Laserfiche®

Laserfiche Data Processing Addendum

Effective Date: October 15, 2025

This Data Processing Addendum, including its Annexes and the Standard Contractual Clauses (collectively, the "**DPA**" or the "**Addendum**") sets forth the parties obligations with respect to the Processing of Personal Data in connection with Laserfiche's provision of Laserfiche cloud services subscribed by you ("**Cloud Services**") in accordance with the Laserfiche Cloud Subscription Agreement or other agreement under which Laserfiche provides the Cloud Services to you (the "**Laserfiche Cloud Subscription Agreement**" or "**Agreement**") between the party identified as "you" or "Subscriber" in the Agreement and Laserfiche. The term "Laserfiche" and any other capitalized terms utilized in this DPA, but not defined herein, have their respective meanings as set forth in the Laserfiche Cloud Subscription Agreement.

This DPA is incorporated into and forms part of the terms and conditions of the Agreement and will remain in force for the duration of the Subscription Term of the Cloud Services.

By entering into the Agreement, you enter into this DPA on behalf of yourself and, to the extent required under Applicable Data Protection Law, in the name and on behalf of your Permitted Affiliates. For the purposes of this DPA only, and except where indicated otherwise, the terms "you" and "Subscriber" shall include you, Subscriber and such Permitted Affiliates.

1. Definitions

1.1 "**Applicable Data Protection Law**" means all data protection and privacy laws and regulations applicable to the Personal Data in question, including, where applicable, (i) European Data Protection Law and the Swiss DPA, (ii) PIPEDA and any applicable provincial law declared substantially similar to PIPEDA, and (iii) applicable federal and state privacy laws of the United States, including the CCPA and any other similar laws that are in effect or that become effective on or after the Effective Date of this DPA.

1.2 "**CCPA**" means Title 1.81.5. California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100–1798.199) and its implementing regulations, as amended, superseded or replaced.

1.3 "**Data Privacy Framework**" means (as applicable) the EU-U.S. Data Privacy Framework, the Swiss-U.S. Data Privacy Framework and the UK Extension to the EU-U.S. Data Privacy Framework self-certification programs operated by the U.S. Department of Commerce, and their respective successors.

1.4 "**Data Privacy Framework Principles**" means the Principles and Supplemental Principles contained in the relevant Data Privacy Framework, as amended, superseded or replaced.

1.5 "**Data Subject**" means a data subject, consumer, or identified or identifiable natural person.

1.6 "**European Data Protection Law**" means (i) Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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 or "**EU GDPR**"); (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (iii) Directive

2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) or (iii); (in each case, as may be amended, superseded or replaced from time to time).

1.7 "**Laserfiche Affiliate**" means the subsidiaries of Compulink Management Center, Inc. that may assist in the performance of the Cloud Services in accordance with this DPA.

1.8 "**Permitted Affiliate**" means any Affiliate of Subscriber which: (i) is subject to Applicable Data Protection Law; and (ii) is permitted to use the Cloud Services pursuant to the Agreement, but has not signed its own Agreement with Laserfiche and is not a "Subscriber" as defined under the Agreement.

1.9 "**Personal Data**" means any personal data, personal information or personally identifiable information (as defined under Applicable Data Protection Law) that Laserfiche processes on behalf of Subscriber in connection with the provision of the Cloud Services, as more particularly described in Annex 1 of this DPA.

1.10 "**PIPEDA**" means the Canadian Personal Information Protection and Electronic Documents Act, 2000.

1.11 "**Processing of Personal Data**" has the meaning subscribed to such term under Applicable Data Protection Law as it relates to the processing described in Annex I.

1.12 "**Restricted Transfer**" means: (i) where the EU GDPR applies, a transfer of Personal Data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of Personal Data from Switzerland to any other country which is not determined to provide adequate protection for personal data by the Federal Data Protection and Information Commission or Federal Council (as applicable).

1.13 "**Standard Contractual Clauses**" means: (i) where the EU GDPR or Swiss DPA applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"); and (ii) where the UK GDPR applies, the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the Data Protection Act 2018 ("**UK Addendum**").

1.14 "**Swiss DPA**" means the Swiss Federal Act on Data Protection 1992 (including as amended or superseded).

1.15 "**Subprocessor**" means direct and indirect subcontractors of Laserfiche and Laserfiche Affiliates, which may Process Personal Data in accordance with this DPA, including, without limitation, Laserfiche Solution Providers. For the avoidance of doubt, a Laserfiche employee, independent contractor or consultant is not a Subprocessor.

Where applicable, the terms "**controller**," "**business**," "**processor**," "**service provider**," "**data subject**," "**consumer**," "**process**," "**personal data**," "**personal information**," "**sell**," "**share**," "**business purpose**," "**commercial purpose**," "**supervisory authority**," "**deidentified**," "**aggregate consumer information**," (or any equivalent terms) shall have the meaning ascribed to them under Applicable Data Protection Law.

