

## Data Protection Addendum – Upper Sigma

### 1. Introduction

- 1.1 If Customer's bill to information listed on the applicable Customer Contract is located in the Americas, **Freedom Solutions Group, L.L.C.**, an Illinois limited liability company, if Customer's bill to information listed on the applicable Customer Contract is located in APAC, **DocsCorp Pty. Ltd.**, if Customer's bill to information listed on the applicable Customer Contract is located outside Americas and APAC, **Workshare Limited** ("Litera Group"). APAC means Asia Pacific Region, which includes all countries bordering the Pacific Ocean on the side of Asia, including Australia and New Zealand. We are members of the Litera Group, which is a group of organizations that, together, form the industry-leading, end-to-end provider of document lifecycle solutions.
- 1.2 We deliver innovative services and customer relationship management technology solutions to legal, corporate, life sciences and other organizations to customers located around the world.
- 1.3 Our customers access and use our services and technology solutions and as part of these arrangements, we process personal information held by our customers for and on behalf of our customers as their processor.
- 1.4 We recognise the importance of keeping safe and secure any personal information which we process on behalf of our customers in providing our services. You can read more about the Litera Group's approach to data protection compliance for our customers by reading the Litera Group's statement about data protection compliance, which is available [here](#).
- 1.5 For our customers located in the United Kingdom or the European Economic Area or otherwise subject to European Union data protection laws (either directly or indirectly), we understand the requirements they are under in relation to the use of processors such as ourselves. In particular, we have developed a set of standard data protection terms, set out below, that are incorporated into each customer contract we enter into and which fulfil the data protection legal requirements our United Kingdom and EEA customers, as well as our other customers that are either directly or indirectly subject to European Union data protection laws, are subject to in relation to their appointment and use of us as their processor.
- 1.6 We have a data protection officer whose job is to oversee our data protection compliance. If you have any queries about these terms, please email us at [legal@litera.com](mailto:legal@litera.com).

### 2. Data processing terms

- 2.1 The data processing terms set out in paragraphs 2 to 8 (inclusive) shall automatically apply to and form part of each Customer Contract.
- 2.2 These data processing terms shall survive termination or expiry of each Customer Contract.
- 2.3 To the extent that there is any conflict or inconsistency between these data processing terms and the other terms of a Customer Contract then these data processing terms shall take precedence.

### 3. Definitions

- 3.1 For the purposes of paragraphs 2 to 8 (inclusive):
- (a) **Controller** means a person which, alone or jointly with others, determines the purposes and means of the Processing of Personal Information;

- (b) **Customer** means a customer of the Litera group:
  - (i) in respect of which we Process Personal Information as the Processor of the customer in connection with the services we provide to the customer; and
  - (ii) which is:
    - (A) located in the United Kingdom or EEA; or
    - (B) otherwise subject to United Kingdom or European Union data protection laws, either directly or indirectly (for example, being contractually obliged to comply with such laws), in respect of the Personal Information we Process as the Processor of the customer in connection with the services we provide to the customer;
- (c) **Customer Contract** means a contract we have entered into with a Customer for the provision of one or more of our document technology services and solutions;
- (d) **Data Protection Laws** means all laws and regulations relating to the Processing of Personal Information as the same may be in force from time to time;
- (e) **Data Subject** means the individual to which the Personal Information relates;
- (f) **EEA** means European Economic Area;
- (g) **Personal Information or Personal Data** means any information relating to an identified or identifiable living individual;
- (h) **Personal Information Breach** means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Information;
- (i) **Processing** means any operation or set of operations which is performed on Personal Information or on sets of Personal Information, whether or not by automated means, and **Process, Processes** and **Processed** shall be construed accordingly;
- (j) **Processor** means a person which Processes Personal Information on behalf of a Controller; and
- (k) **we, us and our** means, in respect of each Customer Contract, the Litera group company that has entered into the Customer Contract, being either Workshare Limited or [*enter name of US entity that enters into Customer Contracts*].

