AIRLOCK DIGITAL

Global Data Protection Agreement
June 2025 v2.1

This DPA supplements any existing and currently valid Airlock Digital terms and conditions, purchase order or other similar agreement (each “Agreement”) previously made between Airlock Digital and the Customer (defined below) (collectively, the “Parties”), if and only to the extent:

a. this DPA is required under Applicable Laws (defined below), and

b. where Airlock Digital Processes Customer Personal Data (both defined below).

This DPA supersedes and replaces any prior Data Protection Agreement, or any other prior understanding or agreement, related to the processing of Customer Personal Data in connection with the Agreement.

a. This DPA will become legally binding upon the earlier of Customer:installing any Airlock Digital software; or

b. executing a software subscription agreement or licence for the use of Airlock Digital’s software or other services.

1. Definitions

1.1 Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect. Cognate terms shall be construed to have the same meaning.

1.2 "Applicable Laws" means any laws that regulate the Processing, privacy or security of Customer Personal Data and that are directly applicable to each respective party to this DPA in the context of Airlock Digital Processing Customer Personal Data.

1.3 “Airlock Digital Affiliate" means an entity belonging to the Airlock Digital group of companies named in Exhibit E as an Airlock Digital Affiliated Subprocessor. The term “Airlock Digital” is inclusive of the applicable Airlock Digital Affiliate when: (i) Applicable Laws require a direct relationship between Airlock Digital Affiliate and the Customer with respect to data protection agreements, and (ii) the Airlock Digital Affiliate processes Customer Personal Data. Airlock Digital represents that it is duly and effectively authorized (or will be subsequently ratified) to act on the Airlock Digital Affiliate’s behalf.

1.4 “Customer” means (i) the person or entity that is indicated below in the signature block, or (ii) if there is no signature block or it is not completed, then Customer is the person or entity that has entered into the Agreement with Airlock Digital. Customer also means a Customer Affiliate when: (i) Applicable Laws require a direct relationship between Airlock Digital and the Customer’s Affiliate with respect to data protection agreements, (ii) Customer is duly and effectively authorized (or subsequently ratified) to act on its Affiliate’s behalf, and (iii) Airlock Digital processes the Affiliate’s Customer Personal Data.

1.5 "Customer Personal Data" means any Personal Data Processed by Airlock Digital or a Subprocessor on behalf of the Customer in the provision of the Services.

1.6 "GDPR" means the General Data Protection Regulation 2016/679 (“GDPR”) and any local laws implementing or supplementing the GDPR.

1.7 “Onward Transfer” means any transfer of Customer Personal Data from Airlock Digital to a Subprocessor.

1.8 "Restricted Transfer" means any export of Customer Personal Data by Customer to Airlock Digital from its country of origin, either directly or via onward transfer, to a third country in the course of Airlock Digital’s provision of the Services under the Agreement that is prohibited under Applicable Laws, unless (a) the destination has been recognized as providing an adequate level of data protection by competent data protection authority, or otherwise in a legally binding way, or (b) Airlock Digital has adopted an appropriate, under Applicable Laws recognized, adequacy mechanism ensuring an adequate level of data protection.

1.9 “Services” means the products or services offered by Airlock Digital.

1.10 “Standard Contractual Clauses” means the standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR as to the European Commission Implementing Decision (EU) 2021/914 or any subsequent final version as adopted by Airlock Digital.

1.11 "Subprocessor" means any contracted service provider (including any third party and Airlock Digital Affiliate but excluding an employee of Airlock Digital or Airlock Digital subcontractors unless specified in an applicable Statement of Work) Processing Customer Personal Data in the course of Airlock Digital’s provisioning of the Services set forth in the Agreement.

1.12 The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", “Processor”, "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR.

1.13 The word "include" shall be construed to mean include without limitation.

2. Processing of Customer Personal Data

2.1 Airlock Digital acts as a Processor, and Customer and those entities that it permits to use the Services act as Controllers under the DPA.

