DATA PROCESSING ADDENDUM

Based on the General Data Protection Regulation (GDPR) and European Commission Decision 2010/87/EU - Standard Contractual Clauses (Processors)

This Data Processing Addendum ("DPA") forms part of the End User License Agreement (or other such titled written or electronic agreement addressing the same subject matter) between CDATA and Customer for the purchase of software and technical support services from CDATA (collectively identified as "Services"), wherein such End User License Agreement is hereinafter defined as the "Agreement," and whereby this DPA reflects the parties' agreement with regard to the Processing of Personal Data. Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent CDATA processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Services to Customer pursuant to the Agreement, CDATA may Process Personal Data on behalf of Customer, and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

HOW TO EXECUTE THIS DPA:

1. This DPA consists of two parts: the main body of the DPA, and Attachment 1 (including Appendices 1 and 2).

2. This DPA has been pre-signed on behalf of CData Software, Inc. The EU Standard Contractual Clauses in Attachment 1 (including Appendices 1 and 2) have been pre-signed by CData Software, Inc. as the data importer.

3. To complete this DPA, Customer must:

    a. Complete the information in the signature box and sign on Page 6
    b. Complete the information in the signature box and sign on Pages 18 and 20

4. Send the completed and signed DPA to CDATA by email to gdpr@cdata.com.

Upon receipt of the validly completed DPA by CDATA at this email address, this DPA will become legally binding.

HOW THIS DPA APPLIES

If the Customer entity signing this DPA is a party to the Agreement, then this DPA is an addendum to and forms part of the Agreement. In such case, the CDATA entity that is party to the Agreement is party to this DPA.

If the Customer entity signing this DPA has executed an Order Form with CDATA or its Affiliate pursuant to the Agreement, but is not itself a party to the Agreement, then this DPA is an addendum to that Order Form and applicable renewal Order Forms, and the CDATA entity that is a party to such Order Form is a party to this DPA.

If the Customer entity signing this DPA is not a party to an Order Form nor an End User License Agreement directly with CDATA, but is instead a customer indirectly via an authorized reseller of Services, this DPA is not valid and is not legally binding. Such entity should contact the authorized reseller to discuss whether any amendment to its agreement with that reseller may be required.

This DPA shall not replace any comparable or additional rights relating to Processing of Customer Data contained in Customer's Agreement (including any existing data processing addendum to the Agreement).

DATA PROCESSING TERMS

1. DEFINITIONS

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"**Authorized Affiliate**" means any of Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and CDATA, but has not signed its own Order Form with CDATA and is not a "Customer" as defined under the Agreement.

"**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data.

"**Customer Data**" means all electronic data submitted by or on behalf of Customer, or an Authorized Affiliate, to the Services.

"**Data Protection Laws and Regulations**" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area (EEA) and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.

"**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

"**EEA**" means the member states of the European Union, as well as Iceland, Liechtenstein, and Norway.

"**EEA Restricted Transfer**" means a transfer (or onward transfer) by Customer to CDATA of Personal Data originating in the EEA or Switzerland that is subject to GDPR or the Swiss Federal Act on Data Protection, where any required adequacy means can be met by entering into the EU Standard Contractual Clauses.

"**EU Standard Contractual Clauses**" means the standard contractual clauses annexed to Commission Implementing Decision (EU) (2021/914) of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant Regulation (EU) 2016/679 of the European Parliament and of the Council under Module 2 (Transfer controller to processor) as entered by the parties and attached to this DPA as **Attachment 1**.

"**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), and for the purpose of this DPA includes the corresponding laws of the United Kingdom (including the UK GDPR and Data Protection Act 2018).

"**Personal Data**" means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Customer Data.

"**Processing**" (including its root word, "**Process**") shall have the meaning given in Data Protection Laws and Regulations.

"**Processor**" means the entity which Processes Personal Data on behalf of the Controller.

