**Part I**

|  |  |
| --- | --- |
| 1. Data Controller | Akamai Technologies [Entity] |
| [Akamai registered address] |
| A provider of content delivery, media acceleration, web performance and Internet security services. |
| 1. Data Processor | [Vendor full legal name] |
| [Vendor registered address] |
| [Please describe the business activities of Vendor] |
| 1. Data Subjects | The processing of Personal Data under this DPA concerns the following categories of Data Subjects (please specify):  prospects (including their personnel)  customers (including their personnel)  employees  contractors (including their personnel)  job applicants  vendors (including their personnel)  other:  [Please identify all other categories of Data Subjects whose Personal Data is processed under this DPA] |
| 1. Categories  of Personal Data | The Personal Data processed under this DPA concerns the following categories of data (please specify):  contact information  personal details  family, lifestyle and social circumstances  login information and credentials  employment, job history and applicant data  education and training details  device and usage data  financial details  other:  [Please identify all other categories of data processed by Data Processor under this DPA] |
| 1. Special categories  of Personal Data | The Personal Data processed under this DPA concerns the following special categories of data (please specify):  racial or ethnic origin  political opinions  religious or philosophical beliefs  trade union membership  genetic data  biometric data (if used to identify a natural person)  health  sex life or sexual orientation  criminal convictions and offences  none of the above |
| 1. Processing operations | The Personal Data processed under this DPA is subject to the following processing activities (please specify):  receiving data, including collection, accessing, retrieval, recording, and data entry  holding data, including storage, organisation and structuring  using data, including analysing, consultation, testing  automated decision making and profiling  updating data, including correcting, adaptation, alteration, alignment and combination  protecting data, including restricting, encrypting, and security testing  sharing data, including disclosure, dissemination, allowing access or otherwise making available  returning data to the data controller or data subject  erasing data, including destruction and deletion  other:  [Please describe all other processing activities of Data Processor] |
| 1. Cross-border transfer | The Personal Data processed under this DPA will be transferred to other jurisdiction(s):  no  yes, to:  [Please name all jurisdictions where the Personal Data will be transferred] |
| 1. Sub-processors | The Personal Data processed under this DPA will be processed by Sub-processors:  no  yes, by:  [Please name all Sub-processors including their registered address] |
| 1. Technical and Organizational Measures | [Please describe in details the technical and organisational measures set forth to ensure an appropriate level of data protection] |

**Part II**

**Preamble**

This Data Processing Agreement (**"DPA"**) is an integral part of the Agreement regarding the purchase of Data Processor's offerings by the Data Controller concluded between the parties. The **“Agreement”** shall mean, as applicable, the Akamai’s Terms and Conditions of Purchase (as attached to the relevant Purchase Order), the Master Service Agreement between Data Controller and Data Processor, and/or any other similar agreement or terms (including but not limited to the end user license agreement, consulting agreement or any other professional service agreement) governing the purchase of Data Processor’s offerings by Data Controller.

This DPA regulates the processing of Personal Data provided to the Data Processor by or on behalf of the Data Controller under the Agreement and is supplemental to the Agreement. If the provisions of this DPA and the Agreement conflict, including any previously executed or incorporated data protection agreement or privacy terms and conditions, then the provisions of this DPA shall prevail. Except for any changes made by this DPA, the Agreement remains unchanged and in full force and effect.

1. **Definitions.** Unless otherwise defined herein, all capitalized terms used in this DPA shall have the meanings assigned to such terms in the Agreement:

|  |  |
| --- | --- |
| **“Cross-Border Transfer Mechanism”** | means applicable legal mechanisms required for the transfer of Personal Data from a Data Controller or a Data Processor in a given jurisdiction to another Data Processor or Sub-processor operating in a separate jurisdiction where applicable Data Protection Laws require a legal mechanism for cross-border transfer. Such mechanisms include, by way of example and without limitation, the EU-U.S. Privacy Shield Framework, Swiss-U.S. Privacy Shield Framework, and the EU standard contractual clauses for Data Processors established in third countries pursuant to European Commission Decision (2010/87/EC) under the EU Directive (95/46/EC), as may be updated or replaced from time to time. |
| **“Data Protection Laws”** | means all applicable laws (including decisions and guidance by relevant Supervisory Authorities) relating to data protection, the processing of Personal Data, and privacy applicable to Data Controller and Data Processor in respect of the processing of Personal Data to provide the services, including such laws, by way of example and without limitation, the General Data Protection Regulation, the California Consumer Privacy Act, and the Personal Information Protection and Electronic Documents Act. |
| **“Data Controller”  “Data Exporter”  “Data Importer”  “Data Processor”  “Data Subject” “Personal Data” “Personal Data Breach”** | shall each have the definitions and meanings ascribed to them by the applicable Data Protection Laws, and shall include any equivalent or corresponding terms applied by such applicable Data Protection Laws (e.g., “Business” instead of “Data Controller” and “Service Provider” instead of “Data Processor” under the California Consumer Privacy Act, or “organization” or “agency” under the Australian Privacy Principles). |
| **“Sub-processor”** | means any third-party appointed by the Data Processor in accordance with this DPA to process the Personal Data on behalf and as instructed by the Data Controller. |
| **“Supervisory Authority”** | means the government agency, department or other competent organization given authority over the processing of Personal Data relevant to this DPA. |

