SWIMLANE

Data Processing Addendum

Last Updated: March 5, 2026

Please contact privacy@swimlane.com for all privacy inquiries, requests, and/or questions related to this Data Processing Addendum (“DPA”).

This Data Processing Addendum (“DPA”) sets forth the terms that apply when personal data is processed by Swimlane. The purpose of the DPA is to ensure that processing is conducted in accordance with applicable Data Protection Laws and respects the rights of individuals whose personal data is processed.

This DPA is incorporated into and forms part of the Agreement entered into by Swimlane and Customer and contains certain terms and conditions relating to data protection, privacy and security to include certain requirements of The General Data Protection Regulation (EU) 2016/679 (“GDPR”) and The California Consumer Privacy Act of 2018 (Cal. Civ. Code, Title 1.81.5 comprising §§ 1798.100 – 1798.198 (as amended) (“CCPA”), where applicable. In the event (and to the extent applicable only) that there is a conflict between the GDPR and the CCPA, the parties agree to comply with the more onerous requirement or higher standard.

This DPA applies where Swimlane is the Processor and Customer is the controller.

1. Definitions

“Agreement” means the Swimlane Software License Agreement or other agreement, as applicable, that is entered into by and between Swimlane, Inc and the Customer, whereby Customer has access to the Swimlane Service.

- “California Personal Information” means Personal Data that is subject to the protection of the CCPA.
- "CCPA" means California Civil Code Sec. 1798.100 et seq. (also known as the California Consumer Privacy Act of 2018).
- "Consumer", "Business", "Sell" and "Service Provider" have the meanings defined in the CCPA.
- “Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- “Data Protection Law” means the GDPR, Member State laws implementing the GDPR, UK Data Protection Laws, the CCPA, and any other data protection laws that apply directly to Swimlane in connection with its Processing of Personal Data.

- “Data Subject Access Request (DSAR)” means a submission by an individual (data subject) to an entity asking to know what personal information of theirs has been collected, how it is stored, and how it is used.
- “GDPR” means (a) the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- “Instructions” means the written, documented instructions issued by a Controller to a Processor, and directing the same to perform a specific or general action with regard to Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available).
- “Personal Data” or “Customer Personal Data” means the Customer Data Processed by Swimlane on behalf of Customer in connection with the Services that consists of “personal data” or “personal information” (or analogous variations of such terms) under Data Protection Law.
- “Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.
- “Process” or “Processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
- “Processor” means the entity which processes Personal Data on behalf of the Controller.
- “Standard Contractual Clauses” means the Standard Contractual Clauses for Transfer of Personal Data to Third Countries approved by the European Commission Decision of June 4, 2021.
- “Sub-Processor” means any Processor engaged by Swimlane to assist in fulfilling its obligations with respect to the provision of the Swimlane Services under the Agreement.
- “Swimlane” means Swimlane, Inc., a Delaware corporation with its principal place of business at 363 Centennial Parkway, Suite 210, Louisville, CO 80027.
- “Swimlane Service” means the cloud-based version of the Swimlane proprietary software to which Licensee is granted access as provided in the Agreement.

2. Customer Responsibilities

a. Compliance with Laws. Within the scope of the Agreement, Customer will be responsible for complying with all requirements that apply to it under applicable Data Protection Laws with respect to its Processing of Personal Data and the Instructions Customer issue to Swimlane. Customer acknowledges and agrees that it is solely responsible for: (1) the accuracy, quality, and legality of all Personal Data; (2) the means by which Customer acquires, collects, and uses Personal Data; (3) ensuring that Customer has the legal basis to transfer, or provide access to, the Personal Data to Swimlane for

Processing in accordance with the terms of the Agreement (including this DPA); (4) ensuring that all Instructions to Customer for the Processing of Personal Data comply with applicable laws, including Data Protection Laws.

b. Controller Instructions. Customer agrees that the Agreement (including this DPA), along with its use of the Swimlane Service, constitute its complete Instructions to Swimlane in relation to the Processing of Customer Personal Data.

c. Security. Customer is responsible for independently determining whether the data security provided for the Swimlane Service meets its obligations under applicable Data Protection Laws. Customer also is responsible for its secure use of the Swimlane Service. Swimlane makes many security controls available to ensure Customer's secure use of the Swimlane Service.

