Data Processing Addendum

This Data Processing Addendum (the "**Addendum**") forms part of the OfficeRnD Terms and Conditions (https://www.officernd.com/terms/), Service Level Agreement (https://www.officernd.com/service-level-agreement/) and the respective Order Form (the "**Principal Agreement**") by and between OFFICERND Limited., a company organized under the laws of England and Wales with office located at 84 Eccleston Square, London, SW1V 1PX, UK ("**OfficeRnD**")
and _____ (the "**Subscriber**") and is subject to the Principal Agreement.

The Addendum sets out the additional terms, requirements and conditions on which OfficeRnD will process the Subscriber's Personal Data when providing services under the Principal Agreement. The Addendum contains the mandatory clauses required by Article 28(3) of the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) for contracts between controllers and processors and the General Data Protection Regulation ((EU) 2016/679).

1. **Definitions.** For the purposes of this Addendum, capitalized terms shall have the following meanings. Capitalized terms not otherwise defined shall have the meaning given to them in the Principal Agreement.

    a. "**Subscriber's Personal Data**" means any personal data that is processed by OfficeRnD on behalf of the Subscriber as a result of, or in connection with, the provision of the Services under the Principal Agreement.

    b. "**Data Protection Laws**" means all laws, rules and regulations which relate to the protection of individuals with regards to the processing of the Subscriber's Personal Data applicable in Europe and/or the UK including (i) national laws implementing the EU Data Protection Directive 95/46/EC and the EU Electronic Communications Data Protection Directive 2002/58/ES; (ii) EU General Data Protection Regulation 2016/679 ("GDPR") and the national laws implementing the GDPR; (iii) The UK GDPR meaning the retained EU law version of the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419);(iv) UK Data Protection Act 2018 as well as (v) any other EU or UK laws, regulations and rules, relating to the processing of the Subscriber's Personal Data, and any guidance or code of practice relating to the such processing issued by relevant regulatory authority or other relevant competent

authority. References to this term include replacements, modifications or re-enactments of Data Protection Laws.

c. "**EEA**" means the European Economic Area.

d. "**OfficeRnD Infrastructure**" means (i) OfficeRnD physical facilities; (ii) hosted cloud infrastructure; (iii) OfficeRnD's corporate network and the non-public internal network, software, and hardware necessary to provide the Services and which is controlled by OfficeRnD; in each case to the extent used to provide the Services.

e. "**Restricted Transfer**" means a transfer of the Subscriber's Personal Data which would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of appropriate safeguards required for such transfers under Data Protection Laws.

f. "**Services**" means the services provided to the Subscriber by OfficeRnD pursuant to the Principal Agreement.

g. "**Standard Contractual Clauses**" means the latest version of the standard contractual clauses for the transfer of personal data to processors established in third countries under Regulation (EU) 2016/679 of the European Parliament and of the Council (the current version as at the date of this Addendum is annexed to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council).

h. The terms "**controller**", "**data subject**", "**Member State**", "**personal data**", "**personal data breach**", "**processor**", "**sub processor**", "**processing**", and "**supervisory authority**" shall have the meanings ascribed to them in the GDPR, and their cognate terms shall be construed accordingly.

i. Notwithstanding anything to the contrary herein, to the extent the UK GDPR applies, any references in this Addendum to defined terms shall be construed and interpreted in accordance with the UK GDPR, as well as to the extent the GDPR applies, the same defined terms and references shall be construed and interpreted in accordance with the GDPR in order to comply with it.

2. **Compliance with Data Protection Laws**

a. Each of OfficeRnD and the Subscriber shall comply with the provisions and obligations imposed on them by the Data Protection Laws and shall procure that

their employees, agents and contractors observe the provisions of the Data Protection Laws.

