Data Processing Addendum

Last Updated: October 17, 2022

This Data Processing Addendum (this "Addendum") forms part of, and is incorporated into, the Prefect Software as a Service (SaaS) Agreement for the provision of Prefect services (as amended from time to "Prefect," "Company," "us," "we") and the customer entity that is a party to the Agreement ("Customer" or "you"). We may update this Addendum from time to time, and we will provide reasonable notice of any such updates. Any terms not defined in this Addendum shall have the meaning set forth in the Agreement.

1. Definitions

1.1 "Affiliate" means (i) an entity of which a party directly or indirectly owns fifty percent (50%) or more of the stock or other equity interest, (ii) an entity that owns at least fifty percent (50%) or more of the stock or other equity interest of a party, or (iii) an entity which is under common control with a party by having at least fifty percent (50%) or more of the stock or other equity interest of such entity and a party owned by the same person, but such entity shall only be deemed to be an Affiliate so long as such ownership exists.

1.2 "Authorized Sub-Processor" means a third-party who has a need to know or otherwise access Customer's Personal Data to enable Company to perform its obligations under this Addendum or the Agreement, and who is either (1) referenced in Exhibit B or (2) subsequently authorized under Section 4.2 of this Addendum.

1.3 "Customer Account Data" means personal data that relates to Customer's relationship with Company, including the names or contact information of individuals authorized by Customer to access Customer's account and billing information of individuals that Customer has associated with its account. Customer Account Data also includes any data Company may need to collect for the purpose of managing its relationship with Customer, identity verification, or as otherwise required by applicable laws and regulations.

1.4 "Customer Usage Data" means Service usage data collected and processed by Company in connection with the provision of the Services, including without limitation data used to identify the source and destination of a communication, activity logs, and data used to optimize and maintain performance of the Services, and to investigate and prevent system abuse.

1.5 "Data Exporter" means Customer.

1.6 "Data Importer" means Company.

1.7 "Data Protection Laws" means any applicable laws and regulations in any relevant jurisdiction relating to the use or processing of Personal Data including: (i) the California Consumer Privacy Act ("CCPA"), (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) ("EU GDPR" or "GDPR"), (iii) the Swiss Federal Act on Data Protection, (iv) the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "UK GDPR"); (v) the UK Data Protection Act 2018 (together with UK GDPR "UK Data Protection Laws"), and (vi) the Privacy and Electronic Communications (EC Directive) Regulations 2003; in each case, as updated, amended or replaced from time to time. The terms "Data Subject", "Personal Data", "Personal Data Breach", "processing", "processor," "controller," and "supervisory authority" shall have the meanings set forth in the GDPR.

1.8 "EU SCCs" means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time).

1.9 "ex-EEA Transfer" means the transfer of Personal Data, which is processed in accordance with the GDPR, from the Data Exporter to the Data Importer (or its premises) outside the European Economic Area (the "EEA"), and such transfer is not governed by an adequacy decision made by the European Commission in accordance with the relevant provisions of the GDPR.

1.10 "ex-UK Transfer" means the transfer of Personal Data, which is processed in accordance with the UK GDPR and the Data Protection Act 2018, from the Data Exporter to the Data Importer (or its premises) outside the United Kingdom (the "UK"), and such transfer is not governed by an adequacy decision made by the Secretary of State in accordance with the relevant provisions of the UK GDPR and the Data Protection Act 2018.

1.11 "Services" shall have the meaning set forth in the Agreement.

1.12 "Standard Contractual Clauses" means the EU SCCs and the UK SCCs.

1.13 "UK SCCs" means the Standard Contractual Clauses, as supplemented by the UK SCCs Addendum.

1.14 "UK SCCs Addendum" means the template International Data Transfer Addendum issued by the UK Information Commissioner's Office (the "ICO") and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as incorporated into this Addendum pursuant to Section 6.4 below.