2.2 The Parties acknowledge and agree that with regard to the Processing of Customer Personal Data, Customer determines the purposes and means of the Processing of Customer Personal Data, and Airlock Digital processes Customer Personal Data on Customer’s behalf in providing the Services.

2.3 Customer acts as a single point of contact and shall obtain any relevant authorizations, consents, and permissions for the processing of Personal Data in accordance with this DPA, including, where applicable approval by Controllers to use Airlock Digital as a Processor.

2.4 Airlock Digital shall:

a. process Customer Personal Data only on relevant Customer’s documented instructions, as set out in the Agreement, this DPA, including Customer providing instructions via configuration tools and APIs made available by Airlock Digital with the Services, and as required by Applicable Laws (the “Documented Instructions”). Any additional or alternate instructions, having an impact to the Services must be agreed upon by the Parties separately in writing; and

b. unless prohibited by Applicable Law, Airlock Digital shall inform the Customer in advance if Airlock Digital determines that:

(i) Customer’s instructions conflict with Applicable Laws; or

(ii) Applicable Laws require any processing contrary to the Customer’s instructions.

2.5 Customer shall:

a. be responsible for complying with Applicable Laws when making decisions and issuing instructions for the Processing of Customer Personal Data, including securing all permissions, consents or authorizations that may be required.

b. defend and indemnify Airlock Digital, Airlock Digital Affiliates, and Airlock Digital Subprocessors for any claim brought against them arising from an allegation of Customer’s breach of this section, whether by a Data Subject or a government authority. This provision does not diminish Customer or Data Subject’s rights under Applicable Laws related to Airlock Digital’s adherence to its obligations under Applicable Laws, and in the event of such a claim, the Parties shall follow the process set forth in the Agreement and if none, then Airlock Digital will:

(i) notify Customer of such claim,

(ii) permit Customer to control the defense or settlement of such claim; provided, however, Customer shall not settle any claim in a manner that requires Airlock Digital to admit liability without Airlock Digital’s prior written consent, and

(iii) provide Customer with reasonable assistance in connection with the defense or settlement of such claim, at Customer’s cost and expense. In addition, Airlock Digital may participate in defense of any claim, and if Customer is already defending such claim, Airlock Digital’s participation will be at Airlock Digital’s expense.

3. Airlock Digital Personnel

3.1 Airlock Digital shall take reasonable steps to:

a. implement appropriate security controls designed to ensure access to Customer Personal Data is limited to those individuals who need to know/access the relevant Customer Personal Data as reasonably necessary for the purposes outlined in this DPA, the Agreement or required under Applicable Laws; and

b. ensure all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 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, Airlock Digital shall in relation to the Processing of Customer Personal Data maintain appropriate technical and organizational measures as specified in the Agreement and designed to ensure a level of security appropriate to the risk, including, as appropriate, the measures referred to in the Applicable Laws.

4.2 In assessing the appropriate level of security, Airlock Digital shall take into account the nature of the data and the Processing activities in assessing the risks posed by a potential Personal Data Breach.

5. Subprocessing

5.1 Airlock Digital is granted a general authorization to subcontract the processing of Personal Data to Subprocessors, provided that:

a. Airlock Digital or Airlock Digital Affiliates on its behalf shall engage Subprocessors under a written (including in electronic form) contract consistent with the terms of this DPA in relation to the Subprocessor's processing of Personal Data. Airlock Digital shall be liable for any breaches by the Subprocessor in accordance with the terms of this Agreement.

b. Airlock Digital will evaluate the security, privacy and confidentiality practices of a Subprocessor prior to selection to establish that it is capable of providing the level of protection of Personal Data required by this DPA; and

c. Airlock Digital' list of Subprocessors in place on the effective date of the Agreement is set out in Exhibit E.