3. **Controller and Processor**

    a. For the purposes of this Addendum, the Subscriber is the controller of the Subscriber's Personal Data and OfficeRnD is the processor of such data where such data is processed in order to provide the Services under the Principal Agreement.

    b. The Subscriber is responsible for its compliance obligations under Data Protection Laws, including but not limited to, providing any required notices and obtaining any required consents to enable OffineRnD to process the Subscriber Personal Data as set out in this Addendum and the Principal Agreement.

    c. The Subscriber warrants that:

        i. The processing of the Subscriber's Personal Data is compliant with the principals of the Data Protection Laws, based on legal grounds for processing, as may be required by Data Protection Laws and that it has made and shall maintain throughout the term of the Principal Agreement all necessary rights, permissions, registrations and consents in accordance with and as required by Data Protection Laws with respect to OfficeRnD's processing of the Subscriber's Personal Data under this Addendum and the Principal Agreement; and

        ii. it is entitled to and has all necessary rights, permissions and consents to transfer the Subscriber's Personal Data to OfficeRnD and otherwise permit OfficeRnD to process the Subscriber's Personal Data on its behalf , so that OfficeRnD may lawfully use, process and transfer the Customer's Personal Data in order to carry out the Services and perform OfficeRnD's other rights and obligations under this Addendum and the Principal Agreement.

4. **Scope of processing**

    a. In order for OfficeRnD to provide the Services under the Principal Agreement, OfficeRnD will process the Subscriber's Personal Data. Annex 1 to this Addendum sets out certain information regarding the processing of the Subscriber's Personal Data as required by the Data Protection Laws. The parties may amend Annex 1 from time to time, as the parties may reasonably consider necessary to meet those requirements.

b. OfficeRnD shall only process the Subscriber's Personal Data (i) for the purposes of fulfilling its obligations under the Principal Agreement and (ii) in accordance with the Subscriber's documented instructions described in this Addendum or as otherwise instructed by the Subscriber in writing from time to time, unless required to use the Subscriber's Personal Data by law to which OfficeRnD is subject; in such a case, OfficeRnD shall inform the Subscriber of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

c. For the purpose of Paragraph 4(b)(ii) the Subscriber's written instructions shall be documented in the applicable order, services description, support ticket, other written communication or as directed by Subscriber using the Services (such as through an API or service portal).

d. Where OfficeRnD reasonably believes that a Subscriber instruction is contrary to: (i) applicable law and regulations or (ii) the provisions of the Principal Agreement or this Addendum, OfficeRnD may inform the Subscriber and is authorized to defer the performance of the relevant instruction until it has been amended by Subscriber or is mutually agreed by both Subscriber and OfficeRnD.

e. The Subscriber is solely responsible for its utilization and management of Subscriber's Personal Data input into or transmitted by the Services, including: (i) verifying recipient's addresses and that they are correctly entered into the Services, (ii) reasonably limiting the amount or type of information disclosed through the Services.

5. **Confidentiality**

a. OfficeRnD shall ensure that its personnel that is authorized to process the Subscriber's Personal Data is subject to confidentiality undertakings or professional or statutory obligations of confidentiality in respect of such Subscriber's Personal Data.

6. **Technical and Organizational Measures**

a. OfficeRnD shall, in relation to the Subscriber's Personal Data, (i) implement and maintain appropriate technical and organisational measures that are designed to protect Subscriber's Personal Data from personal data breaches and to preserve the security and confidentiality of Subscriber's Personal Data and (ii) on reasonable request, take into account such measures as recommended by the Subscriber to protect Subscriber's Personal Data.

b. The measures implemented by OfficeRnD pursuant to Paragraph 6(a)(i) above are those described in Annex 2 of this Addendum which are considered adequate to comply with Article 32 GDPR by both parties.
c. Subject to express written agreement by the OfficeRnD to implement additional measures requested by the Subscriber pursuant to Paragraph 6(a)(ii), the parties agree that all reasonable costs associated with the implementation and maintenance of such additional measures shall be borne solely by the Subscriber and shall be invoiced by the OfficeRnD on a direct, pass-through basis with no additional mark-up.

7. **Audits**

a. Subject to Paragraph 7(b), OfficeRnD shall make available to the Subscriber on reasonable request, information that is reasonably necessary to demonstrate the OfficeRnD's compliance with this Addendum and shall allow for and contribute to audits, including inspections, by the Subscriber or an auditor mandated by the Subscriber in relation to the processing of the Subscriber's Personal Data by OfficeRnD, provided always that any third party auditors mandated by the Subscriber enters into appropriate confidentiality agreements as reasonably required by the OfficeRnD.
b. The audits allowed by OfficeRnD pursuant to Paragraph 7(a) above shall be subject to the Subscriber (i) bearing any costs and expenses of OfficeRnD arising from the provision of such information and audit rights; (ii) giving OfficeRnD reasonable prior notice of such audit, being at least 30 days' prior to the requested audit date; (iii) such audit is undertaken so as to cause minimal disruption to OfficeRnD's business and carried out during OfficeRnD normal operating hours

c. The Subscriber's information and audit rights only arise under Paragraph 7(a) above to the extent that the Principal Agreement and/or any other information available to the Subscriber in relation to the Services does not otherwise give the Subscriber information and audit rights meeting the requirements of Paragraph 7(a) above.

