Data Protection Addendum

This Data Protection Addendum (this "**Addendum"**), effective as of May 25th, 2018 ("**Effective Date**"), is entered into by and between the parties to the service agreement(s) for the Akamai Services as amended (the "**Terms & Conditions**"), entered into by and between Akamai Technologies, Inc. and/or any of its Affiliates (together "**Akamai**") and the customer ("**Customer**") on or prior to the date hereof. This Addendum supplements and amends, as necessary, the Terms and Conditions. If the provisions of this Addendum and the Terms & Conditions conflict, then the provisions of this Addendum shall control. Unless otherwise defined herein, all capitalized terms used herein shall have the meanings assigned to such terms in the Terms & Conditions.

NOW, THEREFORE, in consideration of the following as set forth in this Addendum, the parties hereby agree as follows:

1. Definitions

"Agreement Personal Data"	means the personal data (as defined under Data Protection Laws) in relation to end customers of the Customer and/or users of those Customer websites or web applications, facilities or services which benefit from the Services, as set out in Appendix 1.
"Authorised Processor"	means any third party appointed by Akamai in accordance with these Terms & Conditions to process Agreement Personal Data, for which Akamai serves as a controller, on behalf of and as instructed by Akamai. For the avoidance of doubt, suppliers to Akamai responsible for the transit of communications through Akamai servers located in server colocation and bandwidth connectivity providers around the world, where such providers have no access to such communications nor any data located on Akamai operated servers (i.e., "mere conduits"), shall not be considered Authorised Processors.
"Authorised Sub-Processor"	means any third party appointed by Akamai in accordance with these Terms & Conditions to process Agreement Personal Data, for which Akamai serves as a processor, on behalf of and as instructed by Akamai. For the avoidance of doubt, suppliers to Akamai responsible for the transit of communications through Akamai servers located in server colocation and bandwidth connectivity providers around the world, where such providers have no access to such communications nor any data located on Akamai operated servers (i.e., "mere conduits"), shall not be considered Authorised Sub-Processors.
"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 Akamai and the Customer in respect of the processing of Agreement Personal Data pursuant to these Terms & Conditions, including: prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data ("**Directive**"); on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council 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) ("**GDPR**"); the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended or replaced by or in relation to the proposed Regulation on Privacy and Electronic Communications); and any legislation that, in respect of an EU member country implements the GDPR (or, in respect of the United Kingdom replaces or converts into domestic law the GDPR, the proposed Regulation on Privacy and Electronic Communications or any other law relating to data and privacy as a consequence of the United Kingdom leaving the European Union);

	and references to **"data controller"**, **"controller"**, **"data subjects", "data processor"**, **"processor", "personal data"**, **"process"**, **"processed"** and **"processing"**, shall have the meanings set out in, and will be interpreted in accordance with: in respect of processing undertaken prior to 25 May 2018, the Directive; and in respect of processing undertaken on or after 25 May 2018, GDPR and any data protection legislation in a member country introduced to adopt, clarify and/or supplement GDPR from that date.
"Data Breach Incident"	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Agreement Personal Data transmitted, stored or otherwise Processed.
"Privacy Shield"	means, collectively, the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework self-certification programs operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C (2016)4176 dated July 12, 2016 and by the Swiss Federal Council on January 11, 2017 respectively.
"Standard Contractual Terms for Controllers"	means the EU standard contractual clauses for Data Controllers established in third countries pursuant to European Commission Decision (2004/915/EC) under the EU Directive (95/46/EC), as set out in Schedule 3 or as may be updated or replaced from time to time.
"Standard Contractual Terms for Processors"	means the EU standard contractual clauses for Data Processors established in third countries pursuant to European Commission Decision (2010/87/EC) under the EU Directive (95/46/EC), as set out in Schedule 2 or as may be updated or replaced from time to time.
"Supervisory Authorities"	means any applicable authority that oversees compliance with the Data Protection Laws, including as defined in GDPR.

2. Data Protection

2.1 **Compliance with Law.** Both the Customer and Akamai shall comply with their respective obligations under the Data Protection Laws.

