ANAPLAN DATA PROCESSING ADDENDUM
(Client)

Last modified: February 25, 2025

This Data Processing Addendum ("DPA") is incorporated into the Anaplan SaaS Subscription Agreement or other written or electronic agreement separately entered into by Client and Anaplan Limited or Anaplan, Inc. (as relevant) ("Anaplan") concerning Client's use of the Anaplan Service and/or Professional Services (the "Agreement") to reflect the parties' agreement regarding the Processing of Personal Data in accordance with Data Protection Laws.

This DPA consists of the Data Processing Terms, and any Attachments.

Except for the provisions of this DPA expressly stated to survive termination, this DPA will automatically terminate upon the termination of the Agreement (or Order Schedule, as applicable), or earlier if terminated pursuant to the terms of this DPA.

Anaplan

DATA PROCESSING TERMS

In the provision of the Anaplan Service and/or Professional Services (together, the "Services") to Client pursuant to the Agreement, Anaplan may process Personal Data on behalf of Client. Anaplan agrees to comply with the following provisions with respect to any Personal Data submitted by or for Client to the Services or collected and processed by or for Client using the Services.

1. **Definitions.** Any capitalized term used but not defined in this DPA has the meaning provided to it in the Agreement.
   (a) **"Account Data"** means Personal Data, including the names and contact information of Authorized Users of the Anaplan Service relating to Client's relationship with Anaplan. Account Data is used for the purposes of managing the Client's account, account authentication and verification, support, investigating and preventing system abuse, or fulfilling legal obligations.
   (b) **"Client Data"** means data that is submitted to the Anaplan Service by or on behalf of Client, including without limitation: (i) Client's content, including model data and dashboards provided or submitted by Client or Authorized Users to or through the Anaplan Service for processing (ii) the outputs and modifications to that data obtained from such processing, and (iii) Personal Data that Anaplan processes as a Processor on behalf of Client. Client Data does not include Metadata or Account Data.
   (c) **"Data Controller"** or **"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.
   (d) **"Data Processor"** or **"Processor"** means the entity which processes Personal Data on behalf of the Controller.
   (e) "**Data Protection Laws**" means one or more of the following as may be applicable to the Personal Data processed by Anaplan: the Data Protection Act 2018 (UK), General Data Protection Regulation ("**GDPR**") means: (i) where applicable the General Data Protection Regulation (EU) 2016/679 ("**EU GDPR**"); (ii) where applicable the EU GDPR as implemented into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"), the Swiss Federal Act on Data Protection ("**FADP**"); California Consumer Privacy Act ("**CCPA**" and subsequent California Privacy Rights Act of 2020 "**CPRA**"); Colorado Privacy Act ("**ColoPA**"); Connecticut Personal Data Privacy and Online Monitoring Act ("**CPOMA**"); Utah Consumer Privacy Act ("**UCPA**"); Virginia Consumer Data Protection Act ("**VCDPA**"); the Personal Information Protection and Electronic Documents Act of Canada ("**PIPEDA**"); Australian Privacy Principles and the Australian Privacy Act (1988); the Act on the Protection of Personal Information ("**APPI**"); the Personal Data Protection Act 2012 ("**PDPA**"), and in each case shall include any equivalent legislation in such jurisdictions which shall apply to Processing of Personal Data, in each case as amended, extended or re-enacted from time to time and all orders, regulations, statutes, instruments or other subordinate legislation made thereunder in the European Union ("**EU**"), the European Economic Area ("**EEA**") and their member states, Switzerland, the United Kingdom ("**UK**"), the United States ("**US**"), Canada, and any other country where Anaplan may Process Personal Data from time to time.
   (f) **"Metadata"** means system, administrative and descriptive metadata, usage and activity data related to Client's use of the Anaplan Service, or other data collected as part of the normal operation of the Anaplan Service. Metadata is processed for the purposes of operating the Anaplan Service, monitoring and maintaining performance, improving, or promoting the Anaplan Service.
   (g) "**Personal Data**" or "**Personal Information**" means any information, including personal information, relating to an identified or identifiable natural person ("**Data Subject**").
   (h) **"Personal Data Breach"** means a breach leading to any accidental, unauthorized or unlawful loss, disclosure, destruction, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed by Anaplan. A Personal Data Breach shall not include an unsuccessful attempt or activity that does not compromise the security of Personal Data, including (without limitation) pings and other broadcast attacks of firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents.
   (i) **"Processing"** or **"Process"** means any operation or set of operations performed upon Personal Data, whether or not by automatic means, such as collection, recording, securing, organization, storage, adaptation or alteration, access to, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.
   (j) "**Restricted Transfer**" means: (i) where the EU GDPR applies, a transfer of personal data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy decision by the European Commission; (ii) where the FADP applies, a transfer of personal data from Switzerland to a country outside of the European Economic Area which is not subject to an adequacy decision by the European Commission; and (iii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not subject to adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