#### 4. Arrangements for the Processing of Personal Information

##### 4.1 In respect of each Customer Contract:

- (a) the Customer Contract may require the Processing of Personal Information by us on behalf of the Customer;
- (b) the Customer alone shall determine the purposes for which and the manner in which Personal Information will be Processed by us on behalf of the Customer under the Customer Contract; and
- (c) the Customer shall be the Controller and we shall be the Processor in respect of all such Personal Information.

- 4.2 Where, under or in connection with the Customer Contract, we Process Personal Information on behalf of the Customer as the Customer's Processor, we shall:
- (a) Process the Personal Information only:
    - (i) to the extent reasonably necessary for the performance by us of our obligations under the Customer Contract or as otherwise directed in writing by the Customer. We shall immediately inform the Customer if, in our opinion, Processing the Personal Information in accordance with a written instruction received from the Customer or in the performance of our obligations under the Customer Contract infringes the Data Protection Laws to which either the Customer (in its capacity as a Controller) or we (in our capacity as a Processor) are subject; or
    - (ii) as otherwise required by applicable law, in which case we shall inform the Customer of that legal requirement before Processing the Personal Information (unless that law prohibits us from informing the Customer);
  - (b) ensure that all persons authorised by us to Process the Personal Information:
    - (i) Process the Personal Information in accordance with provisions of this paragraph 4.2; and
    - (ii) are under an appropriate contractual or other legal obligation to keep the Personal Information confidential;
  - (c) taking into account the state of the art, the nature, scope, context and purposes of the Processing and the risks to Data Subjects, implement appropriate technical and organizational measures to ensure the security of the Personal Information and prevent Personal Information Breaches. The current measures implemented by us are described in paragraph 7. We reserve the right to change and adapt our implemented technical and organizational measures in accordance with ongoing and future technical developments, provided that the amended measures do not fall significantly short of the level of protection provided by the measures described in paragraph 7;
  - (d) taking into account the nature of the Processing, implement appropriate technical and organizational measures to assist the Customer to comply with its obligations under the Data Protection Laws to which the Customer is subject to respond to requests from Data Subjects to exercise their legal rights in relation to their Personal Information;
  - (e) taking into account the nature of the processing activities and the information available to us, assist the Customer to comply with its obligations in respect of such Personal Information under the Data Protection Laws to which the Customer is subject in relation to:
    - (i) keeping Personal Information secure;
    - (ii) dealing with Personal Information Breaches;
    - (iii) carrying out data protection impact assessments;
    - (iv) dealing with requests from Data Subjects to exercise their legal rights in relation to their Personal Information; and
    - (v) investigations and enquiries by data protection regulatory authorities;

- (f) notify the Customer without undue delay after becoming aware of a Personal Information Breach in respect of the Personal Information;
- (g) at the Customer's option, permanently and securely delete or return to the Customer all the Personal Information promptly on termination of the Customer Contract, and delete any existing copies of the Personal Information save to the extent that we are required to retain copies of the Personal Information by the laws to which we are subject or when Personal Information is transmitted via email, it will be subject to Company's email retention policy; and
- (h) make available to the Customer all information necessary, redacted at Company's discretion, to demonstrate compliance with our obligations under this paragraph 4.2 and allow for and contribute to audits, including (without limitation) inspections during Company's normal and ordinary working hours, conducted by the Customer or an auditor appointed by the Customer that relate to our compliance with our obligations in respect of the Personal Information under this paragraph 4.2. The audit and the inspections shall be subject to following requirements:
  - (i) without disruption to Company's business operations;
  - (ii) with Company's direct supervision;
  - (iii) where any agents and or audits are subject to confidentiality covenants no less restrictive than the terms in here;
  - (iv) no more than one (1) time per annual period and
  - (iv) with thirty (30) days prior, written notice to Company.

4.3 In respect of each Customer Contract, we may charge the Customer for the time and expenses incurred in providing the assistance required by the Customer under paragraphs 4.2(e), 4.2(g) and 4.2(h).

