Data Processing and Security Terms

These Data Processing and Security Terms, including their appendices (the "**Terms**") are incorporated into the agreement under which Crusoe has agreed to provide the Crusoe Cloud Platform (as described at Services) and related technical support to Customer (the "**Agreement**"). These Terms will be effective and replace any previously applicable data processing and security terms from the Terms Effective Date (as defined below).

Definitions

Capitalized terms defined in the Agreement apply to these Terms. In addition, in these Terms:

- "**Adequate Country**" means:
  a. for data processed subject to the EU GDPR: the EEA, or a country or territory that is the subject of an adequacy decision by the Commission under Article 45(1) of the EU GDPR;

  b. for data processed subject to the UK GDPR: the UK or a country or territory that is the subject of the adequacy regulations under Article 45(1) of the UK GDPR and Section 17A of the Data Protection Act 2018; and/or

  c. for data processed subject to the Swiss FDPA: Switzerland, or a country or territory that (i) is included in the list of the states whose legislation ensures an adequate level of protection as published by the Swiss Federal Data Protection and Information Commissioner, or (ii) is the subject of an adequacy decision by the Swiss Federal Council under the Swiss FDPA.
- "**Alternative Transfer Solution**" means a solution, other than SCCs, that enables the lawful transfer of personal data to a third country in accordance with European Data Protection Law.
- "**Customer Data**" has the meaning given in the Agreement or, if no such meaning is given, means data provided by or on behalf of Customer or Customer End Users via the Services under the Account.
- "**Customer End Users**" has the meaning given in the Agreement or, if not such meaning is given, has the meaning given to "End Users" in the Agreement.
- "**Customer Personal Data**" means the personal data contained within the Customer Data, including any special categories of personal data defined under European Data Protection Law.
- "**Customer SCCs**" means the SCCs (EU Controller-to-Processor), the SCCs (EU Processor-to-Processor), the SCCs (EU Processor-to-Controller), and/or the SCCs (UK Controller-to-Processor), as applicable.
- "**Data Incident**" means a breach of Crusoe's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed by or otherwise controlled by Crusoe.
- "**EEA**" means the European Economic Area.
- "**EMEA**" means Europe, the Middle East and Africa.
- "**EU GDPR**" means 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.

- “**European Data Protection Law**” means, as applicable: (a) the GDPR; and/or (b) the Swiss FDPA.
- “**European Law**” means, as applicable: (a) EU or EU Member State law (if the EU GDPR applies to the processing of Customer Personal Data); and (b) the law of the UK or a part of the UK (if the UK GDPR applies to the processing of Customer Personal Data).
- “**GDPR**” means, as applicable: (a) the EU GDPR; and/or (b) the UK GDPR.
- “**Instructions**” has the meaning given in Customer’s Instructions.
- “**Non-European Data Protection Law**” means data protection or privacy laws in force outside the EEA, the UK and Switzerland.
- “**Notification Email Address**” means the email address(es) designated by Customer in the Admin Console or Order Form to receive certain notifications from Crusoe. Customer is responsible for using the Admin Console to ensure that its Notification Email Address remains current and valid.
- “**Security Documentation**” means all documents and information made available by Crusoe at https://docs.crusoecloud.com/.
- “**Security Measures**” has the meaning given in Crusoe’s Security Measures.
- “**Subprocessor**” means a third party authorized as another processor under these Terms to have logical access to and process Customer Data in order to provide parts of the Services and TSS.
- “**Supervisory Authority**” means, as applicable: (a) a “supervisory authority” as defined in the EU GDPR; and/or (b) the “Commissioner” as defined in the UK GDPR and/or the Swiss FDPA.
- “**Swiss FDPA**” means the Federal Data Protection Act of 19 June 1992 (Switzerland).
- “**Term**” means the period from the Terms Effective Date until the end of Crusoe’s provision of the Services, including, if applicable, any period during which provision of the Services may be suspended and any post-termination period during which Crusoe may continue providing the Services for transitional purposes.
- “**Terms Effective Date**” means the date on which Customer accepted, or the parties otherwise agreed to, these Terms.
- “**UK GDPR**” means the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, and applicable secondary legislation made under that Act.