(k) "**Standard Contractual Clauses**" means where the EU GDPR applies, the standard contractual clauses adopted by the European Commission pursuant to Commission Decision C/2021/3972 for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU Standard Contractual Clauses**" or "**EU SCCs**");
(l) **"Sub-processor"** means (a) Anaplan, when Anaplan is processing Client Data and where Client is itself a processor of such Client Data, or (b) any third-party Processor engaged by Anaplan or its Affiliates to assist in fulfilling Anaplan's obligations under the Agreement and which processes Client Data. Sub-processors may include third parties or Anaplan Affiliates but shall exclude Anaplan employees, contractors or consultants.
(m) **"UK Addendum**" means the International Data Transfer Addendum to the EU Standard Contractual Clauses issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, as such Addendum may be revised under Section 18 therein.
(n) The terms "**Business**", "**Commercial Purpose**", **"Consumer", "Contractor", "Service Provider**", "**Sell", "Share", "Third Party",** and "**Verifiable Consumer Request**" shall bear the respective meanings given them in the applicable Data Protection Laws.

2. Scope and Roles.
(a) This DPA applies when Personal Data is Processed by the Anaplan Service on behalf of Client.
(b) The parties acknowledge and agree that, notwithstanding the terms of section 2 (f) of this DPA, regarding the Processing of Personal Data, Client is the Data Controller and/or Processor, and data exporter, Anaplan is a Data Processor and/or Sub-processor, and data importer.
(c) Client acknowledges that it has exclusive control and responsibility for determining the means and purposes and what Personal Data Client submits to the Anaplan Service and where Client is itself Processor acting on behalf of or jointly with a third-party Controller (or other intermediary) Client represents and warrants that Client's instructions and actions with respect to that Client Personal Data, including its appointment of Anaplan as a Processor or Sub-processor, have been authorized by the relevant Controller or joint Controllers and further warrants it has all authority, grounds, rights and consents and permissions for submission and transfer of Personal Data and Processing by Anaplan and Anaplan's engagement of Sub-processors as described in Section 11 in this DPA and under the Agreement.
(d) The subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of data subjects shall be as set out in Schedule I to this DPA (which may be updated by the parties in writing from time to time) and Client warrants it is accurate.
(e) Client shall comply with the Data Protection Laws in relation to the Personal Data and Anaplan shall comply with the relevant provisions of the Data Protection Laws applicable to it as a Data Processor in respect of the Processing of Personal Data in accordance with these terms.
(f) The parties acknowledge that, regarding the processing of Account Data, Client is a Controller and Anaplan is an independent Controller, not a joint Controller with Client. Anaplan will process Account Data as a Controller (i) in order to manage the relationship with Client; (ii) carry out Anaplan's core business operations; (iii) in order to detect, prevent, or investigate security incidents, fraud, and other abuse or misuse of the Services; (iv) authentication; (v) to comply with Anaplan's legal or regulatory obligations; and (vi) as otherwise permitted under Data Protection Laws and in accordance with this DPA, the Agreement, and the Anaplan's Privacy Statement (https://www.anaplan.com/privacy-statement/).

3. Confidentiality. Anaplan shall ensure that the Anaplan personnel authorized to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4. Client Obligations. To the extent Client, in its use of the Anaplan Service, submits Personal Data to Anaplan, then Client as data exporter shall:
(a) use the Anaplan Service in compliance with the Agreement and the Data Protection Laws;
(b) ensure all instructions given by it to Anaplan in respect of the Processing of Personal Data are at all times in accordance with Data Protection Laws;
(c) ensure all Personal Data provided to Anaplan has been collected in accordance with Data Protection Laws;
(d) keep the amount of Personal Data provided to Anaplan to the minimum necessary for the provision of the Services;
(e) serve as the sole point of contact for Anaplan with regard to any third party Controllers of the Client Personal Data; Anaplan does not need to interact directly with (including seek any authorizations directly from) any such third party Controllers (other than through regular provision of the Services to the extent required by the Agreement); and where Anaplan would (including for the purposes of the EU SCCs) otherwise be required to provide information, assistance, cooperation, or anything else to

such third party Controllers, Anaplan may provide it solely to Client. Notwithstanding the foregoing, Anaplan is entitled to follow the instructions of such third party with respect to such third party's Client Personal Data instead of Client's instructions if Anaplan reasonably believes this is legally required under the circumstances.
(f) immediately forward to the relevant Controller any notice provided by Anaplan under Sections 5(a), 5(d), 9(b), 11(c) or that refers to the EU SCCs.