3. Swimlane Obligations

a. Compliance with Instructions. Swimlane will only Process Customer Personal Data for the purposes described in this DPA or as agreed within the scope of Customer's lawful Instructions, unless otherwise required by applicable law. Swimlane is not responsible for compliance with any Data Protection Laws applicable to Customer or its industry that are not generally applicable to Swimlane.

b. Conflict of Laws. If Swimlane becomes aware that it cannot Process Customer Personal Data in accordance with Customer's Instructions due to a legal requirement under any applicable law, Swimlane will (1) promptly notify Customer to the extent permitted by law; (2) where necessary, cease processing (with exception for providing security over stored data-at-rest) until Customer issues new Instructions consistent with applicable law. If a conflict of law arises, Swimlane will not be liable to Customer under the Agreement for any failure to perform the Swimlane Services until Customer issues new lawful Processing Instructions to Swimlane.

c. Security. Swimlane will implement and maintain technical and organizational controls to protect Customer Personal Data as described in the Annex II of this DPA. Swimlane may update Security Measures in its reasonable discretion provided that the update does not have a material degradation in the protection offered by the Security Measures existing at the start of the Agreement.

d. Confidentiality. Swimlane will ensure that personnel authorized by Swimlane to Process Customer Personal Data are subject to appropriate confidentiality obligations.

e. Personal Data Breach Notification. Swimlane will notify Customer without undue delay, but in no event longer than 48 hours, after becoming aware of any Personal Data Breach. Taking into account the nature of Processing and the information available to Swimlane, Swimlane will assist Customer in ensuring compliance with the notification obligations under Data Protection Law (Articles 33 and 34 of the GDPR).

f. Deletion or Return of Personal Data. Swimlane will delete all Customer Data on termination or expiration of the Swimlane Service in accordance with the Agreement. All Customer Data will be deleted from Swimlane systems with the exception of Customer Data that Swimlane is required to retain by applicable law. This data includes, but is not limited to, Source IP, UserAgent and UserId data in all customer cloud environments via audit logs with which Swimlane retains for one (1) year after the date of termination of services.

Customer may make Data Subject Access Requests (DSARs) to Swimlane by contacting privacy@swimlane.com.

4. Sub-Processors

Customer agrees that Swimlane may engage Sub-Processors to Process Customer Data on Customer's behalf. Swimlane's current Sub-Processors are identified in Annex III of this DPA. Swimlane imposes data protection terms on the Sub-Processors that provide at least the same level of protection for Customer Personal Data as those in this DPA. Swimlane will notify Customer or any additional or replacement Sub-Processors no less than 30 days prior to the effective time of any such changes.

5. Data Transfers

Customer acknowledges and agrees that Swimlane may access and Process Customer Data on a global basis as necessary to provide the Swimlane Service in accordance with the Agreement, and in particular that Customer Personal Data may be transferred to and Processed by Swimlane in the United States and in other jurisdictions where Swimlane's Sub-Processors have operations. Wherever Personal Data is transferred outside its country of origin, each party will ensure such transfers are made in compliance with the requirements of Data Protection Laws. With regard to transfers of Personal Data from the European Economic Area and/or their member states, Switzerland, and/or the United Kingdom (UK) to a country which does not ensure an adequate level of data protection within the meaning of Data Protection Law, to the extent such transfers are subject to such Data Protection Law, such transfer will be made pursuant to the relevant approved transfer mechanisms in accordance with Article 46 of the GDPR.