"**CDATA**" means the CDATA entity which is a party to this DPA, as specified in the Section "How This DPA Applies" above, being CData Software, Inc., a corporation incorporated in North Carolina and its primary address as 101 Europa Drive, Suite 110, Chapel Hill, NC, USA, or an Affiliate of CDATA, as applicable.

"**CDATA Group**" means CDATA and its Affiliates engaged in the Processing of Personal Data.

"**Sub-processor**" means any Processor engaged by CDATA or a member of the CDATA Group.

"**Supervisory Authority**" means an independent public authority which is established by an EU Member State pursuant to the GDPR.

"**UK Restricted Transfer**" means a transfer (or onward transfer) by Customer to CDATA of Personal Data originating in the United Kingdom that is subject to UK GDPR where any required adequacy means can be met by entering into the UK Standard Contractual Clauses.

"**UK Standard Contractual Clauses**" means the standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC pursuant to the European Commission Decision of 5 February 2010, as modified by the UK Information Commissioner's Office and entered by the parties under this DPA.

2. PROCESSING OF PERSONAL DATA

2.1. Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller, CDATA is the Processor and that CDATA or members of the CDATA Group will engage Sub-processors pursuant to the requirements set forth in Section 5 "Sub-processors" below.

2.2. Customer's Processing of Personal Data. Customer shall, in its use of the Services, comply with Data Protection Laws and Regulations. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data must comply with Data Protection Laws and Regulations. Customer shall ensure that Customer is entitled to transfer the relevant Personal Data to CDATA so that CDATA may lawfully use, process, and transfer the Personal Data in accordance with the Agreement on the Customer's behalf. In addition, Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data, including providing any required notices to, and obtaining any necessary consent from, its employees, agents or third parties to whom it extends the benefits of the Services.

2.3. CDATA's Processing of Personal Data. CDATA will process and use Customer Data and Personal Data on Customer's behalf and only in accordance with Customer's instructions (including via email) and to the extent required by law, including but not limited to the GDPR requirements directly applicable to CDATA's provision of the Services. Customer hereby acknowledges that by virtue of using the Services it gives CDATA instructions to process and use Customer Data and Personal Data in order to provide the Services in accordance with the Agreement. Customer takes full responsibility to keep the amount of Customer Data and Personal Data provided to CDATA to the minimum necessary for the performance of the Services.

2.4. Scope of Processing. The subject matter of Processing of Personal Data by CDATA is the provision of the Services pursuant to the Agreement. The nature and purpose of the Processing, the types of Personal Data, and categories of Data Subjects Processed under this DPA are further specified in Attachment 1, Annex I.B to this DPA.

3. RIGHTS OF DATA SUBJECTS

3.1. Data Subject Requests. CDATA shall provide all reasonable and timely assistance (including by appropriate technical and organizational measures) to Customer to enable Customer to respond to: (i) any request from a Data Subject to exercise any of its rights under Data Protection Laws and Regulations, including its rights of access, correction, objection, erasure ("right to be forgotten"), data portability, or to not be subject to an automated individual decision making (each, a **"Data Subject Request"**); and (ii) any other correspondence, inquiry or complaint received from a Data Subject, Supervisory Authority, or other third party in connection with the Processing of the Data to the extent CDATA is legally permitted to do so and that the response to such Data Subject Request is required under applicable Data Protection Laws and Regulations. Customer shall be responsible for any costs arising from CDATA's provision of such assistance, including any fees associated with providing additional functionality. In the event that any such request, correspondence, inquiry or complaint is made directly to CDATA, CDATA shall promptly inform Customer providing full details of the same.

4. CDATA PERSONNEL

4.1. Confidentiality. CDATA shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. CDATA shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2. Reliability. CDATA shall take commercially reasonable steps to ensure the reliability of any CDATA personnel engaged in the Processing of Personal Data.

4.3. Limitation of Access. CDATA shall ensure that access to Personal Data is limited to those personnel who require such access to perform the Agreement.

4.4. Data Protection Officer. CDATA is not required to officially appoint a data protection officer to the extent this is required by Data Protection Laws and Regulations. However, upon request, Customer may contact gdpr@cdata.com with any questions or requests under this DPA.