2. Relationship of the Parties; Processing of Data

2.1 The parties acknowledge and agree that with regard to the processing of Personal Data, Customer may act either as a controller or processor and, except as expressly set forth in this Addendum or the Agreement, Company is a processor. Customer shall, in its use of the Services, at all times process Personal Data, and provide instructions for the processing of Personal Data, in compliance with Data Protection Laws. Customer shall ensure that the processing of Personal Data in accordance with Customer's instructions will not cause Company to be in breach of the Data Protection Laws. Customer is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Company by or on behalf of Customer, (ii) the means by which Customer acquired any such Personal Data, and (iii) the instructions it provides to Company regarding the processing of such Personal Data. Customer shall not provide or make available to Company any Personal Data in violation of the Agreement or otherwise inappropriate for the nature of the Services.

2.2 Company shall not process Personal Data (i) for purposes other than those set forth in the Agreement and/or Exhibit A, (ii) in a manner inconsistent with the terms and conditions set forth in this Addendum or any other documented instructions provided by Customer, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by a Supervisory Authority to which the Company is subject; in such a case, the Company shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest, or (iii) in violation of Data Protection Laws. Customer hereby instructs Company to process Personal Data in accordance with the foregoing and as part of any processing initiated by Customer in its use of the Services.

2.3 The subject matter, nature, purpose, and duration of this processing, as well as the types of Personal Data collected and categories of Data Subjects, are described in Exhibit A to this Addendum.

2.4 Following completion of the Services, at Customer's choice, Company shall return or delete Customer's Personal Data, unless further storage of such Personal Data is required or authorized by applicable law. If return or destruction is impracticable or prohibited by law, rule or regulation, Company shall take measures to block such Personal Data from any further processing (except to the extent necessary for its continued hosting or processing required by law, rule or regulation) and shall continue to appropriately protect the Personal Data remaining in its possession, custody, or control. If Customer and Company have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the parties agree that the certification of deletion of Personal Data that is described in Clause 8.5 of the Standard Contractual Clauses shall be provided by Company to Customer only upon Customer's request.

2.5 CCPA. Except with respect to Customer Account Data and Customer Usage Data, the parties acknowledge and agree that Company is a service provider for the purposes of the CCPA (to the extent it applies) and is receiving personal information from Customer in order to provide the Services pursuant to the Agreement, which constitutes a business purpose. Company shall not sell any such personal information. Company shall not retain, use or disclose any personal information provided by Customer pursuant to the Agreement except as necessary for the specific purpose of performing the Services for Customer pursuant to the Agreement, or otherwise as set forth in the Agreement or as permitted by the CCPA. The terms "personal information," "service provider," "sale," and "sell" are as defined in Section 1798.140 of the CCPA. Company certifies that it understands the restrictions of this Section 2.5.

3. Confidentiality Company shall ensure that any person it authorizes to process Personal Data has agreed to protect Personal Data in accordance with Company's confidentiality obligations in the Agreement. Customer agrees that Company may disclose Personal Data to its advisers, auditors or other third parties

as reasonably required in connection with the performance of its obligations under this Addendum, the Agreement, or the provision of Services to Customer.

4. Authorized Sub-Processors

4.1 Customer acknowledges and agrees that Company may (1) engage its affiliates and the Authorized Sub-Processors identified on the List (as defined below) to access and process Personal Data in connection with the Services and (2) from time to time engage additional third parties for the purpose of providing the Services, including without limitation the processing of Personal Data. By way of this Addendum, Customer provides general written authorization to Company to engage sub-processors as necessary to perform the Services.

4.2 A list of Company's current Authorized Sub-Processors (the "List") will be made available to Customer at the following link: https://www.prefect.io/security/sub-processors/. Such List may be updated by Company from time to time. Company may provide a mechanism to subscribe to notifications of new Authorized Sub-Processors and Customer agrees to subscribe to such notifications where available. At least thirty (30) days before enabling any third party other than existing Authorized Sub-Processors to access or participate in the processing of Personal Data, Company will add such third party to the List and notify Customer via email. Customer may object to such an engagement by informing Company in writing within thirty (30) days of receipt of the aforementioned notice by Customer, *provided* such objection is based on reasonable grounds relating to data protection. Customer acknowledges that certain sub-processors are essential to providing the Services and that objecting to the use of a sub-processor may prevent Company from offering the Services to Customer.