6. Data Protection Impact Assessment

Swimlane shall provide Customer with commercially reasonable cooperation and assistance needed to fulfill its obligation under GDPR to carry out a data protection impact assessment related to Customer's use of the Swimlane Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent Swimlane has access to such information. For more information, please contact privacy@swimlane.com.

7. Audit Rights

a. Customer Audits. Customer may engage a nationally recognized independent auditor to audit Swimlane's compliance with this DPA, at a mutually agreed time following no less than 30 days' prior written notice. Customer shall bear all of its own costs (or costs of the representative) of conducting the audit. Swimlane will provide personnel reasonably necessary to perform the audit effectively. The auditor conducting such audit will (and Customer will be responsible for ensuring that the auditor will): (1) comply with reasonable and applicable on-site policies and procedures provided by Swimlane, (2) sign a standard confidentiality agreement with Swimlane, and (3) not unreasonably interfere with Swimlane's business activities. Customer will provide written communication of any audit findings to Swimlane, and the results of the audit will be the confidential information of Swimlane.

b. Audit Reports. At Customer's written request, and provided that the parties have an applicable NDA in place, Swimlane will provide Customer with copies of our most recent third-party audit reports.

8. Additional Provisions for California Personal Information

a. Scope. The 'Additional Provisions for California Personal Information' section of the DPA will apply only with respect to California Personal Information.

b. Roles of the Parties. When processing California Personal Information in accordance with Customer's Instructions, the parties acknowledge and agree that Customer is a Business, and Swimlane is a Service Provider for the purposes of the CCPA.

c. Responsibilities. The parties agree that Swimlane will Process California Personal Information as a Service Provider strictly for the purpose of performing the Swimlane Service under the Agreement (the "Business Purpose") or as otherwise permitted by the CCPA, including as described in the 'Usage Data' section of Swimlane's Privacy Policy.

9. Liability

Each party's liability under or in connection with this DPA shall be as set forth in the Agreement. For avoidance of doubt, any claims or actions arising out of this DPA shall be governed by the limitations and exclusions of liability as set forth in the Agreement.

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

Section I

Clause 1

Purpose and scope

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

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

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

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

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

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

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

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 – Optional
Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES
Clause 8
Data protection safeguards

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

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

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

8.6 Security of processing
(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more

information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

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

8.8 Onward transfers
The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([2]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:
(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.
Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance
(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data

exporter’s request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

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

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

Clause 9

Use of sub-processors

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

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

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

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

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

Clause 10

Data subject rights

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

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

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

Clause 11

Redress

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

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

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

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

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

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

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

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

Clause 12

Liability

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

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

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

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

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

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

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

Clause 13

Supervision

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

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

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

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

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

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

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

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

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

Clause 15
Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of _______ (*specify Member State*).]

Clause 18

Choice of forum and jurisdiction

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

(b) The Parties agree that those shall be the courts of _____ (*specify Member State*).

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

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

See page below for Annexes

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

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

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

[4] *As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider*

carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

ANNEX I

A. LIST OF PARTIES Data exporter(s):

Name: Customer, as defined in the header of the DPA.

Address: as specified in the applicable Order Form(s)

Contact person's name, position and contact details: as specified in the applicable Order Form(s)

Activities relevant to the data transferred under these Clauses: The data is utilized to allow Customer to build low-code security orchestration, automation, and response playbooks using Customer's third-party system integrations.

Signature and date:

____

Role (controller/processor): controller

Data importer(s):

Name: Swimlane, Inc.

Address: 999 18th St, Suite 2201N, Denver, CO 80202

Contact person's name, position and contact details: Ashok Shah, CFO & DPO, privacy@swimlane.com

Activities relevant to the data transferred under these Clauses: Processing data for purposes of fulfilling business-to-business contracts.

Signature and date:

____

Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred:

Customer may submit Personal Data in the course of using the Swimlane Service, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

Contacts and other end users including employees, contractors, collaborators, customers, prospects, suppliers, and subcontractors. Data Subjects may also include individuals attempting to communicate with or transfer Personal Data to Customer's end users.