The terms “**personal data**”, “**data subject**”, “**processing**”, “**controller**” and “**processor**” as used in these Terms have the meanings given in the GDPR irrespective of whether European Data Protection Law or Non-European Data Protection Law applies.

Duration

Regardless of whether the Agreement has terminated or expired, these Terms will remain in effect until, and automatically expire when, Crusoe deletes all Customer Data as described in these Terms.

Scope of Data Protection Law

Application of European Law

The parties acknowledge that European Data Protection Law may apply to the processing of Customer Personal Data if, for example:

a. the processing is carried out in the context of the activities of an establishment of Customer in the territory of the EEA or the UK; and/or

b. the Customer Personal Data is personal data relating to data subjects who are in the EEA or the UK and the processing relates to the offering to them of goods or services in the EEA or the UK, or the monitoring of their behavior in the EEA or the UK.

Application of Non-European Law

The parties acknowledge that Non-European Data Protection Law may also apply to the processing of Customer Personal Data.

Application of Terms

Except to the extent these Terms state otherwise, these Terms will apply irrespective of whether European Data Protection Law or Non-European Data Protection Law applies to the processing of Customer Personal Data.

Processing of Data

Roles and Regulatory Compliance; Authorization

Processor and Controller Responsibilities

If European Data Protection Law applies to the processing of Customer Personal Data:

a. Crusoe is a processor of that Customer Personal Data under European Data Protection Law;

b. Customer is a controller or processor, as applicable, of that Customer Personal Data under European Data Protection Law; and

c. each party will comply with the obligations applicable to it under European Data Protection Law with respect to the processing of that Customer Personal Data.

Processor Customers

If European Data Protection Law applies to the processing of Customer Personal Data and Customer is a processor:

d. Customer warrants on an ongoing basis that the relevant controller has authorized: (i) the Instructions, (ii) Customer's appointment of Crusoe as another processor, and (iii) Crusoe's engagement of Subprocessors as described in Subprocessors;

e. Customer will immediately forward to the relevant controller any notice provided by Crusoe under Instruction Notifications or Incident Notification); and

f. Customer may make available to the relevant controller any other information made available by Crusoe under Information about Subprocessors.

Responsibilities under Non-European Law

If Non-European Data Protection Law applies to either party’s processing of Customer Personal Data, the relevant party will comply with any obligations applicable to it under that law with respect to the processing of that Customer Personal Data.

Scope of Processing

Customer’s Instructions

Customer may instruct Crusoe to process Customer Personal Data only in accordance with applicable law: (a) to provide, secure, and monitor the Services and TSS; (b) as further specified via Customer’s use of the Services (including the Admin Console and other functionality of the Services) and TSS; (c) as documented in the form of the Agreement (including these Terms); and (d) as further documented in any other written instructions given by Customer and acknowledged by Crusoe as constituting instructions for purposes of these Terms (collectively, the “**Instructions**”).

Crusoe’s Compliance with Instructions

Crusoe will comply with the Instructions unless prohibited by European Law.

Instruction Notifications

Crusoe will promptly notify Customer if, in Crusoe’s opinion: (a) European Law prohibits Crusoe from complying with an Instruction; (b) an Instruction does not comply with European Data Protection Law; or (c) Crusoe is otherwise unable to comply with an Instruction, in each case unless such notice is prohibited by European Law. This Section does not reduce either party’s rights and obligations elsewhere in the Agreement.

Data Deletion

Deletion by Customer during the Term

Crusoe will enable Customer to delete Customer Data during the Term in a manner consistent with the functionality of the Services. Crusoe will comply with a Customer Instruction to to delete Customer Data from Crusoe’s systems as soon as reasonably practicable, unless European Law requires storage.

Return or Deletion at the end of the Term

If Customer wishes to retain any Customer Data after the end of the Term, it may export such data in accordance with Access; Rectification; Restricted Processing; Portability during the Term. All Customer Data (including existing copies) remaining at the end of the Term will be deleted from Crusoe’s systems unless European Law requires storage.

