BUSINESS PREMIUM DATA PROCESSING AGREEMENT

This Data Processing Addendum ("**DPA**") forms part of the Grover Business Terms and Conditions and/or other written or electronic agreement (collectively, the "**Agreement**") entered into between the relevant Grover entity ("**Grover**") as specified in the Agreement and the Customer ("**Customer**") for the purchase of the Services from Grover.

Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Affiliates. For the purposes of this DPA only, and except where indicated# otherwise, any reference to the parties shall include reference to their Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement. In consideration of the mutual obligations set forth herein, the parties hereby agree that the terms and conditions set out below shall be added as an addendum to the Agreement.

1. Definitions

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"**Controller**" means the entity which determines the purposes and means of the processing of Personal Data.

"**Customer Personal Data"** means any Personal Data that is uploaded onto Grover's Grover Business Premium platform, which Grover processes on behalf of Customer in the course of providing Services. Personal Data may include that of its employees, which the Customer has lawful rights to.

"**Data Protection Laws**" means all data protection and privacy laws applicable to the processing of Customer Personal Data under the Agreement.

"**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

"**Services**" means any service offering provided by Grover to Customer pursuant to the Agreement.

"**Sub-processor**" means any Processor engaged by Grover or its Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the

Agreement or this DPA. Sub-processors may include third parties or Grover's Affiliates.

The terms "**Controller**", "**Data Subject**", "**Processor**," "**process**,", "**processing**", "**Personal Data**" and "**Personal Data Breach**" have the meanings given to them under the GDPR.

2. Scope of this DPA

This DPA applies where and only to the extent that Grover processes Customer Personal Data on behalf of Customer (including Customer's employees' data) in the course of providing Services to Customer pursuant to the Agreement. The DPA does not apply where Grover determines the purpose and means of the processing of Personal Data.

3. Roles and Responsibilities

3.1 **Roles of the parties.** The parties agree that Customer is the Controller of Customer Personal Data and Grover shall process Customer Personal Data only as a Processor acting on behalf or on the documented instruction of Customer. The categories of Data Subjects, Customer Personal Data being processed, and the nature and purpose of the processing are provided in Annex 1.

3.2 **Grover processing of Customer Personal Data.** Grover will process Customer Personal Data only for the purposes listed in Annex 1 or on documented instructions to provide the Services as set forth in the Agreement and this DPA unless Grover is required to process certain Personal Data by applicable Data Protection Laws to which Grover is subject. In such a case, Grover shall notify Customer of those legal requirements prior to the processing, unless the law in question prohibits such notification on grounds of substantial public interest.

3.3 Grover shall inform Customer if, in its opinion, an instruction of Customer infringes the applicable Data Protection Laws.

3.4 Grover has appointed a data protection officer whose contact details are provided in Annex 1.

3.5 **Customer processing of Personal Data.** Customer agrees that (i) it shall comply with its obligations as a Controller under Data Protection Laws in respect of its processing of Personal Data and any processing instructions it issues to Grover; and (ii) it has provided notice, has an adequate basis of processing, and has obtained (or shall obtain) all consents and rights necessary under applicable laws

for Grover to process Customer Personal Data and provide the Services pursuant to the Agreement and this DPA. Grover is not responsible for determining the requirements of the laws applicable to Customer's business or that Grover's provision of the Services meets the requirements of such laws. Grover is not responsible for complying with laws specifically applicable to Customer or Customer's industry and to which Grover is not subject by virtue of Grover's role as the provider of a SaaS (software as a service) Service.

4. Security and Confidentiality

4.1 Grover will maintain appropriate technical and organizational measures when processing Customer Personal Data. These will ensure a level of security appropriate to the risk, including those outlined in Annex 3 to this DPA ("**Security Measures**"), and take into account the state of the art; the costs of implementation, the nature, scope, context, and purposes of processing, and the risk of varying likelihood and severity for the rights and freedoms of Data Subjects. Customer acknowledges that Grover may make changes to the Security Measures as Grover deems necessary or appropriate, including to comply with Data Protection Laws, but that no such changes will reduce the overall level of protection for Customer Personal Data.