2.2 **Data Processor Terms.** The parties agree and acknowledge that Akamai, and any relevant Akamai Affiliates, when providing the Services to Customer, will be acting as a data processor in respect of the processing by or for it of End User Personal Data and Customer Personal Data, as defined in Schedule 1, to provide the Services in accordance with the Terms & Conditions and, Customer hereby authorises Akamai to process the End User Personal Data during the term of the Terms & Conditions as a Data Processor (on its and its Affiliates behalf) for the purposes of providing the Services only.

2.2.1 Akamai is authorised to engage, use or permit an Authorised Sub-Processor for the Processing of End User Personal Data and Customer Personal Data provided that:

(a) Akamai undertakes reasonable due diligence on them in advance to try to ensure appropriate safeguards for End User Personal Data and Customer Personal Data and respective individual rights in accordance with applicable Data Protection Laws;

(b) Akamai shall provide Customer with advance written notice of any intended changes to any Authorised Sub-Processor, allowing Customer sufficient opportunity to object; and

(c) The Authorised Sub-Processor's activities must be specified in accordance with the obligations set out in this Section 2.2.

Without prejudice to this Section 2.2.1, Akamai shall remain responsible for all acts or omissions of the Authorised Sub-Processor as if they were its own.

2.2.2 Akamai shall (and procure that any Authorised Sub-Processor shall):

(a) process the End User Personal Data and Customer Personal Data only on documented instructions from Customer, including these Terms & Conditions, technical specifications provided for administration of the Services, and configuration settings set in any of Akamai's customer portals provided for administration of the Services;

(b) without prejudice to Section 2.2.2(a), ensure that End User Personal Data and Customer Personal Data will only be used by Akamai as set forth in these Terms & Conditions;

(c) ensure that any persons authorised to process the End User Personal Data or Customer Personal Data:

(i) have committed themselves to appropriate confidentiality obligations in relation to End User Personal Data and Customer Personal Data or are under an appropriate statutory obligation of confidentiality;

(ii) access and process the End User Personal Data and Customer Personal Data solely on written documented instructions from Customer; and

(iii) are appropriately reliable, qualified and trained in relation to their processing of End User Personal Data and Customer Personal Data;

(d) implement (and assist Customer to implement) technical and organisational measures at a minimum to the standard set out in Schedule 2 to ensure a level of security appropriate to the risk presented by processing the End User Personal Data and Customer Personal Data, in particular from a Data Breach Incident;

(e) notify Customer without undue delay (and in any event no later than 48 hours) after becoming aware of a Data Breach Incident as set forth in Section 5;

(f) assist Customer in:

(i) responding to requests for exercising the Data Subject's rights under the Data Protection Legislation, by appropriate technical and organisational measures, insofar as this is possible, provided that Akamai shall not be required to store or process any data for the purpose of re-identifying an individual when such information is not normally processed or stored by Akamai;

(ii) reporting any Data Breach Incident to any Supervisory Authority or Data Subjects and documenting any Data Breach Incidents;

(iii) taking measures to address the Data Breach Incident, including, where appropriate, measures to mitigate its possible adverse effects; and

(iv) conducting mandatory privacy impact assessments of any processing operations and consulting with any applicable Supervisory Authority or appropriate persons accordingly;

(g) at the choice of Customer, to the extent that End User Personal Data or Customer Personal is stored by Akamai, securely delete or return all End User Personal Data or Customer Personal Data to Customer after the end of the provision of relevant Services relating to processing, and securely delete any remaining copies and certify when this exercise has been completed; and

(h) make available to Customer all information necessary to comply with its obligations to do so under the Data Protection Laws and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer.

2.3 **Data Controller Terms.** The parties agree and acknowledge that Akamai, and any relevant Akamai Affiliates, when providing the Services to Customer, will be acting as a data controller in respect of the processing by or for it of the Logged Personal Data, as defined in Schedule 1, to provide the Services in accordance with the Terms & Conditions and, to the extent that Akamai is acting in its capacity as a data controller in respect of such data, it will, and will procure that its Authorised Processors will, at all times process the data in accordance with its obligations under the Data Protection Laws, the Terms & Conditions and this Addendum, including Schedule 1.

