

Silktide Data Processing Agreement

The data processing terms between you as controller and Silktide as processor, forming part of your agreement.

In effect: October 6, 2026 – present

<https://silktide.com/legal/data-processing-agreement/>

This Data Processing Agreement (**DPA**) is entered into between the Customer (the **Controller**) and the Silktide Entity that contracts with the Customer under the Agreement, identified as described in clause 25 of the Silktide Customer Terms (the **Processor**), and forms part of and is governed by the Agreement. It applies to the extent that the Processor processes Personal Data on behalf of the Controller in providing the Services. The jurisdiction-specific provisions in Exhibit D apply where the relevant law applies to the processing.

By entering into the Agreement, the Controller and the Processor are each deemed to have entered into this DPA, including the Standard Contractual Clauses and the UK Addendum incorporated by reference, without any need for a separate signature.

In respect of the processing of Personal Data, this DPA prevails over the Silktide Customer Terms, and the applicable SCCs and UK Addendum prevail over this DPA, in each case to the extent of any conflict. In all other respects the order of precedence in clause 1.2 of the Silktide Customer Terms applies.

1. Definitions

1.1 Any capitalized term not defined in this DPA has the meaning given to it in the Agreement. In this DPA:

Term	Meaning
Affiliate	any entity that directly or indirectly controls, is controlled by, or is under common control of a party. “Control”, for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of a party.
Agreement	the agreement between the Controller and the Processor for the provision of the Services, comprising the Silktide Customer Terms (including its Schedules), the Order and the other documents incorporated into it.

Australian Privacy Law	the Privacy Act 1988 (Cth), including the Australian Privacy Principles and Part IIIC (Notification of eligible data breaches), and any applicable State or Territory privacy legislation.
CCPA	the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, together with its implementing regulations, each as amended from time to time.
Controller	the Customer, including as applicable in its capacity as a “business” under the CCPA, a “controller” under US State Privacy Laws and an “APP entity” under Australian Privacy Law.
Customer Sites	has the meaning given in the Silktide Customer Terms.
Data Protection Law	all laws and regulations applicable to the processing of Personal Data under the Agreement, as amended, replaced or updated from time to time, including where applicable: (i) the EU GDPR and the laws of the member states of the European Union and the European Economic Area implementing or supplementing it, including the Danish Data Protection Act (databeskyttelsesloven); (ii) the UK GDPR, the UK Data Protection Act 2018 and the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020; (iii) the FADP; (iv) Australian Privacy Law; (v) the Privacy Act 2020 (New Zealand); (vi) the Personal Information Protection and Electronic Documents Act (Canada) and substantially similar provincial laws, including the Quebec Act respecting the protection of personal information in the private sector; (vii) the CCPA and US State Privacy Laws; and (viii) the Privacy and Electronic Communications Directive (2002/58/EC) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426).
Data Subject	an identified or identifiable natural person to whom Personal Data relates, including a “consumer” as defined in the CCPA or US State Privacy Laws.
DPA	this data processing agreement together with Exhibits A, B, C and D.
EEA	the European Economic Area.

EU GDPR	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).
FADP	the Swiss Federal Act on Data Protection of 25 September 2020 and its implementing ordinances, as amended from time to time.
Personal Data	any information relating to a Data Subject that is processed by the Processor on behalf of the Controller in providing the Services, and includes “personal information” as defined in Australian Privacy Law, the CCPA, US State Privacy Laws and other Data Protection Law.
Personal Data Breach	any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed by the Processor or its Sub-processors, including any “eligible data breach” under Australian Privacy Law and any “breach of the security of the system” or equivalent event under the CCPA or US State Privacy Laws.
Processor	the Silktide Entity, including as applicable in its capacity as a “service provider” or “contractor” under the CCPA and a “processor” under US State Privacy Laws.
Restricted Transfer	(i) where the EU GDPR applies, a transfer of Personal Data via the Services from the EEA, either directly or via onward transfer, to any country or recipient outside the EEA not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of Personal Data via the Services from the United Kingdom, either directly or via onward transfer, to any country or recipient outside the United Kingdom not based on adequacy regulations pursuant to Section 17A of the UK Data Protection Act 2018; and (iii) where the FADP applies, a transfer of Personal Data via the Services from Switzerland, either directly or via onward transfer, to any country or recipient outside Switzerland or the EEA not recognized by the Swiss Federal Council as providing an adequate level of protection.

SCCs	(i) where the EU GDPR applies, the standard contractual clauses annexed to European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries (the EU SCCs); (ii) where the UK GDPR applies, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A of the Data Protection Act 2018, as set out in Exhibit C (the UK Addendum); and (iii) where the FADP applies, the EU SCCs as adjusted in accordance with clause 7.3 (the Swiss SCCs).
Services	all services, software applications and solutions provided to the Controller by the Processor under and as described in the Agreement.
Silktide Entity	the member of the Silktide Group that contracts with the Customer under the Agreement, being the entity named in the Order Form, as described in clause 25 of the Silktide Customer Terms.
Sub-processor	any third party (including Processor Affiliates) engaged directly or indirectly by the Processor to process Personal Data under this DPA in the provision of the Services to the Controller. A Sub-processor is either a Core Sub-processor or an Optional Sub-processor , as described in clause 6.2.
Sub-processor Page, Hosting Region and AI Processing Region	have the meanings given in the Silktide Customer Terms (clauses 2.1, 7.7 and 5.1).
Supervisory Authority	a governmental or government-chartered regulatory body having binding legal authority over a party in relation to Data Protection Law, including the data protection authorities of the EEA member states, the UK Information Commissioner, the Swiss Federal Data Protection and Information Commissioner, the Office of the Australian Information Commissioner, the Office of the Privacy Commissioner (New Zealand), the Office of the Privacy Commissioner of Canada and the provincial commissioners, the California Privacy Protection Agency and the attorneys general of the States of the United States.

UK GDPR	the EU GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, as amended.
US State Privacy Laws	the comprehensive consumer privacy laws of the States of the United States, including the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act, the Texas Data Privacy and Security Act, the Oregon Consumer Privacy Act and the Montana Consumer Data Privacy Act, and any other similar State law, in each case to the extent applicable to the processing of Personal Data under the Agreement and together with any implementing regulations.

2. Purpose

- 2.1 The Processor has agreed to provide the Services to the Controller in accordance with the terms of the Agreement. In providing the Services, the Processor processes Customer Data on behalf of the Controller. Customer Data may include Personal Data. The Processor will process and protect such Personal Data in accordance with the terms of this DPA.
- 2.2 The subject matter, duration, nature and purpose of the processing, the categories of Personal Data and the categories of Data Subjects are described in Exhibit A.

3. Scope

- 3.1 In providing the Services to the Controller pursuant to the terms of the Agreement, the Processor will process Personal Data only to the extent necessary to provide the Services in accordance with the terms of the Agreement, this DPA and the Controller's documented instructions. The Agreement, this DPA and the Controller's configuration of and use of the Services (including the Customer Sites it submits for scanning, the documents it submits for remediation, the prompts and platforms it configures and the analytics mode it selects) constitute the Controller's complete and final instructions to the Processor, and any additional or alternative instructions must be agreed in writing by the parties.
- 3.2 The Controller and the Processor will each take steps to ensure that any natural person acting under its authority who has access to Personal Data does not process it except

on the instructions of the Controller, unless required to do so by Data Protection Law.