4.2 Grover will take appropriate steps to ensure compliance with the Security Measures by its employees, agents, contractors, and Sub-Processors to the extent applicable to their scope of performance, including ensuring that all persons authorized to process Customer Personal Data have agreed to appropriate confidentiality obligations.

5. Personal Data Breaches

5.1 **Breach Notification.** Grover will notify Customer without undue delay, and in any event within forty-eight (48) hours, after becoming aware of a Personal Data Breach. Grover's notification to Customer will describe (a) the nature of the Personal Data Breach, including, if known, the categories and approximate number of Data Subjects and Personal Data records concerned; (b) the measures Grover has taken, or plans to take, to respond to and mitigate the Personal Data Breach; (c) a description of the likely consequences of the Personal Data Breach; and (d) information related to Grover's point of contact with respect to the Personal Data Breach. If Grover cannot provide all the information above in the initial notification, Grover will provide the information to Customer as soon as it is available.

5.2 **Breach Response.** Grover will promptly take all actions relating to its Security Measures that it deems necessary and advisable to identify and remediate the cause of a Personal Data Breach.

5.3 **General.** Grover's notification of or response to a Personal Data Breach will not constitute an acknowledgment of fault or liability with respect to the Personal Data Breach. The obligations in this Section do not apply to Personal Data Breaches that are caused by Customer or its users. Except as may otherwise be required by applicable Data Protection Laws, if Customer decides to notify a supervisory authority, Data Subjects, or the public of a Personal Data Breach, Customer will make reasonable efforts to provide Grover with advance copies of the notice(s) and allow Grover an opportunity to provide any clarifications or corrections to them.

6. Sub-processors

6.1 **Authorization**. Customer generally authorizes Grover to engage Sub-processors in accordance with this section, and approves Grover's use of the Sub-processors listed in the Sub-processors List in Annex 2.

6.2 **Sub-processor Requirements**. Grover has entered or will enter into a written agreement with each Sub-processor that contains data protection obligations equivalent to those in this DPA. Grover will be liable for the actions and omissions of its Sub-processors undertaken in connection with Grover's performance under this DPA to the same extent Grover would be liable if performing the Services directly. Grover shall notify the Customer of any failure by the Sub-processor to fulfill its contractual obligations.

6.3 **Sub-processor Updates.** Grover shall inform the Customer of any intended sub-processing or change in the Sub-processor List giving the Customer sufficient time to be able to object to such changes. Grover may, by giving reasonable notice to the Customer, add or make changes to the Sub-processor List. Grover will notify Customer if it intends to add or replace Sub-processors from the Sub-processor List at least ten (10) days prior to any such changes. If Customer objects to the appointment of an additional Sub-processor in writing within ten (10) calendar days of such notice on reasonable grounds relating to the protection of the Personal Data, the parties will discuss such objection in good faith with a view to achieving resolution. In the event that the parties are unable to find such a solution, Customer may suspend or terminate the applicable Agreement with respect only to those Services which cannot be provided by Grover without the use of the objected new Sub-processor without prejudice to any fees incurred by Customer prior to suspension or termination.

7. Cooperation

7.1 **Data Subject Requests.** The Services provide Customer with the ability to retrieve and delete Customer Personal Data. Customer may use these controls to comply with Customer's obligations under applicable Data Protection Laws, including Customer's obligations related to any requests from data subjects ("Data Subject Requests"). To the extent that Customer is unable to independently access the relevant Customer Personal Data using such controls or otherwise, Grover shall provide reasonable cooperation to assist Customer to respond to such Data Subject Requests. In the event that any such Data Subject Request is made directly to Grover, Grover shall, to the extent legally permitted: (i) advise the data subject to submit their Data Subject Request to Customer; (ii) promptly notify Customer; and (iii) not otherwise respond to that Data Subject Request without authorization from Customer unless legally compelled to do so. Customer will be responsible for responding to any such Data Subject Requests.