2.3.1 The parties agree and acknowledge that to the extent that the Customer and any relevant Customer Affiliates will be acting as a separate data controller in respect of the any Agreement Personal Data, that it will at all times:

(a) process the Agreement Personal Data in accordance with its obligations under the Data Protection Laws;

(b) have all necessary rights and consents required to ensure its direct or indirect disclosure of Agreement Personal Data to Akamai and for Akamai to use the Agreement Personal Data as set forth herein and in the Terms & Conditions, is fair and lawful and in accordance with Data Protection Laws. Akamai shall assist as necessary in providing information to permit Customer to provide appropriate notice to its End Users regarding Akamai's processing of Logged Personal Data.

2.4 **Transfers Outside of the EEA.**

2.4.1 To the extent that there is a transfer of End User Personal Data and/or Customer Personal Data from the Customer or a Customer Affiliate in the European Economic Area ("**EEA**") to Akamai (or an Akamai Affiliate) outside the EEA, the Customer and Akamai will:

(a) procure the data exporter and data importer (as defined under Data Protection Laws) enter into Standard Contractual Clauses for Processors as set forth in Schedule 2 hereof; or

(b) otherwise ensure such transfer of End User Personal Data and Customer Personal Data is protected by adequate transfer mechanisms in compliance with the Data Protection Laws, including by certification in the Privacy Shield programs in the United States, or Binding Corporate Rules.

2.4.2 To the extent that there is a transfer of Logged Personal Data from the Customer or a Customer Affiliate in the EEA to Akamai (or an Akamai Affiliate) outside the EEA, the Customer and Akamai will:

(i) procure the data exporter and data importer (as defined under Data Protection Laws) enter into Standard Contractual Clauses for Controllers as set forth in Schedule 3 hereof; or

(ii) otherwise ensure such transfer of Logged Personal Data is protected by adequate transfer mechanisms in compliance with the Data Protection Laws, including by certification in the Privacy Shield programs in the United States, or Binding Corporate Rules.

2.4.3 To the extent that there is a transfer of Logged Personal Data from Akamai or an Akamai Affiliate in the EEA to any Akamai Affiliate and/or other third party appointed by Akamai (or any Authorised Processor appointed by Akamai) to process the Agreement Personal Data outside the EEA, Akamai will (or will procure the Akamai Affiliate will):

(a) where the recipient entity is in the US, ensure such entity has in place a valid Privacy Shield certification, which is maintained for the duration of the processing; or

(b) procure the data exporter and data importer (as defined under Data Protection Laws) enter into Standard Contractual Clauses for Processors as set forth in Schedule 3 hereof; or

(c) otherwise ensure such transfer of Logged Personal Data is protected by adequate transfer mechanisms, such as Binding Corporate Rules, in compliance with the Data Protection Laws.

2.4.4 To the extent that there is a transfer of Logged Personal Data from Akamai or an Akamai Affiliate in the EEA to or for the Customer outside the EEA, Akamai and the Customer will (or will procure that the relevant third party will):

(a) where the recipient entity is in the US, ensure such entity has in place a valid Privacy Shield certification, which is maintained for the duration of the processing; or

(b) where the recipient entity is not in the US or where Privacy Shield does not apply, enter into the Standard Contractual Clauses for Controllers with Akamai as 'data exporter'; or

(c) ensure such transfer of Agreement Personal Data is protected by adequate transfer mechanisms in compliance with the Data Protection Laws.

3. Audits

Akamai shall conduct periodic audits of its processing of Agreement Personal Data to ensure compliance with applicable Data Protection Laws, including applicable organisational and technical measures necessary to protect Agreement Personal Data. Upon reasonable request, Akamai shall deliver to Customer relevant compliance documentation from such audit(s) (e.g., Akamai's then-current SOC 2 Type 2 (or its successor) report) and certain, selected policies, procedures and evidence that have been approved for distribution to customers.

4. Cooperation

Akamai shall reasonably cooperate with Customer to enable Customer to respond to any requests, complaints or other communications from data subjects and governmental, regulatory or judicial bodies relating to the processing of Agreement Personal Data under the Terms & Conditions.

