Data Protection Addendum

1. **Introduction**

1.1 If Customer's bill to information listed on the applicable Customer Contract is located in North America, then Customer is in contract with 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, then the Customer is in contract with DocsCorp Pty. Ltd., , if Customer's bill to information listed on the applicable Customer Contract is located outside North America and APAC, then the Customer is in contract with Workshare Limited (collectively, "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 document 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 either by hosting our software solutions themselves or by using our software-as-a-service platform. 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.

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 to the extent that the Litera Group has retained any Customer Personal Information.

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** 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 Freedom Solutions Group, L.L.C. dba Litera or DocsCorp Pty. Ltd., as applicable

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 tranmitted 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, wirtten 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 instructionin 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	
Subject matter and duration of the Processing	As stated in Annex 1
Nature and purpose of the processing	As stated in Annex 1
Categories and types of personal data being processed	As stated in Annex 1

Categories of data subjects	As stated in Annex 1
Security Measures	Added as Annex 2

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	
Additional provisions that apply in respect of the transfers of Personal Information described in paragraph 6	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: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/

	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 (**Controller to Processor Model Clauses**) 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: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en
Governing Law	The Controller to Processor Model Clauses shall be governed by the law of the jurisdiction in which the *data exporter* is established. 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 *data exporter* is established.

Table 2	
Completing the details needed for the Controller to Processor Model Clauses:	
In respect of each Customer Contract, for the purposes of the Controller to Processor Model Clauses: 1. the Customer shall be the *data exporter* and we shall be the *data importer*; and 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 *data importer* for the purposes of Appendix 2 to the Controller to Processor Model Clauses are as set out in the rest of this table.	
Description of the transfer for the purposes of Appendix 1 to the Controller to Processor Model Clauses	
Data exporter	The *data exporter* has contracted with the *data importer* to access and use one or more of the *data importer's* document technology services and solutions in connection with its business and, as part of those arrangements, is transferring Personal Information to the *data importer*.
Data importer	The *data importer* is a member of the Litera Group, which is a provider of innovative document technology services and solutions. The *data importer's* activities which are relevant to the transfer are the provision of certain document technology services and solutions to the *data* exporter.
Data subjects The personal data transferred concern the following categories of data subjects	The categories of data subjects to which the personal information relates will be determined by the *data exporter*. Details provided in Annex 1
Categories of data The personal data transferred concern the following categories of data	The non-special categories of personal data will be determined by the *data exporter*. Details provided in Annex 1

Special Categories of Data (if appropriate) The personal data transferred concern the following special categories of personal data	The special categories of personal data will be determined by the *data exporter*. Details provided in Annex 1
Processing operations The personal data transferred will be subject to the following basic processing activities	Details provided in Annex 1
Description of the additional technical and organizational security measures implemented by the *data importer* for the purposes of Appendix 2 to the Controller to Processor Model Clauses	

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)	The *data importer* shall:
	
	• Maintain security procedures for the protection and integrity of the personal information in line with current industry good practice, including (without limitation):
	  ○ appropriate technical security safeguards, such as the use of encryption; and
	  ○ appropriate disposal methods in respect of the personal information.
	• Install and maintain logical access tools for identification, authentication, authorisation, and accountability in its technology systems, including (without limitation):
	  ○ restricting access to the personal information to persons on a "need-to-know" basis, for example restricting file access;
	  ○ requiring third parties that have access to the personal information to adhere to the same security standards;
	  ○ 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;
	  ○ undertake regular patch management on software applications used;
	  ○ install and maintain anti-virus and similar protections;
	  ○ carry out proper software license management;
	  ○ maintain appropriate mandatory certification in respect of their technology systems (where required); and
	  ○ carry out periodic internal security audits of their data security procedures and technology systems.
	
	Physical and Building Security
	
	• Control access to the its premises using appropriate security measures.
	• Operate appropriate restrictions on internet connectivity.
	
	Data policy

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

8. **Sub-processors**

8.1 A current list of Subprocessors for the Subscription Products (as added to the Order Form), including the identities of those Subprocessors, the activities they are performing on Company's behalf, and their location can be found at https://prod.litera.com/privacy-notice/list-of-subprocessors/ (the "Sub-process Site"). If Customer would like to receive notifications of new Subprocessors which Company updates to Sub-process Site, Customer must subscribe to the following webpage: https://info.litera.com/01-Sub-Processor-LP.html in order to be notified. Company shall provide the notification of new Subprocessors only if Customer has subscribed to receive the notification.

8.2 Company will restrict the Sub-processors access to Personal Data only to what is necessary to assist Company in providing or maintaining the Subscription Products. Company will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause Company to breach any of its obligations under this DPA.

8.3 Once the Customer is notified of any changes to the Sub-process Site, Customer may object in writing within five (5) days to Company's appointment of a new Sub-processor, provided that such objection is based on reasonable grounds relating to Data Protection Laws. In such event, the parties will discuss such concerns in good faith with a view to achieving resolution. If the parties cannot agree a mutually acceptable resolution, Client shall as its sole and exclusive remedy have the right to terminate the Agreement. Any pre-paid and unused fees paid by the Customer prior to the date of termination shall not be refunded.