4. Processor obligations

- 4.1 The Processor will collect, process or use Personal Data only within the scope of this DPA and the Controller's documented instructions.
- 4.2 The Processor will promptly inform the Controller if, in the Processor's opinion, an instruction regarding the processing of Personal Data infringes Data Protection Law. The Processor is not obliged to carry out a legal review, and this clause does not impose on the Processor any obligation to monitor the Controller's compliance with Data Protection Law.
- 4.3 The Processor will ensure that all employees, agents, officers and contractors involved in the handling of Personal Data: (i) are aware of the confidential nature of the Personal Data and are contractually bound to keep the Personal Data confidential; (ii) have received appropriate training on their responsibilities; and (iii) are bound by obligations no less protective than those in this DPA.
- 4.4 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including as appropriate: (i) the pseudonymization and encryption of Personal Data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability of and access to Personal Data in a timely manner in the event of a physical or technical incident; and (iv) a process for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures. In assessing the appropriate level of security, account will be taken in particular of the risks presented by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.
- 4.5 The technical and organizational measures described in Exhibit B are a minimum security standard and will be adhered to at all times. The Controller accepts that those measures are subject to development and review, and that the Processor may implement alternative measures provided they are at least equivalent to those in Exhibit B and are appropriate in accordance with clause 4.4. The Processor will not materially reduce the overall level of security during a Subscription Term.

- 4.6 The Controller acknowledges that, in the course of providing the Services, it may be necessary for the Processor to access Personal Data to respond to technical problems or Controller queries and to ensure the proper working of the Services. All such access by the Processor will be limited to those purposes.
- 4.7 Taking into account the nature of the processing and the information available to the Processor, the Processor will assist the Controller, by appropriate technical and organizational measures and insofar as this is possible, in fulfilling the Controller's obligations to respond to requests for the exercise of Data Subjects' rights and to comply with its obligations under Data Protection Law in relation to the security of processing, the notification of Personal Data Breaches, data protection impact assessments and prior consultation with Supervisory Authorities.
- 4.8 The Processor will not: (i) sell or share Personal Data; (ii) retain, use or disclose Personal Data for any purpose other than providing the Services in accordance with the Agreement and this DPA, including for any commercial purpose of its own; (iii) retain, use or disclose Personal Data outside the direct business relationship between the Controller and the Processor; or (iv) combine Personal Data with personal data that it receives from or on behalf of another person, or collects from its own interactions with Data Subjects, except as permitted by Data Protection Law for the purpose of providing the Services.
- 4.9 The Processor will maintain a record of its processing activities carried out on behalf of the Controller to the extent required by Data Protection Law, and will make it available to the Controller or a Supervisory Authority on request.

5. Controller obligations

- 5.1 The Controller represents and warrants that: (i) it will comply with this DPA and its obligations under Data Protection Law; (ii) it has obtained, and will maintain, all permissions, authorizations and lawful bases, and has given all notices, necessary to permit the Processor, its Affiliates and Sub-processors to exercise their rights and perform their obligations under this DPA, including in respect of Personal Data contained in or collected from Customer Sites and Personal Data relating to the personnel of the Controller's Clients; (iii) it has the right to have each Customer Site scanned, tested and monitored by the Services and to submit each document it submits for remediation; and (iv) all Affiliates and Clients of the Controller that use the Services will comply with the obligations of the Controller set out in this DPA, and the Controller is responsible for their compliance.

- 5.2 The Controller will implement appropriate technical and organizational measures to protect Personal Data within its control, including the credentials and access rights of its Authorized Users, taking into account the matters described in clause 4.4.
- 5.3 The Controller acknowledges that some instructions or requests, including requests for the Processor to assist with audits, inspections, data protection impact assessments or other assistance beyond that described in this DPA and the standard functionality of the Services, may result in additional fees. In such a case the Processor will notify the Controller of its reasonable fees for providing such assistance in advance and will be entitled to charge the Controller for its reasonable costs and expenses in providing that assistance, unless otherwise agreed or unless the assistance is required as a result of the Processor's breach of this DPA.

6. Sub-processors

- 6.1 The Controller acknowledges and agrees that: (i) Affiliates of the Processor may be used as Sub-processors; and (ii) the Processor and its Affiliates respectively may engage Sub-processors in connection with the provision of the Services.
- 6.2 The Controller authorizes the Processor to use the Sub-processors listed on the Sub-processor Page, published at silktide.com/company/legal/sub-processors. The Sub-processor Page states, for each Sub-processor, the service it provides, the products it supports, where it processes Personal Data and whether it is a Core Sub-processor or an Optional Sub-processor. A Core Sub-processor supports the Services for every Controller in a Hosting Region, for example the hosting, authentication and customer support providers. An Optional Sub-processor processes Personal Data only if the Controller switches on the feature, or selects the provider or platform, that uses it, for example the AI providers used by AI Features (including the automated remediation of content the Controller submits) and the third-party AI platforms and search engines that the Services query on the Controller's instruction under clause 6 of the Silktide Customer Terms. The Processor will give the Controller at least 30 days' notice before a new or replacement Core Sub-processor for the Controller's Hosting Region processes Personal Data, by email to the Controller's account and billing contacts or by notification within the Services. The Controller may also subscribe to notifications through the Sub-processor Page.
- 6.3 The Controller may object to a new or replacement Sub-processor notified under clause 6.2 or clause 6.6 on reasonable grounds relating to data protection, by notifying the Processor in writing within 10 Business Days after receipt of the notice. The parties will

then discuss the objection in good faith. If the Processor cannot reasonably accommodate the objection, the Controller may terminate the Agreement, or the affected Services, by written notice given within 30 days after the Processor's response, and the Processor will refund to the Controller any prepaid Fees covering the remainder of the Subscription Term following the effective date of termination in respect of the terminated Services.

- 6.4 Before a Sub-processor carries out any processing of Personal Data, the Processor will: (i) appoint the Sub-processor under a written contract containing data protection obligations materially the same as, and no less protective than, those imposed on the Processor in this DPA, to the extent applicable to the services provided by the Sub-processor; and (ii) ensure that the Sub-processor complies with those obligations. The Processor remains fully liable to the Controller for the performance of each Sub-processor's obligations, as set out in clause 12.2.
- 6.5 The Controller agrees that the Processor and its Sub-processors may make Restricted Transfers of Personal Data for the purpose of providing the Services to the Controller in accordance with the Agreement. The Processor confirms that each such Sub-processor: (i) is located in a country or territory recognized by the European Commission, the UK Secretary of State, the Swiss Federal Council or another competent Supervisory Authority, as applicable, as providing an adequate level of protection; or (ii) has entered into the applicable SCCs with the Processor; or (iii) has other legally recognized appropriate safeguards in place.
- 6.6 **Optional Sub-processors.** An Optional Sub-processor processes no Personal Data of the Controller until the Controller switches on the feature, or selects the provider or platform, that uses it, in the settings of the Services or as otherwise described in the Silktide Customer Terms (for example, by enabling AI Features and selecting an AI Processing Region and provider under clause 5 of the Silktide Customer Terms, or by selecting a third-party platform for a feature described in clause 6 of the Silktide Customer Terms). By doing so the Controller authorizes and instructs the Processor to use that Optional Sub-processor for that feature. The Controller may reverse its choice at any time through the settings of the Services, after which the Optional Sub-processor processes no further Personal Data of the Controller. Because an Optional Sub-processor processes nothing until the Controller chooses to use it, the Processor may add Optional Sub-processors to the Sub-processor Page at any time without the notice in clause 6.2, and may stop offering an Optional Sub-processor at any time, for example where its provider withdraws or changes the service or the provider's terms or prices

make it impractical to continue, giving reasonable notice to Controllers that are using it. If the Processor itself moves a Controller's processing from an Optional Sub-processor to a replacement, the Processor will give the notice in clause 6.2 and the Controller may object under clause 6.3; no notice is needed where the Controller selects the replacement itself.

