ADDITIONAL TERMS AND CONDITIONS FOR CONCEP SOFTWARE

These Additional Terms and Conditions together with the applicable governing agreement by deployment shall be deemed to be construed as the "Agreement". To the extent there is any conflict between these Additional Terms and Conditions and the applicable governing agreement, these Additional Terms and Conditions shall govern.

1. The Following definitions shall be applicable if Customer is using the products outlined in Order Form.In the event of conflict between the definitions added to the Agreement as referenced in the Order Form and the definitions added in here, the definitions added in here shall prevail:

a) "**Branding Materials**" means those trademarks, logos, artworks, photographic images and other visualor audio materials provided by the Customer to Company for incorporation into the Software.

b) "**End User**" means any employee, agent or subcontractor of the Customer who is authorized by the Customer to access the Software.

c) "**Software**" means the hosted online application as identified in the Order Form which includes an application customized for Customer as stated in the Order Form.

d) "**Working Day/s**" means Monday to Friday excluding all Bank and Public Holidays.

2. In order for Company to render the Software, the Customer will provide Company with all necessary co-operation and access to such information as Company may reasonably request during the Subscription Term. This may include:

a) providing documentation (including where applicable the Branding Materials), Customer Data andsecurity access information;

b) providing configuration services, ensuring that the Customer's network and systems comply with any specifications issued by Company from time to time and accepting and applying updates and upgrades to, and new versions of, the Software;

c) responding promptly and in full to any of Company's reasonable requests for information, instruction or assistance; and

d) making personnel available to instruct and assist Company where reasonably requested by Company.

3. The Customer will be responsible for procuring and maintaining its network connections and telecommunications links from its systems to Company's data centres.

3.1 The Customer will ensure that each End User will keep a secure password for his/her use of the Application and Documentation and that each User will keep his/her password confidential. The Customer will maintain a written, up to date list of current End Users and provide the list to Company upon Company's written request.

3.2 The Customer will comply with, and will ensure that each End User complies with, the Acceptable Use Policy attached hereto as Schedule A.

4. For Customers located at Australia, the fees are Goods and Services Tax (GST) exclusive, and GST will be paid by the Customer in addition to the fees in accordance with the Order Form.

5. The Customer acknowledges that the Software is delivered over third party internet and communications networks and Company will not be liable in relation to any delays, limitations or other problems inherent in such networks or any failure of the Customer to procure and maintain adequate communications networks.

6. Company will not be liable for any delay in or failure to provide the Software which is attributable in whole or in part to any failure of the Customer to perform its obligations under the Agreement, and in such an event Company may adjust any agreed timings as is reasonable.

a) If the Customer does not comply with its obligations, including (without limitation) by refusing to migrate to new platforms made available by Company, then without limiting its other remedies under the Agreement, or at law, Company may charge the Customer for any additional costs or expenses incurred by Company as a result of such non-compliance in addition to the Total Fees and/or may terminate the Order Form by giving written notice to the Customer, provided that Company has given the Customer written notice of the non-compliance and such non-compliance continues for 21 days or more after the date of that notice.

b) Company acknowledges and agrees that the Customer and/or its licensors own all intellectual property rights in the Branding Materials provided by the Customer. The Customer will indemnify Company against any claim by a third party that Company's use of the Branding Materials in accordance with the terms of the Agreement and Order Form infringes that third party's intellectual property rights.

6. Data Recovery

a) The Customer's access to the Software shall cease upon termination or expiry of the Order Form or the Agreement. Any live forms submitted by the Customer shall be removed upon termination or expiry of the Order Form.

b) The Customer shall be responsible for arranging for the transfer or export of Customer Data prior to the termination or expiry of the Order Form or the Agreement. On the Customer's request, Company may provide the Customer with reasonable assistance in relation to such transfer or export prior to termination or expiry of the Order Form which shall be subject to additional fees charged by Company.

c) On termination or expiry of the Order Form or the Agreement, Company shall retain Customer Data for a period of six (6) months, after which time it shall delete all Customer Data in its possession that is stored in live databases. Upon the date of deletion, the data will reside in encrypted backups for a further 100 days, after which it will be overwritten. If during the initial six (6) month period Company receives a written request for the provision to the Customer of access to the Customer Data, Company shall provide such access which shall be subject to additional fees charged by Company.

