**Part I**

|  |  |
| --- | --- |
| 1. Data Controller
 | **Akamai Technologies** [Entity] („Customer“ or „Akamai“) |
| [Akamai registered address] |
| A provider of cloud computing, content delivery, and security services. |
| Contact details: Data Protection Officer, privacy@akamai.com  |
| 1. Data Processor
 | **[Vendor full legal name]** (“Vendor”) |
| [Vendor registered address] |
| [Please describe the business activities of Vendor and Services provided to Akamai] |
| Contact details: [Please provide contact person and contact details for data protection purposes] |
| 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 [ ]  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, stored in or accessible from other jurisdiction(s) than Data Controller’s jurisdiction:[ ]  no[ ]  yes: [Please name all jurisdictions where the Personal Data will be transferred to, stored in or accessible from] |
| 1. Frequency of the cross-border transfer
 | The data is transferred continuously when the Data Processor (data importer) is performing its services to the Data Controller (data exporter). |
| 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 and subject matter of the processing] |
| 1. Data Retention
 | [Please specify the period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period] |
| 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 the European Parliament and the Council (“EU SCCs”), International Data Transfer Addendum to the EU SCC (version B.1.0) as issued by the Information Commissioner's Office under s119A of the Data Protection Act 2018 on February 2, 2022 (“UK Addendum”), 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 and/or on behalf of Data Controller’s affiliates or customers to the extent such affiliates or customers use the services provided by the Data Processor and act as ultimate data controllers, as the case may be.
	2. The parties agree and acknowledge that (i) the Vendor, when providing services to the Data Controller, will be acting as a Data Processor (or sub-processor with respect to Data Controller’s affiliates or customers, if applicable) 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.
	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 under the Agreement; (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 K 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 access to their Personal Data, including but not limited to 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, in the event of transfer of Personal Data which originates from the EU, UK or Switzerland, to the jurisdictions which don’t ensure adequate protection of Personal Data according to applicable Data Protection Laws, the Data Controller and the Data Processor shall be bound by the applicable Cross-Border Transfer Mechanism as outlined in this DPA in Part III. The parties agree that the Cross-Border Transfer Mechanisms outlined in Part III of this DPA are automatically incorporated hereto by signature of this DPA and does not require separate signature. If any similarly applicable standard contractual clauses, other than listed in Part III of this DPA, will be adopted by a Supervisory Authority or other body of competent jurisdiction to govern the cross-border transfer of Personal Data subject to applicable Data Protection Laws the parties agree to incorporate them in accordance with their respective roles.
	4. Where applicable, the Data Controller hereby authorizes the Data Processor to agree on and execute on its behalf (as Data Exporter) the same unmodified standard contractual clauses, as attached to this DPA in Part III, with the authorized Sub-processor (as Data Importer).
5. **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 I 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 providing at least 30 (thirty) days written notice to the Data Controller via email to VendorPrivacy@akamai.com.The Data Controller shall have the right to review and object to the engagement of any new Sub-processor within 30 (thirty) day notice period. If the Data Controller does not provide objection within this period, the engagement of the new Sub-processor shall be deemed accepted. However, the Data Processor remains responsible for ensuring that any Sub-processor complies with the terms of this DPA and applicable Data Protection Laws. In the event Data Controller objects to a new Sub-processor, Data Processor will use commercially reasonable efforts to make available to Data Controller a change in the services or recommend a commercially reasonable change to Data Controller’s configuration without unreasonably burdening Data Controller and without limiting service functionality. If Data Processor is unable to make available such change within a reasonable period of time, which shall not exceed 30 (thirty) days, Data Controller may terminate without penalty the affected order form(s) by providing written notice to Data Processor. Data Processor will refund Data Controller any prepaid fees covering the remainder of the term of such order form(s) without imposing a penalty for such termination on Data Controller.
	3. When the Data Processor has Data Controller’s 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 under this DPA and the Agreement, 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 applicable Cross-Border Transfer Mechanism.
6. **Audits.**

Data Processor shall conduct periodic audits of its processing of Personal Data to ensure compliance with Data Protection Laws and this DPA. Upon Data Controller’s request, Data Processor shall deliver to Data Controller relevant compliance documentation from such audits, certifications (e.g. ISO) or relevant third-party assessment to demonstrate compliance with the Data Protection Laws and this DPA.

In addition, Data Processor shall allow for and contribute to on-site audits of the Data Processor’s processing activities, tools and systems used for processing of Personal Data under this DPA to demonstrate compliance with the Data Protection Laws and this DPA. Such audits shall be limited to one per year unless required by Data Protection Laws, Supervisory Authority or in case of a Personal Data Breach. Audits would have to be notified to Data Processor with no less than 14 (fourteen) days’ prior written notice, shall take place during normal business hours and will be performed by the Data Controller or third party auditor appointed by the Data Controller subject to confidentiality obligations. Each party shall bear own costs of such audit.