7. Restricted Transfers

- 7.1 The parties agree that, where a transfer of Personal Data between the Controller and the Processor, or from the Processor to a Sub-processor, is a Restricted Transfer, it will be subject to the applicable SCCs.
- 7.2 The parties agree that the EU SCCs apply to Restricted Transfers from the EEA. The EU SCCs are deemed entered into, and incorporated into this DPA by reference, and completed as follows:
- (a) Module Two (Controller to Processor) applies where the Controller is a controller of Personal Data and the Processor is processing Personal Data on its behalf;
 - (b) Module Three (Processor to Processor) applies where the Controller is itself a processor of the Personal Data (for example, where it processes Personal Data on behalf of its Clients) and the Processor processes the Personal Data as its sub-processor, and where the Processor uses a Sub-processor to process the Personal Data;
 - (c) Module Four (Processor to Controller) applies where the Processor is processing Personal Data on behalf of a Controller that is not subject to the EU GDPR and transfers Personal Data to that Controller;
 - (d) in Clause 7 of the EU SCCs, the optional docking clause does not apply;
 - (e) in Clause 9 of the EU SCCs, Option 2 (general written authorization) applies, and the time period for giving notice of Sub-processor changes is as set out in clause 6.2 of this DPA;
 - (f) in Clause 11 of the EU SCCs, the optional language does not apply;
 - (g) in Clause 13 of the EU SCCs and Annex I.C, the competent supervisory authority is determined in accordance with Part C of Exhibit A;
 - (h) in Clause 17 of the EU SCCs, Option 1 applies and the EU SCCs are governed by the law of Denmark;

- (i) in Clause 18(b) of the EU SCCs, disputes will be resolved before the courts of Denmark;
- (j) Annex I of the EU SCCs is deemed completed with the information set out in Exhibit A of this DPA; and
- (k) Annex II of the EU SCCs is deemed completed with the information set out in Exhibit B of this DPA.

7.3 The parties agree that the EU SCCs, as completed in clause 7.2, are adjusted as follows where the FADP applies to a Restricted Transfer:

- (a) the Swiss Federal Data Protection and Information Commissioner (**FDPIC**) is the sole Supervisory Authority for Restricted Transfers exclusively subject to the FADP;
- (b) Restricted Transfers subject to both the FADP and the EU GDPR are dealt with by the FDPIC insofar as the transfer is governed by the FADP and by the competent EU Supervisory Authority insofar as the transfer is governed by the EU GDPR;
- (c) references to “member state” in the EU SCCs 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 SCCs;
- (d) where Restricted Transfers are exclusively subject to the FADP, references to the GDPR in the EU SCCs are to be understood as references to the FADP; and
- (e) where Restricted Transfers are subject to both the FADP and the EU GDPR, references to the GDPR in the EU SCCs are to be understood as references to the FADP insofar as the Restricted Transfers are subject to the FADP.

7.4 The parties agree that the UK Addendum applies to Restricted Transfers from the United Kingdom, and the UK Addendum is deemed entered into, and incorporated into this DPA by reference, as set out in Exhibit C.

7.5 If the European Commission, the UK Information Commissioner, the Swiss Federal Council or another competent authority adopts revised or replacement standard contractual clauses or an alternative transfer mechanism, the parties will cooperate in good faith to adopt the revised clauses or mechanism, and the Processor may update this DPA in accordance with clause 20 of the Silktime Customer Terms to reflect them.

- 7.6 If any provision of this DPA contradicts, directly or indirectly, any of the applicable SCCs, the provisions of the applicable SCCs prevail over the terms of this DPA.

8. Data Subject requests

- 8.1 The Controller may, during or after the term of the Agreement, require the correction, deletion, restriction or provision of Personal Data using the self-service functions of the Services or by written request to the Processor. The Processor will fulfill such requests to the extent they are lawful, in accordance with its standard operational procedures and without undue delay.
- 8.2 If the Processor receives a request or complaint from a Data Subject in relation to Personal Data, the Processor will, to the extent permitted by law, promptly notify the Controller and refer the Data Subject to the Controller, and will not respond to the request except on the Controller's documented instructions or as required by law. The Processor will provide reasonable assistance to the Controller in responding to the request. Where a request involves assistance beyond the self-service functions of the Services and the assistance described in this clause, clause 5.3 applies.

9. Audit

- 9.1 The Processor will make available to the Controller all information reasonably necessary to demonstrate compliance with its obligations under this DPA and Data Protection Law, and will allow for and contribute to audits, including inspections, conducted by the Controller or an independent auditor mandated by the Controller.
- 9.2 The Controller's audit right will in the first instance be satisfied by the Processor providing, on request and no more than once in any 12-month period, its most recent independent third-party audit reports, certifications and related summaries (currently including its SOC 2 Type II report), together with written responses to reasonable security questionnaires. If, having reviewed that information, the Controller reasonably considers that a further audit is necessary to verify the Processor's compliance, or a Supervisory Authority requires one, the Controller may conduct a more extensive audit which will be: (i) at the Controller's expense; (ii) limited in scope to matters specific to the Controller's Personal Data and agreed in advance; (iii) carried out during the Processor's usual business hours, no more than once in any 12-month period unless a Supervisory Authority requires otherwise or a Personal Data Breach affecting the Controller's Personal Data has occurred, on not less than four weeks' written notice

unless an identifiable material issue has arisen; and (iv) conducted in a way that does not unreasonably interfere with the Processor's day-to-day business or compromise the security or confidentiality of other customers' data.

- 9.3 All information made available under this clause 9 is the Processor's Confidential Information. This clause does not modify or limit any right of audit conferred on the Controller by Data Protection Law or the SCCs; it clarifies the procedures for exercising it.

10. Personal Data Breach

- 10.1 The Processor will notify the Controller without undue delay, and in any event within 72 hours, after becoming aware of a Personal Data Breach affecting the Controller's Personal Data. The notification will describe, to the extent then known, the nature of the Personal Data Breach, the categories and approximate number of Data Subjects and records concerned, the likely consequences, the measures taken or proposed to address it, and a contact point for further information. Information may be provided in phases as it becomes available.
- 10.2 The Processor will take all commercially reasonable measures to secure the Personal Data, to limit the effects of the Personal Data Breach and to assist the Controller in meeting its obligations under Data Protection Law, including obligations to notify Supervisory Authorities and Data Subjects and, where Australian Privacy Law applies, to assess whether the breach is an eligible data breach.
- 10.3 The Processor's notification of, or response to, a Personal Data Breach is not an acknowledgment of fault or liability. The Processor will not notify Supervisory Authorities or Data Subjects of a Personal Data Breach affecting the Controller's Personal Data on the Controller's behalf unless required by law or agreed with the Controller.

