Data Processing Agreement

Last updated November 6, 2024

between
[name, address]
(herein referred to as the "Controller")

and

Dash0 Inc, 447 Broadway, 2nd Floor, Suite 1929, New York, NY 10013, USA

(herein referred to as the "Processor",
together "the Parties")

1. **Preamble**

   Based on the Service Agreement dated [date], the Processor provides the Dash0 Platform to the Controller, with which the Controller analyzes their telemetry data. As part of the software use, the Processor processes personal data on behalf of the Controller. For this purpose, the parties conclude the following Data Processing Agreement (DPA).

2. **Definitions**

   In this DPA, the following terms shall have the following meanings:

   (1) **“Data Protection Laws”** shall mean the data protection laws of the country in which the Controller are established and any data protection laws applicable to the Controller in connection with the Terms, including but not limited to (a) GDPR, (b) in respect of the UK, the GDPR as saved into United Kingdom by virtue of section 3 of the United Kingdom European Union (Withdrawal) Act 2018 (“**UK GDPR**”) and the Data Protection Act, 2019 (together, “**UK Data Protection Laws**”) (c) the Swiss Federal Data Protection Act and its implementing regulations (“**Swiss DPA**”) (d) California Consumer Privacy Act (“**CCPA”)** as amended by the California Privacy Rights Act (“**CPRA**”) in each case, as may be amended, superseded or replaced.

   (2) “**GDPR**” shall mean the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

   (3) **“Personal Data”** shall mean any information relating to an identified or identifiable natural person as defined by the General Data Protection Regulation of the European Union ("GDPR") that is processed by the Processor as part of providing the services to the Controller. Mean all personal data which is uploaded into the services by Customer and accessed, stored, or otherwise processed by Dash0 as a processor.

(4) “**Controller”** shall mean 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 (usually the client that uses the platform of Dash0)

(5) “**Processor”** shall mean a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

(6) “**Data Subject Request**” means a request from or on behalf of a data subject to exercise any rights in relation to their Personal Data under Data Protection Laws.

(7) **“Restricted Transfer”** means:

a. where the GDPR applies, a transfer of Personal Data from the EEA to a country outside the EEA which is not subject to an adequacy decision by the European Commission;
b. where the UK GDPR applies, a transfer of Personal Data from the UK to any other country which is not based on adequacy regulations pursuant to Section 17A of the Data Protection Act 2018; and
c. where the Swiss DPA applies, a transfer of Personal Data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner.

(8) **Standard Contractual Clauses”** or “**SCCs**” means
a. where the GDPR applies, the standard contractual clauses as approved by the European Commission (Implementing Decision (EU) 2021/914 of 04 June 2021) Implementing Decision (EU) 2021/914 of 04 June 2021) and available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914 (“EU SCCs”);
b. where the UK GDPR applies, the applicable standard data protection clauses adopted pursuant to Article 46(2)(c), or (d) of the UK GDPR (“UK SCCs”) and
c. where the Swiss DPA applies, the applicable standard data protection clauses issued, approved, or recognized by the Swiss Federal Data Protection and Information Commissioner (the “Swiss SCCs”) (in each case, as updated, amended or superseded from time to time).

3. Scope and Purpose

(1) The purpose of this Data Processing Agreement (the "DPA") is to ensure compliance with applicable Data Protection Laws, with respect to each law only if and to the extent applicable to the respective processing activity.
(2) This DPA applies with respect to the processing of personal data as specified in ***Schedule I.***

4. Hierarchy

In the event of a conflict between this DPA and the provisions of any other agreement between the Parties existing at the time when this DPA is agreed or entered into thereafter, this DPA shall prevail, except where explicitly agreed otherwise in text form.

5. Description of processing(s)

The details of the processing operations, and in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the Data Controller, are specified in ***Schedule I***.

6. Instructions

(1) The Data Processor shall process personal data only on documented instructions in writing or via the services of the Data Controller, unless required to do so by law to which the Processor is subject. In this case, the Processor shall inform the Controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the Data Controller throughout the duration of the processing of personal data. Such instructions shall always be documented.
(2) The Data Processor shall immediately inform the Data Controller if, in the opinion of the Data Processor, instructions given by the Data Controller infringe applicable Data Protection Laws.