2. Scope and Applicability of this DPA

2.1 This DPA applies where and only to the extent that Laserfiche processes Personal Data that is subject to Applicable Data Protection Law which impose an obligation directly upon Laserfiche as a Processor or a Service Provider (as applicable) by virtue of the specific Processing of Personal Data in the course of providing the Cloud Services in the specific Laserfiche Cloud Data Center Region (as defined below) that you have subscribed to. For the avoidance of doubt, Laserfiche is not responsible for determining the requirements of laws or regulations applicable to your business, or whether the Cloud Services and related processing by Laserfiche meet the requirements of any laws or regulations that may apply to you or to the Processing of Personal Data.

2.2 As between the parties, Subscriber is responsible for the lawfulness of the Processing of Personal Data under this DPA. Subscriber will not use the Cloud Services or request Processing by Laserfiche in a manner that would violate Applicable Data Protection Law.

3. Role and Obligations of the Parties

3.1 You acknowledge and agree that with regard to the Processing of Personal Data under this DPA, Laserfiche is the Processor or the Service Provider (as applicable) and you are the Controller or Business (as applicable) of the Personal Data or you have obtained the authorization of relevant Controller(s) or Business(es) to agree to the Processing of Personal Data by Laserfiche as set forth in this DPA. You are responsible for the lawfulness of the instructions you provide to Laserfiche regarding the Processing of Personal Data and compliance with your obligations as a Controller or a Business (as applicable) under Applicable Data Protection Law and in accordance with the features and functionality of the Cloud Services and the Documentation. You will not use the Cloud Services in conjunction with Personal Data to the extent that doing so would violate Applicable Data Protection Law.

3.2 You warrant that you have all the necessary rights to provide the Personal Data to Laserfiche for the Processing to be performed in relation to the Cloud Services. To the extent required by Applicable Data Protection Law, you are responsible for ensuring that any necessary notices to Data Subjects or Consumers (as applicable) are provided and any necessary Data Subject or Consumer (as applicable) consents to this Processing are obtained, and for ensuring that a record of such consents is maintained. You have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which you acquired Personal Data.

3.3 During the Subscription Term, you appoint Laserfiche as a Processor or a Service Provider (as applicable) with respect to the Personal Data you provide to Laserfiche under the Agreement and consent to the use of Subprocessors by Laserfiche in order to allow Laserfiche to fulfill its contractual obligations under the Agreement, in accordance with Section 5 of this DPA. Laserfiche is responsible for compliance with its obligations under this DPA and for compliance with its obligations as a Processor or a Service Provider (as applicable) under Applicable Data Protection Law.

3.4 As a Processor or a Service Provider (as applicable), Laserfiche and any Subprocessors, will Process Personal Data solely for the purpose of (i) providing the Cloud Services in accordance with the Agreement and this DPA, as further described in **Annex I** of this DPA; (ii) complying with your documented written lawful instructions, or (iii) complying with Laserfiche's regulatory or other legal obligations, all in accordance with the terms of this DPA.

3.5 To the extent that any Personal Data is "personal information" subject to the CCPA, Laserfiche shall not further: (i) sell or share the Personal Data, (ii) collect, retain, use, or disclose the Personal Data for any purpose, including a commercial purpose, other than for the specific business purpose of providing the Cloud Services specified in the Agreement or as permitted or required under Applicable Data Protection Law, (iii) retain, use, or disclose the Personal Data outside of the parties' direct business relationship; or (iv) combine Personal Data with personal information that Laserfiche receives from or on behalf of another person, or collects from its own interactions with any other sources, provided that Laserfiche may combine personal information to perform any business purpose as otherwise permitted by the CCPA. Laserfiche certifies that it understands these restrictions and will comply with them. Laserfiche further agrees that: (i) Laserfiche shall comply with applicable obligations under CCPA and provide the same level of privacy protection as is required by CCPA; (ii) you have the right to take reasonable and appropriate steps to help ensure that Laserfiche uses Personal Data in a manner consistent with your obligations under CCPA; (iii) Laserfiche shall notify you if it makes a determination that it can no longer meet its obligations under CCPA; and (iv) you have the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data.

3.6 Notwithstanding anything to the contrary in this DPA or the Agreement, to the extent any Personal Data becomes "deidentified" or in the "aggregate" as those terms are defined under Applicable Data Protection Law ("**Deidentified Data**"), Laserfiche may use such Deidentified Data for any commercial purpose in accordance with Applicable Data Protection Law, including but not limited to developing analytics, improving the Cloud Services, and other products and offerings, conducting research and development, and similar legitimate and internal business purposes. Laserfiche may retain, use and disclose Deindentified Data for such purpose, without restriction. ~~Laserfiche may also integrate third-party large language models ("Third-Party LLM") into the Cloud Services for the purpose of enhancing functionality, automating tasks, or improving user experience, and may use for such purpose Deidentified Data, such that neither a Subscriber nor any individual can be identified, unless otherwise agreed in writing by the parties. Subscriber agrees that Laserfiche may (i) make Deidentified Data available to third parties including its other customers service providers, contractors and affiliates, in compliance with applicable law, and (ii) use Deidentified Data to produce results for Subscriber, to maintain, test, evaluate, develop and improve the Cloud Services, for product performance analysis and for any other internal business purposes of Laserfiche, and to the extent and in the manner otherwise not prohibited under applicable law. In such case, Laserfiche shall ensure that any Third-Party LLM provider engaged under this provision is contractually obligated to comply with data privacy, security, and confidentiality standards no less protective than those set forth in this DPA.~~