11. Compliance, cooperation and response

- 11.1 The Processor will notify the Controller promptly of any request, complaint or inquiry from a Supervisory Authority or other public authority regarding the processing of Personal Data that affects the Controller, unless such notification is not permitted under applicable law or a court order.
- 11.2 The Processor may make copies of and retain Personal Data to the extent required by any legal or regulatory requirement, including retention requirements, and will continue

to protect such Personal Data in accordance with this DPA.

- 11.3 The Processor will provide reasonable assistance to the Controller in carrying out data protection impact assessments and prior consultations with Supervisory Authorities relating to the Services, taking into account the nature of the processing and the information available to the Processor.
- 11.4 If a change in Data Protection Law requires a change to this DPA or to the technical and organizational measures in order to maintain compliance, either party may notify the other and the parties will agree the necessary changes in good faith. If the Processor is unable to accommodate a change that is necessary for the Controller's compliance, the Controller may terminate the part of the Services that gives rise to the non-compliance by written notice, and the Processor will refund any prepaid Fees for the remainder of the Subscription Term in respect of the terminated part. The provision of any unaffected Services continues.
- 11.5 The Controller and the Processor and, where applicable, their representatives, will cooperate, on request, with a Supervisory Authority in the performance of their respective obligations under this DPA and Data Protection Law.

12. Liability

- 12.1 The exclusions and limitations of liability set out in the Agreement (including clause 16 of the Silktide Customer Terms) apply to all claims arising out of or in connection with this DPA, whether in contract, tort or otherwise, except to the extent that Data Protection Law or the SCCs do not permit them to be excluded or limited.
- 12.2 The Processor is liable for breaches of this DPA caused by the acts, omissions or negligence of its Sub-processors to the same extent that the Processor would be liable if it had performed the services of each Sub-processor directly under this DPA, subject to the limitations on liability referred to in clause 12.1.
- 12.3 The Controller is liable for breaches of this DPA caused by the acts, omissions or negligence of its Affiliates and Clients as if such acts, omissions or negligence had been committed by the Controller itself.
- 12.4 Neither party is entitled to recover more than once in respect of the same loss, including where the same event gives rise to claims under both this DPA and the SCCs.

13. Term

- 13.1 This DPA takes effect on the Effective Date of the Agreement and continues for as long as the Processor processes Personal Data on behalf of the Controller, including during any retention or retrieval period under the Agreement, notwithstanding the expiry or termination of the Agreement.

14. Deletion and return of Personal Data

- 14.1 **Retrieval period.** Following the end of the provision of the Services, the Controller may export its Personal Data using the export functions of the Services for at least 30 days, as described in clause 7.5 of the Silktide Customer Terms, or may request in writing within that period that the Processor return the Personal Data to it in a commonly used, machine-readable format.
- 14.2 **Retention after the Services end.** Unless the Controller requests earlier deletion under clause 14.3, the Processor will retain the Personal Data for up to 6 months after the end of the provision of the Services so that the Controller can retrieve it or resume the Services. During that period the Processor will only store the Personal Data and protect it in accordance with this DPA, and will not otherwise process it except to return it to the Controller. The Processor will delete the Personal Data from its production systems automatically by the end of that period, and will delete Personal Data held in backups within 6 months after the end of the provision of the Services as the backups are rotated in the ordinary course. The Controller instructs the Processor to retain and delete Personal Data in accordance with this clause 14.
- 14.3 **Earlier deletion on request.** The Controller may at any time after the end of the provision of the Services request in writing that the Processor delete its Personal Data sooner, and the Processor will complete the deletion from its production systems within 30 days of the request; Personal Data in backups is deleted as described in clause 14.2. The Controller may also delete individual Customer Sites, documents submitted for remediation and other Customer Data at any time during the Subscription Term through the functions of the Services, where available.
- 14.4 **Retention required by law.** Where applicable law requires the Processor to retain Personal Data beyond the periods in this clause 14, the Processor will continue to protect it in accordance with this DPA and will process it only for the purpose required by that law.
- 14.5 On the Controller's written request, the Processor will certify in writing that it has complied with this clause 14.

15. Jurisdiction-specific terms

- 15.1 The provisions of Exhibit D apply, in addition to the other provisions of this DPA, where and to the extent the Data Protection Law of the relevant jurisdiction applies to the processing of Personal Data under the Agreement. Where a provision of Exhibit D conflicts with another provision of this DPA, the provision of Exhibit D prevails in respect of processing subject to the relevant Data Protection Law.

16. General

- 16.1 This DPA, together with the Agreement, sets out the entire understanding of the parties in relation to the processing of Personal Data by the Processor on behalf of the Controller, and supersedes any prior data processing agreement between the parties in relation to the Services.
- 16.2 If any provision of this DPA is or becomes invalid, the legal effect of the other provisions is unaffected. A valid provision is deemed to have been agreed which comes closest to what the parties intended commercially and replaces the invalid provision. The same applies to any omission.
- 16.3 Subject to any provision of the SCCs or the UK Addendum to the contrary, this DPA is governed by the law that governs the Agreement under clause 25 of the Silktide Customer Terms, and any dispute arising out of or in connection with this DPA will be resolved in the forum specified for the Silktide Entity in that clause.
- 16.4 The Processor may update this DPA in accordance with clause 20 of the Silktide Customer Terms. An update that is required by Data Protection Law, or that increases the protection afforded to Personal Data or to the Controller, takes effect on notice.
- 16.5 A person who is not a party to this DPA has no right to enforce any of its terms, except that Data Subjects may enforce the SCCs and the UK Addendum to the extent provided in them.

Exhibit A: List of Parties, Description of Processing and Competent Supervisory Authority

This Exhibit A serves as Annex I to the EU SCCs and, where applicable, as the Appendix Information to the UK Addendum.

A. List of Parties

The data exporter (Controller)

Item	Details
Name	The Customer named in the Agreement.
Address	As set out for the Customer in the Order Form or the Customer's account.
Contact person's name, position and contact details	The account owner and billing contacts recorded in the Customer's account and used for notifications and invoicing.
Activities relevant to the data transferred	Use of the Services in accordance with the Agreement.
Signature and date	By entering into the Agreement, the Controller is deemed to have signed the SCCs incorporated into this DPA, including their Annexes, as of the Effective Date of the Agreement.
Role	Controller (or, where the Customer processes Personal Data on behalf of its Clients, processor).
Representative (if applicable)	Any representative in the European Union or the United Kingdom named in the Controller's privacy notice.

The data importer (Processor)

Item	Details
Name	The Silktide Entity that is party to the Agreement, being the entity named in the Order Form, as described in clause 25 of the Silktide Customer Terms.