7. The Software is provided in pursuant to the Data Protection Addendum, attached hereto as Schedule B, which may be modified from time to time.

8. Notwithstanding the Agreement, the Company shall provide Support and Maintenance in accordance with the policy attached hereto as Schedule C.

Schedule A

ACCEPTABLE USE POLICY

This Acceptable Use Policy sets out terms and conditions relating to the Customer's use of the Software. All capitalized terms in this Acceptable Use Policy will have the meanings given the Agreement or, as applicable, the Support and Maintenance Agreement, unless otherwise provided.

1 Use of the Software

1.1 Company may provide training in the use of the Software for all End Users who will have access to it. All requests for training should be made to the Customer's Account Manager at Company, who will provide an Order Form setting out the price and time schedules applicable to such training.

1.2 The Customer will use the Software strictly in accordance with any guidance and instructions made available by Company, including via the Customer helpdesk or during any training session provided by Company.

1.3 If at any time the Customer believes or suspects that any End User is acting or intends to act in breach of this Acceptable Use Policy, it will promptly notify Company and provide relevant information and a plan for cure.

1.4 Company may immediately terminate or suspend any End User's access to the Software where reasonably requested to do so by the Customer. Company will assist the Customer with any investigation into any misuse or potential misuse by such End User upon reasonable request.

1.5 In the event of any actual or suspected breach of this Acceptable Use Policy, Company may without further reference to the Customer, examine materials created by the Customer using the Software for the purpose of monitoring its compliance with the Agreement or Order Form.

1.6 The Customer shall ensure that its use of the Software conforms to Customer’s own policies and procedures governing use of the Internet.

2 SPAM

2.1 The Customer acknowledges that the sending of unsolicited emails to third parties may be considered to be 'spam' and may cause the Software to be identified by companies or internet service providers as a source of spam. This may cause subsequent emails sent by the Software to such companies or email addresses using such internet service providers to be blocked by their Spam-filtering facilities. Accordingly, the Customer agrees that it will not send unsolicited emails to any third party unless:

a) it has obtained that party's consent to receive such emails;

b) it has obtained that party's contact details from that party in the context of a relationship of supplier and customer (actual or prospective) and offers that party the opportunity to unsubscribe from further emails; or

c) it has obtained that party's details from a list compiled using best-practice permission-based marketing.

The Customer also acknowledges that older email addresses may be used as "spam traps", again causing the Software to be identified as a source of spam. Accordingly, the Customer agrees that it shall monitor and maintain its mailing lists and shall not send emails to any address which has not met condition a), b) or c) within the previous year.

2.2 The Customer acknowledges that the identification of the Software as a source of Spam may impact upon other End Users of the Software unconnected with the Customer and may therefore significantly impact upon Company's ability to conduct its business. The Customer will indemnify Company for all losses, claim, or liability of Company attributable to Customer’s or a Customer End User’s improper orunlawful use of the Software will be Customer’s responsibility.

2.3 For communications to persons in the United States of America, the Customer will comply in full with the provisions of the CAN-SPAM Act of 2003 and the Federal Trade Commission Act. See FTC recommendation at http://www.business.ftc.gov/documents/bus61-can-spam-act-compliance- guide-business. For communications to persons in the European Economic Area, the Customer will comply in full with the provisions of the European Union Privacy and Electronic Communications (EC Directive)Regulations 2003. See UK’s application of such directive at

http://www.legislation.gov.uk/uksi/2003/2426/contents/made and, as to email marketing, http://www.legislation.gov.uk/uksi/2003/2426/regulation/22/made. Compliance with these laws and Regulations is a condition of the Customer's access to and use of the Software.

2.4 The Customer will not use the Software to send any commercial electronic mail message (as that term is defined in the CAN-SPAM Act) to any person who has opted out or otherwise objected to receiving such messages.

2.5 The Customer may not use the Software to email to distribution lists, newsgroups, or spam or unsolicited email addresses, including where such email addresses have been purchased from a third party or acquired other than through best-practice permission-based marketing.