7. Purpose limitation

The Data Processor shall process the personal data only for the specific purpose(s) of the processing, as set out in ***Schedule I.***

8. Erasure or return of data

Processing by the Data Processor shall only take place for the duration specified in ***Schedule I.*** Upon termination of the personal data, the Processor shall return all personal data to the Controller and delete existing copies unless the personal data is required by law.

9. Security of processing

(1) The Processor shall at least implement the technical and organizational measures specified in ***Schedule II*** to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state-of-the-art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.
(2) The Processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing, and monitoring of the contract. The Processor shall ensure that the persons authorized to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

10. Documentation and compliance

(1) The Parties shall be able to demonstrate compliance with these clauses.
(2) The Processor shall deal promptly and adequately with inquiries from the Controller about the processing of data in accordance with these clauses.
(3) The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations that are set out in these clauses and stem directly from Data Protection Laws. At the Controller's request, the Processor shall also permit and contribute to audits of the processing activities covered by these clauses, at reasonable intervals or if there are indications of

non-compliance. In deciding on a review or an audit, the Controller may consider relevant certifications held by the Processor.

(4) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be conducted with reasonable notice.

(5) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

11. Use of Sub-processors

(1) The Data Processor has the Data Controller's general authorization for the engagement of Sub-processors. The list of sub-processors of the Data Processor can be found in ***Schedule III***. The Data Processor shall inform in text form the Data Controller of any intended changes to that list through the addition or replacement of Sub-processors at least 14 days in advance, thereby giving the Data Controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Any objections raised shall not be unreasonable. The Parties shall keep the list up to date.

(2) Where the Data Processor engages a Sub-processor for conducting specific processing activities (on behalf of the Data Controller), it shall do so by way of a contract which imposes on the Sub-processor the same obligations as the ones imposed on the Data Processor under this DPA. The Data Processor shall ensure that the Sub-processor complies with the obligations to which the Data Processor is subject pursuant to this DPA.

(3) The Data Processor shall remain fully responsible to the Data Controller for the performance of the Sub-processor's obligations under its contract with the Data Processor. The Data Processor shall notify the Data Controller of any failure by the Sub-processor to fulfil its obligations under that contract.

12. International transfers

(1) The Parties agree that the use of the services of the Processor will involve the transfer of personal data to, and processing of personal data in, locations outside of the EU/EEA, UK, and/or Switzerland, such as for purposes of providing support to customer, including processing in the United States. For the USA, data is transferred based on the EU's adequacy decision within the scope of the EU-US Privacy Framework.

(2) The Parties agree that when the transfer of personal data from the data exporter to data importer is a restricted transfer and applicable Data Protection Laws require that appropriate safeguards are put in place, such transfer shall be subject to the appropriate Standard Contractual Clauses, which shall be deemed incorporated into and form part of this Agreement as follows

(3) The parties agree that the Clauses will apply in respect of that processing and are incorporated into this DPA in accordance with ***Schedule IV***.

13. Assistance to the controller

(1) The Processor shall promptly notify the Controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorized to do so by the Controller.

(2) The Processor shall assist the Controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, considering the nature of the processing. When fulfilling its obligations in accordance with this section, the Processor shall comply with the Controller's instructions

(3) The Processor shall furthermore assist the Controller in ensuring compliance with the following obligations, considering the nature of the data processing and the information available to the Processor:

a. the obligation to conduct an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
b. the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;
c. the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

14. Notification of data breach

(1) In the event of a personal data breach concerning data of the controller processed by the processor, the processor shall notify the controller without undue delay after the processor has become aware of the breach. Such notification shall contain, at least:

a. a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);
b. the details of a contact point for obtaining more information regarding the personal data breach;
c. its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(2) In the event of a personal data breach, the Data Processor shall cooperate in good faith with and assist the Data Controller in any way necessary for the Data Controller to comply with its obligations under Data Protection Laws, including regarding any communication of the personal data breach to data subjects and national data protection authorities.