8. **Data Subject Requests**

a. OfficeRnD shall provide the Subscriber with reasonable cooperation and assistance, in so far it is reasonably possible and taking into account the nature of processing, by providing specific tools in order to assist Subscriber in replying to requests received from data subjects. These tools may include OfficeRnD's APIs and interfaces to Subscriber's Personal Data held on OfficeRnD Infrastructure.

b. If OfficeRnD receives a complaint, inquiry or request (including requests made by data subjects to exercise their rights pursuant to Data Protection Laws) related to the Subscriber's Personal Data directly from data subjects, OfficeRnD will notify and redirect such requests to the Subscriber within 7 days from the receipt of the complaint, inquiry or request.

9. **Data Breach**

a. OfficeRnD shall notify the Subscriber without undue delay and in any event within 24 hours if OfficeRnD becomes aware of a personal data breach affecting the Subscriber's Personal Data.
b. OfficeRnD shall, taking into account the nature of the processing and the information available to OfficeRnD, use commercially reasonable efforts to provide the Subscriber with sufficient information to allow the Subscriber, to meet any obligations to report or inform regulatory authorities, data subjects and other entities of such personal data breach to the extent required under Data Protection Laws.

10. **Data Protection Impact Assessments**

a. OfficeRnD shall, taking into account the nature of the processing and the information available to OfficeRnD, provide reasonable assistance to the Subscriber, with any data protection impact assessments and prior consultations with supervisory authorities or other competent regulatory authorities as required for the Subscriber to fulfill its obligations under Data Protection Laws.
b. The Parties hereby agree that by providing the information in Annex 1 and Annex 2, OfficeRnD fulfils its obligation to assist the Subscriber in ensuring compliance with its obligations to carry out data protection impact assessments and prior consultations with supervisory authorities or other competent regulatory authorities.
c. Notwithstanding the above, if necessary, Subscriber may request OfficeRnD to provide additional support regarding data protection impact assessments and prior consultations with the supervisory authority, which however, may be subject to payment by Subscriber of additional remuneration determined at OfficeRnD’s sole discretion.

11. **Return or Destruction of the Subscriber's Personal Data**

a. Within ninety (90) days of the date of cessation of any Services involving the processing of the Subscriber's Personal Data, OfficeRnD shall at the choice of the Subscriber and at Subscriber’s sole cost (i) return all copies of the Subscriber's Personal Data in the control or possession of OfficeRnD and its sub-processors; or (ii) to the extent reasonably possible delete and procure the

deletion of all copies of the Subscriber's Personal Data processed by OfficeRnD and sub-processors. Notwithstanding the foregoing, OfficeRnD may retain the Subscriber's Personal Data to the extent required by EU Laws solely for the purpose of complying with data retention requirements. OfficeRnD may retain electronic copies of files containing Subscriber's Personal Data created pursuant to automatic archiving or back-up procedures which cannot reasonably be deleted within the abovementioned period solely for the period technically necessary for such archiving or back-up purposes. In these cases, OfficeRnD shall ensure that the Subscriber's Personal Data are not further actively processed and stored in such a manner to protect it from unauthorised access or use. However, once the archiving or back-up period is over, your data will be irreversibly removed from our systems.

b. If any law, regulation, or government or regulatory body requires OfficeRnD to retain any documents, materials or Subscriber's Personal Data that Office RnD would otherwise be required to return or destroy, OfficeRnD will notify the Subscriber of that requirement, giving details and establishing a timeline for deletion or destruction once the retention requirement ends.