5. **Anaplan Obligations.** To the extent Client, in its use of the Anaplan Service, submits Personal Data to Anaplan, then as Data Processor, Anaplan shall:
(a) Process Personal Data as a Data Processor in accordance with Client's documented instructions as set out in this Agreement/Order, Schedule I to the Standard Contractual Clauses (where applicable), and this DPA. Anaplan will promptly notify Client if Anaplan reasonably believes that Client's instructions are inconsistent with Data Protection Laws, unless the law prohibits such information on important grounds of public interest;
(b) assist Client as reasonably needed to respond to requests from supervisory authorities, Data Subjects, customers, or others to provide information related to Anaplan's Processing of Personal Data;
(c) where applicable, act as a Sub-processor of such Personal Data;
(d) notify Client if it receives a request from a Data Subject for access, correction, portability, objection, restriction, or deletion of that Data Subject's Personal Data;
(e) not respond to any request from a Data Subject without the Client's prior consent unless required by law, except to redirect the Data Subject to the Client;
(f) taking into account the nature of Processing and the information available to Anaplan, provide Client with reasonable assistance to enable compliance by Client with its obligations under Data Protection Laws with respect to:
    (i) security of Processing;
    (ii) data protection impact assessments (as such term is defined by EU GDPR);
    (iii) prior consultation with a supervisory authority regarding high-risk Processing; and
    (iv) notifications to the applicable supervisory authority and/or communications to Data Subject by Client in response to any Personal Data Breach;
(g) ensure that it enters into a written agreement with each Sub-processor of Personal Data on terms substantially equivalent to the terms of this DPA;
(h) following termination of the Agreement delete the Personal Data in accordance with the section of the Subscription Agreement that describes treatment of Client Data following expiration or termination unless continued retention and Processing is required or is permitted by Data Protection Laws.

6. **Data Transfer.** Client acknowledges and agrees that Anaplan and its Sub-processors may transfer and Process Personal Data to and in the United States and other locations in which Anaplan, its Affiliates, or its Sub-processors (as more particularly described in Anaplan's list of Sub-processor, found at https://www.anaplan.com/legal/platform-subprocessors or such successor URL as may be designated by Anaplan and communicated to Client) maintain data Processing operations and provided that Anaplan complies with the terms of the Agreement and this DPA relating to the Processing of and security of such Personal Data. Anaplan shall ensure that such transfers are made in compliance with applicable Data Protection Laws and this DPA.

7. **Transfer Mechanism.** The parties agree that when the transfer of Data from Client to Anaplan is a Restricted Transfer it shall be subject to the appropriate Standard Contractual Clauses which shall be deemed incorporated into and form part of this DPA, as follows:
(a) in relation to data that is protected by the EU GDPR, the EU Standard Contractual Clauses will apply as follows:
    (i) Module Two (Controller to Processor) or Module Three (Processor to Processor) shall apply (as applicable);
    (ii) in Clause 7, the optional docking clause shall apply;
    (iii) in Clause 9, Option 2 shall apply, and the time period for prior notice of Sub-processor changes shall be ten (10) days;
    (iv) in Clause 11, the optional language shall not apply;
    (v) in Clause 17, Option 1 shall apply, and the EU SCCs will be governed by the law of Netherlands;
    (vi) in Clause 18(b), disputes shall be resolved before the courts of Netherlands;
    (vii) the provisions of Schedule I will be deemed to be set out in Annex I to the EU SCCs;

(viii) the provisions of Schedule II (Technical and organizational security measures) to this DPA will be deemed to be set out in Annex II to the EU SCCs;

(ix) the provisions of Schedule III (List of Sub-Processors) to this DPA will be deemed to be set out in Annex III to the EU SCCs; and

(b) in relation to data that is protected by the FADP, the EU Standard Contractual Clauses will apply as follows:

(i) the EU SCCs, completed as set out above in Section 7(a) of this DPA shall apply accordingly as applicable, subject to sub-clause (ii) below;

(ii) the term '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 these EU SCCs;

(iii) references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland", or "FADP" (as applicable)

(iv) references to the "Regulation (EU) 2016/679" are to be understood as references to the FADP, insofar as the data transfers underlying these EU SCCs are subject to the FADP;

(v) the provisions of the EU SCCs and all annexes also protect the data of legal entities to the extent that these provisions are applicable to them under the FADP;

(vi) references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland";

(vii) in Clause 17, the Standard Contractual Clauses shall be governed by the laws of Switzerland; and

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

(c) in relation to data that is protected by the UK GDPR, the EU SCCs will apply as follows:

(i) apply as completed in accordance with paragraph 7(a) above; and

(ii) be deemed amended as specified by Part 2 of the UK Addendum, which shall be deemed incorporated into and form an integral part of this DPA. In addition, tables 1 to 3 in Part 1 of the UK Addendum shall be completed respectively with the information set out in Schedule I and Schedule II of this DPA and table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party".

8. Security Responsibilities.

(a) Anaplan is responsible for implementing and maintaining the technical and organizational measures for the Anaplan Service as described in the security standards designed to help Client secure Personal Data against unauthorized Processing and accidental or unlawful loss, access or disclosure, which can be found in Schedule II (Technical and Organizational Security Measures) and at https://www.anaplan.com/legal/policies/security.