5. SUB-PROCESSORS

5.1. Appointment of Sub-processors. Customer acknowledges and agrees that (i) CDATA is entitled to retain its Affiliates as Sub-processors, and (ii) CDATA or any such Affiliate may engage any third parties from time to time to process Customer Data in connection with making the Software and/or the provision of Support. CDATA will only disclose Personal Data to Sub-processors that are parties to written agreements with CDATA including obligations no less protective that the obligations of this DPA with respect to the protection of Customer Data to the extent applicable to the nature of the services provided by such Sub-processor. Customer acknowledges that Sub-processors may be appointed by CDATA in accordance with Clause 9 of Attachment 1.

5.2. List of Current Sub-processors and Notification of New Sub-processors. Customer hereby authorizes CDATA to engage Sub-processors to Process Personal Data on Customer's behalf, including the Sub-processors currently engaged by CDATA. CDATA will notify Customer in the event that it intends to engage different or additional Sub-processors that will Process Personal Data pursuant to this DPA, which may be done by email or posting on a website identified by CDATA to Customer.

5.3. Objection Right for New Sub-processors. Customer may reasonably object to CDATA's use of a new Sub-processor (e.g., if making Personal Data available to the Sub-processor may violate applicable Data Protection Law or decrease protections for such Personal Data) by notifying CDATA promptly in writing within ten (10) business days after receipt of CDATA's notice in accordance with the mechanism set out in Section 5.2. Such notice shall explain the reasonable grounds for the objection. In the event Customer objects to a new Sub-processor, and that objection is not unreasonable, CDATA will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If CDATA is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, either party may terminate the applicable Order(s) with respect only to those aspects of the Services which cannot be provided by CDATA without the use of the objected-to new Sub-processor by providing written notice to CDATA. CDATA will refund Customer any prepaid fees on a prorated basis of such Order(s) following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.

5.4. Liability. CDATA shall be liable for the acts and omissions of its Sub-processors to the same extent CDATA would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

6. SECURITY; AUDIT RIGHTS

6.1. Controls for the Protection of Personal Data. CDATA will maintain appropriate technical and organizational safeguards against unauthorized or unlawful Processing of the Personal Data, and against accidental loss or destruction of, and damage to the Customer Data, according to the measures set forth on Appendix 2 of Attachment 1. CDATA's obligations under this Section 6.1 will be satisfied by complying with terms of such Appendix 2 of Attachment 1.

6.2. Audit Rights. CDATA will allow Customer to perform an on-site audit of CDATA, at Customer's sole expense, for compliance with the technical and organizational measures set forth in the Appendix 2 of Attachment 1 if (i) CDATA notifies Customer of a Security Incident, or (ii) if Customer reasonably believes that CDATA is not in compliance with its security commitments under this DPA, or (iii) if such audit legally is required by Customer's Applicable Laws. Such audit must be conducted in accordance with the procedures set forth in Section 6.5 and may not be conducted more than one time per year.

6.3. Satisfaction of Audit Request. Upon receipt of a written request to audit, and subject to Customer's agreement, CDATA may satisfy such audit request by providing Customer with a confidential copy of an Audit Report (described in Section 6.2) in order that Customer may reasonably verify CDATA's compliance with the technical and organizational measures set forth in Appendix 2 of Attachment 1.

6.4. Audit Process. Customer must provide at least 6 weeks' prior written notice to CDATA of a request to audit. The scope of any audit will be limited to CDATA's policies, procedures and controls relevant to the protection of Customer Data and defined in Appendix 2 of Attachment 1. All audits will be conducted during normal business hours, at CDATA's principal place of business or other location(s) where Customer Data is accessed, processed or administered, and will not unreasonably interfere with CDATA's day-to-day operations. An audit will be conducted at Customer's sole cost and by a mutually agreed upon third party contractor who is engaged and paid by Customer, and is under a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the Agreement, obligating it to maintain the confidentiality of all CDATA Confidential Information and all audit findings. Before the commencement of any such on-site audit, CDATA and Customer shall mutually agree upon the timing, and duration of the audit and in addition CDATA will provide CDATA's reimbursement rate for which Customer shall be responsible (CDATA's then-current professional Software and/or Services rates). CDATA will co-operate with the audit, including providing auditor the right to review but not to copy CDATA security information or materials. CDATA's

policy is to share methodology, and executive summary information, not raw data or private information. Customer shall, at no charge, provide to CDATA a full copy of all findings of the audit.