5.2 Airlock Digital' use of Subprocessors is at its discretion, provided that:

a. Airlock Digital will inform Customer in advance (by email or by posting on the Cloud Service) of any intended additions or replacements to the list of Subprocessors including name, address and role of the new Subprocessor; and

b. Customer may object to such changes as set out in Section 6.

6. Objections to New Subprocessors.

6.1 If Customer has a legitimate reason under Applicable Law to object to the new Subprocessors' processing of Personal Data, subject to the provisions of this Section 6 Customer may terminate the Agreement (limited to the Service(s) for which the new Subprocessor is intended to be used) on written notice to Airlock Digital.

6.2 A termination under section 6.1 shall take effect at the time determined by the Customer which shall be no later than 30 days from the date of Airlock Digital' notice to Customer informing Customer of the new Subprocessor provided that if Customer does not terminate within this 30 day period, Customer is deemed to have accepted the new Subprocessor.

6.3 Within the 30 day period from the date of Airlock Digital' notice to Customer informing Customer of the new Subprocessor, Customer may request that the parties discuss in good faith a resolution to the objection. Such discussions shall not extend the period for termination and do not affect Airlock Digital' right to use the new Subprocessor(s) after the 30 day period.

6.4 Any termination under this Section 6.3 shall be deemed to be without fault by either party and shall be subject to the terms of the Agreement.

6.5 Airlock Digital may replace a Subprocessor without advance notice where the reason for the change is outside of Airlock Digital' reasonable control and prompt replacement is required for security or other urgent reasons. In this case, Airlock Digital will inform Customer of the replacement Subprocessor as soon as possible following its appointment.

7. Data Subject Rights

7.1 Customer represents and warrants to provide appropriate transparency to any Data Subjects concerned with Airlock Digital's Processing of Customer Personal Data and respond to any request filed by Data Subjects as required under Applicable Laws.

7.2 Taking into account the nature of the Customer Personal Data Processing, Airlock Digital shall:

a. not respond to the Data Subject request itself or by Subprocessor unless required by Applicable Laws; and

b. notify Customer without undue delay if Airlock Digital or any Subprocessor receives a request from a Data Subject under any Applicable Laws in respect to Customer Personal Data; and

c. reasonably assist Customer through appropriate technical and organizational measures to fulfil Customer's obligation to respond to Data Subject requests arising under Applicable Law, and where Customer is unable to respond to Data Subject requests through the information available by the Services.

8. Personal Data Breach

8.1 Upon Airlock Digital becoming aware of any Personal Data Breach affecting Customer Personal Data Airlock Digital shall without undue delay, and within the timeframes required by Applicable Laws, notify Customer of such Personal Data Breach, and Airlock Digital will:

a. to the extent known, provide Customer with sufficient information to meet obligations under Applicable Laws to report or inform Data Subjects of such Personal Data Breach; and

b. cooperate with Customer and take commercially reasonable steps to assist in the investigation, mitigation, and remediation of such Personal Data Breach.

9. Obligations to Assist Customer

9.1 Taking into account the nature of the Processing and information available to Customer in each case solely in relation to Airlock Digital's Processing of Customer Personal Data, Airlock Digital shall provide reasonable assistance to Customer with any:

a. necessary data protection impact assessments required of Customer by Applicable Laws;

b. consultation with or requests of a competent data protection authority;

c. inquiries about Airlock Digital's Processing of Customer Personal Data pursuant to the Agreement and this DPA.

10. Deletion of Customer Personal Data

10.1 Processing of Customer Personal Data by Airlock Digital shall only take place for the duration specified in Exhibit A.

10.2 At the end of the duration specified in Exhibit A or upon termination of the Services and pursuant to the Agreement:

a. Customer Personal Data will be deleted within 90 days of the Services being deprovisioned unless the retention of Customer Personal Data is required under Applicable Laws.

b. Upon Customer's written request, Airlock Digital shall:

(i) make Customer Personal Data available for return to Customer where such a request has been made prior to deletion by reasonably providing Customer with a means to retrieve Customer Personal Data from the Services; and

(ii) provide a written certification of deletion of Customer Personal Data to Customer.