(b) Client acknowledges that the security measures are subject to technical progress and development and that Anaplan may update or modify the security measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Service provided to Client.

9. Breach Notification.

(a) Anaplan maintains security incident management policies and procedures specified in the security documentation;

(b) Anaplan shall notify Client at: _____ within 48 hours of confirmation of a Personal Data Breach relating to Client's Personal Data. Anaplan shall provide all such timely information and cooperation as Client may reasonably require in order for Client to fulfil its Personal Data Breach reporting obligations under Data Protection Laws. Anaplan shall further take such measures and actions as it considers necessary or appropriate to remedy or mitigate the effects of the Personal Data Breach and shall keep Client informed in connection with the Data Breach;

(c) Anaplan shall reasonably cooperate with Client in any post-incident investigation, remediation, and communication efforts.

10. Certifications and Audits.

(a) Anaplan shall make available to Client such information as is reasonably necessary to demonstrate Anaplan's compliance with the obligations of this DPA and the obligations under applicable Data Protection Laws;

(b) For the Anaplan Service, during the term of the Agreement, Anaplan will engage independent third-party auditors to perform regular audits (at least annually) and provide an Audit Report (SOC 1 Type 2 and/or SOC 2 Type 2 report) and/or ISO certificate/attestation;

(c) Upon Client's written request but no more than twice annually, and subject to the confidentiality obligations set forth in the Agreement, Anaplan shall provide a copy of Anaplan's then most recent Audit Report or ISO certificate/attestation, or any summaries thereof, that Anaplan generally makes available to its clients at the time of such request.
(d) To the extent that Anaplan's provision of an Audit Report does not provide sufficient information or Client is required to respond to regulatory authority audits, Client agrees to a mutually agreed-upon audit plan with Anaplan that (i) defines the mutually agreed-upon scope, timing and duration of the audit; (ii) ensures the use of an independent third party; (iii) provides notice to Anaplan in a timely fashion; (iv) requests access only during business hours; (v) accepts billing to Client at Anaplan's then current rate; (vi) occurs no more than once annually; (vii) restricts its findings to only data relevant to Client; and (viii) obligates Client, to the extent permitted by law or regulations, to keep confidential any information gathered that, by its nature, should be confidential.
(e) Client acknowledges and agrees that any exercise of its audit rights under Clause 8.9 of the Standard Contractual Clauses will be conducted on accordance with this DPA.

11. Sub-processors.

(a) Client consents to Anaplan engaging Sub-processors in relation to the Personal Data as currently set out in Anaplan's list of Sub-processors found at https://www.anaplan.com/legal/platform-subprocessors, where Client may subscribe to receive notifications of new Sub-processors for the Anaplan Service. If Client subscribes, Anaplan shall provide notification of a new sub-processor(s) before permitting any new Sub-processor(s) to Process Personal Data in connection with the provision of the Anaplan Service.
(b) All Sub-processors are required to abide by substantially equivalent obligations as Anaplan under this DPA as applicable to their performance of the Anaplan Service.
(c) Client may object to Anaplan's use of a new Sub-processor by notifying Anaplan promptly in writing within ten (10) business days after receipt of Anaplan's notice in accordance with the mechanism set out in this Section 11.
(d) In the event Client objects to a new Sub-processor, as permitted in the preceding sentence, Anaplan will use reasonable efforts to make available to Client a change in the Services or recommend a commercially reasonable change to Client's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Client. If Anaplan is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Client may terminate the applicable Order Schedule(s) without liability with respect only to those Services which cannot be provided by Anaplan without the use of the objected-to new Sub-processor by providing written notice to Anaplan and Client shall have no obligation to make any payment of subscription fees for the remaining portion of the Subscription Term under the Agreement.

12. Miscellaneous.

(a) If there is a conflict between the Agreement and this DPA, the terms of this DPA will prevail. To the extent there is any conflict between the Standard Contractual Clauses, and any other terms in this DPA or the Agreement, the provisions of the Standard Contractual Clauses will prevail.
(b) Any claims brought in connection with this DPA will be subject to the exclusions and limitations set forth in the Agreement, except for any liability which cannot be limited or excluded under Data Protection Laws.
(c) Notwithstanding anything to the contrary in this Addendum or in the Agreement (including, without limitation, either party's indemnification obligations), neither party will be responsible for any GDPR fines issued or levied under Article 83 of the GDPR against the other party by a regulatory authority or governmental body in connection with such other party's violation of the GDPR.
(d) Notwithstanding anything to the contrary in this Addendum or in the Agreement (including, without limitation, either party's indemnification obligations), neither party will be responsible for any UK GDPR fines issued or levied under Article 83 of the UK GDPR against the other party by a regulatory authority or governmental body in connection with such other party's violation of the UK GDPR.

Anaplan

Schedule I

A. LIST OF PARTIES

Controller/ Data exporter(s): As identified in the Agreement.

