

## GDPR ADDENDUM

By interacting with Lucence, submitting information to Lucence or using any products or services offered by Lucence, you agree and consent to Lucence collecting, retaining, processing, using, disclosing and transferring your Personal Data to Lucence's authorised service providers and relevant third parties in the manner set out in this GDPR Addendum.

### 1. Definitions

1.1 For the purposes of this GDPR Addendum:

- (a) "**Affiliate(s)**" means any legal entity directly or indirectly controlling, controlled by or under common control with a party, where control means the ownership of a majority share of the stock, equity or voting interests of such entity.
- (b) "**Controller**" means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
- (c) "**Customer**" means the non-Lucence party to this GDPR Addendum that interacts with Lucence.
- (d) "**Customer Data**" means any data, information or material originated by Customer that Customer submits to Lucence.
- (e)
- (f) "**Data Subject**" means the individual to whom Personal Data relates.
- (g) "**EEA**" means the European Economic Area, which constitutes the member states of the European Union and Norway, Iceland and Liechtenstein, as well as, for the purposes of this GDPR Addendum, the United Kingdom.
- (h) "**EU Data Protection Legislation**" means (i) 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, including any applicable national implementations thereof, (ii) 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, and repealing Directive 95/46/EC ("**General Data Protection Regulation**" or "**GDPR**"), as amended, replaced or superseded and (iii) the applicable data protection laws of Switzerland and the United Kingdom.
- (i) "**Personal Data**" means any Customer Data relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- (j) "**Processor**" means an entity which processes Personal Data on behalf of the Controller.
- (k) "**Processing**" means any operation or set of operations which is performed on Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or

destruction.

- (m) " **Supervisory Authority**" means an independent public authority which is established by an EU member state pursuant to EU Data Protection Legislation.

## 2. **Applicability of GDPR Addendum**

- 2.1 Applicability. This GDPR Addendum shall apply only to the extent Customer is established within the EEA or Switzerland and/or to the extent Lucence processes Personal Data of Data Subjects located in the EEA or Switzerland on behalf of Customer or a Customer Affiliate.

## 3. **Details of the Processing**

- 3.1 Types of Personal Data Processed. The categories of Personal Data are determined by the Customer in its sole discretion and may include but are not limited to: first and last name; employer; business role; professional title; contact information (e.g., email, phone, physical address); business network; business experience; business interests; localization data, and; device identification data.
- 3.2 Special Categories of Personal Data. Special categories of Personal Data, if any, are determined by Customer in its sole discretion and may include, but are not limited to, information revealing racial/ethnic origin, political, religious or philosophical beliefs, trade union membership or health data.
- 3.3 Categories of Data Subjects. The categories of Data Subjects whose Personal Data may be processed are determined and controlled by Customer in its sole discretion.
- 3.4 Nature of Processing Operations. Lucence will process Personal Data as necessary to provide the relevant goods or services and may include the following: collecting, recording, organizing, storage, use, alteration, disclosure, transmission, combining, retrieval, consultation, archiving and/or destruction.

## 4. **Roles and Responsibilities**

- 4.1 Parties' Roles. Customer, as Controller, appoints Lucence as a Processor to process the Personal Data on Customer's behalf. In some circumstances Customer may be a Processor, in which case Customer appoints Lucence as Customer's sub-processor, which shall not change the obligations of either Customer or Lucence under this GDPR Addendum, as Lucence will remain a Processor with respect to the Customer in such event.
- 4.2 Purpose Limitation. Lucence shall process Personal Data for the purposes set forth in the relevant forms and only in accordance with the lawful, documented instructions of Customer, except where otherwise required by applicable law. The relevant forms and this GDPR Addendum set out Customer's complete instructions to Lucence in relation to the Processing of Personal Data and any Processing required outside of the scope of these instructions will require prior written agreement of the parties.
- 4.3 Training. Lucence shall ensure that its relevant employees, agents and contractors receive appropriate training regarding their responsibilities and obligations with respect to the Processing, protection and confidentiality of Personal Data.
- 4.4 Compliance. Lucence, as Processor, has complied and will continue to comply with all applicable privacy and data protection laws including, but not limited to, EU Data

Protection Legislation. Customer, as Controller, shall be responsible for ensuring that, in connection with Customer Data:

- (a) it has complied, and will continue to comply, with all applicable privacy and data protection laws, including EU Data Protection Legislation; and
- (b) it has, and will continue to have, the right to transfer, or provide access to, the Personal Data to Lucence for processing in accordance with this GDPR Addendum.

## 5. **Security**

5.1 Security. Lucence shall implement appropriate technical and organisational measures taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects. Such measures shall be designed to ensure a level of security appropriate to the risk in order to protect Personal Data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure, access or use (each a "**Security Incident**").

5.2 Confidentiality of Processing. Lucence shall ensure that any person that it authorizes to Process the Personal Data (including its staff, agents and subcontractors) shall be subject to a duty of confidentiality that shall survive the termination of their employment and/or contractual relationship.

5.3 Security Incidents. Upon becoming aware of a Security Incident, Lucence shall notify Customer without undue delay, but within no more than seventy- two (72) hours, and shall provide such timely information as Customer may reasonably require to enable Customer to fulfil any data breach reporting obligations under EU Data Protection Legislation. Lucence will take steps to immediately identify and remediate the cause of such Security Incident.

## 6. **Cooperation**

6.1 Data Subjects' Rights. Lucence shall provide commercially reasonable assistance, including by appropriate technical and organizational measures as reasonably practicable, to enable Customer to respond to any inquiry, communication or request from a Data Subject seeking to exercise his or her rights under EU Data Protection Legislation, including rights of access, correction, restriction, objection, erasure or data portability, as applicable. In the event such inquiry, communication or request is made directly to Lucence, Lucence shall promptly inform Customer by providing the full details of the request. For the avoidance of doubt, Customer is responsible for responding to Data Subject requests for access, correction, restriction, objection, erasure or data portability involving that Data Subject's Personal Data.

6.2 Supervisory Authority. Lucence shall notify Customer without undue delay if a Supervisory Authority or law enforcement authority makes any inquiry or request for disclosure regarding Personal Data.

6.3 Data Protection Impact Assessments and Prior Consultation. Lucence shall, to the extent required by EU Data Protection Legislation, provide Customer with reasonable assistance with data protection impact assessments and/or prior consultations with Supervisory Authorities that Customer is required to carry out under EU Data Protection Legislation.

## 7. **Security Reports and Audits**

7.1 Lucence shall provide a copy of its most current security report upon Customer's written request

and subject to the confidentiality provisions of the relevant transaction. If the relevant transaction does not include audit rights, Lucence shall allow Customer (or Customer's independent third-party auditor) to conduct an on-site audit of the procedures relevant to the protection of Personal Data, subject to the confidentiality provisions herein. Customer and Lucence will discuss and agree in advance on the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit; and Lucence reserves the right to charge a fee (based on Lucence's reasonable costs) for any such audit. Lucence will provide further details of any applicable fee and the basis of its calculation to Customer in advance of such audit.

**8. Deletion or Return of Customer Data**

- 8.1 Deletion or Return of Data. Upon termination or expiration of the relevant transaction, Lucence shall, in accordance with the terms of the relevant transaction, delete or make available to Customer for retrieval all relevant Personal Data (including copies) in Lucence's possession, save to the extent that Lucence is required by any applicable law to retain some or all of the Personal Data.