11. Audit Rights

11.1 Subject to sections 10.2 to 10.4, Airlock Digital shall make available to Customer on request information necessary to demonstrate compliance with Applicable Laws and this DPA.

11.2 Customer or its independent third party auditor reasonably acceptable to Airlock Digital (which shall not include any third party auditors who are either a competitor of Airlock Digital or not suitably qualified or independent) may audit Airlock Digital' control environment and security practices relevant to Personal Data processed by Airlock Digital only if:

a. Airlock Digital has not provided sufficient evidence of its compliance with the Technical and Organizational Measures that protect the production systems of the Cloud Service through providing either:

b. a certification as to compliance with ISO 27001 or other standards (scope as defined in the certificate); or

c. a valid ISAE3402 or ISAE3000 or other SOC1-3 attestation report.

d. a Personal Data Breach has occurred;

e. an audit is formally requested by Customer's data protection authority; or

f. provided under a mandatory Applicable Law conferring Customer a direct audit right and provided that Customer shall only audit once in any 12 month period unless a mandatory Applicable Law requires more frequent audits.

11.3 Another Controller may assume Customer's rights under Section 11.2 only if it applies directly to the Controller and such audit is permitted and coordinated by Customer.

11.4 Customer shall use all reasonable means to combine audits of multiple other Controllers to avoid multiple audits unless the audit must be undertaken by the other Controller itself under Applicable Law.

11.5 Notwithstanding the foregoing, Airlock Digital may exclude information and documentation that would reveal the identity of other Airlock Digital customers or information that Airlock Digital is required to keep confidential, and any information or records provided pursuant to this assessment process shall be considered Airlock Digital's Confidential Information and subject to the Confidentiality section of the Agreement.

11.6 Customer shall provide at least 60 days advance notice of any audit unless mandatory Applicable Law or a competent data protection authority requires shorter notice.

11.7 Customer audits shall be limited in time to a maximum of 3 business days and beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimize repetitive audits.

11.8 Customer shall provide the results of any audit to Airlock Digital.

11.9 Customer shall bear the costs of any audit unless such audit reveals a material breach by Airlock Digital of this DPA, then Airlock Digital shall bear its own expenses of an audit. If an audit determines that Airlock Digital has breached its obligations under the DPA, Airlock Digital will promptly remedy the breach at its own cost

12. Restricted Transfers from jurisdictions requiring safeguards to cross-border data transfer

12.1 Where, in the use of the Services or performance of the Agreement, Customer directly, indirectly or via onward transfer makes a Restricted Transfer of Customer Personal Data originating from the EEA, Israel, Switzerland and/or the United Kingdom ("UK") to a third country, not determined by the European Commission, on the basis of Article 45 of the GDPR, or another competent supervisory authority under Applicable Laws, offering an adequate level of data protection, and where Airlock Digital has not adopted another legally sufficient adequacy mechanism and provided notice to the Customer, the Standard Contractual Clauses will be incorporated into this DPA and shall apply as follows:

12.2 The Parties acknowledge and agree:

a. Airlock Digital will be a Data Importer acting as Processor of Customer Personal Data (or Subprocessor, as the context below requires) to a Restricted Transfer.

b. Where Customer will be a Data Exporter acting as Controller, Module 2 (Controller to Processor) will apply to a Restricted Transfer.

c. Where Customer will be a Data Exporter acting as a Processor, Module 3 (Processor to Processor) will apply to a Restricted Transfer. Taking into account the nature of the Processing, Customer agrees that it is unlikely that Airlock Digital will know the identity of Customer's Controllers because Airlock Digital has no direct relationship with Customer's Controllers and therefore, Customer will fulfil Airlock Digital's obligations to Customer's Controllers under the Module 3 (Processor to Processor) Clauses.

d. Where Airlock Digital will be Data Importer Processing Customer Personal Data in its own discretion as Controller in the provisioning of the Services agreed, e.g., for administering the Agreement, Module 1 (Controller to Controller) will apply to the relationship between Customer (Data Exporter) and Airlock Digital (Data Importer).

