Limelight NETWORKS

EXPERIENCE FIRST

limelight.com

Limelight Networks, Inc.

Data Protection Addendum (DPA)

Table of Contents

This Data Protection Addendum (this **“Addendum”**), is incorporated into and made part of the Limelight Networks Terms of Service (as amended, the **“Terms of Service”**) entered into between Limelight Networks, Inc., its Affiliates and subsidiaries (**“Limelight”**) and **Customer**. If any provisions of this Addendum conflicts with any provision of the Terms of Service, then the applicable provisions of this Addendum controls. Capitalized terms used in this Addendum without definition have the meanings assigned to them in the Terms of Service.

1. Certain Definitions

“Applicable Privacy Law(s)” means all worldwide data protection and privacy laws and regulations applicable to the processing of Personal Data under this Addendum, including, where applicable, EU Data Protection Law.

“EU Data Protection Law” means Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (**“GDPR”**).

“EEA” means the European Economic Area (including the United Kingdom).

“Model Clauses” means the standard contractual clauses issued June 4, 2021, as approved by the European Commission for the purposes of Article 26(2) of GDPR for the onward transfer of personal data of EU citizens to any country and / or recipient that is not recognized as providing an adequate level of protection for Personal Data.

“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.

“Security Incident” means the unauthorized access, collection, acquisition, use, disclosure or loss of Personal Data processed on behalf of Customer by Limelight.

The terms **“Business”**, **“Consumer”**, **“Controller”**, **“Data Subjects”**, **“Processor”**, **“processing”**, **“Personal Data”**, **“Personal Information”** and **“Sub-processor”** have the meanings given to them in Applicable Privacy Laws, including the EU Data Protection Lav and the California Consumer Privacy Act (“**CCPA**”), as applicable, and include any equivalent or corresponding terms applied by such Applicable Privacy Laws. If and to the extent that Applicable Privacy Laws do not define such terms, then the definitions given in EU Data Protection Law will apply.

2. General

2.1 Limelight provides a secure and privacy hardened content delivery network (CDN) that serves as a conduit for the delivery of content to our client's end-users (**“Services”**). The content itself could, in some use cases, contain information classified as confidential or personal, but, similar to an Internet Service Provider, Limelight doesn’t know or care to know what is in the content. Limelight warrants and represents that, as part of the Services, Limelight does not access, collect, know, process, screen, or divulge the Contents of Customer’s data (the **“Customer Data”**), except to the extent necessary to (a) provide the Services or as otherwise permitted or directed by Customer, (b) provide, maintain, protect, develop and improve the Services or solutions it offers its business customers, (c) detect and prevent potential fraud and security risks, (d) support Limelight’s internal business operations (e.g. billing), and (e) create and distribute aggregate performance, network utilization and threat intelligence analyses and reports; provided, that, any externally distributed analyses and reports do not identify Customer or any of its end users. **“Contents”** for purposes of this section means information concerning the substance, purport, or meaning of that data. Customer warrants and represents that it will not disclose to Limelight the Contents of the Customer Data unless and except as absolutely necessary for the provision and use of the Services.

2.2 Customer remains responsible in its capacity as Controller/Business for any Personal Data or Personal Information that is processed by Limelight pursuant to this Addendum. The use of the Service, its configuration, and the information/data obtained (including whether it is encrypted in transit, how and whether it is stored, how it's legal use is secured, use of cookies, etc.) are all decisions made / controlled by Customer. Customer is responsible for compliance with its obligations as Controller under the EU Data Protection Law, in particular for justification of any transmission of Personal Data to Limelight (including providing any required notices and obtaining any required consents and/or authorizations, or otherwise securing an appropriate legal basis under the EU Data Protection Law), and for its decisions and actions concerning the Processing of such Personal Data. This includes determining the purposes and general means, and the appropriate Services, of Limelight’s processing of Personal Data or Personal Information under the Terms of Service subject to Limelight’s responsibility for determining and implementing the technical and organizational means of the processing envisaged by the Terms of Service and complying with its obligations prescribed by Applicable Privacy Laws for Processors.

2.3 As Limelight does not control Customer Contents, Customer will be responsible for defining or approving metadata and configuration policies for its website(s) and application(s). We encourage you to implement a data classification mechanism, to encrypt or otherwise protect data in transit, and to select the Services appropriate to the type of Contents you are sending.

