Annex A
Data Processing Addendum

1. Definitions

- "**Applicable Data Protection Law**" means all data privacy or data protection laws or regulations globally that apply to the Processing of Personal Data under this Data Processing Agreement, which may include Applicable European Data Protection Law.
- "**Applicable European Data Protection Law**" means (i) the GDPR, as supplemented by applicable European Union member state law; (ii) the Swiss Federal Act on Data Protection 2023, as amended; and (iii) the UK Data Protection Act 2018, as amended.
- "**Business Operations**" means such Personal Data Processing that Customer authorizes Company to carry out for its own internal purposes. For clarity, this includes the use of Service Generated Data in accordance with Section "**Service Generated Data**" in the General Terms.
- "**Individual**" shall have the same meaning as the term "data subject" or the equivalent term under Applicable Data Protection Law.
- "**Process/Processing**", "**Controller**" and "**Processor**" have the meaning set forth under Applicable Data Protection Law, in particular the GDPR.
- "**Personal Data**" means personal data that has the meaning given to it in the Applicable Data Protection Law.
- "**Personal Data Breach**" means a breach of security leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed on Company systems or the Services environment that compromises the security, confidentiality or integrity of such Personal Data.
- "**Regulator**" shall have the same meaning as the term "supervisory authority", "data protection authority" or the equivalent terms under Applicable Data Protection Law.
- "**Subprocessor**" means an Affiliate or a third party which Company subcontracts with and which may Process Personal Data as set forth in Section "**Use of Subprocessors**".

Other capitalized terms have the definitions provided for them in the Order Form and the underlying General Terms and the Services Terms (altogether referred to as the "**Agreement**").

2. Scope and details of the Processing

2.1 This Annex A – Data Processing Addendum or "**DPA**" applies to Company's Processing of Personal Data on behalf of Customer as Processor for the provision of the Services specified in the Order Form.

2.2 In addition, any Processing of Personal Data subject to Applicable European Data Protection Law is subject to the additional terms of the European Data Processing Addendum set out in **Exhibit – European Data Processing Addendum** (**"EU DPA"**).

3. Responsibility for Processing of Personal Data and instruction right

3.1 Customer is a Controller and Company is a Processor for the Processing of Personal Data for the provision of the Services except where Company Processes Personal Data to carry out its Business Operations in which case it acts as a Controller. Each Party is responsible for compliance with its respective obligations under Applicable Data Protection Law.

3.2 Except as for Business Operations, Company shall Process Personal Data solely for the purpose of providing the Services in accordance with the Agreement, in particular the applicable Order Form and this DPA.

3.3 In addition to Customer's instructions incorporated into the Order Form, Customer may provide additional instructions in writing to Company with regard to Processing of Personal Data in accordance with Applicable Data Protection Law. Company shall promptly comply with all such instructions to the extent necessary for Company to (i) comply with its Processor obligations under Applicable Data Protection Law or (ii) assist Customer to comply with its obligations as a Controller under Applicable Data Protection Law relevant to its use of the Services.

3.4 Company shall follow Customer's instructions at no additional cost to Customer and within the timeframes reasonably necessary for Customer to comply with its obligations under Applicable Data Protection Law. To the extent Company expects to incur additional charges or fees not covered by the Fees payable under the applicable Order Form, such as additional license or third-party contractor fees, it shall promptly inform Customer thereof upon receiving the respective instructions. Without prejudice to Company's obligation to comply with Customer's instructions, the Parties shall then negotiate in good faith with respect to any such charges or fees.

3.5 Unless otherwise specified in the applicable Order Form, Customer may not provide Company with any sensitive or special Personal Data within the meaning of Applicable Data Protection Law that imposes specific data security or data protection obligations on Company in addition to or different from those specified in the DPA or the Order Form or the underlying General Terms and the Services Terms.