2.6 If Company receives notice or determines (acting reasonably) that the Customer's use of the Software is generating a higher number of spam complaints than would normally occur if the Customer complied with this Acceptable Use Policy, Company will notify the Customer immediately and may, at its sole and unfettered discretion:

a) suspend the Customer's access to the Software until the issue resulting in the spam complaints has been resolved; or

b) terminate the Agreement or the Order Form without liability by written notice with or without immediate effect.

3 Prohibited Content and Uses

3.1 The Customer may not use the Software to:

a) provide, sell or offer to sell any of the following products or content (or services related to the same): pornography; escort services; illegal goods including illegal drugs, substances and weaponsand pirated computer programs; instructions on how to assemble or otherwise make bombs, grenades or other weapons; or any other products, services or content that it is unlawful to sell or offer to sell in the territory in which the sender or email recipient is located; or

b) display or market material that unlawfully exploits children, or otherwise unlawfully exploits persons under 18 years of age, or that targets children under the age of 13 in violation of the Child Online Pornography Protection Act of 1998; or

c) provide material that is grossly offensive, including blatant expressions of bigotry, prejudice, racism, hatred, or profanity or includes any obscene, lewd, lascivious, violent, harassing, hateful orotherwise legally objectionable or illegal content; or

d) disclose personal data, personally identifiable information, personal health information, personal financial information, or sensitive personal data (e.g., medical or health condition, racial or ethnic origin) in breach of the terms of any state, federal or other law, rule or regulation, including without limitation any state law or the federal Health Insurance Portability and Accountability Actof 1996; or

e) send emails containing or otherwise introducing viruses, worms, harmful code or Trojan horses into the recipient's computer or computer network; or

f) engage in any libelous, defamatory, scandalous, threatening, or harassing activity or illegal conductthat is defined as such within the geographical territory in which the sender or recipient is located; or

g) post any content that advocates, promotes, or otherwise encourages violence against any governments, organizations, groups or individuals or which provides instruction, information or assistance in causing or carrying out such violence; or

h) provide content, including images, that embody or constitute infringing derivatives of the Intellectual Property Rights of a third party such as but not limited to authors, artists, photographers, or others, without the express written consent of the owner of such rights, or in any way infringe the Intellectual Property Rights of any third party; or

i) disparage, make fun of, or satirize the Company name, or any of its products or services; or

j) use the Software in any manner which may bring Company, its affiliates or any of its products orservices into disrepute.

k) take any action that imposes an unreasonable or disproportionately large burden on Company's infrastructure, or that bypasses any measures to protect or restrict access to the Software or the Documentation.

3.3 If Company receives notification from any third party or otherwise has cause to believe that the Customer's use of the Software is in breach of the provisions of this Clause 3, it will notify the Customer immediately and may, at its sole and unfettered discretion:

a) delete any breaching emails or content without notice; and/or

b) suspend the Customer's access to the Software until the issue has been resolved; and/or

c) suspend or terminate the Order Form; and/or

d) terminate the Agreement or the Order Form without liability by written notice with immediate effect.

4 Use of Linking URLs

4.1 The Software contains functionality that enables the recipient of an email to click on a link which will take them to a URL displaying the email online. The Customer acknowledges that this functionality is provided solely to enable recipients whose email package does not enable them to otherwise display orrender the email correctly to see the email using their internet browser, and for no other purpose whatsoever.

4.2 If Company has reason to believe that the Customer has used, or is using, the functionality set out in Clause 4.1 above other than in accordance with the purpose set out therein, it may at its sole and unfettered discretion:

a) create a new Billable Event, such that each view of such affected URL will become billable at the same Billable Event Fee that applies to each email sent, as set out in the applicable Order Form; and/or

b) suspend access to the affected URL; and/or

c) suspend the Customer's access to the Software until the issue has been resolved; and/or

d) terminate the Agreement or the Order Form without liability by written notice with or without immediate effect.