1. **Scope of this DPA.**
   1. This DPA sets out the rights and obligations that apply to handling of Personal Data by the Data Processor on behalf of the Data Controller.
   2. The parties agree and acknowledge that (i) the Data Processor, when providing services to the Data Controller, will be acting as a Data Processor or in a respective role under applicable Data Protection Laws (e.g. a service provider under the CCPA) in relation to the Personal Data defined in Part I of this DPA, (ii) the Data Controller hereby authorizes the Data Processor to process the Personal Data defined in Part I of this DPA for the purpose of providing the services to the Data Controller only.
   3. The processing of Personal Data shall not take place for any purpose other than agreed between the parties in this DPA and the Agreement.
   4. The Data Controller and the Data Processor shall comply with all their respective obligations under the Data Protection Laws, and this DPA shall not exempt the Data Processor from any obligation to which it is subject pursuant to the Data Protection Laws.
2. **The rights and** **obligations of the Data Controller.**
   1. The Data Controller is responsible, among others, for ensuring that the processing of Personal Data which the Data Processor is instructed to perform has a legal basis and for the managing of the Data Subjects’ rights in accordance with the Data Protection Laws.
   2. The Data Controller shall make decisions about the purposes and means of the processing of Personal Data.
   3. The Data Controller shall provide, within the scope of this DPA, documented instructions about type, scope and method of processing of Personal Data. The Data Controller may in addition provide oral instructions which should be confirmed in writing (e.g. by email) by the Data Controller.
   4. The Data Controller shall act as the first and primary contact for the Data Subjects.
3. **The rights and obligations of the Data Processor.**
   1. The Data Processor shall process the Personal Data only in accordance with the Data Controller’s instructions. If the Data Processor acts outside of the Data Controller instructions in such a way that it determines the purpose and the means of processing of the Personal Data, then the Data Processor shall be considered to be a separate data controller (or equivalent in accordance with the Data Protection Laws) and it shall be solely liable for such processing.
   2. The Data Processor shall inform immediately the Data Controller if instructions provided by the Data Controller in the opinion of the Data Processor may violate the Data Protection Laws or if the Data Processor notices any other irregularities in connection with the processing of Personal Data under this DPA. In the above situation the Data Processor shall suspend the execution of such instruction until the Data Controller confirms or alters the instruction.
   3. The Data Processor will not: (a) collect, access, maintain, use, process and transfer Personal Data for any purpose other than as necessary for the purpose of performing services; (b) sell, rent, disclose, release, transfer, make available or otherwise communicate Personal Data to a third party for monetary or other valuable consideration.
   4. The Data Processor warrants that it has implemented appropriate technical and organizational measures to protect Personal Data processed in accordance with the Data Protection Laws, as described in Part I, Section I of this DPA. Such appropriate technical and organizational measures shall include as appropriate:
      1. the pseudonymization and encryption of Personal Data,
      2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services,
      3. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident,
      4. the process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
   5. The Data Processor shall provide the Data Controller with an evidence that the chosen technical and organizational measures are appropriate as required under the Data Protection Laws.
   6. The Data Processor shall assist the Data Controller in its performance of the security and risk analysis in accordance with the Data Protection Laws. In particular the Data Processor shall assist the Data Controller in conducting privacy impact assessments of Personal Data processing operations as required under the Data Protection Laws.
   7. The Data Processor shall keep the Personal Data confidential. The Data Processor's employees involved in the processing of Personal Data shall be under an obligation to maintain the confidentiality of the Personal Data. The Personal Data may be disclosed only to the Data Processor's employees who need to access those data for purposes of performing the Data Processor’s obligations under this DPA or the Agreement.
   8. The Data Processor shall assist the Data Controller in responding to any request related to the processing of Personal Data under this DPA.
   9. The Data Processor will notify the Data Controller without undue delay in the following cases:
      1. the Data Subject contacts the Data Processor requesting information about, correction, deletion or blocking of the Personal Data;
      2. any disruptions of the Data Processor's business with regards to processing of the Personal Data processed for the Data Controller;
      3. any actual or suspected leakages or breach of the Personal Data processed by Data Processor for the Data Controller;
      4. any other irregularities with regards to the Personal Data;
      5. any violation of the provisions of this DPA by the Data Processor, or of the corresponding obligations by any of the Sub-processors;
      6. any breach of the confidentiality of the Personal Data by one of the Data Processor's or Sub-processors’ employees.
   10. The Data Processor shall provide contact details of its data protection representative (e.g. data protection officer).
   11. The Data Processor is subject to, and shall enable effective data protection supervision by the Supervisory Authority. This includes, without limitation, responding to enquiries by the Supervisory Authority in a correct, accurate, and timely manner, assisting in investigations, and executing administrative orders issued by the Supervisory Authority. The Data Processor will notify the Data Controller without undue delay if a Supervisory Authority contacts the Data Processor with regards to the Personal Data processed on behalf of the Data Controller.
4. **Cross-border transfers.**
   1. Any transfer of Personal Data from one jurisdiction to another shall always take place in compliance with the Data Protection Laws and subject to implementation of applicable Cross-Border Transfer Mechanism.
   2. Any cross-border transfer by the Data Processor requires prior approval of the Data Controller and shall occur only on the basis of written instruction from the Data Controller.
   3. Unless another Cross-Border Transfer Mechanism acceptable to both parties is in place:
      1. in the event of transfer made by the Data Controller located in the European Economic Area (“EEA”) to a Data Processor (and Sub-processor if applicable) located outside of the EEA, or
      2. in the event of transfer made by the Data Controller located outside of EEA, relating to the Personal Data which originates from the EEA, to a Data Processor (and Sub-processor if applicable),