4.3 If a Sub-Processor change would cause Company to breach its obligations under the Agreement and this Addendum, Customer may terminate the Agreement in accordance with Sections 7.2 (Defaults) and 7.3 (Termination; Other Remedies) of the Agreement. If Customer does not object to the engagement of a third party in accordance with Section 4.2 within thirty (30) days of notice by Company, that third party will be deemed an Authorized Sub-Processor for the purposes of this Addendum.

4.4 Company will enter into a written agreement with the Authorized Sub-Processor imposing on the Authorized Sub-Processor data protection obligations comparable to those imposed on Company under this Addendum with respect to the protection of Personal Data. In case an Authorized Sub-Processor fails to fulfill its data protection obligations under such written agreement with Company, Company will remain liable to Customer for the performance of the Authorized Sub-Processor's obligations under such agreement.

4.5 With respect to the Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), (i) the above authorizations will constitute Customer's prior written consent to the subcontracting by Company of the processing of Personal Data if such consent is required under the Standard Contractual Clauses, and (ii) the parties agree that the copies of the agreements with Authorized Sub-Processors that must be provided by Company to Customer pursuant to Clause 9(c) of the Standard Contractual Clauses may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by the Company beforehand, and that such copies will be provided by the Company only upon request by Customer.

5. Security of Personal Data Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Company shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing Personal Data. Exhibit C references additional information about Company's technical and organizational security measures.

6. Transfers of Personal Data

6.1 The parties agree that Company may transfer Personal Data processed under this Addendum outside the EEA, the UK, or Switzerland as necessary to provide the Services. Customer acknowledges that Company's primary processing operations take place in the United States, and that the transfer of Customer's Personal Data to the United States is necessary for the provision of the Services to Customer. If Company transfers Personal Data protected under this Addendum to a jurisdiction for which the European Commission has not issued an adequacy decision, Company will ensure that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Data Protection Laws.

6.2 Ex-EEA Transfers. The parties agree that ex-EEA Transfers are made pursuant to the EU SCCs, which are deemed entered into (and incorporated into this Addendum by this reference) and completed as follows:

6.2.1 Module Two (Controller to Processor) of the EU SCCs apply when Customer is a controller and Company is processing Personal Data for Customer as a processor pursuant to Section 2 of this Addendum.

6.2.2 Module Three (Processor to Sub-Processor) of the EU SCCs apply when Customer is a processor and Company is processing Personal Data on behalf of Customer as a sub-processor.

6.3 For each module, where applicable the following applies:

6.3.1 The optional docking clause in Clause 7 does not apply;

6.3.2 In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of sub-processor changes shall be as set forth in Section 4.2 of this Addendum;

6.3.3 In Clause 11, the optional language does not apply;

6.3.4 All square brackets in Clause 13 are hereby removed;

6.3.5 In Clause 17 (Option 1), the EU SCCs will be governed by the laws of Ireland;

6.3.6 In Clause 18(b), disputes will be resolved before the courts of Ireland;

6.3.7 Exhibit B to this Addendum contains the information required in Annex I of the EU SCCs;

6.3.8 Exhibit C to this Addendum contains the information required in Annex II of the EU SCCs; and

6.3.9 By entering into this Addendum, the parties are deemed to have signed the EU SCCs incorporated herein, including their Annexes.

6.4 Ex-UK Transfers. The parties agree that ex-UK Transfers are made pursuant to the UK SCCs, which are deemed entered into and incorporated into this Addendum by reference, and completed as follows:

6.4.1 The information required by Tables 1 – 3 of the template International Data Transfer Addendum is provided in the Agreement, this Addendum and the Exhibits below.

6.4.2 References to the EU, member states and GDPR in the Standard Contractual Clauses are amended *mutatis mutandis* to refer to the United Kingdom, the UK Data Protection Act 2018 (as it may be updated or replaced from time to time), and the ICO.