4.4 We shall not be liable to the Customer for any failure to perform our obligations under a Customer Contract to the extent that such failure is due (either directly or indirectly) to us complying with an instruction of the Customer pursuant to paragraph 4.2(a)(i) or the Data Protection Laws to which either we or the Customer is subject. The Customer shall remain solely responsible for assessing and ensuring the lawfulness of the Processing, and for safeguarding the rights of the Data Subjects, in accordance with Data Protection Laws to which it is subject.

4.5 In respect of each Customer Contract, we may terminate the Customer Contract with immediate effect by giving the Customer notice of such termination in the event that the Customer gives us any instruction in relation to the Personal Information that we Process on behalf of the Customer that is incompatible with the Customer Contract or the services and technology solutions we provide to the Customer.

## 5. Particulars of Processing

5.1 The particulars of Processing to be carried out by us on behalf of a Customer under or in connection with the Customer Contract are set out in the table below:

Data Processing Particulars	
<b>Subject matter and duration of the Processing</b>	<p>We are a member of the Litera Group, which is a provider of innovative customer relationship management technology services and solutions. We have contracted with the Customer to provide certain of our customer relationship management software solutions to the Customer. As part of these arrangements, we will process personal information controlled by the Customer.</p> <p>The personal information that we process (i) when we access the Customer's systems in relation to the provision of support; and/or (ii) when we provide professional services to the Customer.</p> <p>In respect of each Customer, we will process such personal information (i) for</p>

	<p>the duration of the Customer Contract; and (ii) for the period after the termination or expiry of the Customer Contract during which we have surviving obligations that require us to process such personal information or the Customer continues to store such information on our systems.</p>
<p><b>Nature and purpose of the processing</b></p>	<p>In respect of each Customer Contract, we will process personal information only to the extent necessary for the purpose of the provision of our technology services and solutions to the Customer and in performing all other obligations under and in accordance with the terms and conditions of the Customer Contract. This includes processing personal information about end users to verify that they are authorised users of the relevant software. We do not monitor or access the documents that are transmitted through Customer's software by Customer.</p> <p>The purpose of processing will be to provide support and maintenance services, provide professional services and to verify the end users authorized to use the software.</p> <p><b><u>Additional Details:</u></b></p> <p>Processing Activities &amp; Storage: All Customer data is stored and processed on Company's cloud applications.</p> <p>Access: Company does not monitor the Customer data that is stored and processed on Company's cloud applications. Company may have limited access to Customer data and/or personal data when Customer open a support ticket.</p> <p>Dissemination: none. This is controlled by the Customer.</p> <p>Alternation: none. This is controlled by the Customer.</p> <p>Combination: none. This is controlled by the Customer.</p> <p>Consultation (viewing): only in limited instances when a support ticket is opened by Customer</p> <p>Deletion: Data deletion may be controlled by the Customer. Company deletes data upon expiration of the subscription term.</p>

<p><b>Categories and types of personal data being processed</b></p>	<p>The types of personal information being processed by us will be determined by each Customer and may include:</p> <p><b><u>Non-special categories of personal data</u></b></p> <p>Personal details including but not limited to first name, last name and email address; family, lifestyle and social circumstances; education and training details; employment details; financial details; personal information relating to goods or services provided; or personal information relating to civil proceedings.</p> <p><b><u>Special categories of personal data</u></b></p> <p>N/A unless provided by the Customer.</p> <p><b><u>Criminal convictions information</u></b></p> <p>Criminal convictions information – including (alleged) offences, outcomes and sentences – if provided by the Customer</p>
<p><b>Categories of data subjects</b></p>	<p>The category of data subjects to which the personal information relates will be determined by the Customer.</p> <ul style="list-style-type: none"> <li>• It will include staff such as attorneys, partners, directors, employees, volunteers, agents, temporary and casual workers and other personnel engaged by the Customer, Customer’s clients.</li> <li>• It will include any person whose personal information is included in the documents and other materials in respect of which the Customer provides to the Company.</li> </ul>
<p><b>Security Measures</b></p>	<p>Added as Annex 1</p>