12. **Restricted Data Transfers**

a. The Subscriber, as a data exporter, and OfficeRnD, as a data importer established in the United Kingdom, shall access and process the personal data of the Subscriber on the basis of COMMISSION IMPLEMENTING DECISION of 28.6.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom (the "UK adequacy Decision").

b. The Subscriber acknowledges and agrees that the provision of some of the Services and/or the Support, may require the subcontracting by OfficeRnD of any of its subsidiaries or third-party providers which may result in Restricted Transfers and the Subscriber hereby consents to such Restricted Transfers provided such Restricted Transfers are based always to the appropriate safeguards as defined in and in compliance with the Data Protection Laws.

c. If necessary, in case of Restricted Transfers, the parties shall work together in good faith with any importer of data not based in the EEA to meet the requirements as further set out in Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Schrems II) and all subsequent guidance from applicable EU and/or UK data protection supervisory authorities relating to the Schrems II decision.

d. Any revision of the abovementioned Commission Implementing Decision, or occurrence of another event or circumstance which may render this decision totally or partially unenforceable, or invalid, shall require that the Parties hereto work together in good faith to implement appropriate safeguards as required by the Data Protection Laws, including by executing Standard Contractual Clauses

adopted by the European Commission, prior to performing any Restricted Transfer.

e. OfficeRnD shall ensure that any onward transfer is subject to the same appropriate safeguards as the ones established for the Restricted Transfer between the parties. If the Restricted Transfer relies on the Standard Contractual Clauses, OfficeRnD shall ensure that it enters into Standard Contractual Clauses with any recipient the sub-processor.

13. **Sub-processing**

a. The Subscriber hereby authorizes OfficeRnD to appoint sub-processors in accordance with this Paragraph 13, subject to any restrictions in the Principal Agreement. OfficeRnD will ensure that sub-processors are bound by written agreements that require them to provide at least the level of data protection required of OfficeRnD by this Addendum.

b. OfficeRnD may continue to use those sub-processors already engaged as at the date of this Addendum which are those listed in Annex 3 of this Addendum.

c. OfficeRnD shall give the Subscriber prior written notice of the appointment of any new sub-processor. If, within five (5) business days of receipt of that notice, the Subscriber notifies OfficeRnD in writing of any objections (on reasonable grounds) to the proposed appointment, OfficeRnD shall not appoint that proposed sub-processor until reasonable steps have been taken to address the objections raised by the Subscriber and the Subscriber has been provided with a reasonable written explanation of the steps taken. If OfficeRnD and the Subscriber are not able to resolve the appointment of a sub-processor within a reasonable period, OfficeRnD shall have the right to terminate the Principal Agreement for cause.

d. OfficeRnD shall be responsible for the acts and omissions of any sub-processors as it is to the Subscriber for its own acts and omissions in relation to the matters provided in this Addendum.

14. **Governing law and jurisdiction**

a. The parties to this Addendum hereby submit to the competent courts of England and Wales with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity.

b. This Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of England and Wales.

15. **Order of precedence**

a. With regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Principal Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

16. **Changes in Data Protection Laws, etc.**

a. OfficeRnD may modify or supplement this Addendum, with reasonable notice to the Subscriber:

i. If required to do so by a supervisory authority or other government or regulatory entity;

ii. If necessary to comply with applicable law;

iii. To implement new or updated appropriate safeguards for Restricted Transfers, including Standard Contractual Clauses approved by the European Commission ; or

iv. To adhere to an approved code of conduct or certification mechanism approved or certified pursuant to Articles 40, 42 and 43 GDPR.

17. **Severance**

a. Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

18. **Termination**

a. This Addendum will terminate contemporaneously and automatically with the termination of the Principal Agreement.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Principal Agreement with effect from the date first set out above.

OFFICERND, Ltd.
Signature _____
Name: Deyan Varchev
Title: Data Protection Officer
Date Signed:

The Subscriber
Signature _____
Name: _____
Title: _____
Date Signed: _____

ANNEX 1

DETAILS OF PROCESSING OF PERSONAL DATA

This Annex includes certain details of the processing of Personal Data:

Subject matter and duration of the processing of Personal Data

The subject matter and duration of the processing of the Personal Data are set out in the Principal Agreement.

The nature and purpose of the processing of Personal Data

Under the Principal Agreement, OfficeRnD provides certain workspace management services (the “Services”) to the Subscriber. OfficeRnD may therefore process personal data. Such processing activities include (a) providing the Services and any communication related thereto; (b) the detection, prevention and resolution of security and technical issues; and (c) responding to Subscriber support requests and providing Support Services.