Address	Silktide Limited: 1st Floor, The Barwick, 16 Barwick Street, Birmingham, B3 2NT, United Kingdom (company number 04242422). Silktide ApS: Studiestræde 14A, 1455 København K, Denmark (CVR 45514420). Silktide Pty Ltd: Suite 1, Level 3, 62 Lygon Street, Carlton South, VIC 3053, Australia (ACN 682 065 765; ABN 39 682 065 765). Silktide Inc: 106 E 6th Street, Suite 400, Austin, TX 78701, United States.
Contact person's name, position and contact details	Lee Percox, Chief Operating Officer, privacy@silktide.com
Activities relevant to the data transferred	The provision of the Services: a cloud platform through which the Controller scans, tests and monitors its websites, documents and other digital properties; measures how visitors use them; monitors how third-party AI platforms, search engines and similar services present it and its competitors; and submits content for automated improvement or remediation; in each case as the Controller configures, and under which the Processor processes Personal Data on the Controller's instructions in accordance with the Agreement.
Signature and date	By entering into the Agreement, the Processor is deemed to have signed the SCCs incorporated into this DPA, including their Annexes, as of the Effective Date of the Agreement.
Role	Processor (or, where the Controller is itself a processor, sub-processor).
Representative (if applicable)	Representative in the European Union for members of the Silktide Group not established in the EU: Silktide ApS, Studiestræde 14A, 1455 København K, Denmark, privacy@silktide.com. Representative in the United Kingdom for members of the Silktide Group not established in the UK: Silktide Limited, 1st Floor, The Barwick, 16 Barwick Street, Birmingham, B3 2NT, United Kingdom, privacy@silktide.com.

B. Description of processing and transfers

Item	Details
Processing activities covered	The Services process Personal Data in the course of the following activities, each of which the Controller may purchase and configure: (A) Digital property testing: the automated retrieval (crawling), testing and monitoring of the websites, documents and other digital properties that the Controller submits as Customer Sites, and the reporting of the results. (B) Visitor measurement: the measurement of how visitors use Customer Sites on which the Controller has deployed the Services' measurement code, in the mode the Controller selects. (C) External platform monitoring: the submission of prompts the Controller configures to third-party AI platforms, search engines and similar services, the recording of how they present the Controller and the competitors it names, and the retrieval of publicly accessible pages of the Controller's and those competitors' websites for comparison (clause 6 of the Silktide Customer Terms). (D) Content remediation: the automated improvement of content the Controller submits, currently the accessibility remediation of documents such as PDFs, which, where the Controller chooses AI remediation, are processed by the AI provider identified on the Sub-processor Page for the AI Processing Region selected for the Controller's account and returned to the Controller to review and accept (clause 5 of the Silktide Customer Terms). (E) Account, configuration and support: the administration of the Controller's account and Authorized Users and the provision of support. The Documentation describes the products through which Silktide offers these activities; product names may change, and this Exhibit applies to any product of the Services whose processing falls within these activities. Only the activities the Controller has purchased and configured are carried out.

Categories of Data Subjects	(E) All activities: Authorized Users of the Services, being employees, contractors and agents of the Controller, its Affiliates and (where agency use applies) its Clients; individuals whose Personal Data is otherwise included in Customer Data entered into the Services by the Controller, its Authorized Users or Clients; and personnel of the Controller who contact the Processor for support or in connection with the Agreement. (A) Digital property testing: individuals whose Personal Data is contained in the content of the Customer Sites the Controller submits, such as staff, authors, contributors and other persons named or depicted on those websites, documents and digital properties. (B) Visitor measurement: visitors to Customer Sites on which the Controller has deployed the Services' measurement code. (C) External platform monitoring: individuals named or described in the responses returned by the third-party platforms queried on the Controller's instruction, and in the publicly accessible web pages retrieved for comparison. (D) Content remediation: individuals whose Personal Data is contained in the content the Controller submits for remediation, such as the authors, subjects and addressees of a document.
---	---

Categories of Personal Data	(E) All activities: account and identity data of Authorized Users (name, business email address, job title, organization, role and permissions, login credentials (hashed), authentication tokens, IP address, browser and device information, and records of activity within the Services); Personal Data contained in configuration, notes, comments, tasks and other content that Authorized Users enter into the Services; and Personal Data contained in support communications and feedback. (A) Digital property testing: Personal Data published on or contained in Customer Sites and retrieved by the Services when scanning them, which may include names, job titles, contact details, images, biographical text and other information the Controller or its Clients have chosen to publish. (B) Visitor measurement: pages viewed, referring page, date, time and duration of visit, device, browser and operating system, screen size, approximate location derived from IP address, a pseudonymous visitor identifier, and click, scroll and movement data used to generate heatmaps. The Controller chooses the measurement mode for each Customer Site. In the cookieless mode the visitor identifier is a one-way hash of the IP address, browser user agent, the Customer Site's property identifier and a salt that changes daily and is deleted after two days; the IP address and user agent are processed only to derive the identifier and the approximate location and are not stored, and visitors cannot be recognized across Customer Sites or after 24 to 48 hours. In the cookie mode a single first-party cookie set by the Services stores a pseudonymous identifier on the visitor's device so that returning visitors can be recognized for as long as the cookie persists, as described in the Documentation. In the combined mode the cookieless method is used until the visitor consents to cookies and the cookie mode thereafter. The measurement features are designed to measure use of a Customer Site without identifying visitors by name or contact details. (C) External platform monitoring: the prompts configured by the Controller, the responses returned by the third-party platforms, and the publicly accessible content of the web pages retrieved for comparison, each of which may incidentally contain Personal Data such as names, roles and statements about individuals. (D) Content remediation: the full content of the documents or other content the Controller submits, including text, images, form fields and metadata, which may include any Personal Data the Controller or its Clients have included in it, together with the remediated versions. The extent of the Personal Data is determined and controlled by the Controller through the Customer Sites it submits, the content it submits for remediation, the features it deploys and configures, and the content it enters.
---	--

Sensitive data	The Services are not designed to process special categories of Personal Data or other sensitive data, and the Controller must not intentionally submit such data, or configure the Services to collect it, unless expressly agreed in an Order Form (clause 7.3 of the Silktide Customer Terms). This applies in particular to content submitted for remediation, which the Controller should review before submission. Sensitive data may be processed incidentally where it is published on a Customer Site or contained in content that the Controller has instructed the Services to scan or remediate. Any such data is processed only as part of the automated scanning, reporting or remediation of the Customer Site or content and is subject to the same technical and organizational measures as all other Customer Data.
Frequency of the processing and transfer	Continuous for the duration of the Agreement, including scheduled and on-demand scans and prompt runs initiated or configured by the Controller, the collection of visitor measurement data as visitors use Customer Sites on which the Controller has deployed the measurement code, and the remediation of content as the Controller submits it.