**6. International Data Transfers**

- 6.1 Each Customer acknowledges and agrees that the nature of our operations means that it is highly likely we (either directly or via our Sub-processors) will Process Personal Information under a Customer Contract for and on behalf of the Customer in a number of jurisdictions around the world.
- 6.2 Where, in connection with a Customer Contract, we Process Personal Information on behalf of a Customer established in the United Kingdom as its Processor and such Processing would, but for the

application of the provisions set out in this paragraph (as amended from time to time by the Data Protection Laws to which the Customer is subject), be prohibited under the Data Protection Laws to which the Customer is subject, then the additional provisions set out in paragraph 7 (as amended from time to time by the Data Protection Laws to which the Customer is subject) shall apply. To the extent that there is any conflict or inconsistency between the provisions of paragraph 7 (as amended from time to time by the Data Protection Laws to which the Customer is subject) and the other terms of the Customer Contract, the provisions of paragraph 7 (as amended from time to time by the Data Protection Laws to which the Customer is subject) shall take precedence.

6.3 Where, in connection with a Customer Contract, we Process Personal Information on behalf of a Customer established in the EEA as its Processor and such Processing would, but for the application of the provisions set out in paragraph 7, be prohibited under the Data Protection Laws to which the Customer is subject, then the additional provisions set out in paragraph 7 shall apply. To the extent that there is any conflict or inconsistency between the provisions of paragraph 7 and the other terms of the Customer Contract, the provisions of paragraph 7 shall take precedence.

6.4 Where, in connection with a Customer Contract, we Process Personal Information on behalf of a Customer that is established outside of the United Kingdom and the EEA as its Processor and such Processing would, but for the application of the provisions set out in paragraph 7, be prohibited under:

- (a) the United Kingdom or EEA Data Protection Laws to which the Customer is subject on an extra-territorial basis; or
- (b) the contractual terms the Customer has entered into with a third party established in the United Kingdom or EEA in relation to the processing of that Personal Information,

then the additional provisions set out in paragraph 7 shall apply. To the extent that there is any conflict or inconsistency between the provisions of paragraph 7 and the other terms of the Customer Contract, the provisions of paragraph 7 shall take precedence.

## 7. Controller to Processor Model Clauses

Table 1	
<p><b>Additional provisions that apply in respect of the transfers of Personal Information described in paragraph 6</b></p>	<p>If the Customer transfers the personal data of individuals located in United Kingdom, parties agree to incorporate the UK Addendum to EU Commission Standard Contractual Clauses for data transfers published by the UK Information Commissioner and in force from March 21, 2022 as part of this Addendum (“IDTA”). The following options are selected: Module in operation – II, Clause 7 – N/A, Clause 11 – N/A, Clause 9a – Option 2, Clause 9a (Time period) – 30 days, is personal data received from the Importer combined with personal data collected by the Exporter – No. A copy of the IDTA can be found at:</p> <p><a href="https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/">https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/</a></p> <p>If the Customer transfers the personal data of individuals located in the member countries of European Union, the standard contractual clauses for the transfer of personal data from the Community to third countries (controller to processor transfers) set out in Commission Decision 2021/914/EU (<b>Controller to Processor Model Clauses</b>) shall apply and are hereby incorporated into these data processing terms. The following options are selected: Clause 9: Module II - Option 2. A copy of the Controller to Processor Model Clauses can be found at:</p> <p><a href="https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&amp;locale=en">https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&amp;locale=en</a></p>
<p><b>Governing Law</b></p>	<p>The Controller to Processor Model Clauses shall be governed by the law of the jurisdiction in which the <i>data exporter</i> is established.</p> <p>The provisions relating to data protection aspects for sub-processing of the contract referred to in Clause 11 paragraph 1 of the Controller to Processor Model Clauses shall be governed by the law of the jurisdiction in which the <i>data exporter</i> is established.</p>

