

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 organisation: _____

Address: _____

Tel.: _____

Fax: _____ (the **data exporter**)

and

Name of the data importing organisation: **Akamai Technologies, Inc.**,

Address: 145 Broadway, Cambridge MA,02142, USA

Tel.: +1 877-325-2624

Fax: + 1 617-444-3001 (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:

- (a) '*personal data*', '*special categories of data*', '*process/processing*', '*controller*', '*processor*', '*data subject*' and '*supervisory authority*' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- (b) '*the data exporter*' means the controller who transfers the personal data;
- (c) '*the data importer*' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25 (1) of Directive 95/46/EC;
- (d) '*the subprocessor*' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

- (e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2 Details of the transfer:

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

Clause 3 Third-party beneficiary clause:

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4 Obligations of the data exporter:

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical

- and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
 - (e) that it will ensure compliance with the security measures;
 - (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
 - (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
 - (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
 - (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
 - (j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5 Obligations of the data importer:

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement

- investigation,
- (ii) any accidental or unauthorised access, and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
 - (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
 - (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
 - (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
 - (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
 - (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6 Liability:

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.
The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to

its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7 Mediation and jurisdiction:

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
 - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
 - (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8 Cooperation with supervisory authorities:

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9 Governing Law:

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

Clause 10 Variation of the contract:

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

Clause 11 Subprocessing:

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

agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12 Obligation after the termination of personal data processing services:

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the **data exporter**: _____

Name (written out in full): _____

Position: _____

Address: _____

Signature _____

(stamp of organisation)

On behalf of the **data importer**: Akamai Technologies, Inc.

Name (written out in full): James H Hammons

Position: Assistant Secretary

Address: 145 Broadway, Cambridge, MA 02142 USA

Signature  _____

(stamp of organisation)

Appendix 1 to the Standard Contractual Clauses (processor) Data Processing Activities

Data exporter

The Data Controller is:

Data importer

The data importer is:

A provider of content delivery, media acceleration, web performance and Internet security services.

Data subjects

The personal data of the following data subjects is processed under this Agreement:

Internet end-users accessing the web content of the data exporter and/or using the web services of the data exporter.

Categories of data

The personal data transferred concern the following categories of data:

a) End User Personal Data

Akamai processes Personal Data included within Customer Content ("End User Personal Data") when providing the Services to Customer. Upon the Customer's choice, End User Personal Data may include data such as:

- a. Login credentials;
- b. Subscriber name and contact information;
- c. Financial or other transaction information;
- d. Other Personal Data relating to the individual data subject as set by Customer.

b) Logged Personal Data

Akamai processes Personal Data that is included in log files when performing the Services for Customer (Logged Personal Data"). Logged Personal Data is Personal Data logged by Akamai servers, relating to the access to Customer Content over the Akamai platform by Customer's end users, as well as logged personal data associated with user activity and interaction with web and internet protocol sessions transiting Akamai's servers as part of a data subject's session with the Customer's web property. Logged Personal Data include such data as:

- a. End user IP addresses;
- b. URLs of sites visited with time stamps (with an associated IP address);
- c. Geographic location based upon IP address and location of Akamai server;
- d. Telemetry data (e.g., mouse clicks, movement rates, and related browser data).

c) Site Personal Data

Akamai processes Personal Data associated with user activity and interaction with web and internet protocol sessions transiting Akamai's servers as part of a data subject's session with the Customer's web property ("Site Personal Data"). The Site Personal Data consists of user telemetry data (e.g., mouse clicks, movement rates, and user agent and related browser data) designed to measure website performance.

d) Enterprise Security Personal Data

Akamai processes Personal Data on behalf of Customers of Akamai Enterprise Security Services that are provided by Customer or collected during the provision of Services in order to protect users of the Customer's enterprise network and the network itself from Internet security and policy abuse risks ("Enterprise Security Personal Data"). The Enterprise Security Personal Data includes such data as:

- a. Login and user authentication data;
- b. Contents of communications, including attachments
- c. Browser and device information, including location information
- d. URLs visited

e) Special categories of data

Customer as the Data Controller decides which categories of data are included in the End User Personal Data. Where Customer chooses to include special categories of data in the Customer Content, Akamai will process this data as End User Personal Data, as instructed by the Customer.

f) Categories of data processed by particular Akamai Services

Akamai maintains a list of service categories that provide further information regarding the processing of Personal Data conducted in providing Services in each category. This list is available at www.akamai.com/compliance/privacy/.

Description of processing activities:

The following processing activities are performed when providing the Services:

a) End User Personal Data

The data importer processes End User Personal Data on behalf of the data exporter, including instructions given through the service agreement, or via configuration of the Services via the relevant customer portals or support processes.

b) Logged Personal Data

The data importer collects Logged Personal Data and conducts analysis of Logged Personal Data to provide the data exporter with copies of traffic logs and data analytic reports related to the performance of its services and the the data exporter's web properties.

Logged Personal Data is also be processed for purposes of Service issue resolution.

c) Site Personal Data

The data importer processes Site Personal Data to provide website monitoring and analytics services to the data exporter to enable it to understand the nature of end user traffic to their web properties, as well as to monitor the performance of such properties.

d) Enterprise Security Personal Data

The data importer's Enterprise Security Services provides the data exporter with tools and services to protect its employees and guests, as well as its network infrastructure from Internet threats. In addition, these same tools may be used to monitor network activity, provide secure access to applications, and establish and enforce access policies. To provide these services, the data importer processes Enterprise Security Personal Data as needed to access and monitor network traffic, process and store access credentials and related network data as part of the network infrastructure services ordered by the data exporter.

**Appendix 2 to the Standard Contractual Clauses (processor):
Technical and Organisational Measures to secure the Personal Data processed:**

Akamai's Technical and Organisational Measures to secure the Personal Data processed are publicly available in Akamai's Privacy Trust Center,
<https://www.akamai.com/us/en/multimedia/documents/akamai/technical-and-organizational-measures-to-secure-the-personal-data.pdf>