Nature of the processing	Hosting and storage; automated retrieval (crawling) of Customer Sites on the Controller's instructions; automated analysis and testing of the retrieved content for accessibility, content quality, search optimization, privacy and cookie compliance, performance and similar criteria; generation and storage of reports, scores, issues and recommendations; collection of visitor interaction data from Customer Sites on which the Controller has deployed the measurement code and its aggregation into reports and heatmaps; submission of prompts configured by the Controller to third-party AI platforms, search engines and similar services and the retrieval, storage and analysis of the responses; retrieval, storage and analysis of publicly accessible third-party web pages identified by the Controller for comparison; receipt of content submitted for remediation, its transmission to the AI provider for the Controller's AI Processing Region where the Controller chooses AI remediation, the automated remediation of its structure, tags, reading order, alternative text and similar accessibility properties, and the storage and return of the original and remediated versions for the Controller's review and acceptance; where the Controller has enabled AI Features, the analysis of the Customer Data the Controller submits to them by the AI provider it has selected, in the AI Processing Region it has selected, to generate suggestions, summaries, recommendations and other AI Output (clause 5 of the Silktide Customer Terms); user account and access management; notifications and reporting to Authorized Users; technical support; and backup, security monitoring and deletion in accordance with this DPA.
Purpose of the processing and transfer	To provide, maintain, secure and support the Services for the Controller in accordance with the Agreement. Personal Data is transferred to Sub-processors only to the extent they need to process it in order to provide their services to the Processor as part of the Services.
Duration of the processing and retention period	For the Subscription Term and any retrieval period under the Agreement, followed by deletion in accordance with clause 14 of this DPA. Content submitted for remediation and its remediated versions are retained so that the Controller can retrieve them, for the period described in the Documentation, and may be deleted earlier by the Controller through the Services or on request under clause 14.3.

Location of processing	Customer Data is stored and processed in the Hosting Region assigned to the Controller's account as described in clause 7.7 of the Silktide Customer Terms, by the Core Sub-processors listed for that region; the authentication and customer support providers process limited account and support data from the locations shown on the Sub-processor Page. Optional Sub-processors process Personal Data only once the Controller has chosen to use them (clause 6.6): AI Features and content remediation are processed by the AI provider in the AI Processing Region the Controller selects, so that a Controller that selects the EU region has its content remediated in the EU, and the prompts and responses of external platform monitoring are processed by the platform providers the Controller selects, in the locations shown for them on the Sub-processor Page.
Transfers to Sub-processors	The Sub-processor Page published at silktide.com/company/legal/sub-processors identifies each Sub-processor, the service it provides and the products it supports, whether it is a Core or an Optional Sub-processor, the region in which it is used, where it processes Personal Data and the categories of Personal Data it processes. Transfers to Sub-processors are for the duration of the Agreement and for the sole purpose of providing the Services.

C. Competent Supervisory Authority

Where	Competent Supervisory Authority
The EU GDPR applies	The supervisory authority of the EU member state in which the Controller (as data exporter) is established. Where the Controller is not established in the European Union, the Danish Data Protection Agency (Datatilsynet), being the supervisory authority of the member state in which the Processor's representative in the European Union (Silktide ApS) is established.
The UK GDPR applies	The UK Information Commissioner's Office (ICO).
The FADP applies	The Swiss Federal Data Protection and Information Commissioner (FDPIC).

Exhibit B: Technical and Organizational Security Measures

This Exhibit B describes the technical and organizational measures implemented by the Processor (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. Where applicable, this Exhibit B serves as Annex II to the EU SCCs and as the Appendix Information to the UK Addendum. The Processor may update these measures in accordance with clause 4.5 of this DPA.

Measure	Description
Security program and assurance	The Processor operates an information security program that is independently audited each year against the AICPA SOC 2 Trust Services Criteria; a SOC 2 Type II report is in place and a summary of the most recent report, together with a summary of the most recent penetration test, is available to the Controller under the confidentiality provisions of the Agreement on written request no more than once in any 12-month period, in accordance with clause 9.2 of this DPA. Information security policies, including the incident response, vulnerability management, access control and acceptable use policies, are approved by management and reviewed at least annually.
Measures of pseudonymization and encryption of Personal Data	Customer Data is encrypted at rest using AES-256 and in transit using Transport Layer Security (TLS). Credentials of Authorized Users are stored as hashes. Remote access by Processor personnel to production systems is only possible over an encrypted connection with two-factor authentication and full-disk encryption on the accessing device. Where the Services derive identifiers from Personal Data, such as the cookieless visitor identifier in the analytics features, they use one-way hashing with rotating salts so that the underlying data is not stored (Exhibit A).

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Access to Customer Data is granted on the “least privilege” and “need-to-know” principles through a role and authorization concept, so that each role has only the rights needed for the task of the individual. Each Controller’s Customer Data is logically separated from that of other customers and is stored and processed in the Hosting Region assigned to the Controller’s account. Production systems are separated from testing and development systems. Infrastructure is monitored continuously by automated tooling.
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	Applications are built stateless from infrastructure-as-code templates and can be recreated within the Hosting Region. Data is stored across multiple AWS availability zones so that the failure of a data center through flooding, fire, power loss or similar events does not cause loss of Personal Data. Redundancy is maintained throughout the infrastructure, and backups are taken daily in accordance with the Processor’s backup procedures.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	The security program is audited annually for the SOC 2 Type II report. The Services undergo penetration testing at least annually. The codebase and its dependencies are scanned routinely for vulnerabilities under the vulnerability management policy, and findings are prioritized and remediated according to severity. Monitoring of the infrastructure is automated and continuous.

Measures for user identification and authorization	Processor personnel use unique, individually assigned accounts authenticated against a central directory, with two-factor authentication for remote access to production systems; all access attempts, successful and unsuccessful, are logged, and access rights are removed when employment ends. Controllers manage their own Authorized Users, roles and permissions within the Services. Single sign-on through the Controller's own identity provider is available, through which the Controller can enforce multi-factor authentication and its own access policies for its Authorized Users.
Measures for the protection of data during transmission	Data in transit between Authorized Users and the Services, between the Services and Sub-processors, and between the Services and Customer Sites is protected by TLS, using the protocol versions and cipher suites supported by the Customer Site when crawling it.
Measures for the protection of data during storage	Customer Data is stored in the AWS infrastructure of the Hosting Region assigned to the Controller's account, encrypted at rest using AES-256, and is logically separated from the data of other customers.
Measures for ensuring physical security of locations at which Personal Data are processed	Customer Data is hosted in AWS data centers that maintain current ISO 27001 certification and SOC 1 and SOC 2 attestation reports; the Processor will not use a data center provider that does not maintain those or substantially equivalent certifications. The Processor's offices are secured by controlled entry and a monitored alarm, a central record of keyholders is maintained and access is revoked when employment ends. Personnel working remotely are required to comply with the Processor's security policies in full.

Measures for ensuring events logging	Application and infrastructure events, including authentication attempts, administrative actions and changes to the account settings that enable AI Features, select an AI Processing Region or provider, select a third-party platform or set the visitor measurement mode (which evidence the Controller's instructions under clause 6.6), are recorded in log files, so that it can be established retrospectively whether and by whom Personal Data was entered, altered or deleted. Logs are reviewed as part of security monitoring and retained in accordance with the Processor's retention policy.
Measures for ensuring system configuration, including default configuration	System configuration is defined in code and applied and maintained by configuration management tools that detect and correct deviation from the specification. Changes to production systems follow the Processor's change management process, including review and testing before deployment.
Measures for internal IT and IT security governance and management	Personnel are instructed to collect, process and use Personal Data only within the scope and for the purposes of their duties, are bound by confidentiality obligations and complete security awareness training on joining and periodically thereafter. Information security policies are owned by management and reviewed at least annually as part of the SOC 2 program. Sub-processors are assessed before engagement and bound by written contracts in accordance with clause 6.4 of this DPA.