SCHEDULE B

DATA PROTECTION ADDENDUM

1. **Introduction**

1.1 If Customer's bill to information listed on the applicable Customer Contract is located in North America, 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 North America 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 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 at https://www.litera.com/privacy-notice/ .

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.

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.

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 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	
Subject matter and duration of the Processing	Added in Exhibit A
Nature and purpose of the processing	Added in Exhibit A
Categories and types of personal data being processed	Added in Exhibit A
Categories of data subjects	Added in Exhibit A
Security Measures	Added in Exhibit B

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 is located in United Kingdom, 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 2010/87/EU (**Controller to Processor Model Clauses**) shall apply and are hereby incorporated into these data processing terms. A copy of the Controller to Processor Model Clauses can be found at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010D0087&from=en If the Customer is 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. It is recognized that the personal information that the *data importer* processes (i) when it accesses the *data exporter's* systems in relation to the provision of support; and (ii) when the *data exporter* uses the data importer's technology services and solutions to store and otherwise process data, will be determined by 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 about the likely categories of data subject are set out in Exhibit A.
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 about the likely non-special categories of personal data are set out in Exhibit A.

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 about the likely special categories of personal data are set out in Exhibit A.
Processing operations The personal data transferred will be subject to the following basic processing activities	Exhibit A sets out the basic processing activities to which the personal data will be subject.
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, authorization, 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 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 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 in Exhibit C. 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.

EXHIBIT A – DATA PROCESSING DETAILS

	Purpose of Processing	Personal Information is Processed by us in connection with providing the Software requested by the Customer pursuant to the Customer Contract.
	Categories of Data Subjects	The Customer's Clients, contacts, event attendees and employees who receive email campaigns from the Customer using Concep Send.
	Types of Personal Data	For Concep Send, the following types of Personal Data may be Processed: • **Contact data**: email addresses plus any other information about a Data Subject that an End User uploads or adds and/or a Data Subject provides in response to a survey, such as first name, last name, company. The information recorded in relation to each Data Subject is determined by Users and the Data Subject. • **Contact campaign tracking data**: system generated data that Concep Send tracks against a recipient of an email campaign, including views, repeat views, clicks (including the exact link that the use clicked on), replies, opt-outs, bounces and their types and reasons (e.g. hard bounce for an invalid email address) for the purpose of email campaign reporting, location data based on IP addresses, device details such as the type of device and the user version. There is a setting which allows tracking to be disabled for a recipient, and if the recipient selects this, no contact campaign tracking data will be stored. There is also an additional setting which masks an email address in the reporting (e.g. r********r@concep.com). • **Contact survey tracking data**: system generated data that Concep Send surveys collect, including recipients' IP addresses, locations and browser details. If a survey is linked to an email campaign, then the contact data will pull through into the survey reporting.
	Transfers to countries outside the European Economic Area (EEA)	Personal Information may be transferred to or Processed in a country outside the EEA in the following circumstances and subject to the following conditions: 1. Where a Subscription Products listed in the Customer Contract includes training, providing services or support, the provision of that Service may require the downloading of Customer Personal Data by staff in the U.S., UK, EEA or Australia. 2. If the Customer is based in Australia or U.S., Personal Information that is made available to the Customer's CRM in connection with Concep Send will be Processed or transferred via servers hosted in Australia or U.S., as applicable. 3. Where End Users access the Personal Information via the Software in a country outside the EEA, Personal Information will be transferred to and Processed in the country from which they have accessed it.
	Third party Processors	Attached as Exhibit C

EXHIBIT B – SECURITY MEASURES

Physical access controls.
Litera Concep is hosted in AWS datacenters that meet the highest physical security standards recognized by the industry.

- 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 Litera Concep utilizes industry best practices for encryption and enforces the use of TLS (Transport Layer Security) 1.2 and above with strong cypher suites for all data in transit.

- Input controls.

Litera Concep offers 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 and custom fields.

- Data backups.

Litera Concep leverages multiple technical controls to ensure system availability and continuity. This includes regular encrypted backups stored in a high redundancy storage facility.

- Data segregation

The Concep Send platform is a multi-tenant SaaS solution. There is a single database, customer data is separated through logical separation.