6.5. **Notice of Failure to Comply**. After conducting an audit under Section 6.3 or after receiving a CDATA Report under Section 6.4, Customer must notify CDATA of the specific manner, if any, in which CDATA does not comply with any of the security, confidentiality, or data protection obligations in this DPA, if applicable. Any such information will be deemed Confidential Information of CDATA. Upon such notice, CDATA will use commercially reasonable efforts to make any necessary changes to ensure compliance with such obligations.

7. CUSTOMER DATA INCIDENT MANAGEMENT AND NOTIFICATION.

7.1. CDATA shall notify Customer of any breach relating to Personal Data (within the meaning of applicable Data Protection Laws and Regulations) of which CDATA becomes aware and which may require a notification to be made to a Supervisory Authority or Data Subject under applicable Data Protection Law and Regulations (a "**Customer Data Incident**"). CDATA shall make reasonable efforts to identify the cause of such Customer Data Incident and take those steps as CDATA deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident to the extent the remediation is within CDATA's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer, Customer's end users, or any services or software not provided by CDATA.

8. RETURN AND DELETION OF CUSTOMER DATA

8.1. Upon termination of the Agreement for which CDATA is Processing Personal Data, CDATA shall, upon Customer's request, and subject to the limitations described in the Agreement return all Customer Data and copies of such data to Customer or securely destroy them and demonstrate to the reasonable satisfaction of Customer that it has taken such measures, unless the retention of such data is requested by Customer or mandated by applicable law. CDATA agrees to preserve the confidentiality of any retained Customer Data and will only actively Process such Customer Data after such termination date in order to comply with the laws to which it is subject.

9. DATA PROTECTION IMPACT ASSESSMENT

9.1. Upon Customer's request, CDATA shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to CDATA. CDATA shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section 11.2, to the extent required under the GDPR.

10. LIMITATION OF LIABILITY

10.1. Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and CDATA, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

10.2. For the avoidance of doubt, CDATA's and its Affiliates' total liability for all claims from the Customer and all of its Authorized Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Customer and all Authorized Affiliates, and shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA. Also for the avoidance of doubt, each reference to the DPA in this DPA means this DPA including Attachment 1 and Appendices 1-3.

11. TRANSFER MECHANISM FOR DATA TRANSFERS

11.1. If and to the extent CDATA'S performance or Customer's use of the Services involve an EEA Restricted Transfer, CDATA and Customer hereby enter into the EU Standard Contractual Clauses attached hereto as **Attachment 1** to this DPA and agree that the EU Standard Contractual Clauses will govern the parties' obligations with respect to the EEA Restricted Transfer. To the extent there is any conflict between the EU Standard Contractual Clauses and the terms of this DPA, the EU Standard Contractual Clauses will prevail with respect to the EEA Restricted Transfer.

11.2. If and to the extent CDATA'S performance or Customer's use of the Services involve an EEA Restricted Transfer that includes Personal Data originating from Switzerland and is subject to the Swiss Federal Act on Data Protection of 19

June 1992 (the "FADP"), the EU Standard Contractual Clauses are deemed to be supplemented with respect to the transfer of such Personal Data originating from Switzerland with an additional annex that provides as follows:

a. for purposes of Clause 13 and Annex I.C of the EU Standard Contractual Clauses, the competent Supervisory Authority is the Swiss Federal Data Protection and Information Commissioner;

b. the term "member state" as used in the EU Standard Contractual Clauses must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18.c of the EU Contractual Clauses;

c. references in the EU Standard Contractual Clauses to the GDPR should be understood as references to the FADP.