15. CCPA Obligations

(1) Notwithstanding any other provisions of this DPA, this section applies solely to the processing of Personal Information of residents of the State of California, USA. Terms such as "Business," "Service Provider," "Personal Information," "Consumers," "Sell," and "Share" shall have the meanings assigned to them under the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA).
(2) The Controller acknowledges that it is the business, and the Processor (Dash0) acts as the Service Provider with respect to the personal information of consumers provided by the Controller under this Agreement.
(3) The Processor shall not sell or share the personal information of consumers processed on behalf of the Controller, except as required for the provision of the Platform and/or services as outlined in the Terms of Service.

(4) The Processor shall not retain, use, or disclose consumer personal information for any purpose other than the specific purposes of performing the services under this DPA and as part of the direct relationship between the Controller and Processor. Furthermore, the Processor shall not combine personal information received from the Controller with information obtained from any other entity or interaction, except as permitted under the CCPA.
(5) Upon receiving a deletion request from a consumer, the Processor shall, upon the Controller's instruction, promptly delete the relevant personal information and instruct any engaged Sub-processors to do the same. The Processor shall not respond to Consumer deletion requests directly unless legally obligated to do so, and shall inform the Controller of any such obligations.
(6) The Controller is responsible for providing any required notices to consumers regarding the sharing of their personal information with the Processor. The Processor shall immediately notify the Controller if it determines it is unable to comply with its obligations under the CCPA.
(7) The Controller has the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information. The Processor shall cooperate reasonably with the Controller in responding to any requests from consumers or data protection authorities related to personal information processing under this DPA. If the Processor receives a direct request from a consumer, it shall not respond without the Controller's prior authorization unless required by law.
(8) The Processor certifies that it understands and will comply with the restrictions and obligations set forth in this section regarding the processing of personal information under the CCPA.

Signatures

(E-Signature is sufficient)

Client/Controller

Date: _____ Signature: _____
Name:
Function:

Dash0 Inc, Processor

Date: _____ Signature: _____
Name:
Function:

Schedule I – Data Processing Details

Subject Matter of the Processing	Dash0´s of the services to customers.

Nature and purpose of Processing	The processing of personal data pursuant to providing the services to customer as described in the Terms and Conditions.
Types of Personal Data	Dash0 requires the following in order to provide the services: - first name - last name - email address - IP-Adress The platform is also used to process and analyze the customer's telemetry data. This may also contain pseudonymized personal usage data.
Sensitive Personal Data and applied restrictions	None
Categories of Data Subject	- Employees and other personnel and the controllers' customers who have access to the service through a user account. - Data subjects may include all users of the Service about whom Dash0 has received personal data via the services from or on the instructions of the customer. Furthermore, usage data of customers' users may be processed.
The frequency and nature of the processing and the transfer	The data is transmitted on a continuous basis. The processing of personal data occurs for the duration of the provision of services for monitoring applications and IT infrastructures.
Duration of Processing	For the duration of the Agreement, or until the processing is no longer necessary for the purposes.
Location of Data processing	AWS is used to process and store customers' observability (telemetry) data. Customers can choose to store such data within the EU (Ireland, eu-west-1) or the US (Oregon, us-west-2). For all other Types of personal data (see above), Sect. 11, 12 of the Data Processing Agreement applies without deviations.

Schedule II: Technical & Organizational Measures

This section outlines the key technical and organizational measures implemented to ensure the security, integrity, and availability of data. The Processor leverages Amazon Web Services (AWS) for cloud infrastructure, which is certified with industry-leading standards such as ISO 27001, ISO 27017, and ISO 27018, ensuring robust security controls. Furthermore, the Processor holds SOC II certification, demonstrating adherence to strict security, confidentiality, and integrity principles. These certifications reflect a commitment to maintaining high standards of data protection, data security, and cloud security, which are continuously monitored and reviewed for effectiveness. The following measures provide detailed insight into how confidentiality, integrity, availability, and resilience are maintained across the organization's systems.

