ANAPLAN DATA PROCESSING ADDENDUM
(Client)

This Data Processing Addendum (“DPA”) forms part of 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. By executing the DPA, Parties are agreeing to all parts.

This DPA will be effective only if it is executed and submitted to Anaplan as described on this page and all items identified as “Required” in the table are completed accurately and in full. If Client makes any deletions or other revisions to this DPA not otherwise agreed in writing by Anaplan, then the revisions will be null and void. This DPA will only apply to the Client that is named in the “Client” field above the signature block and to its Affiliates to the extent such Affiliates are expressly permitted to benefit from the Anaplan Service and/or Professional Services under the Agreement and/or an Order Schedule.

Client’s signatory represents to Anaplan that he or she has the legal authority to bind Client. If the Client entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. If the Client entity signing this DPA has executed an Order Schedule with Anaplan pursuant to the Agreement, but is not itself a party to the Agreement (i.e., is an Affiliate of the Client), this DPA is an addendum to that Order Schedule. The Anaplan entity that is party to the Agreement or Order Schedule, as applicable, is party to this DPA. This DPA is not valid and is not legally binding if the Client entity signing this DPA is neither a party to an Agreement nor an Order Schedule.

Save in respect of those provisions of this DPA which are expressly stated to survive termination, this DPA will terminate automatically upon termination of the Agreement (or Order Schedule, as applicable), or as earlier terminated pursuant to the terms of this DPA.

This DPA will become legally binding upon Anaplan’s receipt of the DPA executed by Client, provided that the formalities set out above have been satisfied and no changes have been made to the DPA.

Controller:

____ **(“Client”)**

(Full legal name is required.)

By (Required): ______________________________

Name (Required): ______________________________

Title (Required): ______________________________

Date (Required): ______________________________

Address (Required):

____

____

Attention: ______________________________

Email: ______________________________

Processor(s):

Anaplan, Inc., 50 Hawthorne Street, San Francisco, California 94105, U.S.A.

By: ______________________________

Name: ______________________________

Title: ______________________________

Date: ______________________________

Anaplan Limited, 80 Moorbridge Road, Maidenhead, SL6 8BW, United Kingdom

By: ______________________________

Name: ______________________________

Title: ______________________________

Date: ______________________________

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 Client’s content, including model data and dashboards provided or submitted by Client or Authorized Users to or through the Anaplan Service for processing, and the outputs and modifications to that data obtained from such processing. 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.

(e) **“Data Processor"** or **"Processor"** means the entity which processes Personal Data on behalf of the Controller.

(f) “**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**”), the Personal Information Protection and Electronic Documents Act of Canada (“**PIPEDA**”), 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.

(g) **“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.

(h) “**Personal Data**” or “**Personal Information**” means any information, including personal information, relating to an identified or identifiable natural person (“**Data Subject**”).

(i) **“Personal Data Breach”** means a breach leading to any accidental, unauthorized or unlawful loss, disclosure, destruction, loss, 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.

(j) **"Processing"** or **"Process"** means any operation or set of operations performed upon Personal Data, whether or not by automated means, means any operation or set of operations that is 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.

(k) "**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 based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

(l) "**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**");

(m) **"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.

(n) **"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.

(o) The terms "**Business**", "**Commercial Purpose**", "**Consumer**", "**Service Provider**", "**Sell**" 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 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 the Client warrants it is accurate.

(e) The 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.

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 regards to any third party Controllers of the Client Personal Data; Anaplan does not need to interact directly with (including seek any authorisations 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 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://community.anaplan.com/t5/List-of-Subprocessors/List-of-Subprocessors/ba-p/31758 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 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 the 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 organisational 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 the 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.

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 the 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.

(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.

Schedule I

A. LIST OF PARTIES

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

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): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

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 specialised 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 tranfers 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.

Schedule II

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

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers. Description of the technical and organisational 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.

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Anaplan Service, as described below and in the Security Documentation applicable to the specific Anaplan Service purchased by data exporter, and accessible via http://help.anaplan.com or otherwise made reasonably available by data importer, including Anaplan's Data and Security Policy, which can be found at https://www.anaplan.com/legal/policies/security. Data importer 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.

Technical and organisational security measures pursuant to Art. 32 para.1 GDPR for Controllers (Art. 30 para. 1 s. 2 lit. g GDPR) and Processors (Art. 30 para. 2 lit. d GDPR)

1. Pseudonymisation

- Not Applicable, Anaplan does not have permissions to access to Customer Data without the Client's explicit consent. All Customer Data that is housed within the Anaplan Service is the responsibility of the Client to deploy appropriate technical measures to ensure proper compliance with regulations.