11.3. If and to the extent CDATA'S performance or Customer's use of the Services involve a UK Restricted Transfer, CDATA and Customer hereby enter into the UK Standard Contractual Clauses, which are incorporated by reference herein. To the extent there is any conflict between the UK Standard Contractual Clauses and the terms of this DPA, the UK Standard Contractual Clauses will prevail with respect to the UK Restricted Transfer. For the purpose of any UK Restricted Transfer, the UK Standard Contractual Clauses will be deemed completed as follows:

a. Customer will be considered the "Data Exporter" and CDATA will be considered the "Data Importer."

b. References in the UK Standard Contractual Clauses to "the law of the Member State in which the data exporter is established" shall hereby be deemed to mean "the law of the United Kingdom"; and any other obligation in the UK Standard Contractual Clauses determined by the law of the Member State in which the data exporter is established shall hereby be deemed to refer to an obligation under UK data protection laws.

c. The details of Appendix 1 to the UK Standard Contractual Clauses are set forth on Attachment 1, Annex 1 to this DPA.

d. The details of Appendix 2 to the UK Standard Contractual Clauses are set forth on Attachment 1, Annex 2 to this DPA.

12. LEGAL EFFECT; TERMINATION

12.1. This DPA shall only become legally binding between Customer and CDATA when fully executed and will terminate when the Agreement terminates, without further action required by either party.

13. CONFLICT

13.1. In the event of any conflict or inconsistency between this DPA and the Agreement, this DPA will prevail.

IN WITNESS WHEREOF, the parties have caused this Data Processing Addendum to be duly executed. Each party warrants and represents that its respective signatories whose signatures appear below are on the date of signature duly authorized.

On behalf of the Customer: _____	**On behalf of CData Software, Inc.:**
Name (written out in full): _____	Name (written out in full): Kathy L. Priest
Position: _____	Position: Chief Legal Officer
Address: _____	Address: 101 Europa Drive, Suite 110, Chapel Hill, North Carolina 27517 USA
_____	
Signature: _____	Signature: Kathy L. Priest

Attachment 1

STANDARD CONTRACTUAL CLAUSES

Controller to Processor Transfers

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([1]) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Not Used

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([2]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(a) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(b) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(c) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(d) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([3]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([4]);

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION VI – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX 1

This Annex I forms part of the Clauses and must be completed and signed by the parties.

A. LIST OF PARTIES

Data exporter

Name: The entity identified as "Customer" in the Agreement

Address: The address for Customer specified in the Agreement

Contact person's name, position and contact details: The contact details specified in the Agreement

Activities relevant to the data transferred under these Clauses: Customer's use of the Services provided by the data importer pursuant to the Agreement

Signature and date: Located at the end of this Annex I.

Role (controller/processor): Controller

Data importer(s):

Name: CData Software, Inc.
Address: 101 Europa Drive, Suite 110, Chapel Hill, North Carolina 27517 USA

Contact person's name, position and contact details: Kathy L. Priest, Chief Legal Officer

Activities relevant to the data transferred under these Clauses: Provision of the Services to the data exporter pursuant to the Agreement.

Signature and date: Located at the end of this Annex I.

Role (controller/processor): Processor.

B. DESCRIPTION OF TRANSFERS

Categories of data subjects whose personal data is transferred

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

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors (who are natural persons)
- Employees, agents, advisors, consultants of Customer (who are natural persons)

Categories of personal data transferred

The Personal Data transferred concern the following categories of data (please specify):
The data exporter may submit Personal Data to the data importer as part of the Customer Data, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Personal Data: Customer's identification and contact data (name, email address, address, title, contact details, username); employment details (employer, job title, geographic location, area of responsibility); IP address, cookie data and other data collected via automated means from users of websites or apps, such as clickstream data.

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.