Controller/ Data exporter is (i) the legal entity that has subscribed to the Anaplan Service (which allow its Users to enter, amend, use, delete or otherwise process Personal Data as contemplated under the Agreement) and executed this DPA as a Controller/ Data exporter.

Data importer(s): Privacy Office, privacy@anaplan.com

1.
Anaplan, Inc. and its sub-processor is a provider of enterprise cloud computing planning and modelling solutions which processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement.
OR (as applicable);
2.
Anaplan Limited. and its sub-processor is a provider of enterprise cloud computing planning and modelling solutions which processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

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

- Prospects, Clients, business partners and vendors of data exporter (who are natural persons)
- Employees or contact persons of data exporter's prospects, Clients, business partners and vendors
- Employees, agents, advisors, freelancers of data exporter (who are natural persons)
- Data exporter's Users authorized by data exporter to use the Anaplan Service

Categories of personal data transferred

Data exporter may submit Personal Data to the Anaplan Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- Account Data, including the names and contact information
- Metadata, including audit logs and usage data
- Such other categories which data exporter or data exporter's authorized users provide to Anaplan in accordance with the Agreement (e.g. customer support case details, in app communication/notification)

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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

- None

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

The data is being transferred on a continuous basis pursuant to the provisions and period of the SAAS Subscription Agreement agreed between the parties.

Nature of the processing

The objective of Processing of Personal Data by data importer is the performance of the Anaplan Service (SAAS Cloud platform services) pursuant to the Agreement.

Purpose(s) of the data transfer and further processing
The purpose of the transfer is the provision of the services described in this Schedule I to the DPA and in the SAAS Subscription Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
After the termination, Anaplan deletes data exporter's account after 30 days, including remaining data exporter's data, if any, from the Anaplan Service unless legally prohibited.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
As set out in the Anaplan SAAS Subscription Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

Where the data transfers are subject to the GDPR, the Dutch Autoriteit Persoonsgegevens shall be competent supervisory authority.
Where the data transfers are subject to the UK GDPR, the UK Information Commissioner shall be competent the supervisory authority.
Where the data transfers are subject to the Swiss Federal Act on Data Protection (FADP), the FDPIC shall be competent supervisory authority.

Anaplan

Schedule II

TECHNICAL, ORGANIZATIONAL, AND CONTRACTUAL MEASURES

Anaplan maintains integrity of data uploaded to the Anaplan Service, as described below and in the Security Documentation applicable to the specific Anaplan Service purchased by Client, and accessible via http://help.anaplan.com or otherwise made reasonably available by Anaplan including Anaplan's Data and Security Policy, which can be found at https://www.anaplan.com/legal/policies/security. Anaplan may change these at any time without notice by keeping a comparable or better level of security. This may mean that individual measures are replaced by new measures that serve the same purpose without materially diminishing the overall security of the Anaplan Service during a subscription term.

In addition, Anaplan provides contractual and organizational measures which reflect the supplemental measures and support the safeguards provided by the Standard Contractual Clauses and the relevant legislation of the third country where Personal Data is transferred (destination country). Although contractual and organizational measures alone will not overcome access to personal data by Public Authorities of the relevant third country, they may complement the technical measures and strengthen the level of data protection taking into account the nature, scope, context, and purpose of the processing and the risks for the rights and freedoms of natural persons.

1. Technical and Organizational Security Measures	
Domain	**Measure**
1.1 Information Security Program	**Security Program.** Anaplan's Information Security Program is aligned with ISO 27001 standards and NIST 800-53 standards. **Risk Management.** Anaplan utilizes a formal risk management and treatment program and conducts periodic risk assessments of all systems and networks that process Client data. **Security Ownership.** Anaplan's Information Security organization is led by a Chief Information Security Officer who has identified individuals to coordinate and monitor security rules and procedures. **Auditing.** Anaplan undergoes SOC 1 Type II and SOC 2 Type II audits every six months, and ISO 27000 series audits annually. In addition, Anaplan undergoes third-party penetration tests by CREST-certified firms at least annually.
1.2 Pseudonymization	Anaplan does not have permissions to access customer data without the Client's explicit consent. All customer data that is housed within the Anaplan Service is the responsibility of Client and Client is expected to deploy appropriate technical measures to ensure proper compliance with regulations.
1.3 Encryption	**Encryption Protocols.** - All data in transit between Client and server is encrypted via HTTPS/TLS. - Key exchange is done via the browser using 2048-bit certificates. Session key length is negotiated by the end-user browser using the strongest available encryption. - Data at rest within the system is stored in a unique binary format and subject to full-disk AES-256 encryption. - Anaplan's BYOK service allows customers to define and manage unique encryption keys for their Anaplan workspaces.
1.4 Access and	**Access Authorization.**