<b>Table 2</b>	
<b>Completing the details needed for the Controller to Processor Model Clauses:</b>	
<p>In respect of each Customer Contract, for the purposes of the Controller to Processor Model Clauses:</p> <ol style="list-style-type: none"> <li>1. the Customer shall be the <i>data exporter</i> and we shall be the <i>data importer</i>; and</li> <li>2. the description of the transfer for the purposes of Appendix 1 to the Controller to Processor Model Clauses and the description of the technical and organizational security measures implemented by the <i>data importer</i> for the purposes of Appendix 2 to the Controller to Processor Model Clauses are as set out in the rest of this table.</li> </ol>	
<b>Description of the transfer for the purposes of Appendix 1 to the Controller to Processor Model Clauses</b>	
<b>Data exporter</b>	The <i>data exporter</i> has contracted with the <i>data importer</i> to access and use one or more of the <i>data importer's</i> document technology services and solutions in connection with its business and, as part of those arrangements, is transferring Personal Information to the <i>data importer</i> .
<b>Data importer</b>	<p>The <i>data importer</i> is a member of the Litera Group, which is a provider of innovative document technology services and solutions.</p> <p>The <i>data importer's</i> activities which are relevant to the transfer are the provision of certain document technology services and solutions to the <i>data exporter</i>.</p> <p>It is recognized that the personal information that the <i>data importer</i> processes (i) when it accesses the <i>data exporter's</i> systems in relation to the provision of support; and (ii) when the <i>data exporter</i> uses the <i>data importer's</i> technology services and solutions to store and otherwise process data, will be determined by the <i>data exporter</i>.</p>
<b>Data subjects</b>  The personal data transferred concern the following categories of data subjects	<p>The categories of data subjects to which the personal information relates will be determined by the <i>data exporter</i>.</p> <p>Details about the likely categories of data subject are set out in paragraph 5.</p>
<b>Categories of data</b>  The personal data transferred concern the following categories of data	<p>The non-special categories of personal data will be determined by the <i>data exporter</i>.</p> <p>Details about the likely non-special categories of personal data are set out in paragraph 5.</p>
<b>Special Categories of Data</b> (if appropriate)  The personal data transferred concern the following special categories of personal data	<p>The special categories of personal data will be determined by the <i>data exporter</i>.</p> <p>Details about the likely special categories of personal data are set out in paragraph 5.</p>



<p><b>Processing operations</b></p> <p>The personal data transferred will be subject to the following basic processing activities</p>	<p>Paragraph 5 sets out the basic processing activities to which the personal data will be subject.</p>
<p><b>Description of the additional technical and organizational security measures implemented by the <i>data importer</i> for the purposes of Appendix 2 to the Controller to Processor Model Clauses</b></p>	
<p><b>Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) of the Controller to Processor Model Clauses (or document/legislation attached)</b></p>	<p>The <i>data importer</i> shall:</p> <ul style="list-style-type: none"> <li>• Maintain security procedures for the protection and integrity of the personal information in line with current industry good practice, including (without limitation): <ul style="list-style-type: none"> <li>○ appropriate technical security safeguards, such as the use of encryption; and</li> <li>○ appropriate disposal methods in respect of the personal information.</li> </ul> </li> <li>• Install and maintain logical access tools for identification, authentication, authorisation, and accountability in its technology systems, including (without limitation): <ul style="list-style-type: none"> <li>○ restricting access to the personal information to persons on a "need-to-know" basis, for example restricting file access;</li> <li>○ requiring third parties that have access to the personal information to adhere to the same security standards;</li> <li>○ undertake regular vulnerability assessment and penetration testing to identify and remedy weaknesses in its technology systems and to help ensure the security of the personal information;</li> <li>○ undertake regular patch management on software applications used;</li> <li>○ install and maintain anti-virus and similar protections;</li> <li>○ carry out proper software license management;</li> <li>○ maintain appropriate mandatory certification in respect of their technology systems (where required); and</li> <li>○ carry out periodic internal security audits of their data security procedures and technology systems.</li> </ul> </li> </ul> <p><b>Physical and Building Security</b></p> <ul style="list-style-type: none"> <li>• Control access to its premises using appropriate security measures.</li> <li>• Operate appropriate restrictions on internet connectivity.</li> </ul> <p><b>Data policy</b></p> <ul style="list-style-type: none"> <li>• Maintain (and regularly review and, where necessary, update) a data policy setting out guidelines, processes and requirements for ensuring the security of personal information and information and</li> </ul>

	ensure that its employees and other personnel comply with the terms of that policy.]
--	--