ANNEX 1 – DATA PROCESSING DETAILS

Categories of data subjects whose personal data is transferred

Data exporter may submit Personal Information to the Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Information relating to the following categories of data subjects:

Employees and Clients of Customer

Categories of personal data transferred

Data exporter may submit Personal Information to the Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following Personal Information:

Name, Surname, Phone Number, Email address, Physical address of Users of the Products

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous basis

Nature of the processing

The provision of the Products and Service pursuant to the Agreement.

Purpose(s) of the data transfer and further processing

The provision of the Products and Service pursuant to the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

For the duration of the Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Please see Exhibit 2 below.

ANNEX 2 - SECURITY MEASURES

a. Company's Security Program – The security program aligns with the latest industry standards, best practices, and applicable laws and regulations. The security program focuses on: customer data protection and privacy, product security, cloud security, data security and risk detection and prevention, business continuity and disaster recovery and data compliance.

b. Security by Design - Company's team is engaged in a robust, secure development cycle, leveraging industry best practices and tools. Company's security by design program automates processes to quickly identify any potential vulnerabilities within Company's systems and resolve them efficiently and effectively.

c. Data Encryption – Company encrypts data in transit and at rest. Company's security team closely monitors the changing cryptographic landscape and provides service upgrades, while implementing best practices.

1. Data Encryption in Transit - All data transmitted between all customers and Company's software has been securely protected with the right encryption protocols. Our systems support the latest, recommended secure cypher suites, including TLS 1.2 protocols or above, AES256 encryption, and SHA2 signatures, whenever supported by clients.

2. Data Encryption at Rest - Company has taken the appropriate safeguards to encrypt data at rest. Company uses 256-bit Advanced Encryption Standard (AES-256) to encrypt data at rest. This standard applies to all types of data at rest in Company's systems, including relational databases, file stores, database backups, etc. Company has also taken the necessary steps to ensure our encryption keys and processes are secure. Company uses a combination of storage technologies to ensure client data is protected from possible hardware failures, mitigating any associated risks. The company's service relies on leading industry-service providers, offering technological and physical protection for our entire technological environment.

d. Network Security - Company has dedicated networks to increase data protection. Company's production infrastructure is hosted on separate networks from Company's testing and development systems. The company's production fleet servers are hardened and have an applied base configuration image to ensure consistency. The company's production environments have restricted network access from open, public networks and the only open network protocols at our perimeter are those essential to the delivery of the Company's services. To detect and prevent suspicious activities, Company's logs, monitors, and audits system calls, with alerting in place for potential intrusions.

e. Endpoint Security - Company's workstations are also compliant with security best practices. Workstations are configured, updated, tracked, and monitored by Company's endpoint management solutions, with the strongest encryption, strong passwords, and locking when idle. The company is equipped with a high-end endpoint security platform that delivers a solution for advanced threat protection against malware, detection of unauthorized software and vulnerabilities for all workstations. Company's security standards require that mobile devices used to conduct company business are part of our mobile device management system.

f. Access Control -

    1. Provisioning - Company's data protection program incorporates and applies the concept of need-to-know security (least privilege) when provisioning access. This means that data and access to it is available to only those that need it to fulfil their job responsibilities. The company has implemented an advanced set of access, encryption, and logging features so only authorized users are granted access. The company's team continuously reviews access granted and monitors activity to detect potential intrusions.

    2. Authentication - Company uses multi-factor authentication for access to highly sensitive data, including Company's production environment, where our customers' data resides. This reduces the risks of unauthorized access and strengthens our security policies.

    3. Single Sign-on (SSO) - Company enables Single Sign-On (SSO) through SAML 2.0. It strengthens security and mitigates risks across networks for the Company's clients, partners and employees.

g. Cloud Security - Company's data protection and security program are used to ensure the security of our cloud products. Credibility of Company's cloud security comes from using industry services leaders, specifically Amazon Web Services (AWS) and Microsoft Azure Cloud Services. The company enables saving data in virtual private clouds of these cloud providers with the goal of further strengthening data security measures by controlling and filtering access.

h. System Monitoring, Logging & Alerting - At Company, our security team continuously monitors servers, workstations, and mobile devices to analyze, comprehend, and improve the security state of the Company's technological infrastructure. All actions and access are logged and retained for at least two years. The process is automated, detecting and alerting responsible personnel of potential issues.

i. Data Minimization & Retention - Company only processes data that is necessary to perform the specific tasks and duties and not for any other purposes. Company's commitment to the customers also lies in Company's promise to not retain data past its usability point. Company deletes all information from currently running production systems and backups are destroyed within 35 days. The company's hosting providers are responsible for ensuring the removal of data from disks, performing this process in a responsible and secure manner.

j. Disaster Recovery & Business Continuity - With customer data stored in multiple locations in the hosting providers' data centers, the Company further ensures data security and availability. As part of our disaster recovery plan, the Company has secure-tested backups and procedures in case of interruptions or major disasters. Data is backed up automatically and the backups are encrypted and stored securely.

k. Responding to Security Threats & Incidents - Company takes the necessary precautions to avoid system breaches and security vulnerabilities, but is still fully prepared to tackle them. The company's security team has developed detailed processes for responding to and managing potential security threats and incidents. These processes define the types of events that need to occur for the security team to take action, and classify these events based on severity. In case of an incident which affects any of the Company's customers, those affected will be contacted by the security team. The company's incident response procedures are tested and updated annually.