6.4.3 In Clause 17 (Governing Law), the laws of England and Wales shall govern, and in Clause 18 (Choice of forum and jurisdiction), the courts in London, England shall have jurisdiction. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK.

6.4.4 If there is any inconsistency or conflict between UK Data Protection Laws (including the template International Data Transfer Addendum) and the Standard Contractual Clauses, UK Data Protection Laws will govern data transfers from the United Kingdom.

6.4.5 If the meaning of any provision of this Addendum or the UK SCCs is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

6.4.6 Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after these UK SCCs have been entered into.

6.4.7 Although Clause 5 of the Standard Contractual Clauses says that the Standard Contractual Clauses prevail over all related agreements between the parties, the parties agree that the UK SCCs will supersede other provisions of the Standard Contractual Clauses regarding data transfers from the United Kingdom.

6.5 Transfers from Switzerland. The parties agree that transfers from Switzerland are made pursuant to the EU SCCs with the following modifications:

6.5.1 The terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilized in the EU SCCs shall be interpreted to include the Federal Act on Data Protection of 19 June

1992 (the "FADP," and as revised as of 25 September 2020, the "Revised FADP") with respect to data transfers subject to the FADP.

6.5.2 The terms of the EU SCCs shall be interpreted to protect the data of legal entities until the effective date of the Revised FADP.

6.5.3 Clause 13 of the EU SCCs is modified to provide that the Federal Data Protection and Information Commissioner ("FDPIC") of Switzerland shall have authority over data transfers governed by the FADP and the appropriate EU supervisory authority shall have authority over data transfers governed by the GDPR. Subject to the foregoing, all other requirements of Section 13 shall be observed.

6.5.4 The term "EU Member State" as utilized in the EU SCCs shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from exercising their rights in their place of habitual residence in accordance with Clause 18(c) of the EU SCCs.

6.6 Supplementary Measures. In respect of any ex-EEA Transfer or ex-UK Transfer, the following supplementary measures shall apply:

6.6.1 As of the date of this Addendum, the Data Importer has not received any formal legal requests from any government intelligence or security service/agencies in the country to which the Personal Data is being exported, for access to (or for copies of) Customer's Personal Data ("Government Agency Requests");

6.6.2 If, after the date of this Addendum, the Data Importer receives any Government Agency Requests, Company shall attempt to redirect the law enforcement or government agency to request that data directly from Customer. As part of this effort, Company may provide Customer's basic contact information to the government agency. If compelled to disclose Customer's Personal Data to a law enforcement or government agency, Company shall give Customer reasonable notice of the demand and cooperate to allow Customer to seek a protective order or other appropriate remedy unless Company is legally prohibited from doing so. Company shall not voluntarily disclose Personal Data to any law enforcement or government agency. Data Exporter and Data Importer shall (as soon as reasonably practicable) discuss and determine whether all or any transfers of Personal Data pursuant to this Addendum should be suspended in the light of the such Government Agency Requests; and

6.6.3 The Data Exporter and Data Importer will meet regularly to consider whether:

(i) the protection afforded by the laws of the country of the Data Importer to data subjects whose Personal Data is being transferred is sufficient to provide broadly equivalent protection to that afforded in the EEA or the UK, whichever the case may be;

(ii) additional measures are reasonably necessary to enable the transfer to be compliant with the Data Protection Laws; and

(iii) it is still appropriate for Personal Data to be transferred to the relevant Data Importer, taking into account all relevant information available to the parties, together with guidance provided by the supervisory authorities.

6.6.4 If Data Protection Laws require the Data Exporter to execute the Standard Contractual Clauses applicable to a particular transfer of Personal Data to a Data Importer as a separate agreement, the Data Importer shall, on request of the Data Exporter, promptly execute such Standard Contractual Clauses incorporating such amendments as may reasonably be required by the Data Exporter to reflect the applicable appendices and annexes, the details of the transfer and the requirements of the relevant Data Protection Laws.

