APPENDIX 3**  
**Additional Provisions**

1. **Definitions.** Terms used in this DPA shall have the meaning indicated below (also in the body document of this DPA, where defined terms are not capitalized).

- (i) "**Clauses**" shall mean all provisions of this DPA, unless provided otherwise in the relevant context;
- (ii) "**Data Exporter**" shall mean the Data Exporter regardless of its location, whether within or outside the EU/EEA;
- (iii) "**Data Importer**" shall mean the Data Importer regardless of its location, whether within or outside the EU/EEA;
- (iv) "**Member State**" shall mean any country, within or outside the EU/EEA; and
- (v) "**Service**" or "**Services**" shall mean the Juniper Services rendered by Data Importer, as described in more detail in Appendix 1 (also if used with additions or in variations, for instance "processing services").

Other terms that are capitalized but not defined below, shall have the meaning as defined in the Main Agreement.

2. **General provisions**

2.1 **Order of precedence.** If and to the extent there should be contradictions or inconsistencies between this Appendix 3 and the remainder of the DPA, this Appendix 3 shall prevail, unless the Data Exporter is located in the EU/EEA and the Data Importer is located outside the EU/EEA, in which case the provisions of the remainder of the DPA shall prevail. For the avoidance of doubt, even in this case, provisions of Appendix 3 that merely go beyond the remainder of the DPA without contradicting the DPA's terms shall remain valid.

2.2 **Non-applicability of certain Clauses.** Clauses 3, 4 (i), 5 (i), 6, 7, 11 (2) and (3) of the DPA shall not apply, unless the Data Exporter is located in the EU/EEA and the Data Importer either (i) is located outside the EU/EEA or (ii) commissions a subprocessor located outside the EU/EEA.

2.3 **Fulfillment of obligations of Data Importers under Clause 5(j).** Data Exporter herewith instructs Data Importers to send any information in connection with the fulfillment of Data Importers' obligations under Clause 5j) exclusively to Juniper Networks.

2.4 **Bundling of Data Importers for efficiency purposes.** The parties agree that the bundling of the Data Importers as processors within this single DPA is only undertaken for efficiency purposes (i.e., to avoid a multitude of different contract documents) and (i) shall result in legally separate DPAs between the respective Data Exporter and the Data Importer and (ii) shall not create any legal or other relationship whatsoever between the "bundled" Data Importers. The Data Exporter authorizes Juniper Networks to exercise the Data Exporter's contractual rights and powers (i.e., the rights and powers ensuing from this DPA) and the Data Exporter's statutory privacy law-related rights and powers (i.e., the rights and powers ensuing from the Data Exporter's position as data controller) vis-à-vis the other Data Importers (for the avoidance of doubt, the Data Exporter shall remain entitled to exercise these rights and powers in its own name at any time).

2.5 **Data Protection Compliance.** Each party undertakes as soon as reasonably practicable to obtain the requisite registrations under the data protection laws applicable to it, to maintain such registrations throughout the term of this DPA and to comply with the applicable data protection laws insofar as they apply to the Service. The Data Exporter as data controller hereby warrants that it has obtained all permissions required to provide the Data Importers with such personal data of the data subjects specified in Appendix 1 to this DPA as the Data Importers reasonably require to provide the Services.

2.6 **Term.** The term of this DPA is identical with the term of the Main Agreement. Save as otherwise agreed herein, termination rights and requirements shall be the same as set forth in the Main Agreement.

2.7 **Invalidity and/or unenforceability.** Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or - should this not be possible - (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

2.8 **Liability.** The liability under this DPA shall be governed by the liability regime of the Main Agreement.

3. **Local law amendments.** The parties agree to the amendments set out below, which are required for full compliance with mandatory requirements regarding the commissioning of processors under the national laws applicable to the Data Exporter.

3.1 **Amendments for Data Exporters subject to the General Data Protection Regulation.** In order to satisfy the requirements for the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – “GDPR”) the following amendments shall apply:

(a) **Scope of Processing:** As required by Clause 5 (a) of the Standard Contractual Clauses for Processors, the Data Importer will process the personal data only on behalf of the Data Exporter in compliance with the Data Exporter's instructions and this DPA, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Union or Member State law to which the Data Importer is subject; in such a case, the Data Importer shall inform the Data Exporter of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

(b) **Duration of Processing:** The commissioned data processing operations hereunder shall be performed for an indefinite term for as long as the DPA exists and is in effect and force.

(c) **Instructions:** The Data Exporter is entitled to instruct the Data Importer in connection with commissioned data processing operations generally or in the individual case. Instructions shall be given in writing or in electronic form, unless the urgency or other specific circumstances require another (e.g., oral) form. Instructions in another form than in writing or in electronic form shall be documented in appropriate form. The Data Importer shall notify the Data Exporter without undue delay if it holds that an instruction violates applicable laws. Upon providing such notification, the Data Importer shall not be obliged to follow the instruction, unless and until the Data Exporter has confirmed or changed it.