3.7 You warrant that Laserfiche's Processing of Personal Data in accordance with your instructions will not violate or cause Laserfiche to violate Data Protection Law or third-party terms. If Laserfiche reasonably believes that your documented written instructions violate Applicable Data Protection Law, Laserfiche may suspend the performance until you have modified or confirmed the lawfulness of such documented written instructions. If Laserfiche notifies you that either the

documented written instructions or the expense for such written instructions are not feasible you may terminate the Cloud Services by providing Laserfiche with a written notice within one month after notification. Laserfiche will refund a prorated portion of any prepaid charges for the period after such termination date. The parties agree that this DPA and the Agreement set out your complete and final instructions to Laserfiche in relation to the Processing of Personal Data and Processing outside the scope of these instructions (if any) shall require prior written agreement between Subscriber and Laserfiche.

4. Cooperation

4.1 **Correspondence.** To the extent permitted by law, Laserfiche will inform you of (i) requests from Data Subjects or Consumers (as applicable) exercising their rights under Applicable Data Protection Law (including requests to access, restrict, receive and transmit, delete or erase, rectify, or object to Processing of specific Personal Data and right to opt-out from the sale of their personal information as applicable) and (ii) any other correspondence, enquiry or complaint received from a Data Subject, Consumer, regulator or other third party addressed to Laserfiche regarding Personal Data processed by Laserfiche in connection with the Cloud Services (collectively "**Correspondence**") but only where Laserfiche is made aware that such Correspondence relates to you as a Controller. You will be responsible for responding to such Correspondence.

4.2 Unless required by applicable law, Laserfiche will not respond directly to any Correspondence and will reasonably assist you in responding to such Correspondence to the extent that you are unable to independently access the relevant Personal Data within the Services Environment. In such case, you may submit a “service request” by emailing privacy@laserfiche.com, and provide detailed written instructions to Laserfiche (including the Personal Data necessary to identify the Data Subject or the Consumer) on how to reasonably assist with such Correspondence in relation to Personal Data held in your Services Environment. To the extent legally permitted, you will be responsible for any costs arising from Laserfiche’s provision of such assistance.

4.3 If a Data Subject, a consumer or a regulator brings a claim directly against Laserfiche for a violation of Data Subject or consumer rights (as applicable) in connection with Laserfiche's Processing of Personal Data in accordance with your documented instructions, you will indemnify Laserfiche for any cost, charge, damages, expenses or loss arising from such a claim.

4.4 **Data Protection Impact Assessments.** To the extent required under Applicable Data Protection Law, Laserfiche shall provide reasonably requested information regarding Laserfiche's Processing of Personal Data under the Agreement to enable you to carry out data protection impact assessments (or risk assessments) or prior consultations with supervisory authorities as required by Applicable Data Protection Law.

4.5 **General cooperation**. Each party will reasonably cooperate with the other in any activities contemplated by this DPA and to enable each party to comply with its respective obligations under Applicable Data Protection Law.

5. Laserfiche Affiliates and Subprocessors

5.1 Subject to terms and restrictions set forth in this DPA, you agree and provide a general prior authorization to Laserfiche to engage Subprocessors (including Laserfiche Affiliates) to Process

Personal Data on behalf of Laserfiche and assist in the performance of the Cloud Services, including those Subprocessors listed here (the "**Subprocessor List")**.

6. Sub-processors.

6.1 **Sub-processor Obligations.** Laserfiche will enter into a written agreement with each Subprocessor imposing data protection obligations no less protective of Personal Data as this DPA. Laserfiche remains responsible at all times for and the acts or omissions of its Subprocessors that cause Laserfiche to breach any of its obligations under this DPA.

6.2 **Objection to Sub-processors**. Subscriber may subscribe to notifications of new Subprocessors at the subscriber notification portal, and if Subscriber subscribes, Laserfiche shall notify Subscriber if it makes any changes to the Subprocessor List at least 10 days before such change. Within 5 calendar days of Laserfiche providing such notice to you, you may object to the intended involvement of a Subprocessor in the performance of the Cloud Services, providing, in writing, objective justifiable grounds related to the ability of such Subprocessor or Laserfiche Affiliate to adequately protect Personal Data in accordance with this DPA or European Data Protection Law. You should submit this writing to privacy@laserfiche.com. In the event your objection is justified, you and Laserfiche will work together in good faith to find a mutually acceptable resolution to address your objections, including without limitation reviewing additional documentation supporting the Subprocessors' compliance with this DPA or Applicable Data Protection Law, or delivering the Cloud Services without the involvement of such Subprocessor. To the extent you and Laserfiche do not reach a mutually acceptable resolution within a reasonable timeframe, Laserfiche will, at its sole discretion, either (i) not appoint the Subprocessor; or (ii) permit Subscriber to suspend or terminate the affected portion of the Cloud Services in accordance with the termination provisions in the Agreement without liability to either party (but without prejudice to any fees incurred by Subscriber prior to suspension or termination). In such case, Laserfiche shall refund Subscriber for any prepaid unused portion of the affected portion of the Cloud Services.