(i) that Customer's instructions may not conflict with the Services and any additional or alternate instructions, having impact to the Services, must be agreed upon separately between the Parties.

(ii) The following is a mutually agreed instruction: (a) Processing of Customer Personal Data in accordance with the Agreement and any applicable orders; (b) Processing initiated by users in their use of the Airlock Digital Services, and (c) Processing to comply with other reasonable documented instructions provided by Customer (e.g. via email) where such instructions are consistent with the terms of the Agreement.

(iii) A reference to a Clause in this Section 12 is a reference to the Standard Contractual Clauses.

12.3 Customer acknowledges and expressly agrees that the process described in Section 10 of the DPA shall govern the fulfilment of requirements related to data erasure and return of Customer Personal Data.

12.4 Clause 9 (Use of sub-processors). The Parties agree to and choose Option 2 (General written authorization) and specify the time period set forth in Section 6.3 of this DPA provided that Customer further acknowledges and agrees that Airlock Digital may engage existing Subprocessors (Exhibit E), and new Subprocessors as described there and Airlock Digital maintains an up-to-date List of Subprocessors online as outlined in Exhibit E.

12.5 Where the Customer is a Processor to Customer Personal Data, Customer agrees and warrants to be duly authorized to receive and pass on information about Airlock Digital's new Subprocessor engagement to Controllers with whom Airlock Digital has no direct relationship, assisting Airlock Digital to meet its obligation under Clause 9 towards the Controllers.

12.6 Clause 11(a) (Redress). The Parties agree that the option provided shall not apply.

12.7 Clause 13 (Supervision). The options in Clause 13 will be selected in line with the Customer's establishment.

12.8 Clause 17 (Governing law). The Parties agree to and choose Option 2; where such law does not allow for third-party beneficiary rights, the Parties agree that this shall be the law of the Netherlands.

12.9 The Exhibits A to E of this DPA substitutes the Annexes I to III required under the Standard Contractual Clauses providing the mandatory information under Applicable Laws.

12.10 Where the Restricted Transfer concerns Customer Personal Data originating from Switzerland, in line with the Swiss Federal Data Protection and Information Commissioner's statement as of August, 27, 2021, the following additional requirements shall apply to the extent the Customer Personal Data transferred is exclusively subject to the Swiss Data Protection Act (FADP) or to both the FADP and the GDPR: (i) The term 'member state' must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 (c) of these Standard Contractual Clauses. (ii) Insofar as the data transfers underlying these Standard Contractual Clauses are exclusively subject to the FADP, references to the GDPR are to be understood as references to the FADP. Insofar as the data transfers underlying these Standard Contractual Clauses are subject to both the FADP and the GDPR, the references to the GDPR are to be understood as references to the FADP insofar as the data transfers are subject to the FADP. (iii) Until the revised Swiss Data Protection Act (rev. FADP) enters into force, the provisions of these Standard Contractual Clauses and all Exhibits also protect any Customer Personal Data to the extent that these provisions are applicable to them under Applicable Swiss Laws.

12.11 Where the Restricted Transfer concerns Customer Personal Data originating from the UK, the Standard Contractual Clauses will apply subject to the conditions set out by the United Kingdom Information Commissioner Office's ("ICO") International Data Transfer Addendum to the Standard Contractual Clauses that shall be incorporated herein by reference. The Parties acknowledge and agree that this DPA and the Exhibits A to E (i) provide the information needed and required by the ICO for completing Part One of the International Data Transfer Addendum, and (ii) shall be governed by the laws and courts of England and Wales (Clauses 17 and 18 of the Standard Contractual Clauses) for completing Part Two of the International Data Transfer Addendum.