Integrity	- Anaplan maintains a record of Anaplan Staff authorized to access Anaplan Systems that contain customer data. - Staff access to production infrastructure is permitted only with two-factor authentication via secure VPN. - Anaplan ensures that only authorized Anaplan Staff have access to systems that support the Anaplan Service. - Anaplan identifies Staff who may grant, alter, or cancel authorized access to Systems. **Access Limitations**. - Access is based on the information security principles of 'least privilege' and 'need to know' with access strictly limited to a select number of individuals. - Staff cannot see any Client Data without being granted permission by the end user-owner through the native access control system. **Access Logging**. - All changes by a user via the front end are documented in action logs and stored and/or deleted in accordance with statutory law (input control). - Changes are tracked within the Anaplan model, and the history is retained for the entire lifespan of the model. Access to this history is restricted to users authorized by Client. **Authentication**. - Anaplan uses standard industry practices to identify and authenticate users who attempt to access Anaplan systems. - Anaplan implements controls to ensure generated initial passwords are reset on first use and requires that passwords are changed every 90 days, or expire after a period of use. - Password must be a minimum of 8 characters, contain at least one uppercase character, one lowercase and one numeric character, changed every 90 days. - Anaplan implements a password policy that prohibits the sharing of passwords, outlines processes after disclosure of a password and ensures that de-activated or expired identifiers are not granted to other individuals. - Anaplan implements controls to revoke access after several consecutive failed login attempts and terminate a user session after a period of inactivity. - Anaplan supports denial of access to new users by default subject to Client's granting or enabling of end-user access. - Anaplan supports SAML 2.0 SSO (Single Sign-On) - Logical access to systems can only be made using multi-factor authentication via secure VPN; access to Anaplan-managed servers is further protected by the mandatory use of SSH public key infrastructure (PKI) technology. Centralized Identity Management (CIM) allows administrators to manage the users in their tenant within a unified dashboard to secure across users, data, and the environment. **Virtualization Protection.** – All virtual infrastructure is subject to a regular patching and maintenance routine and continuously monitored for vulnerabilities and security threats using industry-leading Cloud Security Posture Management (CSPM). – Anaplan controls and manages virtualized environments to ensure consistent configuration across the environments. These environments use Cloud Workload Protection (CWP) providing container runtime protection, threat monitoring and alerting. **Data Carriers**. Data carriers are subject to strict security guidelines for any transport or destruction.
1.5 Training	**Information Security Training**. Anaplan Staff with access to systems holding Client Data are provided

	with information security awareness training. Such training includes identifying security vulnerabilities and threats to business operations and responsibilities when using a device on the Anaplan network. **Privacy Awareness Training.** Anaplan provides Anaplan Staff with privacy awareness training which includes obligations when collecting and processing Personal Data and responsibilities when sharing data internally and externally.
1.6 Confidentiality	**Confidentiality Obligations**. - All Staff with access to Anaplan's systems are regularly trained and bound by confidentiality undertakings. - Breaches of security guidelines are consistently followed up and are subject to disciplinary measures up to and including termination, depending on the severity of the breach. **Testing**. All systems are regularly controlled and tested by external service providers. **Data Destruction**. Anaplan maintains established rules for the safe and permanent destruction of Client Data that are no longer required. **Customer ID**. Each Anaplan Client receives its own customer ID. All datasets of the respective Client are stored under this ID. Due to the administration rights, Client can only access datasets which are assigned to its own ID. **Lifecycle**. Anaplan implements best practices to manage the secure lifecycle of systems and software from design, development, test, and use to discontinuation.
1.7 Incident Management	**Incident Monitoring.** Anaplan uses an electronic reporting and security system which monitors and reports every security-relevant incident (e.g., an unauthorized attempt to access systems) to the Cyber-Defense team.
1.8 Physical and Environmental Security	**Anaplan Private Cloud.** Anaplan's servers are located in a dedicated room of the colocation service provider. The primary data centers are backed up for disaster recovery purposes to a corresponding data center in the same region. United States data centers are backed up to United States disaster recovery data centers, and European data centers are backed up in Europe. - EU hosting locations: Germany and Netherlands - US Hosting locations: California and Virginia Prior to selection, each facility was subjected to a stringent assessment for the presence, implementation, and ongoing administration of physical security controls Entry to each facility requires prior authorization and a process of identification validation and biometric confirmation. Each facility is fully protected 24x7x365 by security guards, high-security perimeter protection, and video cameras. All access and activity are logged, recorded, and stored for no less than 30 days. Facilities have an annual audit by industry leading firms for ISO 27001 and SSAE 18 Type II compliance. Anaplan performs its own annual data center audits **Anaplan Public Cloud.** - Anaplan engages with third-party providers of cloud infrastructure as identified in our List of Subprocessors to operate the Anaplan Service. Anaplan's clients have the option to run their models in the public cloud. AWS hosting locations: US: Virginia, Ohio, and Oregon. EMEA: Ireland, Germany. APAC: Australia. For information security and data privacy measures, please see Amazon Compliance Certifications.