5. Data Breach Incidents

5.1 Akamai shall notify Customer without undue delay, after becoming aware of a Data Breach Incident by providing notice via e-mail to the 24-hour security contacts provided by Customer in Akamai's Luna Control Center customer portal. Where Akamai needs to notify a supervisory authority about an incident it will align its communication with the supervisory authority with the Customer as reasonable, permitted, and appropriate.

5.2 Furthermore, in the event of a Data Breach Incident, Akamai shall:

5.2.1 provide timely information and commercially reasonable cooperation so that the Customer may fulfil its obligations under Applicable Privacy Laws in regards to any required notifications; and

5.2.2 take all commercially reasonable measures and actions as are appropriate to remedy or mitigate the effects of the Data Breach Incident and shall keep Customer (and where applicable the supervisory authority) up-to-date about all developments in connection with the incident.

6. Authorizations

The Customer hereby acknowledge and accepts that the Akamai platform is made up of servers owned and operated by Akamai or its Affiliates globally and that connections between a Customer web property and one of its End Users may be made through any of these servers dependent upon the location of the Customer's End User. A list of all countries in which Akamai operates servers, a list of all Akamai Affiliates that own such servers, as may be updated from time to time, as well as a list of all sub-processors that Akamai uses to provide the services, can be found at www.akamai.com/compliance/privacy. Customer hereby consents to Akamai's use of the listed sub-processor(s). In addition, to the extent that any applicable Data Protection Laws would deem an Akamai Affiliate by virtue of its ownership of servers used to provide the services, to be a sub-processor for purposes of this Addendum, Customer hereby consents to Akamai's use of such sub-processor(s).

7. Miscellaneous

7.1 Except for the changes made by this Addendum, the Terms & Conditions remain unchanged and in full force and effect. This Addendum 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 Addendum by facsimile or email transmission.

7.2 The obligations placed upon the parties under this Addendum shall survive so long as Akamai possesses Agreement Personal Data processed as a result of Customer's use of the Services.

7.3 This Addendum may not be modified except by a written instrument signed by both parties.

7.4 If any part of this Addendum is held unenforceable, the validity of all remaining parts will not be affected.

Schedule 1 of the Data Protection Addendum:
Details of Akamai's Personal Data Processing Activities

Akamai is a provider of content delivery, media acceleration, web performance and Internet security services.

Data Subjects
Akamai processes the personal data of the following data subjects when performing Services under the Sales Terms & Conditions:

- Internet end-users accessing Customer's content and/or using Customer's services.
- Customer Employees and authorised representatives.

Categories of data
In providing services to Customer, Akamai may process one or more of the following categories of data:

(i) **Personal Data in Customer Content**: Personal data included within Customer Content that is cached or stored on Akamai's servers for purposes of optimization, is provided by a customer for storage on Akamai servers, or that otherwise transits the Akamai servers as part of a data subject's session with the customer's web property ("End User Personal Data"). End User Personal Data may include,

a. Login credentials

b. Subscriber name and contact information

c. Financial or other transaction information

d. Other information relating to the individual data subject as requested or provided by the customer through the use of its web property.

"Customer Content", means content and applications, including any third-party content or applications, provided to Akamai for delivery via or use by the Akamai network.

(ii) **Personal Data in Akamai Logged Data**: Akamai Network Data, logged by Akamai servers, relating to the delivery of information over the Akamai platform, 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"). Logged Personal Data may include,

a. End user IP addresses

b. Page activity data and URLs of sites visited with time stamps (when combined with an associated IP address)

c. Geographic location based upon IP address and location of Akamai server (no more granular than city level)

d. Telemetry data (e.g., mouse clicks, movement rates, and user agent and related browser data)

Akamai Network Data means all models, reports, analyses, statistics, databases and other information created, compiled, analyzed, generated or derived by Akamai in connection with delivery of services and the operation of Akamai's network, regardless of the media in which such Akamai Network Data is embodied.

