Data Processing Addendum

This Data Processing Addendum (this "**Addendum**") forms part of the OfficeRnD Engagement Terms and SLA (the "**Principal Agreement**") by and between OFFICERND, Ltd. ("**OfficeRnD**") and _____ (the "**Customer**") and is subject to the Principal Agreement.

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. "**Customer's Personal Data**" means any personal data that is processed by OfficeRnD on behalf of the Customer to perform the Services under the Principal Agreement.

    b. "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including (with effect from May 25, 2018) by the GDPR and laws implementing, replacing or supplementing the GDPR.

    c. "**GDPR**" means EU General Data Protection Regulation 2016/679.

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

    e. "**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.

    f. "**Restricted Transfer**" means a transfer of the Customer's Personal Data from OfficeRnD to a sub-processor where such transfer would be prohibited by EU Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of EU Data Protection Laws) in the absence of appropriate safeguards required for such transfers under EU Data Protection Laws.

    g. "**Services**" means the services provided to the Customer by OfficeRnD pursuant to the Principal Agreement.

    h. "**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 Directive 95/46/EC of the European Parliament and of the

Council (the current version as at the date of this Addendum is annexed to European Commission Decision 2010/87/EU).

i. 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.

2. **Compliance with EU Data Protection Laws**

a. Each of OfficeRnD and the Customer shall comply with the provisions and obligations imposed on them by the EU Data Protection Laws and shall procure that their employees, agents and contractors observe the provisions of the EU Data Protection Laws.

3. **Controller and Processor**

a. For the purposes of this Addendum, the Customer is the controller of the Customer's Personal Data and OfficeRnD is the processor of such data.

b. The Customer warrants that:

i. The processing of the Customer's Personal Data is based on legal grounds for processing, as may be required by EU 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 EU Data Protection Laws with respect to OfficeRnD's processing of the Customer'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 Customer's Personal Data to OfficeRnD and otherwise permit OfficeRnD to process the Customer'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 Customer's Personal Data. Annex 1 to this Addendum sets out certain information regarding the processing of the Customer's Personal

Data as required by Article 28(3) of the GDPR. 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 Customer's Personal Data (i) for the purposes of fulfilling its obligations under the Principal Agreement and (ii) in accordance with the documented instructions described in this Addendum or as otherwise instructed by the Customer from time to time. Such Customer's instructions shall be documented in the applicable order, services description, support ticket, other written communication or as directed by Customer using the Services (such as through an API or service portal).

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

d. Customer is solely responsible for its utilization and management of 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 each of its, and sub-processors', personnel that is authorized to process the Customer's Personal Data is subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

6. **Technical and Organizational Measures**

a. OfficeRnD shall, in relation to the Customer's Personal Data, (a) take, as appropriate, measures required pursuant to Article 32 of the GDPR in relation to the security of the OfficeRnD Infrastructure and the platforms used to provide the Services as described in the Principal Agreement, and (b) on reasonable request, assist the Customer in ensuring compliance with the Customer's obligations pursuant to Article 32 of the GDPR.

7. **Audits**

a. Subject to Paragraphs 7(b), OfficeRnD shall make available to the Customer on reasonable request, information that is reasonably necessary to demonstrate the Customer's compliance with this Addendum and shall allow for and contribute to

audits, including inspections, by the Customer or an auditor mandated by the Customer in relation to the processing of the Customer's Personal Data by OfficeRnD. The Customer shall be responsible for any costs and expenses of OfficeRnD arising from the provision of such information and audit rights.

b. The Customer'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 Customer in relation to the Services does not otherwise give the Customer information and audit rights meeting the requirements of Paragraph 7(a) above.

8. **Data Subject Requests**

a. OfficeRnD provides specific tools in order to assist customers in replying to requests received from data subjects. These include our APIs and interfaces to search member's data, activity information and user generated content. When OfficeRnD receives a complaint, inquiry or request (including requests made by data subjects to exercise their rights pursuant to EU Data Protection Laws) related to the Customer's Personal Data directly from data subjects OfficeRnD will notify the Customer within 7 days from the receipt of the complaint, inquiry or request. Taking into account the nature of the processing, OfficeRnD shall assist the Customer, by appropriate technical and organizational measures, insofar as this is reasonably possible, for the fulfillment of the Customer's obligation to respond to requests for exercising such data subjects' rights.

9. **Data Breach**

a. OfficeRnD shall notify the Customer without undue delay once OfficeRnD becomes aware of a personal data breach affecting the Customer's Personal Data. OfficeRnD shall, taking into account the nature of the processing and the information available to OfficeRnD, use commercially reasonable efforts to provide the Customer with sufficient information to allow the Customer, 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 EU 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 Customer, with any data protection impact assessments and prior consultations with supervisory authorities or other competent regulatory authorities as required for the Customer to fulfill its obligations under EU Data Protection Laws.