7.2 **Legal Compliance.** To the extent Grover is required under applicable Data Protection Laws, Grover will provide reasonably requested information regarding the Services to enable the Customer to carry out data protection impact assessments and prior consultations with data protection authorities as required by law.

7.3 **Assistance.** Grover will provide assistance in reviewing data breaches and implementing any notification obligations, as well as in complying with the obligation to ensure Customer Personal Data is accurate and up-to-date. Furthermore, Grover will assist with appropriate technical and organizational measures to enable Customer to fulfill its existing obligations towards the Data Subject.

8. Audit

Customer or a person authorized by the Customer is entitled to monitor compliance with the applicable Data Protection Laws to the extent necessary, in particular by gathering information and requests for relevant documents. The inspection of data processing programs or accessing the working rooms of Grover shall only take place during the designated office hours without interrupting the business operations with a minimum of four (4) weeks' prior written notice. Proof of proper data processing can also be provided by appropriate and valid certificates for IT security (e.g. ISO 27001), provided that the specific subject of certification applies to the commissioned data processing.

9. International Data Transfers

9.1 Grover shall carry out the processing in the territory of the Federal Republic of Germany, in a Member State of the European Union or within the European Economic Area. Any transfer of data to a third country by Grover shall be done only on the basis of documented instructions from Customer and shall take place if the specific legal requirements of the GDPR are met.

9.2 Grover shall ensure compliance with the provisions of Articles 44 to 50 of the GDPR in the event of a subprocessing involving a transfer of Personal Data within the meaning of Chapter V of the GDPR by providing, where necessary, appropriate safeguards in accordance with Article 46 of the GDPR. In line with this, Grover has concluded the standard data protection clauses of the European Commission with sub-processors in third countries and carried out Transfer Impact Assessments in order to provide appropriate guarantees for the protection of Personal Data.

10. Term and Termination

This DPA will become effective as of the effective date of the Agreement. It shall continue as long as Customer utilizes Grover's Services.

11. Deletion or Return of Data

Upon termination or expiration of the Agreement, Grover shall (at Customer's election) delete or return to Customer all Customer Personal Data in its possession or control in accordance with the terms of the Agreement. Grover may retain Customer Personal Data to the extent that it is required or authorized to do so under applicable law or to the extent Customer Personal Data is archived on Grover's back-up systems, in which case Grover will securely isolate and protect such data from any further processing, except to the extent required by applicable law.

12. Accession to the DPA

Any entity that is not a Party to this DPA may, with the agreement of all the Parties, accede to this Agreement at any time as a controller or a processor by means of a declaration of accession. In addition to the declaration of accession, Annexes 1 to 3 shall be completed where necessary. From the date of accession, the acceding entity shall be treated as a party to this DPA and have the rights and obligations of a controller or a processor, in accordance with its designation.

13. General

13.1 Liability.

13.1.1 For the avoidance of doubt, any claim or remedies Customer and/or its Affiliates may have against Grover, any of its Affiliates and their respective employees, agents and Sub-processors (hereinafter "**Grover Group**") arising under or in connection with this DPA, including: (i) for breach of this DPA; (ii) as a result of fines (administrative, regulatory or otherwise) imposed upon Customer and/or its Affiliates; and (iii) under applicable Data Protection Laws, including any claims relating to damages paid to a Data Subject, will, in the aggregate, be subject to any limitation of liability provisions (including any agreed aggregate financial cap) that apply in the Agreement.

13.1.2 Customer further agrees that it will defend and indemnify Grover Group against (i) any regulatory penalties incurred by Grover Group in relation to the Customer Personal Data that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this DPA or any applicable Data Protection Laws; and (ii) any claims made by a Data Subject, arising out of Customer's breach of this DPA.

13.2 **Governing Law and Jurisdiction.** This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

13.3 **Entire Agreement; Conflict.** Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this DPA, the terms of this DPA will control.