(d) **Self-monitoring:** The Data Importer shall monitor, by appropriate means, its own compliance with its data protection obligations in connection with the commissioned data processing operations and shall provide the Data Exporter with periodic and occasion-based reports regarding such controls.

(e) **Monitoring by the Data Exporter:** The Data Importer shall make available to the Data Exporter all information necessary to demonstrate compliance with the obligations laid down in this DPA. In accordance with Clause 5 (f) of the Standard Contractual Clauses for Processors, the Data Exporter shall have the right to control, by appropriate means, the Data Importer's compliance with its data protection obligations annually and at any time occasion-based, such controls being limited to information and data processing systems that are relevant to the Services. For these purposes, the Data Exporter shall also have the right to carry out on-site audits, conducted by the Data Exporter or another auditor mandated by the Data Exporter, during regular business hours without disrupting the Data Importer's business operations and in accordance with the Data Importer's security policies, and after a reasonable prior notice. The Data Importer shall tolerate such audits and shall render all necessary support.

(f) **Notification obligation in cases of non-compliance or a security breach:** In addition to Clause 5 (d) (ii) of the Standard Contractual Clauses for Processors, the Data Importer will notify the Data Exporter without undue delay of (i) any (suspected) non-compliance with statutory provisions dealing with the protection of personal data by the Data Importer or its staff, and (ii) any (suspected) non-compliance with the provisions of this DPA. Moreover, the Data Importer will provide the Data Exporter immediately with a data breach notification if the Data Importer becomes aware of any security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data or any other security incident that requires a data breach notification of the Data Exporter according to applicable law. The data breach notification must contain as a minimum all information the Data Exporter requires to comply with applicable law. Taking into account the nature of processing and the information available to the Data Importer, the Data Importer shall provide all assistance to the Data Exporter to deal with the security breach and to comply with the obligations under applicable law and any orders of competent regulators without undue delay.

(g) **Handling of complaints, inquiries and orders:** The Data Importer shall notify the Data Exporter of data subjects' complaints and inquiries (e.g., regarding the rectification, deletion and blocking of or the access to Personal Data, or any other rights data subject has under applicable law) and shall provide assistance to the Data Exporter to respond to such complaints or inquiries in a timely manner. Taking into account the nature of the processing, the Data Importer shall assist the Data Exporter by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Data Exporter's obligations to respond to requests for exercising the data subject's rights under applicable law. The Data Importer shall not independently respond to such complaints, requests and orders without Data Exporter's prior approval, except where required by applicable law. The same shall apply to orders and inquires of courts or regulators.

(h) **Assistance with privacy impact assessment:** If so requested by the Data Exporter, the Data Importer shall provide required assistance to the Data Exporter in ensuring its compliance relating to data protection impact assessments and prior consultation with the supervisory authorities, taking into account the nature of the processing and the information available to the Data Importer.

(i) **Data secrecy and confidentiality:** The Data Importer shall ensure the confidentiality of the Personal Data processed and shall in particular not disclose the Personal Data processed to any third parties unless authorized by the Data Exporter. This obligation continues to apply after the expiration or termination of this DPA. In accordance with applicable law the Data Importer shall ensure that all persons acting under its authority entrusted with the processing of Personal Data (i) have committed themselves to keep Personal Data strictly confidential and not to use such Personal Data for any other purposes except for the provision of the Services hereunder, or (ii) are under an appropriate statutory obligation of confidentiality. This obligation to confidentiality shall continue after the end of the respective engagement of such person. The Data Importer will further instruct such persons regarding the applicable statutory provisions on data protection and shall ensure that access to the Personal Data is limited to those persons with a need to know.

(j) **Subcontracting:** When subcontracting the Services or parts thereof, Data Importer will comply with requirements set forth in Clause 11 of the Standard Contractual Clauses for Processors and in Art. 28 (2) and (4) GDPR. Data Importer is entitled to use subcontractors for the performance of its services hereunder in accordance with the Clause 11 of the Standard Contractual Clauses for Processors and in Art. 28 (2) and (4) GDPR.

(h) **Return and further use of data after end of contract:** After the end of the provision of the Services, unless otherwise instructed by the Data Exporter, the Data Importer shall return to the Data Exporter, without undue delay, all data carriers received from the Data Exporter and all data obtained or generated in connection with the Services, including relevant copies, in whatever format, and shall refrain from any further processing and use of such data, to the extent this is possible without infringing the Data Importer's own statutory obligations. Without undue delay as of expiration or termination of this DPA, Data Importer shall provide Data Exporter with a written statement confirming it acted as per the above.

### 3.2 **Amendments for Data Exporters located outside of the EU/EEA.**

In case the Data Exporter is located outside of the EU/EEA, the local data protection law applicable to such Data Exporter applies and prevails in case of a conflict in connection with the remainder of the DPA.