Data Security

Crusoe’s Security Measures, Controls and Assistance

Crusoe’s Security Measures

Crusoe will implement and maintain technical and organizational measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Appendix 2 (the “**Security Measures**”). Crusoe may update the Security Measures from time to time provided that such updates do not result in a material reduction of the security of the Services.

Access and Compliance

Crusoe will: (a) authorize its employees, contractors and Subprocessors to access Customer Personal Data only as strictly necessary to comply with Instructions; (b) take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Subprocessors to the extent applicable to their scope of performance; and (c) ensure that all persons authorized to process Customer Personal Data are under an obligation of confidentiality.

Crusoe’s Security Assistance

Crusoe will (taking into account the nature of the processing of Customer Personal Data and the information available to Crusoe) assist Customer in ensuring compliance with its (or, where Customer is a processor, the relevant controller’s) obligations under Articles 32 to 34 of the GDPR, by:

a. implementing and maintaining the Security Measures;

b. complying with the terms of Data Incidents;

c. providing Customer with the Security Documentation and the information contained in the Agreement (including these Terms); and

d. if subsections (a)-(c) above are insufficient for Customer (or the relevant controller) to comply with such obligations, upon Customer’s request, providing Customer with additional reasonable cooperation and assistance.

Data Incidents

Incident Notification

After becoming aware of a Data Incident, Crusoe will promptly notify Customer and take reasonable steps to minimize harm and secure Customer Data.

Details of Data Incident

Crusoe’s notification of a Data Incident will describe: the nature of the Data Incident including the Customer resources impacted; the measures Crusoe has taken, or plans to take, to address the Data Incident and mitigate its potential risk; the measures, if any, Crusoe recommends that Customer take to address the Data Incident; and details of a contact point where more information can be obtained.

If it is not possible to provide all such information at the same time, Crusoe's initial notification will contain the information then available and further information will be provided without undue delay as it becomes available.

Delivery of Notification

Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address.

No Assessment of Customer Data by Crusoe

Crusoe has no obligation to assess Customer Data in order to identify information subject to any specific legal requirements.

No Acknowledgement of Fault by Crusoe

Crusoe's notification of or response to a Data Incident under Data Incidents will not be construed as an acknowledgement by Crusoe of any fault or liability with respect to the Data Incident.

Customer's Security Responsibilities and Assessment

Customer's Security Responsibilities

Without prejudice to Crusoe's obligations under Crusoe's Security Measures, Controls and Assistance and Data Incidents), and elsewhere in the Agreement, Customer is responsible for its use of the Services and its storage of any copies of Customer Data outside Crusoe's or Crusoe's Subprocessors' systems, including:

a. using the Services to ensure a level of security appropriate to the risk to the Customer Data;

b. securing the account authentication credentials, systems and devices Customer uses to access the Services; and

c. backing up its Customer Data as appropriate.

Customer's Security Assessment

Customer agrees that the Services, Security Measures implemented and maintained by Crusoe, and Crusoe's commitments under Data Security provide a level of security appropriate to the risk to Customer Data (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Customer Personal Data as well as the risks to individuals).

Impact Assessments and Consultations

Crusoe will (taking into account the nature of the processing and the information available to Crusoe) assist Customer in ensuring compliance with its (or, where Customer is a processor, the relevant controller's) obligations under Articles 35 and 36 of the GDPR, by:

a. providing the Security Documentation;

b. providing the information contained in the Agreement (including these Terms); and

c. if subsections (a) and (b) above are insufficient for Customer (or the relevant controller) to comply with such obligations, upon Customer's request, providing Customer with additional reasonable cooperation and assistance.

Access etc.; Data Subject Requests

Access; Rectification; Restricted Processing; Portability

During the Term, Crusoe will enable Customer, in a manner consistent with the functionality of the Services, to access, rectify and restrict processing of Customer Data, including via the deletion functionality provided by Crusoe as described in Deletion by Customer, and to export Customer Data. If Customer becomes aware that any Customer Personal Data is inaccurate or outdated, Customer will be responsible for using such functionality to rectify or delete that data if required by applicable European Data Protection Law.

Data Subject Requests

During the Term, if Crusoe receives a request from a data subject that relates to Customer Personal Data and identifies Customer, Crusoe will: (a) advise the data subject to submit their request to Customer; (b) promptly notify Customer; and (c) not otherwise respond to that data subject's request without authorization from Customer. Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.