2.4 As a result of providing Services to Customer, Limelight and Limelight personnel may perform the Services on Customer Data where it includes certain information that could relate to Personal Data or Personal Information. Subject to the foregoing, and solely to the extent that Limelight and/or Limelight personnel (i) accesses Customer Content containing Personal Data or Personal Information; or (ii) transfers and/or processes Customer Content related to payments for or the delivery of Services to Customer, Limelight will process all Personal Data or Personal Information received from or on behalf of Customer in accordance with the requirements set forth in this Section 2.4 and only for the purposes set forth in the Terms of Service, and only as directed by Customer.

2.5 Limelight is authorized to engage and use Sub-Processors for the Processing of Personal Data or Personal Information provided that: (a) Limelight undertakes reasonable due diligence on such Sub-Processor(s) in advance to ensure appropriate safeguards for Personal Data and respective individual rights in accordance with Applicable Privacy Laws; (b) the Sub-Processor's activities are limited to those specified in Section 2.1; and (c) Limelight remains responsible for all acts or omissions of the Sub-Processor(s) as if they were its own. Further, to the extent that any Applicable Privacy Laws would deem a Limelight Affiliate to be a Sub-processor for purposes of this Agreement, Customer hereby authorizes Limelight's use of such Affiliate as a Sub-Processor. Limelight has entered into the Model Clauses with all of its Affiliates.

3. Information Security

3.1 Limelight will maintain reasonable operating standards and security procedures in accordance with industry standard security risk management practices designed to protect from Security Incidents and to preserve the security, integrity and confidentiality of Personal Data and Personal Information. If you would like additional information about Limelight's operating procedures and security standards, please contact us, and we will be happy to share additional information under cover of a Non-Disclosure Agreement.

4. Compliance with Applicable Privacy Law; Model Clauses

4.1 Each Party will comply with its obligations under Applicable Privacy Law(s) with respect to any Personal Data or Personal Information it processes or controls under the Terms of Service.

4.2 The parties acknowledge and agree that Limelight operates a global content-neutral transitory network in connection with its delivery of Services to Customer, and any Personal Data or Personal Information that is provided to Limelight by Customer may be transferred from the country in which it is collected by the Limelight network to the United States, for the purposes set forth herein.

4.3 To the extent that Limelight, including its Affiliates and Sub-processors, transfer Personal Data of EU citizens to / from the United States, such transfer will be governed by the Model Clauses. To the extent that Customer is located in the United Kingdom, the pre-2021 version of the Model Clauses will continue to govern. To the extent applicable, the applicable version of the Model Clauses are agreed and incorporated herein between Customer (as Data Exporter) and Limelight (as Data Importer), and Appendix 1 of the Model Clauses is deemed to be prepopulated with the relevant sections of Schedule 1 attached hereto, Appendix 2 is deemed to be prepopulated with the relevant sections of Schedule 2 attached hereto, and (for non-UK Customers) Appendix 3 is deemed to be prepopulated with the relevant sections of Schedule 3 attached hereto. For the avoidance of doubt, Customer's acceptance of Limelight's Terms of Service constitutes Customer's authorization for Limelight to agree to the Model Clauses on Customer's behalf as Data Exporter with Limelight as Data Importer. Alternatively, if you are located outside of the United Kingdom, you may enter into the Model Clauses by clicking here and if you are located within the United Kingdom, you may enter into the Model Clauses by clicking here.

To the extent any similarly applicable standard contractual clauses are adopted by a Supervisory Authority or other body of competent jurisdiction to govern the cross-border transfer of Personal Data subject to Applicable Privacy Laws, such clauses shall be incorporated herein by the parties. Such clauses shall be supplemented and/or prepopulated (as applicable) with the relevant sections of this Agreement and its appended Schedules.

4.4 Limelight previously participated in and self-certified compliance with the U.S.-EU Privacy Shield Framework, including the Supplemental Principles, and the Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce (collectively, the **"Principles"**), through July 25, 2021. While Limelight chose not to re-certify following the July 16, 2020 judgment of the Court of Justice of the European Union invalidating the Privacy Shield Framework as a valid transfer mechanism, Limelight nonetheless continues to adheres to the general principles espoused by the Framework and the GDPR. Limelight will not, however, rely upon the Framework as a legal mechanism for cross-border transfers of Personal Data, and instead relies on the Model Clauses.