2. Encryption

- Anaplan support standard TLS 1.2 & 1.3 encryption protocols for data transmission.
- A server authentication takes place via the use of accredited certificate provider RSA (2048 bits), respectively. Customer Data is considered Restricted Information and is encrypted in transit and at rest.
- The Agreement has a clause prohibiting the upload of certain types of sensitive personal information. Please refer to the Agreement for details.

3. Confidentiality

- Each Anaplan Client receives its own customer ID. All datasets of the respective customer are stored under this ID. Due to the administration rights the Client can only access datasets which are assigned to its own ID.
- Anaplan implements best practices to manage the secure lifecycle of systems and software from design, development, test, and use to discontinuation
- Anaplan's servers are located in a dedicated room of the third-party provider Equinix, Inc. in Amsterdam, Frankfurt, & Virginia.
- The data centres employ proximity cards and biometric controls for physical access. Access to the facility requires written approval from managers. Guards monitor the facility 24x7/365 and security cameras, motion detection sensors, and alarms are enabled.
- Ensured that personnel without access authorization (e.g., technicians, cleaning personnel) are accompanied all times when access data processing areas All servers are protected by firewall servers; each operational software maintenance and clearance uses 2-factor authentication.
- Only persons who were specially authorized by Anaplan and have a 'need-to-know' have access to personal data. Further, Anaplan uses a special electronic reporting and security system, which monitors and reports every security-relevant incident (e.g., an attempted unauthorized access to the systems).

- All systems are regularly controlled and tested by external service providers. To the extent Anaplan collects Personal Data it is separated from the data which can be viewed by the customer.
- Established rules for the safe and permanent destruction of Customer Data that are no longer required
- All employees who are working with 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.
- Passwords must be at least eight (8) characters long and must contain at least three of the following character types: Upper case letters: (A,B,C,…Z), Lower case letters: (a,b,c,…z), Numbers: (0,1,2,3,…9)
- Passwords are changed regularly, with a rotation period of no more than 90 days. Account lockout is enforced after 5 failed login attempts. Previous 10 passwords cannot be used.
- Anaplan also supports SSO integration via SAML2.0, which allows customers to control authentication parameters.

4. Integrity

- Ensured that access control is supported by an authentication system
- 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 can always be traced by Anaplan's technology department upon request of the customer and in accordance with Anaplan's data management policy.
- Implemented a password policy that prohibits the sharing of passwords, outlines processes after a disclosure of a password and requires the regular change of passwords
- Data carriers are subject to strict security guidelines for any transport or destruction.

5. Availability

- Arrangements to create back-up copies stored in specially protected environments
- Arrangements to perform regular restore tests from backups
- 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.
- Additional independent tests may further be carried out pursuant to special arrangements with the customers.
- Servers are protected by state-of-the art anti-virus programs.

6. Resilience of processing systems

- All Customer Data is stored redundantly in several data centers in different regional locations. As an additional safeguard, the entire data pool is regularly backed up.
- Anaplan’s data centers have uninterruptible power supply (UPS) and onsite power generation with guaranteed fuel delivery contracts.

7. Process to restore the availability and access to personal data in the event of a physical or technical incident

- Anaplan has developed special emergency/contingency plans (Disaster Recovery Plan – DRP) and are regularly testing recovery scenarios.

8. Process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures

- Anaplan's technical and organisational measures are audited annually by external certifiers in the form of SSAE 18/SOC 1 Type 2 and SOC 2 Type 2 audits (twice per year). In addition, Anaplan undergoes 3rd party penetration test by CREST certified vendor at least annually.

Schedule III

LIST OF SUB-PROCESSORS

Please reference https://www.anaplan.com/wp-content/uploads/2021/07/PlatformSubprocessors.pdf for the list of sub-processors.

Schedule IV

Anaplan Service: means Anaplan's hosted service (accessible by Users via supported web browsers through the login page at www.anaplan.com), which may include ancillary Anaplan-proprietary products, Anaplan Applications and/or Professional Services provided to Client by Anaplan, as specified in an Order Schedule or SOW. The Anaplan Service excludes Third Party Applications.

Schedule V
Confirmation of CCPA Obligations

CCPA. If Anaplan processes Personal Information governed by CCPA on behalf of Client in its provision of the Anaplan Service, this Attachment 2 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 CCPA, 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 it shall not retain, use or disclose Personal Information for a commercial purpose other than providing the Services to Client.

2. **No Sale of Personal Information.** Anaplan will not Sell 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 the 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, the 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 CCPA and shall assist Client, where possible, with enabling Client to respond to CCPA Consumer Rights Requests as required by CCPA.

6. **Notice of Requests**. Anaplan shall promptly notify Client of any request received by Anaplan from a CCPA Consumer regarding the Personal Information of the CCPA Consumer processed by Anaplan on behalf of Client with the Anaplan Service, and shall not respond to the CCPA Consumer except to direct such CCPA Consumer to contact the Client.