

These terms (the “**Data Processing Terms**”) are incorporated in full into each Order between Vorboss Limited, a company incorporated in England and Wales (company number 05678571), with Registered Office Devonshire House, 60 Goswell Road, London EC1M 7AD, United Kingdom (“**Vorboss**”) and the counterparty detailed in the Order (the “**Customer**”) (each a “**Party**” and together “**Parties**”). Capitalised terms not defined in these Data Processing Terms shall have the meaning set out in the General Terms where applicable.

1. SCOPE OF THESE DATA PROCESSING TERMS

1.1 A Customer or its end users may provide data to Vorboss under or through the Services (“**Customer Data**”). That Customer Data may include Personal Data (“**Customer Personal Data**”).

1.2 These Data Processing Terms apply to the Processing of Customer Personal Data that is subject to EU Data Protection Law under any Agreements between the Parties.

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

1.4 Terms such as “**Process**”, “**Processing**”, “**Personal Data**”, “**Data Controller**” and “**Data Processor**” shall have the meaning ascribed to them in the EU Data Protection Law.

1.5 Vorboss may act as Data Controller in respect of certain Personal Data provided by Customer to Vorboss. This includes, for example, account information (such as usernames, email addresses and billing information) that Customer provides to Vorboss in connection with the creation and administration of Customer’s account. These Data Processing Terms do not apply where Vorboss Processes such data as Data Controller.

2. ROLES AND RESPONSIBILITIES

2.1 Customer is the Data Controller of the Customer Personal Data covered by these Data Processing Terms. The Customer will determine the scope, purposes and manner by which the Customer Personal Data may be accessed or processed by Vorboss.

2.2 Vorboss provides many of its Customers computing infrastructure as a service (“**IaaS**”). In such cases, Customer has the flexibility to choose how to use the IaaS and, for example, what data to process on the infrastructure. In such cases, Vorboss will be unaware whether the IaaS is being used to process Personal Data. In such cases, Vorboss will not be able to ascertain the basis for any processing or how the IaaS is used.

2.3 Customer will:

(A) comply with its obligations as a Data Controller under EU Data Protection Law in how it Processes Customer Personal Data and when giving instructions to Vorboss;

(B) provide notice and/or obtain all consents and rights necessary for Vorboss to Process Customer Personal Data under the Agreements and provide the Services, and will ensure it keeps a record of these; and

(C) immediately give notice to Vorboss of any revocation of consent or similar related to Customer Personal Data covered by these Data Processing Terms.

2.4 Vorboss is the Data Processor. Vorboss will Process the Customer Personal Data only for the following purposes (“**Authorised Purposes**”):

(A) to perform Services in accordance with the Agreements;

(B) to perform any of the steps necessary for the Services; and

(C) to comply with any other lawful and reasonable written instructions from Customer that are consistent with the Agreements.

2.5 Where Vorboss is unable to Process Customer Personal Data under clause 2.4 because of a legal obligation (including EU Data Protection Law), Vorboss shall inform Customer unless the law prohibits this.

3. CONFIDENTIALITY

3.1 Without prejudice to the existing contractual confidentiality arrangements between the Parties, Vorboss shall ensure any person authorised by Vorboss to Process Customer Personal Data has signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation 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, without prejudice to any other security standards agreed upon by the Parties, Vorboss and Customer shall implement appropriate technical and organisational measures to ensure a level of security of the processing of Customer Personal Data appropriate to the risk. These measures shall include as appropriate:

(A) the measures referred to in Article 32(1); and

(B) the measures further detailed in Schedule 1.

4.2 In assessing the appropriate level of security account shall be taken in particular of all the risks that are presented by Processing, for example from accidental or unlawful destruction, loss, or alteration, unauthorised or unlawful storage, Processing, access or disclosure of Customer Personal Data.

4.3 Where Vorboss provides IaaS to Customer, Customer will be responsible for the requirements set out in clause 4.1 within the IaaS provided.

4.4 Vorboss will maintain records of its security standards and certifications. Upon Customer’s written request, Vorboss will provide (on a confidential basis) copies of relevant external certifications, audit report summaries and/or other documentation as reasonably required by Customer to satisfy it of compliance with these Data Processing Terms. Vorboss shall in addition provide responses to Customer’s reasonable written questions relating to information security as necessary to confirm compliance with these Data Processing Terms.

4.5 Customer acknowledges that security measures are constantly being improved and Vorboss may update these measures and the related policies, provided that these do not reduce the overall security of Customer’s Services.

5. TRANSFER

5.1 Where Personal Data originated within the European Economic Area, Vorboss will not transfer this Customer Personal Data outside the European Economic Area without Customer’s written authorisation.

6. INCIDENT MANAGEMENT

6.1 A “**Data Incident**” means a breach of Vorboss security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Data transmitted, stored or otherwise processed by Vorboss.

6.2 Where Vorboss provides IaaS to Customer, Vorboss will not review the Customer Data to determine whether any Customer Data affected by the Data Incident has any particular legal requirements. Customer will be solely responsible for reviewing the affected Customer Data and fulfilling any notification or other requirements.

6.3 Vorboss shall, upon becoming aware of a Data Incident affecting Customer's Services:

- (A) promptly notify Customer about the Data Incident; and
- (B) at all times cooperate with Customer, and shall follow Customer's instructions relating to the Data Incident, to enable Customer to perform a thorough investigation into the Data Incident, to formulate a correct response, and to take suitable further steps in respect of the Data Incident.