4. Inquiries and requests submitted by Individuals

4.1 If Customer receives a request or inquiry from an Individual related to Personal Data Processed by Company for the provision of the Services under an applicable Order Form, Customer may either (i) securely access the Services environment that holds Personal Data to address the request or (ii) to the extent such access is not available to Customer, submit a service request to Company with detailed written instructions to Company on how to assist Customer with such request.

4.2 If Company directly receives any requests or inquiries from Individuals that have identified Customer as the Controller, it shall pass on such requests to Customer without undue delay and without responding to the Individual. Otherwise, Company shall advise the Individual to identify and contact the relevant Controller(s).

5. Use of Subprocessors

To the extent Company engages Subprocessors to Process Personal Data, such entities shall be subject to the same level of data protection and security as Company under the terms of the Order Form and this DPA. Company is responsible for the performance of such Subprocessors' obligations in compliance with the terms of this DPA and Applicable Data Protection Law.

6. Cross-border Personal Data transfers

6.1 Without prejudice to any applicable restrictions for hosted Services specified in the Agreement, Company may Process Personal Data globally as necessary to perform the Services.

6.2 To the extent such global access involves a transfer of Personal Data subject to cross-border transfer restrictions under Applicable Data Protection Law, such transfers shall be subject to security and data privacy requirements consistent with the relevant requirements of this DPA and Applicable Data Protection Law.

7. Audit rights

7.1 Customer may audit Company's compliance with its obligations under this DPA up to once (1) per year. In addition, to the extent required by Applicable Data Protection Law, Customer or Customer's Regulator may perform more frequent audits.

7.2 If a third party is to conduct the audit, such third party must be mutually agreed to by Customer and Company (except if such third party is a Regulator). Company shall not unreasonably withhold its consent to a third-party auditor requested by Customer. The third-party auditor must execute a written confidentiality agreement acceptable to Company or otherwise be bound by a statutory or legal confidentiality obligation.

7.3 To request an audit, Customer must submit a detailed proposed audit plan to Company at least two (2) weeks in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Company will review the proposed audit plan and provide Customer with any concerns or questions. Company will work cooperatively with Customer to agree on a final audit plan.

7.4 The audit must be conducted during regular business hours at the applicable facility, subject to the agreed final audit plan and Company's health and safety or other relevant policies and may not unreasonably interfere with Company's business activities.

7.5 Upon completion of the audit, Customer shall provide Company with a copy of the audit report, which is subject to the confidentiality terms of the Agreement. Customer may use the audit reports only for the purposes of meeting its regulatory audit requirements and/or confirming compliance with the requirements of this DPA.

7.6 Each Party will bear its own costs in relation to the audit, unless Company promptly informs Customer upon reviewing the audit plan that it expects to incur additional charges or fees in the performance of the audit that are not covered by the Fees payable under the applicable Order Form. The Parties shall negotiate in good faith with respect to any such charges or fees.

7.7 Without prejudice to the rights granted in this Section "**Audit rights**", if the requested audit scope is addressed in a SOC, ISO, NIST, PCI DSS, HIPAA or similar audit report issued by a qualified third-party auditor within the prior twelve (12) months and Company provides such report to Customer confirming there are no known material changes in the controls audited, Customer agrees to accept the findings presented in the third-party audit report in lieu of requesting an audit of the same controls covered by the report.

8. Security and Confidentiality

8.1 Company has implemented and shall maintain appropriate technical and organizational security measures for the Processing of Personal Data designed to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data. These security measures govern all areas of security applicable to the Services, including physical access, system access, data access, transmission and encryption, input, data backup, data segregation and security oversight, enforcement and other security controls and measures.

8.2 Company and all used Subprocessors that Process Personal Data, are subject to appropriate written confidentiality arrangements, including confidentiality agreements, regular training on information protection and compliance with Company policies concerning protection of confidential information, as applicable.

9. Incident management and breach notification

9.1 Company has implemented controls and policies designed to detect and promptly respond to incidents that create suspicion of or indicate destruction, loss, alteration, unauthorized disclosure or access to Personal Data transmitted, stored or otherwise Processed. Company shall define escalation paths to investigate such incidents in order to confirm if a Personal Data Breach has occurred, and to take reasonable measures designed to identify the root cause(s) of such Personal Data Breach, mitigate any possible adverse effects and prevent a recurrence.