The types of Personal Data to be processed

The personal data which may be processed includes: name, email, address, phone number, IP address and any additional personal data of the data subjects that the Subscriber may require to insert into the system.

The categories of data subject to whom the Personal Data relates

Employees of the Subscriber, individuals with whom the Subscriber has business relationship developed using the Services as well as Users, Members, Account Holders and other clients of the Subscriber.

ANNEX 2

INFORMATION SECURITY

For the purpose of securing the personal data processed, OfficeRnD uses industry best practices, including:

1. **Access Control**
    a. **Preventing Unauthorized Product Access**

Outsourced processing: OfficeRnD hosts its Service with outsourced cloud infrastructure providers. Additionally, OfficeRnD maintains contractual relationships with vendors in order to provide the Service in accordance with our Data Processing Agreement. OfficeRnD relies on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

Physical and environmental security: OfficeRnD hosts its product infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications.

Authentication: OfficeRnD implemented a uniform password policy for its customer products. Subscribers who interact with the products via the user interface must authenticate before accessing non-public customer data.

Authorization: Subscriber data is stored in multi-tenant storage systems accessible to Subscribers via only application user interfaces and application programming interfaces. Subscribers are not allowed direct access to the underlying application infrastructure. The authorization model in each of OfficeRnD's products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

Application Programming Interface (API) access: Public product APIs may be accessed using an access tokens.

b. **Preventing Unauthorized Product Use**

OfficeRnD implements industry standard access controls and detection capabilities for the internal networks that support its products.

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

Static code analysis: Security reviews of code stored in OfficeRnD's source code repositories is performed, checking for coding best practices and identifiable software flaws.

External vulnerability testing: OfficeRnD maintains relationships with industry recognized vulnerability testing service providers for four annual vulnerability tests. The intent of the vulnerability tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

c. **Limitations of Privilege & Authorization Requirements**

Product access: A subset of OfficeRnD's employees have access to the products and to Subscriber data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Employees are granted access by role. Employee roles are reviewed at least once every six months.

Background checks: All OfficeRnD employees undergo a background check prior to starting employment, in accordance with the applicable laws. All employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

2. Transmission Control

In-transit: OfficeRnD makes HTTPS encryption (also referred to as SSL or TLS) available on every one of its login interfaces. OfficeRnD's HTTPS implementation

uses industry standard algorithms and certificates.

At-rest: OfficeRnD stores user passwords following policies that follow industry standard practices for security.

3. **Input Control**

Detection: OfficeRnD designed its infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities. OfficeRnD personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: OfficeRnD maintains a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, OfficeRnD will take appropriate steps to minimize product and Subscriber damage or unauthorized disclosure.

4. **Availability Control**

Infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.95% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

Fault tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Subscriber data is backed up to multiple durable data stores and replicated across multiple availability zones.

Online replicas and backups: Where feasible, production databases are designed to replicate data between no less than 1 primary and 1 secondary database. All databases are backed up and maintained using the latest industry standard methods.

OfficeRnD's products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists OfficeRnD operations in

maintaining and updating the product applications and backend while limiting downtime.

ANNEX 3

APPROVED SUB-PROCESSORS

Name	**Purpose**
Amazon Web Services	Cloud Infrastructure
Google Workspaces	Mail and Drive - email and document management
Google Analytics	Application analytics and performance
Zendesk	Support and Chat
Hubspot	CRM
Mailgun	Transactional email sending
Xero	Accounting
Planhat	Customer Success management
Appcues	Product adoption
OneSignal	Mobile Push notifications
HelloSign	E-signing
OfficeRnd EOOD	Provides a portion of product services for OfficeRnD LTD.
Stripe, Inc.	Credit card payment processing
PandaDoc Inc.	Document Management
Hotjar	Product Analytics
TalkDesk	Phone Support system

On behalf OFFICERND, Ltd.:

Name (written out in full): Deyan Varchev
Position: Data Protection Officer
Address: 84 Eccleston Square, London, SW1V 1PX, UK

Other information necessary in order for the contract to be binding (if any):

Signature.....

On behalf _____

Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature.....