Data Transfers

Data Storage and Processing Facilities

Subject to Crusoe's data location commitments under the Service Specific Terms and to the remainder of Data Transfers, Customer Data may be processed in any country in which Crusoe or its Subprocessors maintain facilities.

Permitted Transfers

The parties acknowledge that European Data Protection Law does not require an Alternative Transfer Solution in order for Customer Personal Data to be processed in or transferred to an Adequate Country (“**Permitted Transfers**”).

Restricted Transfers

If the processing of Customer Personal Data involves any transfers that are not Permitted Transfers, and European Data Protection Law applies to those transfers (as certified by Customer under Certification by Non-EMEA Customers if its billing address is outside EMEA) (“**Restricted Transfers**”), then:

a. if Crusoe announces its adoption of an Alternative Transfer Solution for any Restricted Transfers, then Crusoe will ensure that they are made in accordance with that Alternative Transfer Solution; and/or

b. if Crusoe has not adopted an Alternative Transfer Solution for any Restricted Transfers, then:
    i. if Crusoe's address is in an Adequate Country:
        1. the SCCs (EU Processor-to-Processor, Crusoe Exporter) will apply with respect to all Restricted Transfers from Crusoe to Subprocessors; and in addition,
        2. if Customer's billing address is not in an Adequate Country, the SCCs (EU Processor-to-Controller) will apply (regardless of whether Customer is a controller and/or processor) with respect to Restricted Transfers between Crusoe and Customer; or
    ii. if Crusoe's address is not in an Adequate Country:
        1. the SCCs (EU Controller-to-Processor) and/or SCCs (EU Processor-to-Processor) will apply (according to whether Customer is a controller and/or processor) with respect to Restricted Transfers between Crusoe and Customer that are subject to the EU GDPR and/or the Swiss FDPA; and
        2. the SCCs (UK Controller-to-Processor) will apply (regardless of whether Customer is a controller and/or processor) with respect to Restricted Transfers between Crusoe and Customer that are subject to the UK GDPR.

Certification by Non-EMEA Customers

If Customer's billing address is outside EMEA, and the processing of Customer Personal Data is subject to European Data Protection Law, Customer will certify as such, and identify its competent Supervisory Authority, via the Admin Console.

Subprocessors

Consent to Subprocessor Engagement

Customer specifically authorizes the engagement as Subprocessors of those entities listed as of the Terms Effective Date at the URL specified in Information about Subprocessors. In addition, Customer generally authorizes the engagement as Subprocessors of any other third parties ("**New Subprocessors**").

Information about Subprocessors

Information about Subprocessors, including their functions and locations, is available at Crusoe Cloud Subprocessors (as may be updated by Crusoe from time to time in accordance with these Terms).

Requirements for Subprocessor Engagement

When engaging any Subprocessor, Crusoe will ensure that: (a) the Subprocessor only accesses and uses Customer Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Agreement (including these Terms); and (b) if the processing of Customer Personal Data is subject to European Data Protection Law, the data protection obligations described in these Terms (as referred to in Article 28(3) of the GDPR, if applicable), are imposed on the Subprocessor.

Support; Processing Records

Support

Crusoe will provide prompt and reasonable assistance with any Customer queries related to processing of Customer Personal Data under the Agreement and can be contacted at support@crusoecloud.com (and/or via such other means as Crusoe may provide from time to time).

Crusoe's Processing Records

Crusoe will keep appropriate documentation of its processing activities as required by the GDPR. To the extent the GDPR requires Crusoe to collect and maintain records of certain information relating to Customer, Customer will use the Admin Console to supply such information and keep it accurate and up-to-date. Crusoe may make any such information available to the Supervisory Authorities if required by the GDPR.

Controller Requests

During the Term, if Crusoe receives a request or instruction from a third party purporting to be a controller of Customer Personal Data, Crusoe will advise the third party to contact Customer.

Appendix 1: Subject Matter and Details of the Data Processing

Subject Matter

Crusoe’s provision of the Services and TSS to Customer.