1. Confidentiality

Measures to ensure confidentiality focus on preventing unauthorized access to systems, data, and services, maintaining strict access controls, and ensuring only authorized personnel have access to sensitive information.

Access Controls

1.1 User Authentication:

- All users must authenticate with unique credentials to ensure identity verification.
- Multi-factor authentication (MFA) is enforced for accessing sensitive systems and data, adding an additional layer of security.
- User access is managed through AWS Identity Center, ensuring centralized control of user authentication.

1.2 Authorization and Role-Based Access:

- Access to systems and data is granted based on job responsibilities, following a clear Authorization Concept.
- Regular access reviews are conducted to ensure permissions remain appropriate, keeping access up to date in line with job roles and responsibilities.
- Strong identity and access management policies enforce role-based access control, ensuring no over-provisioning of rights.

1.3 Vendor Management:

- Third-party risk assessments are performed before vendor onboarding, ensuring vendors meet strict security and compliance standards.
- Ongoing monitoring and audits of third-party vendors ensure their continued compliance with security requirements.

2. Integrity

Integrity measures focus on ensuring data accuracy, protecting data during transfer, and preventing unauthorized modification or deletion.

Data Protection

2.1 Data Encryption:

- All sensitive data, whether in transit or at rest, is encrypted using industry-standard encryption protocols, ensuring data cannot be accessed or tampered with during transmission or storage.
- Encryption keys are securely managed, with regular key rotation policies in place to ensure their integrity and security.

2.2 Data Minimization:

- Data processing is limited to the specific purposes required by the organization. For application and infrastructure performance monitoring, only necessary data such as logs, metrics, and traces are collected.

2.3 Data Integrity:

- Mechanisms, including data validation processes, are employed to maintain the accuracy and integrity of data.
- Access logs and audit trails are maintained to monitor data access, ensuring data integrity, and providing full visibility of any changes made to data.

Change Management

2.4 Change Approval Process:

- All system and application changes undergo a formal review and approval process to assess potential impacts on security, functionality, and compliance.
- Changes are thoroughly documented, ensuring traceability and accountability for each change made.

2.5 Post-Incident Analysis:

- After an incident, a root cause analysis is conducted to identify and resolve vulnerabilities. Corrective measures are implemented to prevent future incidents, ensuring data integrity is maintained.

3. Availability

Availability measures ensure data and systems are consistently available when needed and protected from disruptions, ensuring business continuity.

Data Backup and Recovery

3.1 Regular Backups:

- Regular data backups are performed, with email confirmations verifying successful backup completion.
- Backup restoration tests are conducted every 6 months, ensuring the readiness to restore data in case of data loss or failure.
- Comprehensive disaster recovery plans are in place, ensuring timely restoration of data and services in the event of an incident.

3.2 Incident Management:

- Incident response procedures are in place to manage and mitigate any security incidents. A resolute incident response team manages security threats and data breaches efficiently, ensuring service availability.

- An incident reporting system ensures employees can quickly notify the response team of any suspected security breaches.

3.3 Security Awareness and Training:

- Employees receive regular training on security best practices, including phishing awareness and social engineering prevention, ensuring all personnel are prepared to maintain system availability by avoiding common threats.
- Clear communication channels keep employees updated on new security protocols and good practices.

4. Resilience

Resilience measures ensure that systems and data can withstand and recover from incidents, disruptions, or failures, maintaining operational continuity.

Rapid Recoverability

4.1 Backup Policy:

- Daily backup copies are created to ensure the ability to restore data in case of a system failure or disruption.
- Backups are stored in a secure, remote location away from the primary data processing site, ensuring data is protected from physical risks.
- Backup recoverability tests are performed annually to ensure the integrity and effectiveness of backups.

4.2 System Monitoring:

- Continuous monitoring of servers and systems for vulnerabilities ensures prompt detection of potential threats.
- Identified vulnerabilities are immediately addressed, ensuring systems can recover quickly from any security issues.