Measures for incident detection, response and notification	The Processor maintains an incident response policy and procedures, audited under its SOC 2 program, covering the detection, classification, containment, investigation and remediation of security incidents and the notification of affected Controllers within the time required by clause 10 of this DPA. Incidents are reviewed after resolution and corrective actions tracked. Security vulnerabilities may be reported to security@silktide.com in accordance with section 6 of the Acceptable Use Policy.
Measures for certification/assurance of processes and products	SOC 2 Type II attestation of the Processor's security program, renewed annually. AWS certifications and attestation reports for the hosting infrastructure. Reports are provided to the Controller as described in the first row of this Exhibit and are Confidential Information under the Agreement.
Measures for ensuring data minimization	The Services process the Customer Sites, documents, prompts and analytics data that the Controller configures and no more, and features that process Personal Data beyond the core scanning of Customer Sites (AI Features, visitor measurement, the querying of third-party platforms, content remediation) operate only when the Controller enables or uses them. Personal Data that is no longer required for the purposes for which it was processed is deleted; deletions are first marked and then completed after a short delay to protect against accidental or malicious deletion.
Measures for ensuring data quality	The data processed is provided or configured by the Controller. The Processor does not assess its accuracy, and provides reporting and export tools within the Services to help the Controller review and validate the data stored.

Measures for ensuring limited data retention	The Processor classifies the data it stores and its retention policy specifies how each class is retained. When a record containing Personal Data is deleted it is removed from the active databases and remains in backups only until they are rotated, within the periods stated in clause 14 of this DPA.
Measures for ensuring accountability	All personnel acknowledge the information security policies on joining and when they change. A disciplinary procedure applies to personnel who do not adhere to them. Responsibility for the security program rests with named management owners.
Measures for allowing data portability and ensuring erasure	The Services include functions that allow the Controller to export Customer Data in the formats described in the Documentation and to delete Customer Sites, documents and other Customer Data, and clause 14 of this DPA governs deletion at the end of the Services.
Measures to be taken by the (Sub-) processor to be able to provide assistance to the Controller (and, for transfers from a Processor to a Sub-processor, to the Data Exporter)	Personal Data is transferred to a Sub-processor only under a written contract meeting clause 6.4 of this DPA and only for the purpose of providing the Services. Where Personal Data is transferred outside the EEA, the United Kingdom or Switzerland, the Processor ensures an adequate level of protection at the recipient, for example through the EU SCCs, the UK Addendum or an adequacy decision, as described in clauses 6.5 and 7 of this DPA.

Exhibit C: International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (UK Addendum)

VERSION B1.0, in force 21 March 2022. This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract. The Mandatory Clauses in Part 2 are reproduced from the Approved Addendum without amendment.

Part 1: Tables

Table 1: Parties

	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Start date	The Effective Date of the Agreement.	The Effective Date of the Agreement.
Parties' details	Full legal name: the Customer named in the Agreement. Main address: as set out in the Order Form or the Customer's account. Official registration number (if any): where set out in the Order Form.	Full legal name: the Silktide Entity that is party to the Agreement. If Silktide Limited: 1st Floor, The Barwick, 16 Barwick Street, Birmingham, B3 2NT, United Kingdom; company number 04242422. If Silktide ApS: Studiestræde 14A, 1455 København K, Denmark; CVR 45514420. If Silktide Pty Ltd: Suite 1, Level 3, 62 Lygon Street, Carlton South, VIC 3053, Australia; ACN 682 065 765, ABN 39 682 065 765. If Silktide Inc: 106 E 6th Street, Suite 400, Austin, TX 78701, United States.
Key contact	As set out in Annex I of the Approved EU SCCs (Exhibit A).	Lee Percox, Chief Operating Officer, privacy@silktide.com
Signature (if required for the purposes of Section 2)	See the Agreement.	See the Agreement.

Table 2: Selected SCCs, Modules and Selected Clauses

The Addendum EU SCCs are the Approved EU SCCs, including the Appendix Information, with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation) and time period	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	No	Not used	Not used	Not applicable	Not applicable
2	Yes	Not used	Not used	General Authorisation; 30 days	Not applicable
3	Yes	Not used	Not used	General Authorisation; 30 days	Not applicable
4	Yes	Not used	Not used	Not applicable	No

Table 3: Appendix Information

“Appendix Information” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex	Where set out
Annex 1A: List of Parties	Exhibit A, Part A of this DPA.
Annex 1B: Description of Transfer	Exhibit A, Part B of this DPA.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data	Exhibit B of this DPA.
Annex III: List of Sub-processors (Modules 2 and 3 only)	The Sub-processor list published at silktide.com/company/legal/sub-processors , as referred to in clause 6.2 of this DPA.

Table 4: Ending this Addendum when the Approved Addendum changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19
	Importer and Exporter.

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Term	Meaning
Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.

Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.
10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
 - (a) together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
 - (b) Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
 - (c) this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.
14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.
15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

- (a) References to the “Clauses” means this Addendum, incorporating the Addendum EU SCCs;
- (b) In Clause 2, delete the words: “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”;
- (c) Clause 6 (Description of the transfer(s)) is replaced with: “The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter’s processing when making that transfer.”;
- (d) Clause 8.7(i) of Module 1 is replaced with: “it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer”;
- (e) Clause 8.8(i) of Modules 2 and 3 is replaced with: “the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;”
- (f) References to “Regulation (EU) 2016/679”, “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)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;
- (g) References to Regulation (EU) 2018/1725 are removed;
- (h) References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;
- (i) The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;
- (j) Clause 13(a) and Part C of Annex I are not used;
- (k) The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;

- (l) In Clause 16(e), subsection (i) is replaced with: “the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;
- (m) Clause 17 is replaced with: “These Clauses are governed by the laws of England and Wales.”;
- (n) Clause 18 is replaced with: “Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and
- (o) The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

- 16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.
- 17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
- 18. From time to time, the ICO may issue a revised Approved Addendum which: (a) makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or (b) reflects changes to UK Data Protection Laws. The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.
- 19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in: (a) its direct costs of performing its obligations under the Addendum; and/or (b) its risk under the Addendum, and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of

a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Exhibit D: Jurisdiction-Specific Terms

The provisions of this Exhibit D apply in addition to the other provisions of this DPA where, and to the extent that, the Data Protection Law of the relevant jurisdiction applies to the processing of Personal Data under the Agreement, as set out in clause 15 of this DPA.