Duration of the Processing

The Term plus the period from the end of the Term until deletion of all Customer Data by Crusoe in accordance with the Terms.

Nature and Purpose of the Processing

Crusoe will process Customer Personal Data for the purposes of providing the Services and TSS to Customer in accordance with the Terms.

Categories of Data

Data relating to individuals provided to Crusoe via the Services, by (or at the direction of) Customer or by Customer End Users.

Data Subjects

Data subjects include the individuals about whom data is provided to Crusoe via the Services by (or at the direction of) Customer or by Customer End Users.

Appendix 2: Security Measures

As from the Terms Effective Date, Crusoe will implement and maintain the Security Measures described herein.

Data Centers

Infrastructure

Crusoe maintains geographically distributed data centers. Crusoe stores all production data in physically secure data centers.

Redundancy

Infrastructure systems have been designed to minimize single points of failure and the impact of anticipated environmental risks. Reasonable technical measures have been taken, where possible, to provide this redundancy. The Services are designed to allow Crusoe to perform certain types of preventative and corrective maintenance without interruption. When customer interruption is expected as part of a planned maintenance event, Crusoe will provide notice to customers ahead of the event. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to documented procedures.

Power

The data center electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, 7 days a week. In most cases, a primary as well as an alternate power source, each with sufficient capacity to power a data center, is provided for critical infrastructure components in the data center. Backup power is provided by various mechanisms such as uninterruptible power supplies (UPS) batteries, which supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If primary power is interrupted, backup power is designed to provide transitory power to the data center, at full capacity, until the backup generator systems take over. The backup generators are capable of automatically starting up within seconds to provide enough emergency electrical power to run the data center at full capacity typically for a period of days.

Networks and Transmission

Data Transmission

Data centers are typically connected via high-speed private links to provide secure and fast data transfer between data centers. This is designed to prevent data from being read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. Crusoe transfers data via Internet standard protocols.

External Attack Surface

Crusoe employs multiple layers of network devices and intrusion detection to protect its external attack surface. Crusoe considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems.

Intrusion Detection

Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Crusoe’s intrusion detection involves controlling the size and make-up of Crusoe’s attack surface through preventative measures.

Incident Response

Crusoe monitors a variety of communication channels for security incidents, and Crusoe’s security personnel will react promptly to known incidents.

Encryption Technologies

Crusoe makes HTTPS encryption (also referred to as SSL or TLS connection) available. Crusoe servers support ephemeral elliptic curve Diffie-Hellman cryptographic key exchange signed with RSA and ECDSA. These perfect forward secrecy (PFS) methods help protect traffic and minimize the impact of a compromised key, or a cryptographic breakthrough.

Site and Access Controls

Crusoe maintains formal access procedures for allowing physical access to the data centers. Only authorized employees, contractors and visitors are allowed entry to the data centers. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving.

Customer’s administrators and Customer End Users must authenticate themselves via a central authentication system in order to use the Services.

Crusoe’s internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to Crusoe’s systems. Crusoe designs its systems to only allow authorized persons to access data they are authorized to access. Crusoe employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. Crusoe’s authentication and authorization systems utilize SSH certificates and security keys, and are designed to provide Crusoe with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. Crusoe requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel’s job responsibilities; job duty requirements necessary to perform authorized tasks; and a need to know basis. The granting or modification of access rights must also be in accordance with Crusoe’s internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies that follow at least industry standard practices are implemented. These standards include restrictions on password reuse and sufficient password strength.

Data

Crusoe stores data in a multi-tenant environment on Crusoe-owned servers. Subject to any Instructions to the contrary (e.g., in the form of a data location selection), Crusoe replicates Customer Data between multiple data centers. Crusoe also logically isolates Customer Data. Customer will be given control over specific data sharing policies. Those policies, in accordance with the functionality of the Services, will enable Customer to determine the product sharing settings applicable to Customer End Users for specific purposes.

Personnel

Crusoe personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Crusoe conducts reasonably appropriate background checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations. Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Crusoe's confidentiality and privacy policies.

Subprocessors

Before onboarding Subprocessors, Crusoe ensures Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Crusoe has assessed the risks presented by the Subprocessor, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.