(iii) **Personal Data in Customer Contact Information**: Personal data of Customer employees and representatives collected and maintained by Akamai to support the customer relationship ("Customer Personal Data"). Customer Personal Data may include, by way of example only,

a. contact names

b. titles

c. business addresses

d. email addresses

e. telephone numbers

f. portal credentials

Special categories of data

Akamai does not collect or process special categories of data except to the extent that Customer Content includes any special or otherwise sensitive data. Customer controls what data is included in Customer Content and ensures that in case any special categories of data are included, end user notice as for Akamai's processing activities has been provided and respective explicit consent has been received. Akamai makes tools available to Customer to ensure secure treatment of such data. Akamai, however, is not typically in a position to know what personal data is contained within Customer Content.

Description of Akamai's Personal Data processing activities:

The following provides a more detailed description of the processing applied in each case.

End User Personal Data

Akamai operates largely as a conduit for End User Personal Data collected, processed and transmitted by its customers via the Akamai services. The Customer determines what End User Personal Data is collected or otherwise used by its web property; whether and for how long such End User Personal Data should be cached by Akamai's servers; whether to use secure services offered by Akamai for encrypted delivery of its web traffic; and whether and for how long End User Personal Data is stored on Akamai's NetStorage servers. Akamai determines how such End User Personal Data is transmitted via its server platform by determining optimal routes and caching, and other necessary service parameters based upon numerous factors including customer configurations, Internet congestion, and best available routes.

As described above Customer determines through design and configuration of its web property what End User Personal Data will flow across Akamai's servers. The Customer, therefore, will be responsible for compliance with applicable laws for such processing (e.g., appropriate end user notices or consents, and having chosen services appropriate for the type of End User Personal Data transiting Akamai's servers (e.g., PCI compliant services)).

Absent Customer request, Akamai does not store or otherwise process End User Personal Data other than as required to provide the services purchased by the customer.

Logged Personal Data

Akamai conducts analysis of Logged Personal Data traffic in order to deliver and improve its services, and provide customers with data analytics products related to performance of the services and the customers' web properties, as well as fraud and Bot management capabilities. Akamai also conducts traffic analysis to derive and compile information relating to the type, nature, content, identity, behavior, signature, source, frequency, reputation and other characteristics of malicious Internet traffic and activity. The resulting threat data is integrated into Akamai's tools, products (including data products that contain a subset of the threat data), and services to protect itself and its customers from cyber-attacks, hacking, malware, viruses, fraud, exploits and other malicious activity.

Logged Personal Data may also be processed for purposes of service issue resolution, and, subject to applicable confidentiality obligations, aggregate reporting (i.e., the report does not identify the Customer or the data subjects visiting its web properties) such as Akamai's "State of the Internet".

Customer Personal Data

Akamai collects and processes Customer Personal Data to provide access to and use of services, communications with customers, and to manage customer relations. This data is stored by Akamai in its portal(s) (such as Luna), customer community and developer sites, and in internal business process tools.

Schedule 2 to the Data Protection Addendum

EU Standard Contractual Clauses (processor)

For the purposes of Article 26(2) of Directive 95/46/EC and Article 42 (2b) of the Regulation EU 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("GDPR") 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: Customer with registered offices in the European Union.

……

(the data exporter)

And

Name of the data importing organisation:

Akamai Technologies, Inc., 150 Broadway, Cambridge MA,02142, USA

……

(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.

And

HAVE AGREED to comply with the GDPR (once in effect) and all other Data Protection Laws applicable to the processing of data by the data importer on behalf of the data exporter.

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 and the GDPR;

(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 and Article 41 (2) of the GDPR;

(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 or the GDPR;

(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.

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

Data Exporter = Data Controller

The Data Controller is

An entity using the data importer's services to deliver and secure the Data Controller's web properties.

Data Importer = Data Processor

The Data Processor 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 Data Controller's content and/or using Data Controller's services.

Categories of data

The personal data transferred concern the following categories of data:

Personal Data in Customer Content: Personal data included within the Customer Content that is cached or stored on Data Processor's servers for purposes of optimization, is provided by the Data Controller for storage on Data Processor servers, or that otherwise transits the Data Processor servers as part of a data subject's session with the Data Controller's web property ("End User Personal Data"). End User Personal Data may include,

a. Login credentials

b. Subscriber name and contact information

c. Financial or other transaction information

d. Other information relating to the individual data subject as requested or provided by the Data Controller through the use of its web property.