7. Security Measures; Confidentiality

7.1 Each party agrees that it has implemented and will maintain appropriate and reasonable technical and organizational measures to ensure a level of security of the Processing of Personal Data appropriate to the risk. These measures will take into account the nature, scope and purposes of Processing as specified in this DPA, as appropriate, and are intended to protect Personal Data against the risks inherent to the Processing of Personal Data in the performance of the Cloud Services, in particular risks from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

7.2 Laserfiche has specifically implemented system access, data access, transmission and encryption, input, data backup, and security oversight, enforcement and other security controls and measures specified in the Documentation ("**Security Measures**"). The Security Measures shall, at a minimum, include the measures identified in Annex II of this DPA. You are advised to carefully review the applicable Documentation to understand which specific Security Measures and practices apply to the particular Cloud Services ordered by you, and to ensure that these Security Measures and practices are appropriate for the Processing of Personal Data pursuant to this DPA. You hereby instruct Laserfiche to Process Personal Data in accordance with the Documentation.

7.3 You acknowledge that the Security Measures are subject to technical progress and development and that Laserfiche may update or modify its Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Cloud Service you have purchased.

7.4 All parties hereto will ensure all such persons or parties, within their respective controls, that may have access to Personal Data subject to this DPA have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are subject to an appropriate statutory obligation of confidentiality.

8. Audits

8.1 Upon written request, Laserfiche may demonstrate the measures it has taken pursuant to Section 8 in relation to the Personal Data applicable to this DPA. Laserfiche will reasonably contribute to such audits by providing you or your Supervisory Authority with the information and assistance reasonably necessary to conduct the audit. You acknowledge and agree that you shall exercise your audit rights under this DPA (including this Section 8) by instructing Laserfiche to comply with the audit measures described in Section 8.2 below.

8.2 You acknowledge that Laserfiche is periodically audited against recognized data protection and security standards by independent third-party auditors and/or internal auditors respectively. Upon written request, Laserfiche shall supply (on a confidential basis) a summary copy of its most current audit report(s), which is a SOC 2 Type 2 attestation report under the AICPA Statement on Standards for Attestation Engagements (SSAE) 18 standard, ("**Report**") to you, so that you can verify Laserfiche's compliance with the audit standards against which it has been assessed and this DPA. If the Report does not, in your reasonable judgement, provide sufficient information to confirm Laserfiche's compliance with this DPA, then Laserfiche shall also provide written responses (on a confidential basis) to all reasonable requests for information made by you, including responses to information security and audit questionnaires that are necessary to confirm Laserfiche's compliance with this DPA, provided that you shall not exercise this right more than once per calendar year.

8.3 While it is the parties' intention to ordinarily rely on the Report described above to verify Laserfiche's compliance with this DPA, where a Supervisory Authority requires it, you may provide Laserfiche with thirty (30) days' prior written notice requesting that a third party conduct an audit of Laserfiche's facilities, equipment, documents and electronic data relating to the Processing of Personal Data under the Agreement ("**Audit**"), provided that: (a) the Audit shall be conducted at the Subscriber's expense; (b) the parties shall mutually agree upon the third party chosen to conduct the Audit and the scope, timing, duration and confidentiality basis of the Audit; and (c) the Audit shall not unreasonably impact Laserfiche's regular operations.

8.4 You agree to promptly notify Laserfiche with any information in regard to non-compliance during the course of an Audit and will provide Laserfiche any audit reports generated in connection with any Audit, unless prohibited by Applicable Data Protection Law or otherwise instructed by a Supervisory Authority. You may use the audit reports only for the purposes of meeting your regulatory audit requirements and/or confirming compliance with the requirements of this DPA. The audit reports, information and any artifacts to support the audit provided by Laserfiche are Confidential Information of the parties under the terms of the Agreement.

9. Incident Notification

9.1 To the extent Laserfiche becomes aware and determines that a security incident qualifies as a breach of security leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed on Laserfiche systems or the Services Environment that compromises the security, confidentiality or integrity of such Personal Data ("**Incident**"), Laserfiche will inform you of such Incident without undue delay or otherwise in accordance with Applicable Data Protection Law and provide such information as you may reasonably require as required by Applicable Data Protection Law. However, Laserfiche may not have the ability to evaluate or respond to security incidents where your Users are the source of unauthorized access or disclosure of Personal Data and/or the source is a Solution Provider or another agent whom your Users have granted access to Laserfiche systems or the Services Environment.