1. **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 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.
2. **Term and termination.** The term of this DPA is co-terminus with the term of the Agreement unless the Agreement will be renewed or otherwise extended by the parties. 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.
3. **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.
4. **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.
5. **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**

**Cross-Border Transfer Mechanism**

 **I. EU Data Transfer**

## Transfers of Personal Data which originates from the EU are made pursuant to the EU SCCs, which are deemed entered into (and incorporated into this DPA by this reference) and completed as follows:

1. Applicable EU SCCs Modules:
	1. **Module Two** (Controller to Processor) of the EU SCCs applies when Customer is a controller and Vendor is processing Personal Data for Customer as a data processor pursuant to Part II Section 2 of this DPA.
	2. **Module Three** (Processor to Processor) of the EU SCCs applies when Customer is a data processor and Vendor is processing Personal Data on behalf of Customer’s affiliates or customers as a sub-processor pursuant to Part II Section 2 of this DPA.
2. For each applicable EU SCCs Module, where applicable the following applies:
	1. The optional Docking Clause in Clause 7 shall apply.
	2. In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of sub-processor changes shall be as set forth in Part II Section 6.2 of this DPA.
	3. In Clause 11, the optional language does not apply.
	4. All square brackets in Clause 13 are removed.
	5. In Clause 17 (Option 1), the EU SCCs will be governed by German law.
	6. In Clause 18(b), disputes will be resolved by the courts of Germany.
	7. Annex I. A of the EU SCCs shall be completed as follows:

**Data exporter:**

*Name*: Akamai Technologies entity as specified in Part I Section A of the DPA.

*Contact person’s name, position and contact details:* See Part I Section A of the DPA.

*Activities relevant to the data transferred under these Clauses*: See Part I Section F of the DPA.

*Signature and date*: See DPA.

*Module 2: Role (controller/processor):* Data Controller

*Module 3: Role (processor/processor):* Data Processor

**Data importer:**

*Name:* Vendor entity as specified in Part I Section B of the DPA.

*Contact person’s name, position and contact details:* See Part I Section B of the DPA.

*Activities relevant to the data transferred under these Clauses:* See Part I Section B and F of the DPA.

*Signature and date:* See DPA.

*Module 2: Role (controller/processor):* Data Processor

*Module 3: Role (processor/processor):* Data Processor

* 1. Annex I. B of the EU SCCs shall be completed as follows: See Part I of the DPA.
	2. Annex I. C of the EU SCCs shall be completed as follows: The competent supervisory authority of the data exporter is the Bavarian Data Protection Authority.
	3. Annex II of the EU SCCs shall be completed as follows: Technical and organizational measure are outlined in Part I Section K of the DPA. In case of transfers to sub- processors, the related details are outlined in the data importer’s sub-processing documentation.

**II. UK Data Transfer**

## Transfers of Personal Data which originates from the UK are made pursuant to the UK Addendum, which is deemed entered into (and incorporated into this DPA by this reference) and completed as follows:

1. For Tables 1 and 3 in Part 1 of the UK Addendum - information as set forth in the above Section I EU Data Transfers of this Part III shall apply.
2. For Table 2 in Part 1 of the UK Addendum - the version of the approved EU SCCs with Modules Two and Three as outlined in the above Section I EU Data Transfers of this Part III shall apply.
3. For Table 4 in Part 1 of the UK Addendum - both “Importer” and “Exporter” are selected.

**III. Swiss Data Transfer**

## Transfers of Personal Data which originates from Switzerland are made pursuant to the EU SCCs, which are deemed entered into (and incorporated into this DPA by this reference) and completed as set forth under section I. EU Data Transfer with the following modifications:

1. All references to 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 (“GDPR”) as included in the EU SCCs shall be interpreted to include the Swiss Federal Act on Data Protection of 25 September 2020 (“FADP”) with respect to data transfers subject to the FADP.
2. Clause 13 of the EU SCCs is modified to provide that the Federal Data Protection and Information Commissioner (“FDPIC”) of Switzerland shall have authority over data transfers governed by the FADP.
3. With regards to Clauses 17 and 18 of the EU SCCs, these clauses shall be governed by the law of Switzerland and the parties agree to the jurisdictions of the courts of Switzerland with regard to any disputes that arise from these clauses.
4. The term “EU Member State” as used in the EU SCCs shall not be interpreted in such a way as to exclude data subjects in Switzerland from exercising their rights in their place of habitual residence in accordance with Clause 18(c) of the EU SCCs.