Categories of personal data transferred:

The types of Customer Personal Data collected are dependent on Customer's use of and interaction with the Swimlane Services. Examples can include, but are not limited to first name, last name, e-mail address and issues or queries.

The Swimlane Enterprise Security Operations Center collects Source IP, User-Agent and UserId data in all customer cloud environments via audit logs for the protection and security posture management of the Swimlane cloud infrastructure.

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:

Swimlane and Customer do not anticipate the transfer of sensitive data.

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

Continuous, as required for the Services.

Nature and purpose of the processing:

The data is utilized to allow Customer to build low-code security orchestration, automation, and response playbooks using Customer's third-party system integrations.

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

Subject to the 'Deletion or Return of Personal Data' section of this DPA, Swimlane will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

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

As specified in the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

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

Supervisory Authority of the EU country in which the data exporter is located.

Note: *When executing this DPA between Swimlane and a Customer not located in the European Union, Section C Competent Supervisory Authority is irrelevant and all disputes will be handled per Section 10.8 Governing Law within the Agreement.*

ANNEX II

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

Description of the technical and organizational measures implemented by the 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.

Swimlane's technical and organisational measures for data security and privacy are outlined in the control table below:

Control Family Name	Control Details

Cybersecurity & Data Privacy Governance	● Executive leadership, Board, and CISO oversee security program ● Annual review of risks, internal control KPIs, risk treatment plans, and internal audit findings ● GRC team manages policies, audits, and compliance governance ● DPO oversees privacy program aligned to GDPR and US privacy laws
Artificial and Autonomous Technology	● AI impact assessment performed annually and aligned with ISO42001 and ISO42005 ● AI asset inventory maintained ● AI product features undergo input and output validation testing ● Model performance monitoring is conducted prior to each new release ● Red teaming on AI assets based on OWASP Top 10 for LLM
Asset Management	● Unified CMDB/ITAM tracks all Identities, Mobile Devices, Enterprise IT Assets, Cloud Infrastructure, Third-Party Systems, and Data Stores ● CMDB/ITAM are continuously updated in near real-time ● All assets are classified and labeled based on Business Criticality, Mission Assurance Category & Data Sensitivity
Business Continuity & Disaster Recovery	● Written BC/DR plan reviewed annually ● DR tabletop exercise performed annually ● Cloud architected with redundancy and regional failover ● Kubernetes-based fault tolerance ● Backup restoration testing performed at least annually ● Cloud backup and snapshot retention schedule as follows: *Hourly Snapshots are retained for 3 days / Daily Snapshots are retained for 8 days / Weekly Snapshots are retained for 5 weeks / Monthly Snapshots are retained for 3 months and then automatically deleted*.
Capacity & Performance Planning	● Kubernetes clusters with redundancy and Helm packaging ensure scalability ● AWS multi-region deployment options for customers
Change Management	● Formal change management policy aligned with secure SDLC ● All changes logged in ticketing system ● Testing in non-production required ● Documented approvals before release