9.2 In order to address an Incident, Laserfiche defines escalation paths and response teams involving internal functions such as Information Security and the legal department. The goal of Laserfiche's Incident response will be to restore the confidentiality, integrity, and availability of the Services Environment and the Personal Data that may be contained therein, and to establish root causes and remediation steps. Depending on the nature and scope of the Incident and to the extent required by Applicable Data Protection Law, Laserfiche may also involve and work with you and outside law enforcement to respond to the Incident.

10. Return and Deletion of Personal Data upon Termination of Cloud Services. Upon termination of the Cloud Services or upon expiry of the retrieval period following termination of the Cloud Services (if available), Laserfiche will as soon as reasonably practicable delete all Personal Data (including copies) from the Services Environment by rendering such Personal Data unrecoverable, except as may be required by law and the Agreement. Laserfiche may retain Personal Data where necessary for you to comply with applicable law or legal obligations or protect its rights or those of a third party.

11. International Transfers

11.1 **Data Center Region**. Unless separately agreed to by the parties in writing, Laserfiche will host your Subscription to Laserfiche Cloud from AWS data centers located in the region(s) as specified here (such regions, the "**Laserfiche Cloud Data Center Regions**", and such list, the "**Laserfiche Cloud Data Center Regions List**". Laserfiche may offer hosting from data centers of a different hosting provider or in new regions in the future by amending the Laserfiche Cloud Data Center Regions List. Subscriber is solely responsible for the regions from which its Users upload or access Personal Data and for any transfer or sharing of Personal Data by Subscriber or its Users.

11.2 **Cross-Border Data Transfers.** You acknowledge and agree that Laserfiche may transfer and Process Personal Data to and in the United States and other countries in which Laserfiche, its Affiliates or Subprocessors maintain data processing operations. You and Laserfiche shall at all times ensure such transfers are made in compliance with the requirements of Applicable Data Protection Law.

11.3 **Data Privacy Framework.**

11.3.1 Laserfiche is self-certified under the Privacy Shield Framework, now superseded by the Data Privacy Framework, as administered by the U.S. Department of Commerce, in order to implement appropriate safeguards for transfers of Personal Data to the United States pursuant to Article 46 of the GDPR. To the extent the Data Privacy Framework can be used to lawfully transfer Personal Data to the United States, and for as long as Laserfiche is self-certified to the Data Privacy Framework, Laserfiche will adhere to the Data Privacy Framework Principles, including by: (a) processing such Personal Data only for the limited and specified purposes set out in the Agreement, including this DPA; (b) providing at least the same level of privacy protection to the Personal Data as is required by the Data Privacy Framework Principles; (c) promptly notifying you if it makes a determination that it can no longer meet its obligation under (b) above, and in such event, promptly taking reasonable and appropriate steps to stop and remediate any processing until such time as the processing meets the level of protection as is required by the Data Privacy Framework Principles; and (d) at your sole election, ceasing the processing of the Personal Data if, in your reasonable discretion, Laserfiche is not providing the same level of protection to the Personal Data as is required by the Data Privacy Framework Principles. Laserfiche intends to remain self-certified under the Data Privacy Framework as long as the Data Privacy Framework is recognized as a valid transfer mechanism under Applicable Data Protection Law. Details about Laserfiche's self-certification to the Data Privacy Framework are available at: https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt00000008RnHAAU&status=Active

11.3.2 You acknowledge that Laserfiche may disclose this DPA and any relevant privacy provisions in the Agreement to the US Department of Commerce, the Federal Trade Commission, a relevant European supervisory authority or other public or regulatory authority, court or tribunal, upon their request.

11.3.3 If Laserfiche is unable to comply with this Clause 11.3, Clause 11.4 shall apply.

11.4 **Restricted transfers.** The parties agree that when the transfer of Personal Data from Subscriber to Laserfiche is a Restricted Transfer it shall be subject to the appropriate Standard Contractual Clauses as follows:

11.4.1 in relation to Personal Data that is protected by the EU GDPR, the EU Standard Contractual Clauses will apply completed as follows:

a) Module Two will apply;

b) in Clause 7, the optional docking clause will apply;

c) in Clause 9, Option 2 will apply, and the time period for prior notice of subprocessor changes shall be as set out in Section 6 of this DPA;

d) in Clause 11, the optional language will not apply;

e) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the Republic of Ireland law;

f) in Clause 18(b), disputes shall be resolved before the courts of the Republic of Ireland;

g) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex I to this DPA; and

h) Annex II of the EU SCCs shall be deemed completed with the information set out in Annex II to this DPA.