4.3 Security Information and Event Management (SIEM):

- Security events, unauthorized access attempts, and other anomalies are detected through automated SIEM systems, ensuring rapid identification and response to any issues threatening system resilience.

4.4 External Audits:

- Independent third-party audits are conducted regularly to assess the effectiveness of security controls. Findings from these audits are addressed through corrective actions to improve resilience.

5. Procedures for regular review, assessment, and evaluation

5.1 Data Protection Management

- The Processor has implemented a data protection management system which is based on the structure of the ISO/IEC 27001/ISO/IEC 27701 standard.
- Accordingly, implemented technical and organizational measures are regularly reviewed for effectiveness as part of internal controls and developed further if necessary.

5.2 SOC II Certification

- The Processor is certified in accordance with SOC II and follows a continuous improvement process.
- This includes regular reviews of cloud security measures to ensure their effectiveness and adherence to established security controls.

5.3 Order Control

To ensure that Personal Data is processed only in accordance with the Controller’s instructions, the Processor has established the following measures:

- All orders for the processing of personal data are governed by written contracts, clearly defining roles and responsibilities.
- Basic requirements regarding liability, security measures, and control rights are explicitly outlined in these contracts.
- The Processor will assist the Controller's data protection officer in exercising control rights, ensuring compliance with data protection provisions related to contracted data processing and application security.
- Regular audits and assessments will be conducted to verify adherence to contractual obligations and to ensure that necessary technical and organizational measures are in place, in alignment with the requirements of this agreement and the applicable data protection laws.

Schedule III: Sub-processors

This Schedule lists the Sub-processors used by the Processor to help provide services involving the processing of personal data. These third-party vendors support areas like cloud hosting, analytics, and customer support. Each Sub-processor is carefully vetted to ensure sufficient guarantees that are in line with security and privacy standards, including compliance with data protection laws. The complete subprocessor list and all relevant information can be found here.

Schedule IV: International Data Transfer

I. Standard-Contractual Clauses (EU)

1. For the purposes of this Annex, the EU Clauses (Module II), available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN, shall be incorporated by reference to this Annex and the DPA and shall be considered an integral part thereof, and the Parties' signatures in the DPA shall be construed as the Parties' signature to the EU Clauses. In the event of an inconsistency between the DPA and the EU Clauses, the latter will prevail.
2. For the purposes of the EU Clauses, the following shall apply:

   - Customer/Controller shall be the data exporter and Dash0 shall be the data importer. Each Party agrees to be bound by and comply with its obligations in its role as exporter and importer respectively as set out in the EU Clauses.
   - in Clause 7, the optional docking clause will apply;
   - Clause 9 (Use of Sub-processors): OPTION 2 – GENERAL WRITTEN AUTHORISATION shall apply. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors as set out in clause 10 of the DPA.
   - in Clause 11, the optional language will not apply;
   - in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the law of Germany;
   - in Clause 18(b), disputes shall be resolved before the courts of Germany;

ANNEX I to Section I of Schedule IV

A. **LIST OF PARTIES**

Data exporter(s):
Name: as defined in the Service Agreement
Address: as defined in the Service Agreement
Contact person's name, position, and contact details: as defined in the Service Agreement
Activities relevant to the data transferred under these Clauses: data exporter will transfer personal data to the data importer as required for the provision of services by the data importer under the Terms and Conditions and as set out in the DPA.
Signature and date: please refer to signature and date in the DPA.
Role (Controller/Processor): **Controller**

Data importer(s):
Name: Dash0, Inc.
Address: 447 Broadway 2nd floor suite 1929, New York, NY 10013, United States
Contact person's name, position, and contact details: Mirko Novakovic, Chief Executive Officer, e-mail: mirko.novakovic@dash0.com
Activities relevant to the data transferred under these Clauses: Providing Application and IT Infrastructure monitoring services as set out in the Terms and *Conditions.*
Signature and date: signature and date in the DPA.
Role (Controller/Processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred
See Schedule I to the DPA

Categories of personal data transferred
See ***Schedule I*** to the DPA

Sensitive data transferred (if applicable) and applied restrictions or safeguards
See ***Schedule I*** to the DPA

Frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).
Transfers will occur from time to time as required during the course of the performance of the services under the Agreement.