9.2 Company shall notify Customer of a confirmed Personal Data Breach without undue delay but at the latest within twenty-four (24) hours. As information regarding the Personal Data Breach is collected or otherwise reasonably becomes available to Company, Company shall also provide Customer with (i) a description of the nature and reasonably anticipated consequences of the Personal Data Breach, (ii) the measures taken to mitigate any possible adverse effects and prevent a recurrence, and (iii) where possible, information about the types of Personal Data that were the subject of the Personal Data Breach. Customer agrees to coordinate with Company on the content of the intended public statements, if any, or required notices for the affected Individuals and/or notices to the relevant Regulators regarding the Personal Data Breach.

10. Return and deletion of Personal Data

10.1 Upon termination of the applicable Order Form, Company will promptly return, including by providing available data retrieval functionality, or delete any remaining copies of Personal Data on Company systems or Services environments, except as otherwise stated in the Agreement or except as Applicable Data Protection Law requires storage of such Personal Data. Export and retrieval may be subject to technical limitations, in which case Company and Customer will find a reasonable method to allow Customer to access Personal Data.

10.2 For Personal Data held on Customer's systems or environments or for Services for which no data retrieval functionality is provided by Company as part of the Services, Customer is advised to take appropriate action to back up or otherwise store separately any Personal Data while the production Services environment is still active prior to termination.

11. Mandatory Personal Data access

11.1 Company may be required by law to provide access to Personal Data, such as to comply with a subpoena or other legal process, or to respond to Regulator's requests, including public and government authorities for national security and/or law enforcement purposes.

11.2 Company shall promptly inform Customer of requests to provide access to Personal Data, unless otherwise required by law.

12. Miscellaneous

12.1 For the avoidance of doubt, Section "**Limitation of liability**" in the General Terms applies with respect to Company's liability under this DPA.

12.2 The term of this DPA corresponds to the Term.

12.3 Customer shall inform Company without undue delay if it considers that this DPA does not meet the requirements of a data Processing contract according to the relevant provisions of Applicable Data Protection Law and/or any relevant guidelines, recommendations or other positions of the Regulator. In such case Customer and Company shall endeavor to adapt this DPA to the respective legal and/or official requirements.

12.4 Amendments and additions to this DPA require written form. This also applies to any waiver of the written form requirement.

Exhibits:

Exhibit – European Data Processing Addendum

Exhibit
European Data Processing Addendum

This EU DPA supplements the main body of the DPA to include additional Processor terms applicable to the Processing of Personal Data subject to Applicable European Data Protection Law. Except as expressly stated otherwise in the main body of the DPA, the Agreement, this EU DPA, in the event of any conflict between these documents, the following order of precedence applies (in descending order): (i) this EU DPA, (ii) the main body of the DPA and (iii) the Agreement.

1. Cross-border transfer of Personal Data

Company and any of its Subprocessors shall Process Personal Data exclusively in the European Economic Area, including the European Union. If Company or its Subprocessors provide the Services outside of the European Economic Area, including the European Union, Company shall ensure the lawfulness under Applicable Data Protection Law by taking the appropriate measures (e.g., in accordance with Article 28 and Articles 45, 46, 47 GDPR).

2. Details of Processing of Personal Data

2.1 The subject matter of the Processing is the provision of the Services as per the Agreement and as further specified in the applicable Order Form.

2.2 The duration of the Processing is determined by the term as specified in the Order Form.

2.3 The Processing serves the purpose of the provision of the Services as per the Agreement and as further specified in the applicable Order Form. Insofar as Company Processes Personal Data in order to assist Customer in fulfilling its obligation to respond to requests from Individuals or to comply with other stipulations of Applicable European Data Protection Law, the Processing also serves the purpose of fulfilling the legal obligations of Customer under the Applicable European Data Protection Law.