11.4.2 in relation to Personal Data that is protected by the UK GDPR, the UK Addendum will apply completed as follows:

a) The EU SCCs, completed as set out above in Section 11.3.1 of this DPA shall also apply to transfers of such Personal Data, subject to sub-section (b) below; and

b) Tables 1 to 3 of the UK Addendum shall be deemed completed with relevant information from the EU SCCs, completed as set out above, and the options "neither party" shall be deemed checked in Table 4. The start date of the UK Addendum (as set out in Table 1) shall be the date of this DPA.

11.4.3 In relation to Personal Data that is protected by the Swiss DPA, the EU SCCs will apply as set out in Section 11.4.1 amended as follows:

a) references to 'Regulation (EU) 2016/679' in the EU SCCs will be deemed to refer to the Swiss DPA;

b) references to specific articles of 'Regulation (EU) 2016/679' will be deemed replaced with the equivalent article or section of the Swiss DPA;

c) references to 'EU', 'Union' and 'Member State' will be deemed replaced with 'Switzerland';

d) references to the 'competent supervisory authority' and 'competent courts' are replaced with the 'Swiss Federal Data Protection Information Commissioner' and 'applicable courts of Switzerland' (as applicable);

e) in Clause 17, the EU SCCs will be governed by the laws of Switzerland; and

f) in Clause 18(b), disputes shall be resolved before the competent courts of Switzerland.

11.5 **Onward transfers.** Laserfiche shall not participate in (nor permit any Subprocessor to participate in) any other Restricted Transfers (whether as an exporter or an importer of the Personal Data) unless the Restricted Transfer is made in full compliance with Applicable Data Protection Law.

11.6 **Alternative Transfer Arrangements**. To the extent Laserfiche adopts an alternative data export mechanism (for Restricted Transfer not described in this DPA ("**Alternative Transfer**

Mechanism"), the Alternative Transfer Mechanism shall apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with European Data Protection Law and extends to the territories to which Personal Data is transferred) and you agree to execute such other and further documents and take such other and further actions as may be reasonably necessary to give legal effect such Alternative Transfer Mechanism. In addition, if and to the extent that a court of competent jurisdiction or a Supervisory Authority with binding authority orders or determines (for whatever reason) that the measures described in this DPA cannot be relied on to lawfully transfer such Personal Data, you acknowledge and agree that Laserfiche may implement any additional measures or safeguards that may be reasonably required to enable the lawful transfer of such Personal Data.

12. Limitation of Liability. Each party's liability (and each of its Affiliate's liability) taken together in the aggregate, arising out of or related to this DPA (including the Standard Contractual Clauses) whether in contract, tort, or under any other theory of liability, is subject to the limitation of liability provisions of the Agreement. Any reference in such limitation of liability provisions to the liability of a party means the aggregate liability of that party and all of its Affiliates (including Subscriber Affiliates) under the Agreement and this DPA (including the Standard Contractual Clauses), taken together.

13. Miscellaneous

13.1 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict or inconsistency between this DPA and the Agreement, the provisions of the following documents (in order of precedence) shall prevail: (a) Standard Contractual Clauses (where applicable); then (b) this DPA; and then (c) the main body of the Agreement.

13.2 Notwithstanding anything to the contrary in the Agreement (including this DPA), Laserfiche shall have a right to collect, use and disclose data relating to the use, support and/or operation of the Cloud Services ("**Service Data**") in connection with its legitimate interests, such as billing, account management, technical support, and product development. To the extent any such Service Data is considered personal data under Applicable Data Protection Law, Laserfiche shall be responsible for and shall Process such data in accordance with the Laserfiche Privacy Notice located at https://www.laserfiche.com/legal/privacy/ (as updated from time to time) and Applicable Data Protection Law. Subscriber shall make a copy of Laserfiche's Privacy Notice available to any data subjects whose Personal Data is provided by the Subscriber to Laserfiche in connection with the Cloud Services. For the avoidance of doubt and except for this Section 13.2, the terms of this DPA shall not apply to Service Data.

13.3 Subscriber acknowledges that Laserfiche may disclose this DPA (including the Standard Contractual Clauses) and any relevant privacy provisions in the Agreement to the US Department of Commerce, the Federal Trade Commission, a supervisory authority, or any other Canadian, US or European judicial or regulatory body upon their request.

13.4 Notwithstanding anything else to the contrary in the Agreement and without prejudice to Section 3 (Roles and Obligations of the Parties), Laserfiche may periodically make modification to this DPA as may be required to comply with Applicable Data Protection Law.

13.5 This DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by Applicable Data Protection Law.

Annex I

Data Processing Description

This Annex I forms part of the DPA and describes the processing that the processor will perform on behalf of the controller.

