**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 standard contractual clauses for the transfer of personal data to third countries under the EU Regulation (EU) 2016/679 of of the European Parliament and the Council, 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 transfer of personal data to third countries pursuant Regulation (EU) 2016/679, as attached to this DPA in Part III. The parties agree that the module of these EU standard contractual clauses covering their roles 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**

**STANDARD CONTRACTUAL CLAUSES**

**MODULE TWO: Transfer controller to processor**

**SECTION I**

*Clause 1*

***Purpose and scope***

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)

have agreed to these standard contractual clauses (hereinafter: “Clauses”).

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

*Clause 2*

***Effect and invariability of the Clauses***

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

*Clause 3*

***Third-party beneficiaries***

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

*Clause 4*

***Interpretation***

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

*Clause 5*

***Hierarchy***

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

*Clause 6*

***Description of the transfer(s)***

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

*Clause 7*

***Docking clause***

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

**SECTION II – OBLIGATIONS OF THE PARTIES**

*Clause 8*

***Data protection safeguards***

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

**8.1 Instructions**

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

**8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

**8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

**8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

**8.5 Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

**8.6 Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

**8.7 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter “sensitive data”), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

**8.8 Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[[1]](#footnote-1) (in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

**8.9 Documentation and compliance**

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter’s request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

*Clause 9*

***Use of sub-processors***

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter’s general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects[[2]](#footnote-2). The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter’s request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor’s obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

*Clause 10*

***Data subject rights***

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects’ requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

*Clause 11*

***Redress***

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

*Clause 12*

***Liability***

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer’s responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

*Clause 13*

***Supervision***

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

**SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

*Clause 14*

***Local laws and practices affecting compliance with the Clauses***

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[[3]](#footnote-3);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

*Clause 15*

***Obligations of the data importer in case of access by public authorities***

**15.1 Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

**15.2 Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

**SECTION IV – FINAL PROVISIONS**

*Clause 16*

***Non-compliance with the Clauses and termination***

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

*Clause 17*

***Governing law***

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

*Clause 18*

***Choice of forum and jurisdiction***

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Germany.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

**APPENDIX**

**ANNEX I**

**A. LIST OF PARTIES**

**Data exporter(s):**

1. Name: Akamai Technologies entity as specified in the service agreement and, if applicable, in Part I Section A of the DPA.

Contact person’s name, position and contact details: The Akamai business relationship owner as outlined in the service agreement and its related documents.

*Processing activities relevant to the data transferred under these Clauses:*

The activities relevant for the data transferred under these Clauses are outlined in Part I Section F of the DPA.

Signature and date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Role (controller/processor): **Data Controller.**

**Data importer:**

1. Name:The vendor entity is outlined in Part I Section B of the DPA.

*Contact person’s name, position and contact details:*

[Vendor privacy contact]

*Activities relevant to the data transferred under these Clauses:*

The activities relevant to the data transferred under these Clauses are outlined in Part I Section F of the DPA.

Signature and date: … \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

h

**B. DESCRIPTION OF TRANSFER**

***Categories of data subjects*** *whose personal data is transferred*

The data subjects are outlined in Part I Section C of the DPA.

***Categories of personal data*** *transferred:*

The categories of personal data are outlined in Part I Section D of the DPA.

***The frequency of the transfer***

The data is transferred continuously when the date importer is performing its services to the data exporter.

***Nature of the processing***

The nature of the processing is outlined in Part I Section F of the DPA.

For transfers to (sub-) processors*, also specify subject matter, nature and duration of the processing*

Transfers to sub-processors are outlined in Part I Section H of the DPA.

**C. COMPETENT SUPERVISORY AUTHORITY**

*Identify the competent supervisory authority/ies in accordance with Clause 13*

*The competent supervisory authority of the data exporter is The Bavarian Data Protection Authority.*

**ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

The data importer’s technical and organizational measure are outlined in Part I Section I of the DPA.

In case of transfers to (sub-) processors, the related details are outlined in the data importer’s sub-processing documentation.

1. The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses. [↑](#footnote-ref-1)
2. This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7. [↑](#footnote-ref-2)
3. As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies. [↑](#footnote-ref-3)