	Google hosting locations: US: Virginia and Iowa. APAC: Japan. Canada: Toronto and Montreal. For information security and data privacy measures, please see Google Cloud Trust Center. Microsoft Azure hosting locations: US East, North Europe, West Europe, Canada Central, Japan East Azure. For information security and data privacy measures, please see Privacy and Security Azure.
1.9 Availability and Resilience of Systems	**Backups**. - Client Data is stored with redundancy in mind, with each model store being replicated to a secondary unit that will assume responsibility in the event of a primary failure. - All data is held on a redundant disk encrypted storage using industry-standard AES-256 encryption technology. - Data is streamed in near-real time to backup and disaster recovery storage. **Resilience**. - Anaplan's data centers have uninterruptible power supply (UPS) and onsite power generation with guaranteed fuel delivery contracts. - Anaplan's systems are specifically designed to impede or prevent hacker attacks and cross-site scripting attempts. For this purpose, Anaplan regularly carries out simulated tests and audits. Anaplan servers are protected by a "defense-in-depth" security architecture consisting of next-generation firewalls, , Endpoint Detection and Response (EDR) which includes anti-virus/antimalware protection, DDoS protection monitoring, and logging and monitoring capabilities.
1.10 Disaster Recovery and Business Continuity	**Disaster Recovery Plan:** Anaplan maintains emergency and contingency plans for systems that process customer data and regularly test recovery capabilities. - Anaplan utilizes disaster recovery facilities that are geographically remote from primary data centers. In the event that production capabilities at the primary data centers become unavailable, the disaster recovery facilities would be enabled and brought online. Since customer data is already streamed and held at these facilities, recovery time is greatly decreased.

2. Contractual Measures	
Domain	**Measure**
2.1 Assessment	Anaplan assesses third-country legislation and practices that are relevant to the safeguards contained in the Standard Contractual Clauses and Schedule II to the best of Anaplan's knowledge and after using best efforts to obtain such information.
2.2 Transparency	Anaplan publishes a Transparency Report and provides Client with relevant information on requests received. Anaplan provides information about the requesting body, type of request, type of data requested, whether requests have been challenged and whether a disclosure was made. For information on Anaplan's relevant and documented experience with prior instances of requests for disclosure from public authorities, if any, please refer to our Transparency Report.

2.3 Notifications	If Anaplan receives a legally binding request or demand by a public authority to access Personal Data transferred pursuant to the Agreement, unless prohibited by law, Anaplan will notify Client in accordance with Anaplan's policies.
2.4 Notice of Change	Anaplan has assessed third-country transfers including onward transfers and has no reason to believe that the laws and practices in any third country including any country Anaplan or its sub-processors transfer Personal Data, prevent Anaplan from fulfilling its obligations under these Standard Contractual Clauses and Schedule II. If Anaplan reasonably believes that any existing or future enacted or enforceable laws and practices in the destination third country applicable to its Processing of Personal Data will have a substantial adverse effect on the obligations provided by these Standard Contractual Clauses and Schedule II, Anaplan will promptly notify Client as soon as it is aware. Anaplan shall use reasonable efforts to recommend a commercially reasonable change to Client's use of the Services to facilitate compliance with applicable laws and practices. If Anaplan is unable to make such a change available, Client may terminate the transfer of Personal Data of only those services which cannot be provided by Anaplan in accordance with applicable laws and practices.
2.5 Standard Contractual Clauses	Transfers are governed by Standard Contractual Clauses approved by the European Commission or Intra-company Agreements, which include these supplementary measures. Anaplan reviews, and, where necessary, adapts the supplementary measures it has periodically implemented to address data protection regulatory developments.
2.6 Backdoors	Anaplan has not built, and will not purposefully build, backdoors to enable government actors to access its data or information systems, and has not changed, and will not purposefully change, its processes in a manner that facilitates government access to data. Please see our Transparency Report for more information.

3. Organizational Measures	
Domain	**Measure**
3.1 Public Authority Request Policy	Anaplan maintains and implements an internal policy that governs the procedures Anaplan must undertake upon receiving a request for access from a Public Authority. Such procedures include an assessment by Anaplan Legal to determine whether the request is valid, legal, and consistent with Anaplan Policies and how to clarify, narrow or otherwise modify the request.
3.2 Data Privacy Framework ("DPF")	Anaplan Inc. ("Anaplan-U.S.") complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Anaplan-U.S. has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regards to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. Anaplan-U.S. has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regards to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. To learn more about the Data Privacy Framework ("DPF") program, and to view our certification, please visit https://www.dataprivacyframework.gov/s/.
3.3 APEC CBPRs and APEC PRP	Anaplan's privacy program has been certified under the Asia-Pacific Economic Cooperation ("APEC") Cross-Border Privacy Rules System ("CBPRs") and APEC Privacy Recognition for Processors ("PRP"), government-backed data privacy certifications that demonstrate compliance with internationally-recognized data privacy protections. Anaplan will process personal data in accordance with the