13.4 **Invalidity.** If any provision of this DPA is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, then the invalidity or unenforceability of such provision does not affect any other provision of this DPA and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

13.5 **Amendments.** Notwithstanding anything to the contrary in the Agreement and this DPA, Grover reserves the right to make any updates or changes to this DPA to ensure continued compliance with all applicable Data Protection Laws.

Annex 1

A. Details of Data Processing

(a) Subject matter of the processing. Grover's provision of the Grover Business Premium platform to Customer as set forth in the DPA.

(b) Nature and purpose of the processing. Grover will process Customer Personal Data for the purposes of providing the Services to Customer in accordance with and as described in the Agreement and this DPA.

(c) Categories of Personal Data processed. Customer may submit Personal Data to the Grover Business Premium platform, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but not limited to, the following categories of Personal Data: Customer's employee name, business email address, employee number, home address as shipping address.

(d) Categories of data subjects whose personal data is processed. Customer' employees, and any other individuals whose personal data are uploaded or transmitted via Grover's software.

(e) Duration of the processing. For the term of this DPA and the period from expiry of the term of this DPA until the anonymization, return, or deletion of data in accordance with this DPA.

B. Contact Details of Grover's Data Protection Officer

Name: datenschutz nord GmbH
Address: Kurfürstendamm 212, 10719 Berlin, Germany
Email: office@datenschutz-nord.de

Annex 2

Sub-processor's List

Sub-processor	Subject Matter	Nature and purpose of processing	Registered Address	Location(s) of processing
Amazon Web Services EMEA SARL	Personal data contained on the Grover Business Premium platform	Cloud infrastructure	38 avenue John F. Kennedy L-1855 Luxembourg	Germany, Ireland
Intercom, Inc.	Personal data contained in communications via chatbot	Customer support services	55 2nd Street, 4th Fl., San Francisco, CA 94105, USA	Ireland, the USA
Grover Group GmbH	Personal data contained on the Grover Business Premium platform and in communications via chatbot	Provision of the Grover Services	Potsdamerstraße 125, 10783 Berlin, Germany	Germany

Annex 3

Security Measures

The following sections define Grover's current technical and organizational measures. Grover may change these at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

1. Access Controls

- Grover personnel access Grover's systems via unique user IDs, and are required to authenticate through VPN and multi-factor authentication.
- Grover personnel access Customer Personal Data as necessary to provide the Services under the Agreement, to provide customer support upon a customer's request, or to comply with the law or a binding order of a governmental body.
- Grover has proper controls in place for requesting, approving, granting, modifying and revoking users access to systems and applications.

2. Physical & Environmental Controls

2.1 **Data Centers**. Grover hosts all Customer Personal Data in Amazon AWS. Grover regularly reviews Amazon's physical and environmental controls for its relevant data centers, as audited by Amazon's third-party auditors. Such controls include, but are not limited to:

- Physical access to the facilities is controlled at the building ingress points;
- Visitors are required to present ID and are signed in;
- Physical access to servers is managed by access control devices;
- Physical access privileges are reviewed regularly;
- Facilities utilize monitor and alarm procedures;
- Fire detection and protection systems;
- Power back-up and redundancy systems.

2.2 **Grover Corporate Offices.** While Customer Personal Data is not hosted at Grover's corporate offices, Grover's technical, administrative, and physical controls for its corporate offices include, but are not limited to, the following:

- Physical access to the corporate offices is controlled at office ingress points;
- Visitors are required to sign in;
- Tagging and inventory of Grover-issued laptops and network assets;
- Fire detection and sprinkler systems.
- Alarms

3. Security Program

Grover's systems are designed according to established industry best security practices, and includes many technical and administrative security controls, including, without limitation:

3.1 **Secure Data Centers.** Grover's systems are fully embedded within Amazon's AWS platform. For more information about Amazon's AWS security, refer to https://aws.amazon.com/security/.

3.2 **Information Security Policy.** Grover has developed and implemented, and will maintain, security policies that govern all relevant aspects of its security program, and are aligned with security industry standards. Information security policies are reviewed periodically and Grover may amend new policies as it deems reasonable to maintain protection of services and content processed therein. The Information Security Policy may be made available to customers upon request.