A. LIST OF PARTIES

Controller(s) / Data exporter(s): *Identity and contact details of the controller(s) /data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*

1.	Name:	The party identified as the "Subscriber" in the Agreement and this DPA
	Address:	The address provided in the Agreement
	Contact person's name, position and contact details:	As set out in the Agreement
	Activities relevant to the data transferred under these Clauses:	See B. below
	Signature and date:	Executed as per Agreement
	Role (controller/processor):	Controller

Processor(s) / Data importer(s):

1.	Name:	The party identified as "Laserfiche" in the Agreement and this DPA
	Address:	As set out in the Agreement
	Contact person's name, position and contact details:	Wylie Strout, Chief Legal Officer and DPO
	Activities relevant to the data transferred under these Clauses:	See B. below
	Signature and date:	Executed as per Agreement
	Role (controller/processor):	Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:	Subscriber may submit Personal Data to the Cloud Services, the extent of which is determined and controlled by Subscriber in its sole discretion, and which may include, but is not limited to, Personal Data relating to the following categories of data subjects:

	• Employees, contractors or job applicants of Subscriber; • Individuals authorized to use the Cloud Services by Subscriber; • Current and potential customers, business partners or vendors of Subscriber; and • Any other data subjects whose data may be processed from time to time pursuant to the Agreement and this DPA.
Categories of personal data transferred:	The categories of Personal Data processed by Laserfiche are determined and controlled by Subscriber in its sole discretion and may include, but are not limited to the following categories of Personal Data: • Contact data (name, title, email address, telephone number, mailing address); • Account credentials; and • IP address.
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:	Subscriber, or third parties acting on their behalf, or through their subscription may submit Personal Data that contains special categories of data to Laserfiche in connection with the Cloud Service, the nature and extent of which is exclusively determined and controlled by Subscriber. See Annex II for the restrictions and safeguards applied.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous
Nature of the processing:	Providing the Cloud Services to Subscriber. Personal Data transferred will be processed in accordance with the Agreement and may be subject to the following processing activities: (A) storage and other processing necessary to provide, maintain, and improve the Cloud Services, as applicable, provided to Subscriber; and/or (B) disclosures in accordance with the Agreement and/or as compelled by applicable laws.
Purpose(s) of the data transfer and further processing:	Processing (a) to perform any steps necessary for the performance of the Agreement; (b) to provide

	the Cloud Services in accordance with the Agreement; (c) initiated by users in their use of the Cloud Services; (d) to comply with other reasonable instructions provided by Subscriber that are consistent with the terms of the Agreement and this DPA; and (e) to comply with any legal obligations under applicable law, including Applicable Data Protection Law.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	The duration of the Agreement plus the period from the expiry of the Agreement until deletion of the Personal Data by Customer in accordance with the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 SCCs)	The competent supervisory authority, in accordance with Clause 13 of the EU SCCs, is either (i) the supervisory authority applicable to the data exporter in its EEA country of establishment or, (ii) where the data exporter is not established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed pursuant to Article 27(1) of the GDPR, or (iii) where the data exporter is not obliged to appoint a representative, the supervisory authority applicable to the EEA country where the data subjects relevant to the transfer are located. With respect to personal data regulated by the UK GDPR, the competent supervisory authority is the Information Commissioners Office. With respect to the processing of Personal Data to which the Swiss DPA applies, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner. With respect to the processing of Personal Data to which PIPEDA applies, the competent supervisory authority is the Office of the Privacy Commissioner of Canada.

Annex II

Technical and Organizational Security Measures

Description of the technical and organizational measures implemented by the processor(s) / data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Measure	Description
Measures of pseudonymisation and encryption of personal data	• Data that resides in Amazon Web Services (AWS) is encrypted at rest using AES-256 as stated in AWS' documentation and whitepapers. • Encryption keys are secured against unauthorized access during generation, storage, use and destruction. • Customer interfaces to Laserfiche Cloud is encrypted using TLS encryption. • Backup databases are stored in encrypted EBS snapshots.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	• Access controls are implemented to enforce confidentiality, integrity and availability. • Access to in-scope systems requires a user ID plus SSH Keys and/or password authentication. Where passwords are used, password parameters enforce minimum length, password age and complexity requirements. • Privileged access to Laserfiche Cloud systems is restricted to appropriate personnel. • Access to Laserfiche Cloud production systems is logically and physically segregated from the Laserfiche network. • Antivirus software is used to protect Laserfiche workstations used to access the Laserfiche Cloud system from malicious code or viruses. • Laserfiche employees are prohibited from accessing customer data without prior customer request and authorization.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	• Customer databases are backed up at regular intervals throughout the day by an automated process. • Backup restorations are tested ona quarterly basis. • Backups are configured to be retained for at least seven days. Laserfiche generally does not support restoring a customer repository or specific data from backups, as Laserfiche Cloud backups are solely intended for recovering the multitenant SaaS platform from a systemwide outage event. The Laserfiche data backup system is not meant as a backup solution for individual accounts with restore points.