4.4 Limelight does not have reason to believe that U.S. or other governmental agencies wish to access its infrastructure, nor does Limelight does voluntarily permit U.S. or other governmental agencies to access its infrastructure. If Limelight were to receive such a request, Limelight may disclose Personal Data to the extent required to meet a legal obligation, including national security or law enforcement obligations and applicable law, rule, order, or regulation. However, Limelight will object to any such request where there is a legitimate basis to do so. Additionally, Limelight will promptly notify Customer (and where possible, the Data Subject) of any legally binding request for disclosure of Personal Data by a law enforcement authority, unless prohibited from doing so by law.

5. Cooperation

5.1 Limelight will reasonably cooperate with Customer to enable Customer to respond to third party requests, complaints or other communications from Data Subjects and governmental, regulatory, or judicial bodies relating to the processing of Personal Data under the Terms of Service, including requests from Data Subjects or Consumers seeking to exercise their rights under Applicable Privacy Laws. If any such request, complaint or communication is made directly to Limelight, Limelight will promptly pass this onto Customer and, unless otherwise required by applicable law, will not respond to such communication without Customer's express authorization.

6. Security Incidents

6.1 Subject to any restrictions or obligations of applicable law or confidentiality, Limelight will inform Customer promptly, but in any event within 48 hours after Limelight discovers or reasonably believes it has discovered a Security Incident impacting Personal Data controlled by Customer by providing notice via e-mail to the Customer's main point of contact with Limelight or, if none, the authorized person listed on the Order Form as provided by Customer. Limelight will provide Customer with information available to Limelight through commercially reasonable investigation regarding any Security Incident.

6.2 Except to the extent required by applicable law, Limelight agrees not to notify any regulatory authority on behalf of Customer of any Security Incident unless Customer specifically requests that Limelight do so and, in such event, Customer reserves the right to review and approve the form and content of any notification before it is provided to such regulatory authority.

6.3 In the event of a Security Incident, Limelight will:

> (a) provide timely information and commercially reasonable cooperation so that Customer may fulfil its obligations under Applicable Privacy Laws; and (b) take commercially reasonable measures and actions, as appropriate, to remedy or mitigate the effects of the Security Incident and will keep Customer up to date about all developments in connection with the Security Incident.

7. Audit Rights

7.1 The parties hereby agree that Customer will have the right to audit Limelight's information security program and processing of Personal Data (if any) once each calendar year during the Term. Any initial audit will consist of an audit questionnaire to be answered by Limelight. In the event that Customer reasonably believes Limelight's answers to the audit questionnaire warrant further examination of Limelight's information security program and/or processing of Personal Data, upon Customer's request, one follow-up audit per calendar year during the Term may be conducted at a representative Limelight facility involved in delivery of the Services upon reasonable notice to Limelight, at reasonable times during business hours and at Limelight's then-current rates.

8. Miscellaneous

8.1 Except for the changes made by this Addendum, the Terms of Service remain unchanged and in full force and effect.

8.2 The obligations placed upon the parties under this Addendum will survive so long as Limelight processes Personal Data collected via Customer's use of the Services.

8.3 If any provision or portion of any provision of this Addendum is held to be invalid, illegal or unenforceable in any respect under any applicable law in any jurisdiction, such invalidity, illegality or unenforceability will not affect any other provision or portion of any provision in such jurisdiction.

SCHEDULE 1

DETAILS OF LIMELIGHT'S PROCESSING ACTIVITIES

Data Exporter

Data Exporter is the legal entity having entered into a contractual relationship with Limelight for the purchase of Services, as represented by an Order Form.

Data Importer

Limelight provides a secure and privacy hardened content delivery network (CDN) that serves as a conduit for the delivery of content to our client's end-users. The use of the service, its configuration, and the information/data obtained (including whether it is encrypted in transit, how and whether it is stored, how it's legal use is secured, use of cookies, etc.) are all decisions made / controlled by its Customer.

Description of Transfer

Data Subjects

Limelight may, in limited instances, process data on behalf of its Customers that may contain the Personal Data of the end users accessing Customer's Content and/or using Customer's services when performing Services for the Customer. "**Content**" means all data, regardless of format or owner (including, but not limited to, content, websites, applications and the like), provided or identified to Limelight to be sent or received using the Services, and content hosted, stored, or cached by Limelight at the direction of Customer or its Affiliates, agents, customers, or end-users.