## 8. Sub-processors

- 8.1 In respect of each Customer Contract, we may engage third party Processors to Process Personal Information on behalf of the Customer (**Sub-processors**) in the course of performing our obligations under the Customer Contract. We shall enter into a contract with each Sub-processor that imposes on the Sub-processor obligations equivalent to, or more onerous than, the ones imposed on us by these data processing terms. Notwithstanding any other provision of the Customer Contract, we shall remain fully liable and responsible to the Customer in accordance with the Customer Contract for all acts and omissions of the Sub-processors in relation to their Processing of the Personal Information.
- 8.2 A list of the Sub-processors that we currently use is available below. . Where, in respect of a Customer Contract, we engage an additional or replacement Sub-processor to Process Personal Information on behalf of the Customer, we shall notify the Customer of the change before the Processing starts.

### List of Sub-Processors:

Salesforce - Globally recognized CRM used to track and manage customer support requests hosted in the United States.

Y Meadows - AI-based application that will integrate with Salesforce to determine the intent of the text-based emails (cases being opened by customers) and then direct the cases to the correct queue/support subgroup. This is executed by a series of APIs and web-based automations. Hosted in the United States.

Office 365 - Provides corporate email and collaboration resources. This system will process general business to business correspondence. This system will process incoming email customer support requests as part of the communication chain to Salesforce. Hosted in the United States.

Mimecast - industry recognized mail filter and spam prevention tool. All mail sent and received by Litera's O365 environment is processed through this system. This system will process incoming email customer support requests as part of the communication chain to Salesforce. Hosted in the United States.

Zoom Contact Center – It's used to perform inbound/outbound call routing, intelligent queuing and call distribution to Litera's global support team. Hosted in USA.

## **ANNEX 1 – SECURITY MEASURES**

- Physical access controls.

Litera follows industry best practices and leverages least privilege access control for privileged administrators. Litera maintains an ISO-27001 certification and aligns and tests these controls with the standard.

- System access controls.

Litera follows industry best practices and leverages least privilege access control for privileged administrators. Litera maintains an ISO-27001 certification and aligns and tests these controls with the standard.

- Data access controls.

Litera follows industry best practices and leverages least privilege access control for privileged administrators. Litera maintains an ISO-27001 certification and aligns and tests these controls with the standard.

- Transmission controls.

The Upper Sigma products utilize industry best practices for encryption and enforces the use of TLS 1.2 and above with strong cypher suites for all data in transit.

- Input controls.

Upper Sigma products offer standard input validation controls for privileged areas/fields within the application. However, the application is highly configurable and will not restrict or deny the customers flexibility or use of free text fields and checklist items.

- Data backups.

Upper Sigma products leverage multiple technical controls to ensure system availability and continuity. This includes real-time database replication to secondary resiliency nodes and regularly scheduled database backups.

- Data segregation

Upper Sigma products utilizes logical segregation to provide customer data isolation.

- Pen Testing and Code Scanning

Litera performs regular static, dynamic and software composition analysis scans on the Upper Sigma products code base. Litera also performs annual third-party penetration tests of the Upper Sigma products application.

- Encryption at Rest

Upper Sigma products utilize industry best practices and enforces the use of AES-256 for encryption of data at rest.

- Regular review of audit logs

Upper Sigma products are under continuous monitoring and alerting for system performance and security events. System level audit logs are assessed to detect unusual behavior and application performance. Upper Sigma products provide logs to the customer to assess user activity, permissions and roles assignment, and individual user activity.