the Data Controller and the Data Processor shall be bound by the unmodified EU standard contractual clauses for Data Processors established in third countries pursuant to European Commission Decision (2010/87/EC) under the EU Directive (95/46/EC), as attached to this DPA in Part III. The parties agree that those EU standard contractual clauses are automatically incorporated hereto.

* 1. Where applicable, the Data Controller hereby authorizes the Data Processor to agree on and execute on its behalf (as Data Exporter) the same unmodified EU standard contractual clauses, as attached to this DPA in Part III, with the authorized Sub-processor (as Data Importer).

1. **Sub-processors.** 
   1. The Data Processor shall meet the requirements specified in the Data Protection Laws in order to engage Sub-processors in processing of Personal Data on behalf of Data Controller. The Data Processor shall undertake reasonable due diligence on Sub-processors in advance in order to ensure appropriate safeguards for Personal Data.
   2. Except for the Sub-processors identified in Part I, section H of this DPA, the Data Processor shall not engage any other Sub-processors for the processing of Personal Data on behalf of the Data Controller without the prior specific written authorization of the Data Controller.
   3. When the Data Processor has a written authorization to use the Sub-processors, the Data Processor shall ensure that the Sub-processor is subject to the same data protection obligations as those specified in this DPA on the basis of a contract or other legally binding document, which provides the necessary guarantees in the area of implementation of appropriate technical and organizational measures, meets the Data Protection Laws requirements and ensures an appropriate Cross-Border Transfer Mechanism.
   4. Authorized Sub-processors are permitted to use the Personal Data only for processing purposes outlined in this DPA and the Agreement.
   5. The Data Processor shall remain responsible for all acts or omissions of its Sub-processors, when it concerns the processing of Personal Data on behalf of the Data Controller, as if they were its own.
   6. Upon request, the Data Processor shall submit to the Data Controller further details regarding Sub-processors engaged, including the detailed technical and organizational measures and a copy of the signed data processing agreements and the EU standard contractual clauses.
2. **Audits.** The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the Data Protection Laws and this DPA and allow for and contribute to annual on-site audits of the Data Processor’s data processing tools and systems. Such audits may take place at the Data Controller convenience during normal business hours and will be performed by the Data Controller or third party auditor authorized by the Data Controller. In addition, the Data Processor shall provide to the Data Controller copies of relevant third-party assessments or certifications showing its compliance with the Data Protection Laws.
3. **Personal Data Breach.** 
   1. If the Data Processor becomes aware of a Personal Data Breach, which occurred during the processing of Personal Data on behalf of the Data Controller by Data Processor or its Sub-processors, then the Data Processor shall:
      1. take appropriate actions to remedy or mitigate effects of such Personal Data Breach,
      2. notify the Data Controller about such Personal Data Breach, via (i) an e-mail to: [VendorPrivacy@akamai.com](mailto:VendorPrivacy@akamai.com) and (ii) a phone call to the Data Controller’s relevant business point of contact; in any event no later than 24 hours after the Data Processor becomes aware of such Personal Data Breach to enable the Data Controller to trigger its response program,
      3. reasonably cooperate with the Data Controller to investigate the nature and scope of such Personal Data Breach, including determining (i) the nature of the Personal Data Breach, (ii) the categories and the approximate number of affected Data Subjects, (iii) probable consequences of the Personal Data Breach, (iv) measures which have been taken or are proposed to manage the Personal Data Breach,
      4. assist the Data Controller in reporting Personal Data Breach to the Supervisory Authority or Data Subjects in accordance with applicable Data Protection Law.
   2. The Data Processor will comply with the Personal Data Breach-related obligations and requirements applicable to it under the Data Protection Laws.
4. **Term and termination.** The term of this DPA is co-terminus with the term of the Agreement. In case this DPA will be terminated, the conditions of this DPA shall continue to apply to any processing of Personal Data which is necessary for the winding-up of this DPA until the completion of the winding-up period, return or deletion of the Personal Data, as the case may be.
5. **Deletion and return of the Personal Data.** 
   1. The Data Subject and respectively when applicable the Data Controller maintains all rights in and title to the Personal Data processed by the Data Processor and or its Sub-processors on behalf of the Data Controller.
   2. After the end of provisioning of relevant services to the Data Controller relating to processing of Personal Data or after the termination of this DPA, the Data Processor shall securely delete or return to the Data Controller all Personal Data without undue delay.
6. **Limitation of Liability.** Any claims brought under this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations, set forth in the Agreement.
7. **Miscellaneous.**
   1. This DPA is governed by the law of the Agreement.
   2. This DPA may be executed in two or more counterparts, each of which shall be deemed an original and all of which taken together shall be deemed to constitute one and the same document. The parties may sign and deliver this DPA by facsimile or email transmission.
   3. This DPA may not be modified except by a subsequent written instrument signed by both parties.
   4. If any part of this DPA is held unenforceable, the validity of all remaining parts will not be affected.