Nature of the processing
See ***Schedule I*** to the DPA

Purpose(s) of the data transfer and further processing
See ***Schedule I*** to the DPA

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
See ***Schedule I*** to the DPA

For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing
See ***Schedule III*** to the DPA

C. COMPETENT SUPERVISORY AUTHORITY
Identify the competent supervisory authority/ies in accordance with Clause 13

The Processor has identified the following supervisory authority: [Competent Authority]

Where Controller is the data exporter, the supervisory authority shall be the competent supervisory authority that has supervision over the controller in accordance with Clause 13 of the SCCs.

ANNEX II of Section 1 of Schedule IV- TECHNICAL AND ORGANISATIONAL MEASURES: See Schedule III of the DPA

ANNEX III of Section 1 of Schedule IV- LIST OF SUB-PROCESSORS : See Schedule III to the DPA

II. UK Standard Contractual Clauses
This section applies to customers in the UK if data is processed in countries outside the UK.

1. The parties agree that the terms of the Standard Contractual Clauses, as amended by the UK Standard Contractual Clauses and further amended by this Section II, are hereby incorporated by reference, and shall apply to transfers of Customer Data from the UK to other countries that are not deemed Adequate Countries.
2. This Annex V is intended to provide the appropriate safeguards for the purposes of transfers of Customer Data to a third country in reliance on Article 46 of the UK GDPR, with respect to data transfers from Controller to Processor or from Processor to Sub-Processors.
3. Terms used in this Annex V that are defined in the Standard Contractual Clauses shall retain the same meaning as in the Standard Contractual Clauses.
4. This Annex V shall: (i) be read and interpreted in light of UK Data Protection Laws to ensure it provides the appropriate safeguards required under Article 46 of the UK GDPR,

and (ii) not be interpreted in a manner that conflicts with the rights and obligations under UK Data Protection Laws.

5. Amendments to the UK Standard Contractual Clauses:

Part 1: Tables

- **Table 1 Parties**: To be completed as set out in Section 4 of Annex IV above.
- **Table 2 Selected SCCs, Modules, and Selected Clauses**: To be completed as outlined in Sections 2 and 3 of Annex IV above.
- **Table 3 Appendix Information**:

    1. **Annex 1A: List of Parties**: To be completed as set forth in Section 2 of Annex IV above.
    2. **Annex 1B: Description of Transfer**: To be completed as outlined in Annex I above.
    3. **Annex II: Technical and organizational measures, including measures to ensure the security of the data**: To be completed as described in Annex II above.
    4. **Annex III: List of Sub-Processors**: To be completed as set forth in Annex III above.

- **Table 4 Ending this Addendum when the Approved Addendum Changes:** To be completed as “neither party.”

III. Supplementary Clauses for Swiss Data Protection Law

The following terms supplement the Clauses only if and to the extent they apply with respect to data transfers subject to Swiss Data Protection Law, specifically the Swiss Federal Data Protection Act (FDPA):

1. The term "Member State" will be interpreted to allow Data Subjects in Switzerland to exercise their rights under the Clauses in their place of habitual residence (Switzerland), in accordance with Clause 18(c) of the Clauses.
2. The Clauses protect the Customer Data of legal entities until the entry into force of the revised FDPA.
3. All references in this DPA to the GDPR shall be understood as references to the FDPA where data transfers are subject to the FDPA.
4. References to the "competent supervisory authority," "competent courts," and "governing law" shall be interpreted as references to Swiss Data Protection Laws, the Swiss Information Commissioner, the competent courts in Switzerland, and the laws of Switzerland (for Restricted Transfers from Switzerland).
5. In respect of data transfers governed by Swiss Data Protection Laws, the EU SCCs will also apply to the transfer of information relating to an identifiable legal entity, where such information is protected similarly as Personal Data under Swiss Data Protection Laws, until such laws are amended to no longer apply to legal entities.
6. The competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.