Categories of Data

An overwhelming majority of Limelight's customers deliver or store media that does not contain any Personal Data. However, in some cases, Content may contain Personal Data such as names, email addresses, contact information, financial or transactional information, or login credentials. Additionaly, Limelight may collect and process logged data, such as IP addresses or geo-location data, for the purpose of mapping / routing, threat detection, and service improvement.

Sensitive Data

No Sensitive Data is processed by Limelight

Frequency of the Transfer

Data is transferred on a continuous basis as Limelight performs Services for its Customers.

The Period for which Personal Data is Retained

Limelight recommends that Customer configures its Services to not cache end-user Personal Data. When configured as recommended by Limelight, Personal Data is not stored on Limelight servers or elsewhere. Logged data may be retained by Limelight for 90 days.

Nature of Processing

Personal Data transferred, if any, will be subject to the following basic processing activities:

As part of the Services, Limelight does not access, collect, know, process, screen, or divulge the Contents of Customer's data (the "Customer Data"), except to the extent necessary to (a) provide the Services or as otherwise permitted or directed by Customer, (b) provide, maintain, protect, develop and improve the Services or solutions it offers its business customers, (c) detect and prevent potential fraud and security risks, (d) support Limelight's internal business operations (e.g. billing), and (e) create and distribute aggregate performance, network utilization and threat intelligence analyses and reports; provided, that, any externally distributed analyses and reports do not identify Customer or any of its end users. "**Contents**" for purposes of this section means information concerning the substance, purport, or meaning of that data. Customer warrants and represents that it will not disclose to Limelight the Contents of the Customer Data unless and except as absolutely necessary for the provision and use of the Services.

Supervisory Authority

The competent Supervisory Authority shall be the Supervisory Authority of the country in which the Data Exporter is located. If the Data Exporter is located outside of the EEA, the competent Supervisory Authority shall be that of the Netherlands.

SCHEDULE 2

LIMELIGHT'S TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

Physical security measures

Limelight implements security measures across all components such that it safeguards the confidentiality, availability and integrity of customer and Limelight data. Limelight aims to meet all legal and regulatory requirements; and uses its best endeavours to prevent unauthorized individuals from gaining access to command and control systems and services. Some of the physical security measures employed by Limelight are:

Command and control facilities: All Limelight Command and Control facilities are protected as reasonably practicable from environmental hazards or related damage. They have alternative sources of power, and adequate smoke/fire detection and suppression mechanisms. These facilities are monitored for temperature and humidity conditions, and the structures are designed to protect against environmental threats such as wind, water, and fire.

Access Control: Physical access is monitored and controlled locally and remotely. Access requires specific badge access permission, obtained with approval from a designated member of Limelight's management team, and is restricted and managed individually by the internal IT group. All access permissions are manually reviewed on a quarterly basis.

Entry Control: All Limelight office premises are protected by appropriate entry controls to ensure that only authorized personnel are allowed access. Offices are used for Limelight business purposes, which may include customer and vendor visits.

Operational Organizational Measures

Limelight implements the following operational organizational measures:

Change management: Any production configuration changes are addressed via a structured change management process.

Incidence response and security management process: Limelight manages incident response processes to efficiently and effectively report, assess impact, and manage incidents, and, to take corrective action to restore service, and preventive actions to limit likelihood or impact of a reoccurrence. Additionally, Limelight undergoes an annual third-party audit under SOC 2 Type 2 and other assessments and certifications, in order to evaluate continued compliance with such certifications.

Segregation of system administrative duties: Duties and responsibilities are segregated to reduce opportunities for unauthorized modification or misuse of information. System Administrators, Developers, and Operations Engineers have clear segregation of duties.

Security training and privacy – Induction training: All Limelight employees undergo an induction training process upon hiring that emphasizes the importance of information security and privacy and provides best practices for good security hygiene. The HR department, supported by the Information Security team, is responsible for ensuring that the new associates/inductees are made aware of the importance of information security, the correct use of information processing facilities/resources, role and responsibilities relevant to information security, security incident reporting to minimize possible security risks.   This training is reinforced periodically to ensure all Limelight employees maintain awareness of security and privacy policies and their obligations.

Reference checks: Reference checks for prospective employees are carried out using the references provided by the prospective employee. Reference checks include the authentication of educational qualifications and previous employment history. Individuals hired into senior leadership positions, as well as certain individuals working with our financial data are also subjected to background checks.