Cloud Security	● Hosted on AWS ● Customer data logically separated ● Encryption in transit (TLS 1.2/TLS 1.3) and at rest (AES-256) ● AWS KMS for key management ● Tenant-level isolation ● Cloud instances hardened to CIS benchmarks ● Cloud infrastructure monitored with CNAPP/CDR & CSPM
Compliance	● Third-party audits for SOC 2 Type II, ISO/IEC 27001:2022, ISO/IEC 27701: 2019, and ISO/IEC 42001:2023 ● Common controls framework maintained internally and mapped against SOC 2, ISO27001, ISO27701, ISO42001 NIST 800-171, NIST 800-53, PCI-DSS, HIPAA, and GDPR
Configuration Management	● Infrastructure-as-code (IaC) (Terraform, Helm, Kustomize, and CloudFormation) ● CNAPP/CDR/CSPM tools enforce continuous secure configurations on cloud and Kubernetes infrastructure ● SSPM tools monitoring of our Corporate SaaS systems for posture, drift, and configuration changes
Continuous Monitoring	● 24/7 SOC monitoring and automated playbooks developed for incident investigation, triage, and remediation ● Cloud activity log monitoring (365 days retention) with anomaly detection ● Cloud observability and performance monitoring tools configured to trigger alerts when pre-defined thresholds are breached
Cryptographic Protections	● AES-256 encryption at rest ● TLS 1.2/ mTLS 1.3 encryption in transit ● AWS KMS key management ● SHA1+salt for Swimlane application password storage ● JWT authentication for Swimlane APIs
Data Classification & Handling	● Data classified as Public, Internal, Confidential, Restricted, CIU Restricted ● Stricter requirements for higher levels; encryption + network and privileged access controls ● Required data labeling on corporate file storage and collaboration tools

Endpoint Security	● EDR + MDM tools enforce anti-malware, encryption, OS patching, device lock, and other automated device posture checks ● EDR does hourly polling against baseline for all devices ● Non-compliant devices are flagged by the SOC and Enterprise IT ● Zero-Trust Network Access (ZTNA) is required on all devices to access corporate and production networks (Policy Management)
Human Resources Security	● Background checks required for employees (criminal, education, employment) ● Confidentiality agreements ● Mandatory annual SAT training for all employees ● Disciplinary measures for violations
Identification & Authentication	● Identities centrally managed via IAM tool ● Role-Based Access Control (RBAC) and least privilege enforced on corporate and production systems and accounts ● SSO/SAML authentication for corporate and production systems based on risk ● MFA mandatory for all corporate user accounts and system admin accounts ● Password policy as follows: o 16-character minimum o Complexity requirements (uppercase, lowercase, number, symbol) o Lockout after four failed attempts (60-minute reset period) o Credential sharing is strictly prohibited unless an approved exception is documented o Passwords required to be stored in company-managed password manager o Password for one time use and/or password reset requests are only valid for 72 hours after issuance and are invalid after password reset. o Password reset URLs are a random, unique value.

Incident Response	● Incident Response (IR) plan annually reviewed and externally assessed by a third party CMMI audit ● IR plan tested annually through a mandatory tabletop exercise ● Pre-defined playbooks for incident triage, notification, and law enforcement coordination ● Breach notification to customer is required within no longer than 48 hours after identification
Information Assurance	● Internal audits conducted based on annual audit plan ● Customer can request access to security artifacts including external audit reports, internal policies, and pen test summaries
Mobile Device Management	● Corporate devices managed by MDM ● MDM tools configured to remotely block and/or wipe data on managed devices in real-time if needed
Network Security	● Zero-Trust VPN with device posture checks enforced to gain access to corporate and production networks ● Network segmentation for office, corporate, cloud, and production environments ● IDS/IPS and WAF rules enforced on networks ● DNS filtering
Physical & Environmental Security	● HQ protected with physical, and digital badge access ● Visitor sign-in required in corporate HQ ● Monthly physical access reviews performed ● Restricted server room access ● Clean desk/screen enforced ***Note: Corporate HQ infrastructure does not host customer production environments, nor any systems that process customer data.***