6.6.5 If either (i) any of the means of legitimizing transfers of Personal Data outside of the EEA or UK set forth in this Addendum cease to be valid or (ii) any supervisory authority requires transfers of Personal Data pursuant to those means to be suspended, then Data Importer may by notice to the Data Exporter, with effect from the date set out in such notice, amend or put in place alternative arrangements in respect of such transfers, as required by Data Protection Laws.

7. Rights of Data Subjects

7.1 Company shall, to the extent permitted by law, notify Customer upon receipt of a request by a Data Subject to exercise the Data Subject's right of: access, rectification, erasure, data portability, restriction or cessation of processing, withdrawal of consent to processing, and/or objection to being subject to processing that constitutes automated decision-making (such requests individually and collectively "Data Subject Request(s)"). If Company receives a Data Subject Request in relation to Customer's data, Company will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to such request, including, where necessary, by using the functionality of the Services. Customer is solely responsible for ensuring that Data Subject Requests for erasure, restriction or cessation of processing, or withdrawal of consent to processing of any Personal Data are communicated to Company, and, if applicable, for ensuring that a record of consent to processing is maintained with respect to each Data Subject.

7.2 Company shall, at the request of the Customer, and taking into account the nature of the processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Customer in complying with Customer's obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, *provided that* (i) Customer is itself unable to respond without Company's assistance and (ii) Company is able to do so in accordance with all applicable laws, rules, and regulations. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Company.

8. Actions and Access Requests; Audits

8.1 Company shall, taking into account the nature of the processing and the information available to Company, provide Customer with reasonable cooperation and assistance where necessary for Customer to comply with its obligations under the GDPR to conduct a data protection impact assessment and/or to demonstrate such compliance, *provided that* Customer does not otherwise have access to the relevant information. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Company.

8.2 Company shall, taking into account the nature of the processing and the information available to Company, provide Customer with reasonable cooperation and assistance with respect to Customer's cooperation and/or prior consultation with any Supervisory Authority, where necessary and where required by the GDPR. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Company.

8.3 Company shall maintain records sufficient to demonstrate its compliance with its obligations under this Addendum, and retain such records for a period of three (3) years after the termination of the Agreement. Customer shall, with reasonable notice to Company, have the right to review, audit and copy such records at Company's offices during regular business hours.

8.4 Upon Customer's written request at reasonable intervals, and subject to reasonable confidentiality controls, Company shall, either (i) make available for Customer's review copies of certifications or reports demonstrating Company's compliance with prevailing data security standards applicable to the processing of Customer's Personal Data, or (ii) if the provision of reports or certifications pursuant to (i) is not reasonably sufficient under Data Protection Laws, allow Customer's independent third party representative to conduct an audit or inspection of Company's data security infrastructure and procedures that is sufficient to demonstrate Company's compliance with its obligations under Data Protection Laws, *provided that* (a) Customer provides reasonable prior written notice of any such request for an audit and such inspection shall not be unreasonably disruptive to Company's business; (b) such audit shall only be performed during business hours and occur no more than once per calendar year; and (c) such audit shall be restricted to data relevant to Customer. Customer shall be responsible for the costs of any such audits or inspections, including without limitation a reimbursement to Company for any time expended for on-site audits. The parties agree that the audits described in Clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with this Section 8.4.

8.5 Company shall immediately notify Customer if an instruction, in the Company's opinion, infringes the Data Protection Laws or Supervisory Authority.

8.6 In the event of a Personal Data Breach, Company shall, without undue delay, inform Customer of the Personal Data Breach and take such steps as Company in its sole discretion deems necessary and reasonable to remediate such violation (to the extent that remediation is within Company's reasonable control).

8.7 In the event of a Personal Data Breach, Company shall, taking into account the nature of the processing and the information available to Company, provide Customer with reasonable cooperation and assistance necessary for Customer to comply with its obligations under the GDPR with respect to notifying (i) the relevant Supervisory Authority and (ii) Data Subjects affected by such Personal Data Breach without undue delay.