Technical Security Measures

All Limelight information systems, applications, operating systems, networks, databases and facilities are assigned an internal owner. Owners of the particular Limelight information systems, applications, operating systems, networks, databases and facilities are responsible for maintaining and assigning the appropriate access privileges to users. Data is classified into classes, each with its own security measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, disclosure or access, storage, transmission, retention and destruction.

Limelight has implemented the following technical security measures:

Secure transport of data during transmission: Provisions exist to encrypt customer data delivery from end to end. Limelight services support customer's encryption of its data; however, Limelight is directed by the customer, who sets their own requirements based on their specific data privacy needs. Limelight implements appropriate business and technical controls during the transmission of its own data including appropriate encryption techniques and a private network backbone across which the data is transmitted.

Confidentiality, integrity and availability of data through data security methodology: Network connections from a customer will terminate at a known router address so that the address can be validated and verified.

Virus management: The Virus Management Policy describes the processes required for detecting and managing malicious code. Industry leading antivirus software is used on servers and desktops and is used at all external gateways. Limelight provides virus protection to all appropriate systems. Detection and prevention controls to protect against malicious software are established.

Logically separated network environment: All logical and physical access to Limelight's systems is approved and granted on a least privilege basis. Access to information resources and systems is controlled based on business requirements, as well as an individual's role and responsibility level. Access is monitored and anomalies are reviewed.

Privilege Management: The allocation and use of privileges are restricted and controlled. Any privilege given on any system within Limelight is managed on a least privilege basis. Logical access is controlled via lightweight directory access protocol / Active Directory ("**LDAP/AD**") groups on a least privilege basis. Procedures for administering logical access rights to information systems and resources cover all stages of user access, from the initial registration of new users, to the final de-registration of users who no longer require, or should not be granted, access to information resources and Limelight systems.

User authorization: All users of Limelight systems and networks, including employees and contractors, are required to sign nondisclosure agreements prior to being permitted to access Limelight' systems.

Password Guidelines: The purpose of guidelines and recommendations on Individual Authentication (user id and password pair) is to ensure protection and restricted access to data importer's and client's CONFIDENTIAL information.

- Passwords expire after 90 days. Thereafter new passwords must be entered.
- Password must be at least 8 characters long containing at least 1 numeric, 1 special and 1 upper case character.
- 24 generations of password are remembered, meaning that a user may not re-use the same password that he or she utilized in the last 24 iterations.
- A user account will be locked after 5 unsuccessful password access attempts.
- No group or shared passwords are permitted.

E-mail policy: Limelight has an email policy to ensure proper use of the e-mail facility by data importer's employees and to prevent its misuse.

Backup strategy: Backup copies of essential business information and software are taken regularly. Any data classified as critical by the information owner is backed up at regular intervals. A back up cycle has been designed to ensure that all data is copied at appropriate intervals.

SCHEDULE 3

AUTHORIZED SUB-PROCESSORS

Limelight Networks Canada Inc.
Limelight Networks Do Brasil Ltda
Limelight Networks Germany GmbH
Limelight Networks France SARL
Limelight Networks Italia S.r.l.
Limelight Networks Netherlands B.V.
Limelight Networks (UK) Limited
Limelight Networks Ukraine, LLC
Limelight Web Technologies (IL) Ltd.
Limelight Networks Hong Kong Limited
Limelight Networks India Private Limited
Limelight Networks Japan, Ltd.
Limelight Networks Korea Ltd.
Limelight Networks Singapore PTE LTD.

Limelight has entered into the Model Clauses with all of its subsidiaries.

Appendix: Document Version Information

Version	Date	Details
1.0	October 2017	
2.0	June 2020	Improved clarity. Addressed requirements and definitions included in the California Consumer Privacy Act of 2018 and other global privacy legislation enacted since version 1.0. Immaterial formatting modifications.
3.0	August 2020	Incorporated Model Clauses in light of ECJ's July 16, 2020 decision in *Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems*, Case No. C-311/18 [2020] (Grand Ct.) (Ir.) (*Schrems II*) invalidating the Privacy Shield Framework as an approved data transfer mechanism. Added Schedules 1 and 2.
4.0	September 2021	Current version. Incorporated Revised Model Clauses implemented by the European Commission on June 4, 2021. Revised Schedules 1 and 2. Added Schedule 3.