**IN WITNESS WHEREOF, the Parties hereto have caused this DPA to be duly executed and delivered by their respective authorized representatives as of the date of last signature below.**

|  |  |
| --- | --- |
| Akamai as **Data Controller** | Vendor as **Data Processor** |
| Signature:  Name: [Full legal name]    Position: [Your position]  Date: [Date] | Signature:  Name: [Full legal name]    Position: [Your position]  Date: [Date] |

**Part III**

**EU 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.

Name of the data exporting organization:

**Akamai entity as defined in Part I, Section A of the DPA**

(as the **data exporter**),

and

**Vendor as defined in Part I, Section B of the DPA**

(as 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.

**Clause 1 - Definitions**

For the purposes of the Clauses:

1. ‘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;
2. ‘the data exporter’ means the controller who transfers the personal data;
3. ‘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;
4. ‘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;
5. ‘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;
6. ‘technical and organizational security measures’ means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized 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:

1. 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;
2. 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;
3. that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;
4. 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, unauthorized 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;
5. that it will ensure compliance with the security measures;
6. 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;
7. 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;
8. 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 sub-processing 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;
9. that, in the event of sub-processing, 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
10. that it will ensure compliance with Clause 4(a) to (i).

**Clause 5 - Obligations of the data importer**

The data importer agrees and warrants:

1. 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;
2. 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;
3. that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred;
4. that it will promptly notify the data exporter about:
5. 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;
6. any accidental or unauthorized access; and
7. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;
8. 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;
9. 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;
10. to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, 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;
11. that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
12. that the processing services by the sub-processor will be carried out in accordance with Clause 11;
13. 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 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 sub-processor of its obligations in order to avoid its own liabilities.

1. 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:
2. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
3. to refer the dispute to the courts in the Member State in which the data exporter is established.
4. 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 Clause.

**Clause 11 - Sub-processing**

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 sub-processing 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 sub-processing 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.

**Appendix 1 to the Standard Contractual Clauses:**

**Data Processing Activities**

Data Exporter

The data exporter is defined in **Part I, Section A** of the DPA.

Data Importer

The data importer is defined in **Part I, Section B** of the DPA.

Data Subjects

The personal data of the following data subjects is processed under this Agreement: As specified in **Part I, Section C** of the DPA.

Categories of data

The personal data transferred concern the following categories of data: As specified in **Part I, Section D** of the DPA.

Special categories of data

As specified in **Part I, Section E** of the DPA.

Description of processing activities:

Any personal data transferred will be subject to the following processing activities: As specified in **Part I, Section F** of the DPA.

**Appendix 2 to the Standard Contractual Clauses:**

**Technical and Organizational measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):**

The technical and organizational security measures implemented by the data importer are as specified in **Part I, Section I** of the DPA.