2.4 Company in relation to the provision of the Services Processes the following categories of Personal Data: Customer contact data, Customer Data and/or Service Requests.

3. Customer’s instructions

3.1 Customer’s right to provide instructions to Company as specified in Section “**Responsibility for Processing of Personal Data and instruction right**” of the main body of the DPA encompasses instructions regarding (i) data transfers as set forth in Section “**Cross-border transfer of Personal Data**” of this EU DPA and (ii) assistance with Individual’s requests to access, delete or erase, restrict, rectify, receive and transmit (data portability), block access to or object to Processing of specific Personal Data or sets of Personal Data as described in Section “**Inquiries and requests submitted by Individuals**” of the main body of the DPA.

3.2 To the extent required by the Applicable European Data Protection Law, Company shall immediately inform Customer if, in its opinion, Customer’s instruction infringes Applicable European Data Protection Law. Customer acknowledges and agrees that Company is not responsible for performing legal research and/or for providing legal advice to Customer.

4. Notice and objection right to new Subprocessors

4.1 Subject to the terms and restrictions specified in this Section "**Notice and objection right to new Subprocessors"** of this EU DPA and Section "**Use of Subprocessors**" of the main body of the DPA, Customer provides Company a general written authorization to engage the following Subprocessors to assist in the performance of the Services:

Name	Address	Scope of Processing
Open-Xchange GmbH	Olper Huette 5f, 57462 Olpe, Germany	**Service Vendor / Cloud Operator / Support:** Provision and operate the cloud service; process customer tenant/user data to deliver the service; provide support and incident handling; monitoring/logging, backups and security operations.
czichos.net GmbH	Königsweg 220, 14129 Berlin, Germany	**Provisioning Portal Vendor / Support:** Provide and maintain the provisioning portal; process tenant and admin user data to enable ordering, provisioning, configuration and lifecycle management; portal support and troubleshooting.
GBuzz Ltd.	57 Newtown Road, Hove, East Sussex, BN3 7BA, UK	**Marketing & Sales Agency:** Process business contact data for marketing and go-to-market activities related to provisioning and services (e.g., campaign execution, communications, analytics/reporting).

4.2 Company shall inform Customer of any intended changes, thereby granting Customer the right to object to such changes within two (2) weeks after receiving the information.

Customer may object to the intended involvement of a Subprocessor in the performance of the Services, providing objective justifiable grounds related to the ability of such Subprocessor to adequately protect Personal Data in accordance with the DPA or Applicable European Data Protection Law in written form.

4.3 In case of an objection, the Parties shall work together in good faith to find a mutually acceptable resolution to address such objection, including but not limited to reviewing additional documentation supporting the Subprocessor's compliance with the DPA or Applicable European Data Protection Law or delivering the Services without the involvement of such new/additional Subprocessor. To the extent the Parties do not reach a mutually acceptable resolution within a reasonable timeframe, Customer shall have the right to terminate the relevant Services (i) upon serving thirty (30) days prior notice, (ii) without liability to Company and (iii) without relieving Customer from its payment obligations under the Agreement up to the date of the effect of such termination. If such termination only pertains to a part of the Services under the applicable Order Form, Customer will enter into an amendment or replacement Order Form to reflect such partial termination.

5. Information and assistance

5.1 For hosted Services, the audit rights under Section "**Audit right**" of the main body of the DPA include the right to conduct inspections of the applicable Services data center facility that hosts the Personal Data in question.

5.2 In addition, Customer may request that Company audits a Subprocessor or provides confirmation that such an audit has occurred (or, where available, obtains or assists Customer in obtaining a third-party audit report concerning the Subprocessor's operations to verify compliance with the Subprocessor's obligations. Customer shall also be entitled, upon written request, to receive copies of the relevant privacy and security terms of Company's agreement with any Subprocessors that may Process Personal Data.

5.3 Company provides Customer with information and assistance reasonably necessary for Customer to conduct Customer's data protection impact assessments or consult with Customer's Regulator(s), by granting Customer electronic access to a record of Processing activities.