"Customer Content", means content and applications, including any third-party content or applications, provided to Data Processor for delivery via the Data Processor network.

Special categories of data

Not applicable

Description of processing activities:

Data Processor operates largely as a conduit for End User Personal Data collected, processed and transmitted by its customers via the its services. The Data Controller determines what End User Personal Data is collected or otherwise used by its web property; whether and for how long such End User Personal Data should be cached by Data Processor's servers; whether to use secure services offered by Data Processor for encrypted delivery of its web traffic; and whether and for how long End user Personal Data is stored on Data Processor's NetStorage servers. Data Processor determines how such End User Personal Data is transmitted via its server platform by determining optimal routes and caching, and other necessary service parameters based upon numerous factors including customer configurations, Internet congestion, and best available routes.

As described above customer determines through design and configuration of its web property what End User Personal Data will flow across Data Processor's servers. The Data Controller, therefore, will be responsible for compliance with applicable laws for such processing (e.g. appropriate end user notices or consents, and having chosen services appropriate for the type of End User Personal Data transiting Data Processor's servers (e.g., PCI compliant services)).

Absent customer request, Data Processor does not store or otherwise process End User Personal Data other than as required to provide the services purchased by the Data Controller.

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

1. Measures to prevent unauthorized persons from gaining entry to data processing systems with which personal data are processed or used (**entry control**):
   The Data Processor monitors its servers and the rooms in which the servers are deployed with perimeter cameras. It requires its co-location facility partners to restrict physical access to its servers to persons that have been authorized in advance to access the servers, inter alia by picture identification. Such persons are checked in and escorted to the servers by the personnel of the Data Processor's co-location facility partner. The Data Processor also requires its co-location facility partners to enforce verification of the requester prior to answer any service request. The co-location facility partner may not attempt to gain any sort of access to the Data Processor's data systems without written instructions from the Data Processor. Physical access to the servers by field technicians for purposes of first instalment or maintenance is limited to the technical functions of the servers. Field technicians do not have control over the ability of such servers to process the customer's ("Data Controller's") content.

2. Measures to prevent processing systems from being used without authorisation (**entry control**):
   The Data Processor limits the access to its data systems according to its business requirements and the least privilege principle. For example, field technicians are not granted administrative access to servers processing Data Controller's content. Field technicians performing system diagnostics and analysis are provided with read-only logins. Administrative access is restricted to trained and authorized employees of the Data Processor. Field technicians are not granted administrative access to the servers processing the Data Controller's content. Remote administrative access is only available via cryptographically secure connections, systems authenticate administrative connections using asymmetric key cryptography. User administrative access is provided through an access control gateway, which enforces a need-have access grant authorization model. All connections through the authorization gateway are logged. User SSH system are routinely rotated and access is immediately removed in case of reports of theft of devices or the termination of a person's employment.

3. Measures to ensure that persons entitled to use a data processing system have access only to the data to which they have access rights to and that personal data cannot be read, copied, modified or removed without authorization during processing or use and after storage (**access control**):
   A system of grants is used to track and permit access to all data processing systems of the Data Processor.
   Access to the Data Processor's systems used to process the Data Controller's content is gained via the Data Processor's authorization gateway. Access to the authorization gateway itself requires possession of a grant authorized by one or more second parties, as well as a deployed SSH key. Issuance of a deployed SSH key requires access to the corporate network environment using a device with a corporate PKI issued Network Access Control (NAC) certificate, valid corporate authentication credentials for the Data Processor's corporate web services, and either confirmation of possession of a usable, unexpired prior key or the confirmation by the Data Processor's Network Operations Command Center (NOCC) of the user's identity.