Special categories of data are not required to use the Services, and the parties do not anticipate the transfer of special categories of data. The safeguards applied to Personal Data are described on Attachment 1, Annex II of this DPA.

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

Personal Data may be transferred on a continuous basis during the Term of the Agreement.

Nature of the processing

The nature of the processing is the data importer's performance of the Services under the Agreement, including for the purposes of: (a) setting up, operating, monitoring, and providing the Services; (b) communicating with Users; and (d) executing other agreed-upon written instructions of the data exporter.

Purpose(s) of the data transfer and further processing

The purpose of the data transfer and further processing is the data importer's performance of the Services under 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

Personal Data will be retained for the duration of the Agreement and subject to Section 8 (Return and Deletion of Customer Data) of the DPA.

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

The subject matter, nature, and duration of processing undertaken by sub-processors will be the same as set forth in this Annex 1.B with respect to the data importer.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The competent supervisory authority will be the supervisory authority that has supervision over the data exporter in accordance with Clause 13.

On behalf of the data exporter:	**On behalf of the data importer:**
On behalf of: _____	On behalf of CData Software, Inc.:
Name (written out in full): _____	Name (written out in full): Kathy L. Priest
Position: _____	Position: Chief Legal Officer
Address: _____	Address: 101 Europa Drive, Suite 110
	Chapel Hill, North Carolina 27517 USA
Signature: _____	Signature: Kathy L. Priest

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

This Annex II forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organizational security measures implemented by the data importer in accordance with Clause 8.6(a) (or document/legislation attached):

The data importer currently abides by the security standards in this Appendix II. The Data Importer may update or modify these security standards from time to time provided such updates and modifications will not result in a material degradation in the security of the Services during the term of the Agreement.

CDATA shall implement and maintain a written information security management policy with standards that are no less rigorous than accepted industry practices, comply with all applicable law to protect the personal data from loss or unauthorized access, destruction, use, modification, disclosure or other Processing, as well as comply with the provisions of this Appendix II. Consistent with this policy, CDATA shall implement physical, technical, and administrative information safeguards that adequately provide for: (a) protection of business facilities, paper files, servers, computing equipment, including all mobile devices and other equipment with information storage capability, and backup systems containing the personal data; (b) network, application (including databases), and platform security; (c) business systems designed to optimize security; (d) secure, encrypted transmission and secure, encrypted storage of personal data; (e) authentication and access control mechanisms; and (f) personnel security, including recent strong background checks on all such personnel to the extent permitted by law, use of unique, robust passwords, and annual training on how to comply with CDATA's physical, technical, and administrative information security safeguards.

CDATA shall regularly test and monitor the effectiveness of its security practices and procedures relating to the personal data, and will evaluate and adjust its information security program in light of the results of the testing and monitoring, any relevant changes to its operations or business arrangements, or any other circumstances that CDATA knows or reasonably should know may have a material effect on the effectiveness of its information security program.

Without limiting the foregoing, CDATA shall implement the following security controls:

1. Admittance Control (physical):
   - CDATA will prevent unauthorised persons from gaining access to the systems used to process personal data.
   - CDATA will protect offices in which personal data is processed against access by unauthorized persons.

2. Entry Control (systems):
   - CDATA will prevent data processing systems from being used without authorisation.
   - CDATA will only grant the personnel of CDATA and its permitted subprocessors access to applications that process personal data to the extent they require it to fulfill their function.
   - CDATA will ensure that the entry control is supported by an authentication system that includes regular, iterated grant checks.
   - CDATA shall conduct appropriate systems hardening, including appropriate intrusion detection and network-level isolation.

3. Access Control (data):
   - CDATA will ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access (including in QA, staging and live systems), and that personal data cannot be read, copied, modified or removed without authorisation in the course of processing or after storage.
   - CDATA will enforce password complexity rules and other brute force protection methods on its personnels' accounts on appropriate systems.
   - CDATA will grant authorisation to access personal data only to personnel who need the access to perform their functions. Additionally, CDATA will only grant the personnel the level of access (e.g., roles) required by such personnel to perform their respective functions. CDATA will ensure that only authorised CDATA personnel can access the personal data.
   - CDATA also shall provide user management features to Customer. For example, the CDATA account owner shall be able to assign different roles and permissions to account users.