Data Privacy	● Privacy program aligned with GDPR/CCPA regulations ● Data Subject Access Request (DSAR) process is defined ● Cookie consent management enabled on public-facing websites through a Consent Management Platform (Osano), including mechanisms for obtaining affirmative consent (where required), enabling users to modify or withdraw consent, and maintaining consent records in accordance with applicable Data Protection Laws. ● Sub-processor change notification process is defined ● Law enforcement/government privacy request handling process is defined ● Data Protection Impact Assessment (DPIA) required prior to major product releases
Project & Resource Management	● Security objectives integrated into annual leadership planning ● Cross-team responsibilities defined (IT, Security, Infra, GRC, Engineering, HR)
Risk Management	● Annual risk assessment and risk treatment plan performed by leadership ● Risks are logged in a centralized risk register ● Decisions to accept, transfer, or mitigate risks require leadership approval
Secure Software Development Framework (SSDF) Standard	● Secure SDLC document is maintained ● Separation of duties enforced on production code repositories and CI/CD pipeline ● Code PRs require secrets scanning, peer review, automated SAST/DAST scanning, and dependency checks ● Critical and High priority vulnerabilities identified must be remediated prior to deploying new releases
Security Operations	● Dedicated SOC team monitors alerts, logs, IAM anomalies ● 24/7 monitoring of infrastructure and applications
Security Awareness & Training	● Annual mandatory security awareness training includes phishing, acceptable use, access management, and data protection modules ● Secure code training required for engineering personnel ● AI security training required for personnel involved in AI/LLM development ● Security awareness training is monitored for completion by GRC team

Third-Party Management	● Vendor onboarding risk assessment ● Annual security reassessment for high-risk vendors ● Vendor access via SSO/SAML ● Vendor inventory is maintained and reviewed at least annually
Threat Management	● SOC leverages threat intel feeds (C2, Tor infra, exploits, malware) to enrich alerts ● Proactive threat hunting is conducted by security based on industry and/or newsfeeds
Vulnerability & Patch Management	● Vulnerability scans run daily and findings are aggregated for remediation monthly ● Vulnerability remediation prioritized by CVSS/EPSS criticality exploitability + reachability, asset criticality and data sensitivity ● Vulnerabilities are defined and categorized by a risk impact rating ● Third-party pen tests conducted at least annually ● IaC (Terraform, Helm, ArgoCD) leveraged to roll out patched workloads consistently ● Patches are tested in staging environment prior to deployment in production
Web Security	● Customer environments protected by WAF + IDS/IPS ● TLS 1.2 or higher enforced for all traffic ● Bug bounty program for web vulnerabilities ● APIs secured with standard security protocols
Customer System Access & Data Protection	● Customer data access restricted to authorized staff with privileged request tickets ● User activity in Swimlane applications is logged and audited ● Access to underlying cloud and database infrastructure is restricted to authorized personnel based on RBAC and least privilege ● Technical troubleshooting and break glass procedures require customer notification and a root-cause-analysis (RCA) summary be provided

ANNEX III
LIST OF SUB-PROCESSORS

Swimlane uses the following sub-processors. Please note that Swimlane products generally use a subset of these. For security and privacy purposes, further details about Sub-processors specific to Customer's Swimlane services, locations, or the types of processing these entities perform may be requested by emailing privacy@swimlane.com.

Sub-Processor	Nature and purposes of processing & transfer	Location of processing (and, where applicable, transfer)	Frequency and duration of Processing	Security Measures of Sub-processor
Amazon Web Services, Inc.	Infrastructure & Security	USA. Data Center region located in the region selected by the customer.	Continuous & Ongoing	https://aws.amazon.com/trust-center/
Salesforce	Customer Relationship Management	USA	Continuous & Ongoing	https://trust.salesforce.com/en/
Elastic	Infrastructure & Security	USA	Continuous & Ongoing	https://www.elastic.co/trust
Google Workspace	Collaboration & Communication	USA	Continuous & Ongoing	https://cloud.google.com/trust-center
Slack	Collaboration & Communication	USA	Continuous & Ongoing	https://slack.com/trust
MongoDB	Application DBaaS	USA. Data Center region located in the region selected by Customer.	Continuous & Ongoing	https://www.mongodb.com/products/platform/trust

Atlassian	Incident Response Ticketing System	USA	Continuous & Ongoing	https://www.atlassian.com/trust
Freshworks	Customer Helpdesk Ticketing System	USA	Continuous & Ongoing	https://trust.freshworks.com/
Pendo	Product feedback and analytics platform	USA	Continuous & Ongoing	https://trust.pendo.io/