D1. United States: California and other US State Privacy Laws

- D1.1 **Roles and business purpose.** For the purposes of the CCPA, the Controller is a business and the Processor is a service provider, and for the purposes of US State Privacy Laws, the Controller is a controller and the Processor is a processor. The Controller discloses Personal Data to the Processor solely for the business purpose of providing, maintaining, securing and supporting the Services in accordance with the Agreement (the **Business Purpose**). The nature and purpose of the processing, the type of Personal Data and the duration of the processing are described in Exhibit A.
- D1.2 **Restrictions.** The Processor will not: (a) sell or share Personal Data, as those terms are defined in the CCPA; (b) retain, use or disclose Personal Data for any purpose, including any commercial purpose, other than the Business Purpose or as otherwise permitted by the CCPA and its regulations for service providers; (c) retain, use or disclose Personal Data outside the direct business relationship between the Controller and the Processor; or (d) combine Personal Data received from or on behalf of the Controller with personal information that the Processor receives from or on behalf of another person, or collects from its own interactions with the Data Subject, except as expressly permitted by the CCPA and its regulations.
- D1.3 **Compliance and protection.** The Processor will comply with the obligations applicable to service providers and processors under the CCPA and US State Privacy Laws, and will provide the same level of privacy protection as those laws require of the Controller. The Processor will notify the Controller within 10 Business Days if it determines that it can no longer meet its obligations under the CCPA or US State Privacy Laws.
- D1.4 **Controller's rights.** The Controller may take reasonable and appropriate steps to ensure that the Processor uses Personal Data in a manner consistent with the

Controller's obligations under the CCPA and US State Privacy Laws, including through the audit rights in clause 9 of this DPA, and may, on written notice, require the Processor to stop and remediate any unauthorized use of Personal Data.

- D1.5 **Consumer requests.** The Processor will cooperate with the Controller in responding to verifiable consumer requests, including requests to know, access, correct, delete, or opt out, by providing the assistance described in clause 8 of this DPA, and will not respond directly to a consumer except as instructed by the Controller or as required by law.
- D1.6 **Sub-processors and assessments.** The Processor will engage any subcontractor that processes Personal Data only under a written contract that imposes obligations no less protective than those in this Exhibit D1, and will notify the Controller of subcontractor engagements in accordance with clause 6 of this DPA, giving the Controller the opportunity to object. The Processor will make available the information necessary to demonstrate its compliance, and will allow and cooperate with reasonable assessments by the Controller or its designated assessor, or arrange for a qualified independent assessor to conduct an assessment and provide a report to the Controller, in each case in accordance with clause 9 of this DPA.
- D1.7 **Confidentiality and deletion.** Each person processing Personal Data on behalf of the Processor is subject to a duty of confidentiality in accordance with clause 4.3 of this DPA. At the Controller's direction, and in any event at the end of the provision of the Services, the Processor will delete or return all Personal Data in accordance with clause 14 of this DPA, unless retention is required by law.
- D1.8 **Certification.** The Processor certifies that it understands the restrictions in this Exhibit D1 and will comply with them.

D2. Australia

- D2.1 **Roles.** The Controller is the APP entity that collects the Personal Data, and the Processor handles Personal Data on the Controller's behalf. Where the Processor is itself an APP entity, it will comply with the Australian Privacy Principles in relation to the Personal Data to the extent they apply to it, and in any event will handle Personal Data only in accordance with the Controller's instructions and in a manner that will not cause the Controller to breach the Australian Privacy Principles.
- D2.2 **Overseas disclosure.** The Controller acknowledges that the Processor and its Sub-processors may process Personal Data outside Australia, in the locations identified in the Sub-processor list, and authorizes such disclosure for the purposes of Australian

Privacy Principle 8 on the basis that the Processor has taken the steps described in clauses 6.4 and 6.5 of this DPA to ensure that each overseas recipient handles the Personal Data in a manner consistent with the Australian Privacy Principles. The Controller is responsible for including any notice of overseas disclosure required by Australian Privacy Principle 5 in its own privacy notices.

- D2.3 **Eligible data breaches.** The Processor will notify the Controller of any Personal Data Breach in accordance with clause 10 of this DPA and will assist the Controller in assessing, within the time required by Australian Privacy Law, whether the breach is an eligible data breach and in preparing any statement to the Office of the Australian Information Commissioner and any notification to affected individuals. The Processor will not notify the Commissioner or individuals of a breach affecting the Controller's Personal Data unless required by law or agreed with the Controller.
- D2.4 **Use and disclosure.** The Processor will not use or disclose Personal Data for direct marketing, will not adopt, use or disclose any government-related identifier contained in Personal Data except as required to provide the Services, and will assist the Controller in responding to requests for access to or correction of Personal Data under Australian Privacy Principles 12 and 13.
- D2.5 **Controller obligations.** The Controller warrants that it has collected the Personal Data in accordance with Australian Privacy Principles 3 and 5 and that its instructions to the Processor comply with Australian Privacy Law.

D3. New Zealand

- D3.1 The Processor holds Personal Data as the Controller's agent for the purposes of the Privacy Act 2020 (New Zealand). The Processor will protect Personal Data with security safeguards that are reasonable in the circumstances in accordance with Information Privacy Principle 5, will not use or disclose Personal Data except for the purpose of providing the Services, and will notify the Controller of any Personal Data Breach in accordance with clause 10 of this DPA so that the Controller can assess whether it is a notifiable privacy breach.
- D3.2 The Controller authorizes the disclosure of Personal Data to the Processor's Sub-processors outside New Zealand for the purposes of Information Privacy Principle 12, on the basis that the Processor has ensured, in accordance with clauses 6.4 and 6.5 of this DPA, that each recipient is required to protect the Personal Data in a way that, overall, provides comparable safeguards to those in the Privacy Act 2020.

D4. Canada

- D4.1 The Processor processes Personal Data on behalf of the Controller for the purposes of the Personal Information Protection and Electronic Documents Act and substantially similar provincial laws. The Processor will use Personal Data only to provide the Services, will protect it with security safeguards appropriate to its sensitivity, will notify the Controller of any Personal Data Breach in accordance with clause 10 of this DPA so that the Controller can assess whether there is a real risk of significant harm, and will assist the Controller in responding to access and correction requests.
- D4.2 Where the Quebec Act respecting the protection of personal information in the private sector applies: (a) this DPA constitutes the written agreement required by section 18.3 of that Act, and the Processor will take the measures required to protect the confidentiality of the Personal Data, use it only for the purposes of providing the Services, not keep it after the end of the provision of the Services (subject to clause 14), notify the Controller without delay of any breach or attempted breach of the confidentiality obligation, and allow the Controller to conduct verifications relating to confidentiality in accordance with clause 9; and (b) the Controller acknowledges that Personal Data will be processed outside Quebec, in the locations identified in the Sub-processor list, and is responsible for conducting any privacy impact assessment required by section 17 of that Act, for which the Processor will provide reasonable information on request.

D5. Switzerland

- D5.1 Where the FADP applies, the adjustments to the EU SCCs set out in clause 7.3 of this DPA apply, references in this DPA to Personal Data include personal data of legal entities to the extent protected by the FADP, and the competent Supervisory Authority is the FDPIC.

D6. United Kingdom, European Union and Denmark

- D6.1 Where the UK GDPR applies, the UK Addendum in Exhibit C applies to Restricted Transfers from the United Kingdom, and the competent Supervisory Authority is the UK Information Commissioner.
- D6.2 Where the EU GDPR applies, this DPA constitutes the contract required by Article 28(3) of the EU GDPR, the EU SCCs apply to Restricted Transfers from the EEA as set out in clause 7.2 of this DPA, and, where the Controller is established in Denmark, the Danish Data Protection Act (databeskyttelsesloven) applies in addition to the EU GDPR. Where a

Controller that is a Danish public authority is required by Danish law to use the standard contractual clauses for processors adopted by the Danish Data Protection Agency, the parties will agree in the Order Form how those clauses are to be incorporated.