4. Transfer Control:

- CDATA will ensure that personal data cannot be read, copied, modified or removed without authorisation during electronic transmission or transport, and that it is possible to check and establish to which parties the transfer of personal data is envisaged.
- CDATA will encrypt all personal data if it is stored in an environment without physical access control or if it is stored or transferred outside CDATA's logical and physical access control system.
- CDATA will encrypt data while transferred through internal or external networks, including between CDATA data centers. For example, all data transfers between an end user and the CDATA platform that the user has logged into are encrypted.
- Communications between data centers shall be secured and encrypted for all connections, including, management, control, backup and replication data flows.

5. Input Control:

- CDATA will ensure that it is possible to check and establish whether and by whom personal data has been entered into data processing systems, modified or removed.
- CDATA may permit only authorised personnel to modify any personal data within the scope of their function.
- CDATA must record any changes made to the personal data, if not made by Customer.
- This will be achieved by means of logging of system access events, console events, and user-issued commands.

6. Job Control:

- CDATA will carry out the services and, in particular, the data processing services, for Customer only in accordance with Customer's instructions as set forth in the Addendum.

7. Availability Control:

- CDATA will protect personal data against accidental destruction or loss.
- CDATA will implement measures that enable CDATA to resume the services within a commercially reasonable timeframe if there is a breakdown of the services.
- Safeguards include Regular backups and Disaster recovery testing at least annually

8. Purpose Separation:

- CDATA will ensure that personal data collected for different purposes can be processed separately.

9. Security Incident Protection:

- A "**Security Incident**" is any reasonably suspected or actual loss of or unauthorized processing of personal data.
- Unless prohibited by law, CDATA will notify the data exporter without undue delay of any actual or suspected Security Incident or privacy or security-related complaint relating to the personal data or the services provided by CDATA. Such disclosure shall describe the incident, the suspected effect on the data exporter, its personal data and affected individuals, CDATA's actual and anticipated corrective action to respond to the incident, and (if possible) the outcome of the incident. CDATA shall provide at least daily updates of this information as new information emerges. CDATA shall provide information related to the Security Incident to the data exporter in a timely fashion and as reasonably necessary for the data exporter to maintain compliance with the Data Protection Laws and Regulations**.**
- CDATA also shall take immediate steps to investigate, remedy and mitigate the harm caused by the Security Incident at CDATA's expense. Without limiting the foregoing, CDATA shall permit an independent qualified third party auditor to perform an investigation (including the installation of monitoring or diagnostic software or equipment) to locate the source and scope of the breach and provide the data exporter with any material information related to the data exporter that such independent auditor discovers with respect to the incident.
- Except as may be strictly required by applicable law, CDATA agrees that it will not inform any third party of any such Security Incident without first obtaining the data exporter's prior written consent, other than to inform affected individuals who inquire about the incident that their inquiry has been forwarded to the data exporter's legal department. If, however, such disclosure is, in the opinion of legal counsel, required by applicable law, the parties agree to work with each other regarding the content of such disclosure so as to minimize any potential adverse impact upon the data exporter and on any individuals whose personal data was involved in the Security Incident.

- CDATA shall immediately notify the data exporter of any investigations of its information use or privacy or information security practices or Security Incident by a governmental, regulatory, or self-regulatory organization, to the extent legally permissible.

On behalf of the data exporter:

On behalf of: _____

Name (written out in full): _____

Position: _____

Address: _____

Signature: _____

On behalf of the data importer:

On behalf of CData Software, Inc.:

Name (written out in full): Kathy L. Priest

Position: Chief Legal Officer

Address: 101 Europa Drive, Suite 110

Chapel Hill, North Carolina 27517 USA

Signature: Kathy L. Priest