	Anaplan CBPR and PRP certifications, to the extent applicable. For more information about CBPRs and PRP, and to view our certifications, please visit https://cbprs.org/compliance-directory/.
3.4 Review	Anaplan adopts and reviews internal policies to assess the suitability of supplementary measures and implement additional or alternative solutions when necessary to ensure that an essentially equivalent level of Personal Data protection to that guaranteed within the EEA is maintained.
3.5 Onward transfer	Anaplan reviews onward transfers of Personal Data within the same or other third countries and suspends ongoing transfers when an essentially equivalent level of data protection to that afforded within the EEA cannot be guaranteed in the third country.
3.6 TRUSTe Enterprise Privacy Seal	Anaplan has been awarded and strives to maintain the TRUSTe Enterprise Privacy Seal signifying that Anaplan's Privacy Statement and associated practices related to Anaplan have been reviewed by TRUSTe for compliance with TRUSTe's program requirements, including transparency, accountability, and choice regarding the collection and use of Personal Data.
3.7 ISO Certifications	Anaplan has adopted the ISO 27000 framework as the basis for information security and privacy policies and maintains the following ISO 27000 certifications: 1. **ISO 27001**: International standard for information security, sets specifications for an effective Information Security Management System (ISMS). 2. **ISO 27017**: International information security framework for cloud service providers. 3. **ISO 27018**: International standard for protecting personal information in public clouds for cloud service providers. 4. **ISO 27701**: International standard for management of personally identifiable information.

Schedule III

LIST OF SUB-PROCESSORS

Please reference https://www.anaplan.com/legal/platform-subprocessors for the list of sub-processors.

Anaplan

Schedule IV
Confirmation of CCPA and CPRA Obligations

CCPA and CPRA. If Anaplan processes Personal Information governed by CCPA or CPRA and their corresponding regulations (collectively, "the Act") on behalf of Client in its provision of the Anaplan Service, this Schedule IV shall apply to Anaplan's processing of such Personal Information. Parties acknowledge and agree that regarding the Personal Information that is processed by Anaplan on behalf of Client, for the purposes of the Act, Client is the Business and Anaplan is the Service Provider.

1. **Purpose of Processing**. Anaplan will not retain, use or disclose Personal Information for any purpose other than for the specific purpose of providing the Services to Client. Anaplan acknowledges and agrees that Client is disclosing Personal Information only for the limited and specified purpose of providing the Services to Client, and Anaplan shall not retain, use, combine, or disclose Personal Information for a commercial purpose other than providing the Services to Client unless otherwise permitted by the Act.

2. **No Sale or Sharing of Personal Information.** Anaplan will not Sell or Share any Personal Information to any third party without the prior written consent of Client.

3. **Transfer of Personal Information**. Anaplan shall not disclose, release, transfer, make available or otherwise communicate any Personal Information to any third party without the prior written consent of Client unless and to the extent that such disclosure is made to a Subprocessor for a business purpose, provided that Anaplan has entered into a written agreement with Subprocessor which imposes the same obligations on the Subprocessor with regard to their Processing of Personal Information as are imposed on Anaplan under this DPA and the Agreement. Notwithstanding the foregoing, nothing in this Agreement shall restrict Anaplan's ability to disclose Personal Information to comply with applicable laws.

4. **Required consents.** Where required by applicable laws, Client will ensure that it has obtained/will obtain all necessary consents, and has given and will give all necessary notices, for the Processing of Personal Information by Anaplan.

5. **Consumer Rights Requests.** Anaplan shall comply with applicable requirements of the Act and shall assist Client, where possible, with enabling Client to respond to Consumer Rights Requests under the Act as required by the Act.

6. **Notice of Requests**. Anaplan shall promptly notify Client of any request received by Anaplan from a Consumer exercising his or her rights under the Act regarding the Personal Information of the Consumer processed by Anaplan on behalf of Client with the Anaplan Service, and shall not respond to the Consumer except to direct such Consumer to contact Client. Client shall notify Anaplan of any request received by Client from a Consumer exercising his or her rights under the Act regarding the Personal Information of the Consumer processed by Anaplan on behalf of Client with the Anaplan Service and provide the instructions and information necessary for Anaplan to comply with the request.

7. **Sub-contractors.** In the event that Anaplan engages its own sub-contractors to assist it in providing the Anaplan Service to Client, Anaplan is required to engage that sub-contractor with a written contract that contains substantially equivalent terms as Anaplan in this DPA, and that are consistent with the terms required for Service Provider and Contractor contracts in the Act.

8. **Notice to Client.** Anaplan shall notify Client no later than thirty (30) business days after Anaplan determines it can no longer meet its obligations under the Act.

9. **Unauthorized Use**. Client shall have the right, upon notice to Anaplan, to take reasonable and appropriate steps to stop and remediate Anaplan's unauthorized use of Personal Information.