   Access to the Data Processor's corporate network requires using a device with a corporate PKI issued NAC certificate. Access to data processing systems within the corporate network requires the NAC certificate as well as user authentication via either the Duo Security, Inc. Trusted Access System or the corporate active directory username and password management system.
   In case of password authentication, the complexity of the password is ensured by the Data Processor's password policy (e.g. multiple character types, length of min. 8 characters, change requirement after 120 days, inability to reuse a password within the following 12 month).
   The Data Processor does not provide user accounts to servers transmitting content. Administrative access to such servers is limited to a number of authorized employees of the Data Processor. Access to these servers by authorized employees on a user level is logged by an authentication gateway. Remote access via the authentication gateway utilizes SSH keys and asymmetric cryptography. Introduction of a new SSH key requires either direct confirmation of identity with the Data Processor's NOCC or possession of the prior SSH key, the prior SSH key password, a machine's NAC for the Data Processor's corporate network and a corporate Active

Directory username and password.

4. Measures to ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged (**transmission control**):
   The Data Processor has put in place a robust alert management system that provides for extensive monitoring of all servers. Fine grained monitoring of running processes allows the definition of predefined alerts to catch unexpected and suspicious behavior, including the execution of rogue processes.
   In addition, the Data Controller can control access to the personal data in its content while having the Data Processor transmitting traffic to its server over encrypted and authenticated connections by its configuration of the services in the Data Processor's "LUNA Portal". The Data Controller can control storage of personal data in its content by configuring property specific content caching rules. By it configuration the Data Controller can also limit the storage of personal data in its content to servers with enhanced physical security controls only.

5. Measures to ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems, modified or removed (**input control**):
   Access to the Data Processor's server is logged and monitored via audit systems and processes. Log data gathered by web-servers is digitally signed by "Edge Servers" and is audited by the distributed data processing facilities, to ensure that it is not modified or corrupted. Respective access logs consisting of aggregated and anonymized log data are provided to the Data Controller as part of the Data Processor's "Log Delivery Service" offering.

6. Measures to ensure that during processing the personal data, is processed strictly in accordance with the instructions of the Data Controller (**instruction compliance control**):
   The Data Processor's robust alert system ensures that it transmits the content only in accordance with the instructions of the Data Controller (which he has provided by way of its configuration how to process the content within the Data Processor's LUNA Portal).
   The Data Controller is responsible for defining or approving configuration policies for the content. The Data Processor does not cache personal data unless instructed to do so by the Data Exporter through configuration policies or otherwise. In addition, the Data Controller's content is cached according to the TTL (Time-To-Live) specified by him, and the Data Controller may select service levels which include enhanced physical security for Edge Servers and appropriate physical security controls. The Data Processor's GHost control language provides a mechanism for controlling caching of content, manipulating, and transmitting content passing through the Secure Content Delivery Network. The Data Processor has storage controls in place addressing the processing of Log Data in accordance with the instructions by the Data Exporter. Such controls are subject to various third party assessments, e.g. the Data Processor's annual ISO 27002 assessment.

7. Measures to ensure that personal data are protected from accidental destruction or loss (**availability control**):
   The Data Processor's web server networks have been created matching the principles of availability. The server network is self-curing and ensures that the content of the Data Controller is transmitted via the server network, even in case of an outage of single servers. The integrity of the Log Data is ensured by various storage controls (e.g., log retention control) that are subject to several regular third party assessment, e.g., the Data Processor's annual ISO 27002 assessment.

8. Measures to ensure that data collected for different purposes are processed separately (**segregation control**):
   The Data Processor separates the environment for development, software, engineering, from the environment for testing and the environment for operations and has put in place several controls to ensure the code development, testing and production data handling environments are separated. E.g. employees within the development team do not have access to the same systems as the employees within the test or operation team. Separate cryptographic credentials are used to access development, test, operations and production environments, critical network operations systems are further isolated from the corporate, development and test network environments. The separation is supervised by granular logging of access to the production and operations servers, change control processes and by the responsible management.

Schedule 3 to the Data Protection Addendum

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)

Data transfer agreement

between

Customer, with registered address in the European Union

hereinafter "data exporter"

and

Akamai Technologies, Inc., 150 Broadway, Cambridge MA 02142, USA

hereinafter "data importer"

each a "party"; together "the parties".