- Pen Testing and Code Scanning

Litera performs regular static, dynamic and software composition analysis scans on the Concep code base. Litera also performs an annual third-party penetration test of the Litera Concep application.

- Encryption at Rest

Litera Concep utilizes industry best practices and enforces the use of AES-256 for encryption of data at rest.

- Regular review of audit logs

Litera Concep is under continuous monitoring and alerting for system performance and security events. System level audit logs are assessed to detect unusual behavior and application performance.

EXHIBIT C – LIST OF SUBPROCESSORS

AWS (Amazon Web Services) –

1. hosts the Litera Concep application. All hosting locations reside in the EU (European Union) region.
2. provides the infrastructure (IaaS) which hosts Litera's mail server.

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

JIRA - 2nd line customer support ticket management and product management solution. No specific location.

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.

Schedule C

CUSTOMER SUPPORT SLA

The Company provides two primary forms of support. The first is document support whereby Customer Support personnel assist customers when document issues are encountered. The second form of support provided is application (product) support whereby Customer Support personnel provide support when product issues (bugs) are encountered. All times referenced are US Eastern time (Standard or Daylight).

Issue Reporting

Customer shall report issues to Company via any method described below

Customer Support Community

The Customer Support Community can be used to report and manage communications on all support issues for / by Customer.

Customer may access the Customer Support Community at any time to monitor updates on any of theirissues.

Email Support

Email support is provided from 4:00 a.m. to 8:00 p.m. Monday through Friday, excluding US Holidays.

Telephone Support

Telephone support is provided from 4:00 a.m. to 8:00 p.m. Monday through Friday, excluding US Holidays.

Issue Classification, Course of Action, and Initial Response – Product Support

Company will use all reasonable efforts to provide solutions, changes and corrections in a timely manner to assure the Product(s) operate as designed.

Issue Classification and Course of Action

Customer will make an initial nonbinding classification of the issue they are reporting when initiallyreporting an issue.

Company Customer Support team reviews the issue including Customer-designated classification and makes the final determination of classification as well as action and ownership.

Course of Action and Expected Time to Resolution will be based on Issue Classification.

Classification	Definition	Course of Action
Severity 1	An issue that affects or restricts major functionality company wide, or for many users, and makes continued use of said functions impossible. A workaround is not available andoperation cannot continue in a restricted fashion.	Company will use commercially available "best efforts" to (a) isolate and resolve the problem immediately, ifpractical, and (b) provide customer with daily status updates on the progress of a software fix or (c) workaround, if available, or (d) include the software fixin the current product release.
Severity 2	An issue that severely affects or restricts major functionality. The problem is of a time sensitive nature and important to long-term productivity but is not causing an immediate work stoppage. A workaround may be available, and operation can continue in a restrictedfashion.	Company will use commercially reasonable efforts to provide the customer with a "workaround", if known, or include the fix in the (a) current release, (b) the nextscheduled service pack release or (c) next major product release.

Severity 3	A minor issue that does not have a major effect on production operationfor which an acceptable customer workaround exists.	Company will use commercially reasonable efforts tofix the error in the next major product release.
Severity 4	A minor condition or issue that has no significant impact on the customer's operations or additional requests for feature suggestions, which are defined as new functionality.	All requests are submitted to Product Management for consideration in future releases of the product.

Initial Response

Company will respond with initial acknowledgment of issue within one hour if reported during normalbusiness hours, or by 8:00 a.m. on the next Business Day.

Course of Action, and Initial Response – Document SupportInitial Response

Company will respond with initial acknowledgment of issue within 1 hour if reported during normal USbusiness hours, or by 8:00 a.m. on the next Business Day.

Targeted Resolution and Course of Action

Company targets a two hour turnaround time for all Document Support issues. Once a document issue has been reported to Customer Support, it is processed as follows:

Time	Action
0-60 minutes	Customer Support Representative reviews and attempts to resolve the issue. If unable, the issue is escalated.
61-120 minutes	Senior Customer Support Representative reviews and attempts to resolve the issue. If unable, the issue is escalated
After 120 minutes	Lead Customer Support Representatives work with the Development team in an attempt to resolve the issue.