	Customers are responsible for their own data backups for content stored in the Laserfiche Cloud repository. • Services requiring high availability are deployed across multiple availability zones within an AWS region. • Services that are not deployed across multiple availability zones are monitored and will trigger alerts to manually restore services in alternate availability zones.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	• A global independent accounting and advisory firm performs annual testing of Laserfiche Cloud controls via inquiry, observation, and inspection, and provides an attestation report under the AICPA Statement on Standards for Attestation Engagements (SSAE) 18 standard. • Laserfiche uses a third-party security firm to conduct annual external penetration testing of the Laserfiche Cloud systems. • Laserfiche performs periodic network vulnerability scans and addresses critical issues using a risk-based approach. • Security incident response plans are tested annually, and plans are updated, if necessary. • Laserfiche assesses the effectiveness of its security awareness program through quarterly employee simulated phishing campaigns.
Measures for user identification and authorisation	• Access to Laserfiche Cloud operational and production environments is controlled by user IDs, passwords, role-based access and least privilege principle. Multi-factor authentication (MFA) is made available to customers to further enhance security and restrict access to their data. • Identity and access management processes for Laserfiche user account provisioning, de-provisioning and changes are enforced.
Measures for the protection of data during transmission	• Customer interfaces to Laserfiche Cloud is encrypted using TLS encryption.
Measures for the protection of data during storage	• Access controls restrict access to customer data. • Customer databases and backup databases in Laserfiche Cloud are encrypted. • Customer data is logically segregated on its own database and customer files are segregated on its own virtual disk. • Endpoint security software is used to protect workstations used to access the Laserfiche Cloud system from malicious code or viruses.
Measures for ensuring physical security of locations at which	• Laserfiche utilizes AWS for its production environments. The physical and environmental controls related to the facilities housing the production environments are managed by the subservice organization.

personal data are processed	• The subservice organization SOC reports are reviewed on an annual basis in accordance with Laserfiche's security standards.
Measures for ensuring events logging	• An IDS is deployed to monitor for potential security incidents that are reviewed, escalated and tracked through resolution by Laserfiche.
Measures for ensuring system configuration, including default configuration	• Laserfiche has a change management policy to manage configuration changes. • Any changes made to the Laserfiche Cloud production environment are logged in the ticketing system and are reviewed and approved by authorized individuals prior to deployment.
Measures for internal IT and IT security governance and management	• Laserfiche has established an Information Security Management System (ISMS) in accordance with the ISO 27001. • Laserfiche has a documented Information Security Policy, which is approved by the Laserfiche Board of Directors. • The Laserfiche Board of Directors and management provide oversight over the Information Security program through periodic updates on risk assessments, third-party attack and penetration studies, and compliance with information security policies. • The Laserfiche CEO is accountable for the security, availability and confidentiality of information assets. The CTO has overall responsibilities over the software development life cycle and security for Laserfiche products. The CIO provides IT and security governance, along with the Information Security Officer. • The Laserfiche Board of Directors has authorized the CIO and Information Security Officer to enforce Laserfiche Cloud and information security policies. • A formal security awareness program is in place to make all employees aware of the company's security policy, standards, and obligations of users. • Employees are required to read and sign company policies, confidentiality agreements, and code of conduct upon hire.
Measures for certification/assurance of processes and products	• A global CPA firm performs annual testing of Laserfiche Cloud controls via inquiry, observation, and inspection, and provides an attestation report under the AICPA Statement on Standards for Attestation Engagements (SSAE) 18 standard. • Laserfiche has aligned its information security program to ISO 27001. • Laserfiche has a Laserfiche Gold, Platinum and Administration certification training programs that are available to a Subscriber, Solution Providers and other third parties. `

Measures for ensuring data minimisation	• Laserfiche policies limit data collection to the purposes of processing (or the data that the Subscriber chooses to provide). • Security measures are implemented to provide Laserfiche employees with only the minimum amount of access necessary to perform required functions.
Measures for ensuring data quality	• Laserfiche has a process that allows individuals to exercise their privacy rights, including a right to amend and update information, as described in Laserfiche's Privacy Notice available at https://www.laserfiche.com/legal/privacy/. • Laserfiche has a quality assurance team that is responsible for data quality for Laserfiche products.
Measures for ensuring limited data retention	• Database backups are retained to support Laserfiche Cloud system recovery operations in the event of a disaster or other contingency. Laserfiche does not make specific Subscriber commitments for data retention. • Data for provisional customers and subscription customers is removed after the end of the trial period and upon written notice by the customer, respectively.
Measures for ensuring accountability	• Security responsibilities are included in Laserfiche job descriptions for administrators. • Laserfiche Information Security Policy, Laserfiche AI Governance and Usage Policy and Employee Handbook contain employee sanctions on noncompliance with policies. • Laserfiche policies require violations of information security policies to be reported to People Operations and/or Information Security. • Laserfiche has agreements with its Solution Providers that includes requirements to comply with all applicable laws, perform in an ethical manner, and adhere to a data processing agreement.
Measures for allowing data portability and ensuring erasure	• Laserfiche has a process that allows individuals to exercise their privacy rights, including a right of erasure or a right to data portability, as described in Laserfiche's Privacy Notice available at https://www.laserfiche.com/legal/privacy/. • Subscribers have ownership and control over their data in Laserfiche Cloud.