12.12 Where the Restricted Transfer concerns Customer Personal Data originating from Argentina, the standard contractual clauses made under Regulation No. 60-E/2016 will be incorporated into this DPA by reference and shall apply to the extent required under Applicable Laws and where this DPA does not provide adequate safeguards.

12.13 Where the Restricted Transfer concerns Customer Personal Data originating from another jurisdiction requiring certain privacy safeguards, standard contractual clauses, or any other contractual privacy provisions, not provided through this DPA, the Standard Contractual Clauses will be incorporated into this DPA by reference and shall apply to the extent required under Applicable Laws and where this DPA does not provide adequate safeguards. For the avoidance of any doubt, by applying the Standard Contractual Clauses in this event, the Parties do not intend to grant third-party beneficiary rights to Data Subjects under the Standard Contractual Clauses when Data Subjects concerned would not otherwise benefit from such rights under the Applicable Laws or this DPA.

13. General Terms

Governing law and jurisdiction

13.1 The Parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity. Where, in line with section 11 of this DPA the Standard Contractual Clauses apply, and it is required under Applicable Laws, for disputes arising the governing law and jurisdiction are stipulated in Clause 17 of the Standard Contractual Clauses.

Order of precedence

13.2 Any conflict between the terms of the Agreement and this DPA related to the processing of Customer Personal Data are resolved in the following order of priority:

a. the Standard Contractual Clauses (where applicable and materially affecting the adequacy of the Restricted Transfer);

b. this DPA;

c. the Agreement.

13.3 For the avoidance of doubt, provisions in this DPA, that merely go beyond the Standard Contractual Clauses without contradicting them, shall remain valid. The same applies to conflicts between this DPA and the Agreement where this DPA shall only prevail regarding the Parties' Personal Data protection obligations.

13.4 Should any provision of this DPA be invalid or unenforceable then the remainder of this DPA shall remain valid and in force and the invalid or unenforceable provision shall be either:

13.5 amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, should this not be possible; or

13.6 construed in a manner as if the invalid or unenforceable part had never been contained therein.

13.7 For the avoidance of doubt, by applying the provisions of this DPA, the Parties do not intend to grant third-party beneficiary rights to Data Subjects under the DPA when those Data Subjects would not otherwise benefit from such rights under the Applicable Laws.

Limitation of Liability

13.8 Unless required by Applicable Laws, Customer shall exercise any right or seek any remedy on behalf of itself, its Affiliates, and any other Controller that Customer instructs Airlock Digital to process Customer Personal Data for under this DPA (collectively, the "Customer Parties").

13.9 Customer shall exercise any such rights or seek any such remedies in a combined manner for all Customer Parties together, rather than separately for each entity individually.

13.10 To the maximum extent allowed by Applicable Laws, the limitations of liability and any exclusions of damages set forth in the Agreement govern the aggregate liability for all Customer Parties' claims arising out of or related to this DPA, and/or the Agreement against Airlock Digital and any Airlock Digital Affiliate(s).

13.11 These limitations of liability and exclusions of damages apply to all claims, whether arising under contract, tort or any other theory of liability, and any reference to the liability of Airlock Digital means the aggregate liability of Airlock Digital and all Airlock Digital Affiliates together for claims by Customer and all other Customer Parties.

13.12 To the extent required by Applicable Laws:

a. this section is not intended to modify or limit the Parties' liability for Data Subject claims made against a Party where there is joint and several liability, or

b. limit either Party's responsibility to pay penalties imposed on such Party by a regulatory authority.

EXHIBIT A

DESCRIPTION OF PROCESSING AND TRANSFER OF CUSTOMER PERSONAL DATA

This Exhibit A includes certain details of the Processing and Restricted Transfer of Customer Personal Data as required by Article 28(3) GDPR and the Standard Contractual Clauses.

Subject matter, nature and duration of the Processing and transfer of Customer Personal Data

The subject matter, nature and duration of the Processing and the transfer of the Customer Personal Data are set out in the Agreement and this DPA and depend on the nature and scope of the Services, manner of receipt, collection, storage, use, dissemination (towards Subprocessors in line with the Agreement and this DPA), retention and erasure of Customer Personal Data, and Customer's Documented Instructions.