Definitions

For the purposes of the clauses:

a) "personal data", "special categories of data/sensitive data", "process/processing", "controller", "processor", "data subject" and "supervisory authority/authority" shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby "the authority" shall mean the competent data protection authority in the territory in which the data exporter is established);

b) "the data exporter" shall mean the controller who transfers the personal data;

c) "the data importer" shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country's system ensuring adequate protection;

d) "clauses" shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

I. Obligations of the data exporter

The data exporter warrants and undertakes that:

a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.

d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.

e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

II. Obligations of the data importer

The data importer warrants and undertakes that:

a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

b) It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.

c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

d) It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.

e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).

f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).

g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.

h) It will process the personal data, at its option, in accordance with:

i. the data protection laws of the country in which the data exporter is established, or

ii. the relevant provisions[1] of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data[2], or

iii. the data processing principles set forth in Annex A.

Data importer to indicate which option it selects: (iii)

Initials of data importer: AS

i) It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

i. the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

ii. the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

iii. data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or

iv. with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer.

III. Liability and third party rights

a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

IV. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

V. Resolution of disputes with data subjects or the authority

a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

c) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or

of the authority which is final and against which no further appeal is possible.

VI. Termination

a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

b) In the event that:

i. the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

ii. compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

iii. the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

iv. a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or

v. a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VII. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VIII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

ANNEX A

DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.

2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.

4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.

7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to "opt-out" from having his data used for such purposes.

8. Automated decisions: For purposes hereof "automated decision" shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

a) i. such decisions are made by the data importer in entering into or performing a contract with the data subject, and

ii. the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

or

b) where otherwise provided by the law of the data exporter.

ANNEX B

DESCRIPTION OF THE TRANSFER

Data subjects

The personal data transferred concern the following categories of data subjects:

- Internet end-users accessing the Data Exporter's content and/or using its services.
- Data Exporter Employees and authorised representatives.

Purposes of the transfer(s)

The transfer is made for the following purposes:

The Logged Personal Data is collected and transferred to aggregated processing systems for the purpose of providing, developing and improving content delivery, media acceleration, web performance and analytics, and Internet security services. The Processing of such data is described in Schedule 1 of the Data Protection Addendum.

The Customer Personal Data is collected and processed for purposes of contract and service administration, via parties interactions and Data Importer service portals (e.g. Luna).

Categories of data

The personal data transferred concern the following categories of data:

(i) **Personal Data in Akamai Logged Data**: Akamai Network Data, logged by Data Importer servers, relating to the delivery of information over the Data Importer platform, as well as logged personal data associated with user activity and interaction with web and internet protocol sessions transiting Data Importer's servers as part of a data subject's session with the Data Exporter's web property ("Logged Personal Data"). Logged Personal Data may include,

a. End user IP addresses

b. Page activity data and URLs of sites visited with time stamps (when combined with an associated IP address)

c. Geographic location based upon IP address and location of Akamai server (no more granular than city level)

d. Telemetry data (e.g. mouse clicks, movement rates, and user agent and related browser data)

Akamai Network Data means all models, reports, analyses, statistics, databases and other information created, compiled, analyzed, generated or derived by Akamai in connection with delivery of services and the operation of Akamai's network, regardless of the media in which such Akamai Network Data is embodied.

(iii) **Personal Data in Customer Contact Information**: Personal data of Data Exporter employees and representatives collected and maintained by Akamai to support the customer relationship ("Customer Personal Data"). Customer Personal Data may include, by way of example only,

a. contact names

b. titles

c. business addresses

d. email addresses

e. telephone numbers

f. portal credentials

Recipients

The personal data transferred may be disclosed only to the following recipients or categories of recipients:

Employees of the data importer and its Affiliates who need to have access to the personal data transferred during the course of the provisioning of the data importer's services to the data exporter, as well as for support of the services and administration of the contract(s) between the parties.

Sensitive data

Not applicable

Contact points for data protection enquiries
Dr. Anna Schmits, Data Protection Officer EMEA,
Akamai Technologies GmbH, Parkring 20-22, 85748 Garching, Germany

---

[1] "Relevant provisions" means those provisions of any authorisation or decision except for the enforcement provisions of any authorisation or decision (which shall be governed by these clauses).
[2] However, the provisions of Annex A.5 concerning rights of access, rectification, deletion and objection must be applied when this option is chosen and take precedence over any comparable provisions of the Commission Decision selected.