11. Return or Destruction of the Customer's Personal Data

a. The Customer may at the Customer's cost, by written notice to OfficeRnD, require OfficeRnD, within ninety (90) days of the date of cessation of any Services involving the processing of the Customer's Personal Data to (i) return all copies of the Customer's Personal Data in the control or possession of OfficeRnD and sub-processors; or (ii) to the extent reasonably practicable delete and procure the deletion of all copies of the Customer's Personal Data processed by OfficeRnD and sub-processors. Notwithstanding the foregoing, OfficeRnD may retain the Customer's Personal Data to the extent required by EU Laws. OfficeRnD may retain electronic copies of files containing Customer's Personal Data created pursuant to automatic archiving or back-up procedures which cannot reasonably be deleted In these cases, OfficeRnD shall ensure that the Customer's Personal Data are not further actively processed.

12. Data Transfers

a. The Customer acknowledges and agrees that OfficeRnD and its sub-processors may provide the Services and Support from any state, province, country or other jurisdiction. Following execution of this Addendum, OfficeRnD shall, if requested to do so by the Customer and if required by EU Data Protection Laws, enter into the Standard Contractual Clauses as data importer with the Customer acting as data exporter. If OfficeRnD's arrangement with a sub-processor involves a Restricted Transfer, OfficeRnD shall ensure that the onward transfer provisions of the Standard Contractual Clauses are incorporated into the Principal Agreement, or otherwise entered into, between OfficeRnD and the sub-processor. The Customer agrees to exercise its audit right in the Standard Contractual Clauses by instructing OfficeRnD to conduct the audit set out in Paragraph 7.

13. Sub-processing

a. The Customer 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. OfficeRnD may continue to use those sub-processors already engaged as at the date of this Addendum. OfficeRnD shall give the Customer prior written notice of the appointment of any new sub-processor. If, within five (5) business days of receipt of that notice, the Customer 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 Customer and the Customer has been provided with a reasonable written explanation of the steps taken. If OfficeRnD and the Customer 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.

b. OfficeRnD shall be responsible for the acts and omissions of any sub-processors as it is to the Customer 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 choice of jurisdiction stipulated in the Principal Agreement 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 the country or territory stipulated for this purpose in the Principal Agreement.

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 Customer:

   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 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 and the Standard Contractual Clauses will terminate contemporaneously and automatically with the termination of the Principal Agreement.

   b. OfficeRnD may terminate this Addendum and the Standard Contractual Clauses if OfficeRnD offers alternative mechanisms to Customer that comply with the obligations of the European Union privacy laws for the transfer of Personal Data outside the EEA.

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 Customer
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 to the Customer. OfficeRnD may therefore process personal data. Such processing activities include (a) providing the Services; (b) the detection, prevention and resolution of security and technical issues; and (c) responding to Customer support requests.

The types of Personal Data to be processed

The personal data transferred may name, email, address, phone number, IP address and any additional personal data that the Customer may require to insert into the system.

The categories of data subject to whom the Personal Data relates

Clients and Employees of the Customer.

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. Customers who interact with the products via the user interface must authenticate before accessing non-public customer data.

   Authorization: Customer data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers 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 customer 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 Customer 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. Customer 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.

Schedule 1
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

The Customer entity that is a party to the Addendum to which these Standard Contractual Clauses are attached.

Customer Legal Entity Name:_____
Customer Address: _____
Customer e-mail: _____
(the **data exporter**)

AND

OFFICERND, Ltd.
4 Crown Pl, London EC2A 4BT, UK
e-mail: privacy@officernd.com

(the **data importer**)
each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a)   *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

(b)   '*the data exporter'* means the controller who transfers the personal data;

(c)   *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d)   *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e)   '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f)   *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

---

[1]   Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1.   The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2.   The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.   The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4.   The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a)   that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b)   that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c)   that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d)   that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e)   that it will ensure compliance with the security measures;

(f)   that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g)   to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h)   to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i)   that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j)   that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

(a)   to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b)   that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c)   that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d)   that it will promptly notify the data exporter about:

---

[2]   Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2.   If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3.   If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1.   The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a)   to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b)   to refer the dispute to the courts in the Member State in which the data exporter is established.

2.   The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1.   The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2.   The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3.   The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely _____.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1.   The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[3]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2.   The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3.   The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4.   The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1.   The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all

---

3   This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2.   The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf OFFICERND, Ltd.:

Name (written out in full): Deyan Varchev
Position: Data Protection Officer
Address: 4 Crown Pl, London EC2A 4BT, 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..