6.4 Where the Data Incident is reasonably likely to require a data breach notification by the Customer under EU Data Protection Law, Vorboss shall notify Customer no later than 24 hours of becoming aware of the Data Incident.

7. SUB-PROCESSORS

7.1 Vorboss will not subcontract any of its Service-related activities consisting (partly) of the processing of Personal Data or requiring Customer Personal Data to be processed by any third party without the prior written authorisation of Customer.

7.2 Vorboss will ensure that the sub-processor is bound by materially the same data protection obligations contained in these Data Processing Terms and must, in particular, ensure that the sub-processor meets the requirements of EU Data Protection Law.

7.3 Even if authorised under clause 7.1, Vorboss shall remain responsible for ensuring that the sub-processor's Processing of Customer Personal Data meets these Data Processing Terms.

8. RETURN OR DESTRUCTION OF PERSONAL DATA

8.1 This section 8 shall apply where Customer Personal Data no longer needs to be Processed by Vorboss because:

- (A) the Agreements or any Order has been terminated; and/or
- (B) all purposes for the Processing of Customer Personal Data in relation to the Services have been fulfilled.

8.2 Customer may make a written request for Vorboss to delete, destroy or (at Customer's request) return all Customer Personal Data to Customer and delete, destroy or return any existing copies, unless the law requires storage. Vorboss shall in such cases notify within 25 Business Days that this clause has been complied with.

8.3 Where Customer does not make a request under clause 8.2 within 30 days, Vorboss will delete or destroy all Customer Data in accordance with applicable law. Vorboss will complete this as soon as reasonably practicable and within a maximum period of 180 days, unless the law requires storage.

8.4 Where Vorboss provides IaaS to Customer, Customer shall be solely responsible for deleting Customer Personal Data from within the IaaS provided, or alternatively instructing Vorboss to delete or destroy the entire relevant IaaS Service (e.g. the virtual machine containing any Customer Personal Data).

8.5 Customer shall be responsible for exporting any Customer Data that it wishes to retain before clause 8.1 applies.

9. ASSISTANCE TO DATA CONTROLLER

9.1 Vorboss shall assist Customer by appropriate technical and organisational measures, insofar as this is possible, for the

fulfilment of Customer's obligation to respond to requests for exercising the data subject's rights under the GDPR.

9.2 Vorboss shall assist Customer in ensuring compliance with the obligations under section 4 above and prior consultations with supervisory authorities required under Article 36 of the GDPR taking into account the nature of processing and the information available to Customer.

9.3 Vorboss shall make available to Customer all information necessary to demonstrate compliance with Customer's obligations, including as set out in clause 4.3 above.

10. LIABILITY AND INDEMNITY

10.1 Vorboss indemnifies Customer and holds Customer harmless against all claims arising in connection with a breach of these Data Processing Terms by Vorboss.

10.2 Customer indemnifies Vorboss and holds Vorboss harmless against all claims arising in connection with a breach of these Data Processing Terms by Customer.

11. DURATION AND TERMINATION

11.1 These Data Processing Terms shall come into effect on the Commencement Date of the Order into which the Data Processing Terms are incorporated, and shall remain in force for the duration of that Order.

11.2 Termination or expiry of these Data Processing Terms shall not discharge Vorboss from its confidentiality obligations under clause 3.

12. MISCELLANEOUS

12.1 In the event of any inconsistency between these Data Processing Terms and any other terms in the Agreements in relation to those matters covered by clause 1.2, these Data Processing Terms shall prevail.

12.2 As set out in the General Terms, the Agreements shall be governed by and interpreted in accordance with the laws of England, the courts of England shall have exclusive jurisdiction to settle any disputes (including non-contractual disputes) arising out of or in connection with the Agreements, and the Parties hereby submit to the exclusive jurisdiction of the English courts.

13. SCHEDULE 1: SUBJECT MATTER AND DETAILS OF PROCESSING

13.1 Subject matter: Vorboss Services provided to Customer, including compute, storage and content delivery on the Vorboss network.

13.2 Duration of Processing: As per section 11.

13.3 Categories of Data: As per clauses 1.1 and 1.2.

13.4 Data Subjects: Data subjects include individuals about whom Customer Personal Data is provided to Vorboss.

14. SCHEDULE 2: SECURITY MEASURES

14.1 Vorboss takes security extremely seriously and maintains security policies and procedures that are assessed and regularly audited against ISO 27001 and covering all areas related to Processing Customer Data.

14.2 **Physical Access Control:** All Customer Data storage locations are staffed 24x7, monitored with CCTV and physical access controlled through a restricted list of named individuals.

14.3 **Data and Administrative Access:** Authentication, credential management, and privilege control systems restrict administrative access to systems to a limited number of authorised personnel.

14.4 Vorboss further has specific policies, within scope of its ISO 27001 certification, addressing the following areas:

- (A) **Removable Devices Policy** defining requirements, encryption standards and limitations on use.
- (B) **Disposal of Media and Equipment Policy** detailing the process for securely wiping, degaussing and physically destroying (as applicable) media and equipment after use.
- (C) **Use of Cryptographic Controls Policy** setting out encryption usage, PKI, and transport encryption.
- (D) **Password Policy** governing the generation, strength, storage and rotation of passwords, PINs and cryptographic private keys.
- (E) **Backup and Antivirus Policy** dictating the usage of antivirus and anti-malware protection and detailing backup policy.
- (F) **Information Security Events, Reporting and Investigation Procedure** detailing the process to be followed upon discovery of any actual or perceived system weaknesses or breaches.