Purpose for which the Personal Data is Processed and transferred on behalf of the Customer

The purposes of the Processing and transfer of the Customer Personal Data is to enable Airlock Digital and Airlock Digital's Subprocessor to provision and deliver the Services and perform its obligations as set forth in the Agreement, this DPA, and Customer's Documented Instructions or as otherwise agreed by the Parties in mutually executed written form.

Categories of Personal Data Processed and Transferred including sensitive Personal Data

The Customer, rather than Airlock Digital, determines which categories of Personal Data exist and will be disclosed to and Processed by Airlock Digital in the provisioning of the Services because (i) Customer's infrastructure (e.g., endpoint, virtual machine and cloud environments) is unique in configurations and naming conventions, (ii) Airlock Digital enables the Customer to configure settings in the Services, and (iii) Customer controls (such as via deployment, configuration, and submission) which Customer Content is uploaded, or is collected by, the Airlock Digital Services.

Categories of Data Subjects whose Personal Data is Processed

The Customer, rather than Airlock Digital, determines which Data Subjects' Personal Data is Processed by Airlock Digital through the Customer Content put into, or collected by, the Airlock Digital Services.

Frequency of the Transfer of Personal Data

Taking into account Airlock Digital's Customer Personal Data Processing including the manner of receipt, collection, storage, and use of Customer Personal Data, the frequency of the transfer of Customer Personal Data depends on the nature and scope of the Services agreed to under the Agreement, the Customer's Documented Instructions and Airlock Digital's need to transfer Personal Data for the performance of the Services. Consequently, transfers may happen on either a continuous or one-off basis, until the termination of the Agreement.

Period for which the Personal Data will be Retained, or Criteria Used to Determine that Period

As set out in the Agreement, this DPA and Customer's Documented Instructions.

EXHIBIT B

LIST OF PARTIES

Data exporter:

Name: Customer

Address: As specified in the Agreement

Contact person's name, position and contact details: As specified in the signature box of this DPA

Activities relevant to the data transferred under these Clauses: As specified in Exhibit A

Role: Controller and/or, to the extent applicable, Processor

Data importer:

Name: Airlock Digital Pty Ltd.

Address: As specified in the Agreement

Contact person's name, position and contact details:

Data Protection Officer, dpo@Airlockdigital.com

Activities relevant to the data transferred under these Clauses: As detailed in Exhibit A to this DPA and the Agreement

Role: Processor and/or, to the extent applicable, Controller

EXHIBIT C

COMPETENT SUPERVISORY AUTHORITY

Where Customer makes a Restricted Transfer of Customer Personal Data originating from the EEA, the competent supervisory authority shall be determined in accordance with Clause 13 of the Standard Contractual Clauses.

Where Customer makes a Restricted Transfer of Customer Personal Data originating from Switzerland, and the Standard Contractual Clauses apply, the competent supervisory authority shall be the Swiss Federal Data Protection and Information Commissioner with respect to the Customer Personal Data originating from Switzerland.

Where Customer makes a Restricted Transfer of Customer Personal Data originating from the UK, and the Standard Contractual Clauses apply, the competent supervisory authority shall be the ICO with respect to the Customer Personal Data originating from the UK.

Where Customer makes a Restricted Transfer of Customer Personal Data originating from another jurisdiction requiring the determination of the competent supervisory authority under Applicable Laws, the competent supervisory authority shall be determined by Applicable Laws.