8.8 The obligations described in Sections 8.6 and 8.7 shall not apply in the event that a Personal Data Breach results from the actions or omissions of Customer. Company's obligation to report or respond to a Personal Data Breach under Sections 8.6 and 8.7 will not be construed as an acknowledgement by Company of any fault or liability with respect to the Personal Data Breach.

9. Conflict. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms in the Standard Contractual Clauses; (2) the terms of this Addendum; and (3) the Agreement. Any claims brought in connection with this Addendum will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement.

Exhibit A

Details of Processing

Nature and Purpose of Processing: Company will process Customer's Personal Data as necessary to provide the Services under the Agreement, for the purposes specified in the Agreement and this Addendum, and in accordance with Customer's instructions as set forth in this Addendum.

Duration of Processing: Company will process Customer's Personal Data as long as required (i) to provide the Services to Customer under the Agreement; (ii) for Company's legitimate business needs; or (iii) by applicable law or regulation. Customer Account Data and Customer Usage Data will be processed and stored as set forth in Company's Privacy Policy available at the following link: https://www.prefect.io/legal/privacy-policy/.

Categories of Data Subjects: Customer end-users/customers.

Categories of Personal Data: Company processes Personal Data contained in Customer Account Data, Customer Usage Data, and any Personal Data provided by Customer (including any Personal Data Customer collects from its end users and processes through its use of the Services) or collected by Company in order to provide the Services or as otherwise set forth in the Agreement or this Addendum. Categories of Personal Data include full name, email address, company name, and some basic digital information surrounding usage such as last login time.

Sensitive Data or Special Categories of Data: None.

Exhibit B

The following includes the information required by Annex I and Annex III of the EU SCCs, and Appendix 1 of the UK SCCs.

1. The Parties

Data exporter(s): The Customer

Contact details: As designated by Customer in notice section of the Agreement

Signature and date: By entering into the Agreement, Data Exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, as of the Effective Date of the Agreement.

Role (controller/processor): The Data Exporter's role is set forth in Section 2 of this Addendum.

Data importer(s): Prefect Technologies, Inc.

Address: 1200 18th Street NW Suite 700, Washington, DC 20036

Contact person's name, position and contact details: Brian Russell, Head of Legal, legal@prefect.io.

Signature and date: By entering into the Agreement, Data Importer is deemed to have signed these Standard Contractual Clauses incorporated herein, as of the Effective Date of the Agreement.

Role (controller/processor): The Data Importer's role is set forth in Section 2 of this Addendum.

2. Description of the Transfer

Data Subjects	As set out in Exhibit A of this Addendum.
Categories of Personal Data	As set out in Exhibit A of this Addendum.
Special Category Personal Data (if applicable)	As set out in Exhibit A of this Addendum.
Nature of the Processing	As set out in Exhibit A of this Addendum.
Purposes of Processing	The only internal processing of user's Personal Data that occurs is (i) in service of accessing the Data Controller's personal user interface (via email address), (ii) production of limited customer analytics, and (iii) displaying the above information in the Data Controller's user interface. Otherwise, no processing occurs on the information outlined above. As indicated above, Other processing of Personal Data may take place by the execution of program flows written by the Data Controller, which is required for the remote monitoring and execution of workflows that the Prefect Cloud SaaS provides.
Duration of Processing and Retention (or the criteria to determine such period)	As set out in Exhibit A of this Addendum.
Frequency of the transfer	As necessary to provide the Services or as otherwise authorized under the Agreement or Addendum.
Recipients of Personal Data Transferred to the Data Importer	A list of the Company's Sub-Processors can be found at the following link: https://www.prefect.io/security/sub-processors/

3. Competent Supervisory Authority

The supervisory authority shall be the supervisory authority of the Data Exporter, as determined in accordance with Clause 13.

4. List of Authorized Sub-Processors

A list of the Company's Authorized Sub-Processors is available at the following link: https://www.prefect.io/security/sub-processors/

Exhibit C

Description of the Technical and Organisational Security Measures implemented by the Data Importer

The following includes the information required by Annex II of the EU SCCs and Appendix 2 of the UK SCCs.