3.3 **Encryption.**

- Grover maintains a secure environment for the transmission of Personal Data, utilizing encryption consistent with industry standard practices such as Federal Information Processing Standards FIPS 140-2 and/or NIST SP800-52 and utilizing industry accepted encryption technologies such as server certificate-based authentication within the Grover environment. Data in motion is encrypted with TLS 1.2 or greater. Secure Shell (SSH) is the approved cryptographic network protocol for file transfer and remote login and command execution, and Virtual Private Network (VPN) is used to secure tunnel data to and from a remote network.

- Grover maintains a secure environment for the storage of Personal Data, utilizing encryption consistent with industry standard practices such as Federal Information Processing Standards FIPS 140-2 and/or NIST SP800-52. Data at rest is encrypted using AES encryption algorithm with 256 bits key size.

3.4 **Availability.** In order to provide redundancy, scalability and high availability Grover services are deployed on container orchestration systems which allows for automated software deployment and scaling. All the services are deployed on multi availability zones which are designed to fail-over between data centers automatically.

3.5 **Backup.** Customer data is backed up and monitored utilizing AWS and done automatically by software provided by AWS.

3.6 **Change Control.** Grover maintains documented change management policy and procedure to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

4. Vulnerability Detection and Management

4.1 **Anti-Virus and Vulnerability Detection.** Grover leverages threat detection tools to monitor and alert Grover to suspicious activities, potential malware, viruses and/or malicious computer code (collectively, "Malicious Code"). Grover does not monitor Customer Personal Data for Malicious Code.

4.2 **Penetration Testing and Vulnerability Detection.** Grover regularly conducts penetration tests throughout the year and engages one or more independent third parties to conduct penetration tests of the services at least annually.

4.3 **Vulnerability Management.** Incident reporting and response policies and procedures are in place to guide Grover personnel in reporting the information technology incident. Vulnerabilities meeting defined risk criteria trigger alerts and are prioritized for remediation based on their potential impact to the Services.

4.4 **Risk Management.** Grover has implemented a Risk Management Standard that identifies and manages risks that could potentially affect the Grover's ability to provide reliable service to customers. Grover identifies the risks, measures the impact to organization and establishes mitigation plans to manage the risk and have acceptable risk tolerance levels.

4.4 **Endpoint Controls.** Grover has implemented different security controls on end-user devices and monitors the devices to be in compliance with security standards, some of the security controls implemented are: hard drive encryption, requiring password during login, lock screen, antivirus software, firewall and appropriate patch levels. Grover will securely sanitize the hard drive prior reuse and will securely destroy the media that will not be used anymore. Grover logically separates its endpoints and end user environment from the other Grover environment. Multi-factor authentication is required to access the AWS environment.

4.5 **Monitoring and Logging.** Grover monitors its environment 24/7/365 and centralizes its logs. Anomalies are investigated and prioritized on a 24/7/365 basis. Only authorized personnel can view the logs. No personnel may edit, delete, or otherwise alter security logs of users or system accounts. Security Information and Event Management (SIEM) software is in place to collect and analyze the logs from users and system accounts. SIEM is able to analyze the data from different log sources, correlate events among the log entries, identify and prioritize significant events and initiate responses to events.

4.6 **Program Testing.** Grover regularly tests and evaluates its security program.

5. Administrative Controls

5.1 **Personnel Training.** Grover maintains a documented security awareness and data privacy training programs for its personnel, including but not limited to onboarding and annual training to aid in the prevention of unauthorized use or disclosure of sensitive data and how to effectively report and respond to security incidents. Grover also conducts role-based security awareness training for its employees. All records for onboarding and annual training are documented and retained for tracking purposes.

5.2 **Personnel Agreements.** Grover personnel are required to sign confidentiality agreements upon hire and to acknowledge Grover's Information Security Policy.

5.3 **Personnel Access Reviews and Separation.** Grover re-evaluates the access rights of its employees that have access to systems and applications. The access rights review is done periodically and the removal of access is done on a timely basis for all its personnel.