EXHIBIT D

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

Security Control Category	Description
Governance	Assign to an individual or a group of individuals appropriate roles for developing, coordinating, implementing, and managing Airlock Digital's administrative, physical, and technical safeguards designed to protect the security, confidentiality, and integrity of Personal Data. Use of data security personnel that are sufficiently trained, qualified, and experienced to be able to fulfill their information security-related functions
Risk Assessment	Conduct periodic risk assessments designed to analyze existing information security risks, identify potential new risks, and evaluate the effectiveness of existing security controls Maintain risk assessment processes designed to evaluate likelihood of risk occurrence and material potential impacts if risks occur Document formal risk assessments Review formal risk assessments by appropriate managerial personnel
Information Security Policies	Create information security policies, approved by management, published and communicated to all employees and relevant external parties. Review policies at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.
Human Resources Security	Maintain policies requiring reasonable background checks of any new employees who will have access to Personal Data or relevant Airlock Digital Systems, subject to local law Regularly and periodically train personnel on information security controls and policies that are relevant to their business responsibilities and based on their roles within the organization
Asset Management	Maintain policies establishing data classification based on data criticality and sensitivity Maintain policies establishing data retention and secure destruction requirements Implement procedures to clearly identify assets and assign ownership

Security Control Category	Description
Access Controls	Identify personnel or classes of personnel whose business functions and responsibilities require access to Personal Data, relevant Airlock Digital Systems and the organization's premises Maintain controls designed to limit access to Personal Data, relevant Airlock Digital Systems and the facilities hosting the Airlock Digital Systems to authorized personnel Review personnel access rights on a regular and periodic basis Maintain physical access controls to facilities containing Airlock Digital Systems, including by using access cards or fobs issued to Airlock Digital personnel as appropriate Maintain policies requiring termination of physical and electronic access to Personal Data and Airlock Digital Systems after termination of an employee Implement access controls designed to authenticate users and limit access to Airlock Digital Systems Implement policies restricting access to the data center facilities hosting Airlock Digital Systems to approved data center personnel and limited and approved Airlock Digital personnel Maintain dual layer access authentication processes for Airlock Digital employees with administrative access rights to Airlock Digital Systems
Cryptography	Implement encryption key management procedures Encrypt sensitive data using a minimum of AES/128 bit ciphers in transit and at rest
Physical Security	Require controls to access office premises Register and escort visitors on premises
Operations Security	Perform periodic network and application vulnerability testing using dedicated qualified internal resources Contract with qualified independent 3rd parties to perform periodic network and application penetration testing Implement procedures to document and remediate vulnerabilities discovered during vulnerability and penetration tests
Communications Security	Maintain a secure boundary (e.g. using firewalls and network traffic filtering) Require internal segmentation to isolate critical systems from general purpose networks Require periodic reviews and testing of network controls
System Acquisition, Development and Maintenance	Assign responsibility for system security, system changes and maintenance Test, evaluate and authorize major system components prior to implementation
Supplier Relationships	Periodically review available security assessment reports of vendors hosting Airlock Digital systems to assess their security controls and analyze any exceptions set forth in such reports

Security Control Category	Description
Information Security Breach Management	Monitor the access, availability, capacity and performance of the Airlock Digital Systems, and related system logs and network traffic using various monitoring software and services Maintain incident response procedures for identifying, reporting, and acting on Security Breaches Perform incident response table-top exercises with executives and representatives from across various business units Implement plan to address gaps discovered during exercises Establish a cross-disciplinary Security Breach response team
Business Continuity Management	Design business continuity with goal of 99.5% uptime SLA Conduct scenario-based testing annually
Compliance	Establish procedures designed to ensure all applicable statutory, regulatory, and contractual requirements are adhered to

Exhibit E

LIST OF SUBPROCESSORS

The Controller has authorized the use of the following subprocessors.

Airlock Digital Pty Ltd of Level 2, 136 Greenhill Road, Unley, South Australia, 5061, Australia (compliance@Airlockdigital.com)

Airlock Digital's full list of Subprocessors in place on the effective date of the Agreement is published by Airlock Digital at www.airlockdigital.com/subprocessor-list or Airlock Digital will make it available to Customer upon request, including the name, address and role of each subprocessor Airlock Digital uses to provide the Service.