On Customer's request and subject to appropriate confidentiality obligations Prefect will provide to Customer a copy of its current SOC 2 audit report and other applicable certifications.

Technical and Organizational Security Measure	**Details**
Measures of pseudonymisation and encryption of personal data	Processing is conducted on secure servers hosted on Google Cloud Platform. All storage systems are encrypted with industry standard algorithms. Data is encrypted in transit at all times. Access to Prefect systems is based on least privilege and a minimal set of engineers have access to Prefect production systems based on role. All Prefect laptops are encrypted and enforced using MDM.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Prefect runs highly available cloud services on Google Cloud Platform. Prefect conducts an annual penetration test with a third party and runs annual company-wide disaster recovery and business continuity playbook simulations. Audits of system access logs and user access logs are conducted quarterly for critical production systems and bi-annually for all other systems.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Prefect runs a highly available, multi-regional database system on Google Cloud Platform. Prefect tests disaster recovery simulations annually.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Prefect attained SOC 2 Type II certification in February 2022. The SOC 2 Type II report is available upon request and outlines Prefect's company-wide controls for the security of Prefect's data and systems and to ensure the availability of our services to Prefect users.
Measures for user identification and authorization	Access to all critical systems and production environments is protected using strong passwords and multi-factor authentication. Where possible, SSO is used for centralized access control.
Measures for the protection of data during transmission	Traffic is encrypted at all times and a minimum of TLS 1.2 is enforced on all our endpoints.
Measures for the protection of data during storage	All storage systems are encrypted with industry standard algorithms.
Measures for ensuring physical security of locations at which personal data are processed	Prefect does not maintain physical servers, and employees do not download sensitive data to their machines.
Measures for ensuring events logging	Prefect logs application events with tracing and monitoring tools and logs security events with intrusion detection and prevention tools. These tools are configured with defined thresholds,

	alerting policies and machine learning. Notifications for events are sent to Company Slack channels, paging systems (if applicable) and ticketing system for triage and remediation.
Measures for ensuring system configuration, including default configuration	Prefect runs infrastructure-as-code and therefore all changes to our systems follow our standard PR approval process. In addition, Prefect has a change control procedure that manages all changes that occur outside of code control.
Measures for internal IT and IT security governance and management	Chris White is Prefect's Chief Information Security Officer (CISO). This role oversees Prefect's day-to-day operations to ensure a secure environment, in addition setting security standards that apply to our organization as a whole.
Measures for certification/assurance of processes and products	Prefect attained SOC 2 Type II certification in February 2022. The SOC 2 Type II report is available on request and outlines our company-wide controls for the security of our data and systems and to ensure the availability of Prefect's services to our users.
Measures for ensuring data minimisation	Prefect uses a hybrid approach to managing and orchestrating customer workflows in their respective environments. Because of this hybrid approach, Prefect collects minimal user details for user management and login access to our cloud, and for the workflow orchestration itself, Prefect only depends on Prefect's workflow metadata. All customer code and data is executed and stored in the customer environment and not collected by Prefect on Prefect servers.
Measures for ensuring data quality	Prefect maintains a formal process for making non-automated changes to production data, and Prefect Cloud's API is strongly typed to ensure payloads are structured correctly.
Measures for ensuring limited data retention	Prefect retains sensitive and confidential data only for as long as necessary to fulfill the purposes for which it is collected and processed. Prefect provides customers with a process to request full account and data deletion.
Measures for ensuring accountability	All Prefect employees conduct annual training of security awareness and incident response. All Prefect employees are required to sign the Prefect Employee Handbook and Information Security Policy. All Prefect engineers are required to conduct additional training on Secure Coding.
Measures for allowing data portability and ensuring erasure	Prefect provides customers with a process to request full account and data deletion.
Technical and organizational measures of sub-processors	Prefect enters into Data Processing Agreements with its Authorized Sub-Processors with data protection obligations substantially similar to those contained in this Addendum.

An additional description of the Company's security practices can be found here: https://www.prefect.io/security/overview/, and may be amended from time to time.