Data Processing Agreement

RECITALS

This Data Processing Agreement (the "**Data Processing Agreement**"), dated as of _____ (the "**Effective Date**") by and between _____, a _____ corporation, having its principal place of business at _____ ("**Customer**"), and **Billow Myndbend, Inc.,** a New York corporation, having its principal place of business at 33 Irving Place, New York, NY 10003 ("**Service Provider**"). This Data Processing Agreement refers to Customer and Service Provider individually as a "**Party**" and collectively as the "**Parties**".

WHEREAS, Customer and Service Provider have entered into a separate agreement for Services (as defined below), as may have been amended, amended and restated, supplemented, or otherwise modified from time to time in accordance with its provisions (the "**Services Agreement**"), which defines Service Provider's obligations with respect to the provision of Services to Customer;

WHEREAS, the Service Provider may be processing personal data as part of delivering the Services;

WHEREAS, it is therefore necessary for the Parties to enter into an appropriate data processing agreement which reflects the roles of the Parties and their obligations under applicable Data Protection Laws and the Parties wish to enter into such an agreement.

AGREEMENT

NOW, THEREFORE, in consideration of the premises set out above and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows.

1. DEFINITIONS. Capitalized terms used and not defined in this Data Processing Agreement have the respective meanings assigned to them in the Services Agreement.

"**Affiliate**" shall mean any entity that directly, or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the Party. For purposes of this definition, the term "control" means the power (or, as applicable, the possession or exercise of the power) to direct, or cause the direction of, the management, governance, or policies of a given entity, directly or indirectly, through any applicable means (whether through the legal, beneficial, or equitable ownership, of more than fifty percent (50%) of the aggregate of all voting or equity interests or securities of such entity, through partnership, or through some other form of ownership interest, by contract, or other applicable legal document, or otherwise).

"**Applicable Law**" shall mean all regional, national, and international laws, rules, regulations, and standards including those imposed by any governmental or regulatory authority which apply from time to time to the person or activity in the circumstances in question.

"**Cloud Service Provider**" means any provider of network services, infrastructure, or business applications or services in the cloud (e.g. Amazon Web Services (AWS), Microsoft Azure, Google Cloud, or any other substantially similar service)

"**Controller**" has the meaning set forth in the applicable Data Privacy Law.

"**Customer**" has the meaning set forth in the Preamble.

"**Customer Data**" shall mean any Personal Data that Service Provider processes as a Processor in providing the Services to a Customer pursuant to this Services Agreement.

"**Data Privacy Law**" means, as the case may be, the EU Data Protection Directive 95/46/EC (the "**Directive**") or, when applicable, EU General Data Protection Regulation 2016/679 ("**GDPR**"), the implementing acts of the foregoing by the Member States of the European Union and/or any other Applicable Law or regulation relating to the protection of Personal Data, personally identifiable information or protected health information.

"**Data Processing Agreement**" has the meaning set forth in the Preamble.

"**Data Subject**" has the meaning set forth in the applicable Data Privacy Law.

"**Effective Date**" has the meaning set forth in the Preamble.

"**Member State**" means a member state of the European Union and/or the European Economic Area, as may be amended from time to time.

"**Monitoring Service Provider**" has the meaning set forth in Section 9.3(e).

"**Party**" has the meaning set forth in the Preamble.

"**Personal Data**" means any information relating to an identified or identifiable natural person; an identifiable person is one who can be defined, directly or indirectly, notably but not limited to by reference to a user identification such as a name, an identification number, geo-location data, an online user identification, or by reference to one or more factors specific to his physical, physiological, genetic, mental, economic, cultural, or social identity, including, without limitation, "personal data" as that term is used in a Data Privacy Law (even if no Data Privacy Law applies to the Customer or provider), "protected health information" as that term is used under the Health Insurance Portability and Accountability Act (even if such act is not applicable to Customer or Provider), "nonpublic personal information" as that term is defined under the Gramm-Leach-Bliley Act (even if such act is not applicable to Customer or Provider), and all other personal information protected under any Applicable Law.

"**Process**" has the meaning set forth in the applicable Data Privacy Law.

"**Processing**" has the correlative meaning to Process as set forth in the applicable Data Privacy Law.

"**Processor**" has the meaning set forth in the applicable Data Privacy Law.

"**Security Incident**" has the meaning set forth in Section 7.1.

"**Service Provider**" has the meaning set forth in the Preamble.

"**Services**" means the provision of services or other work products by the Service Provider as described and set out in the Services Agreement, and such other services as the Parties may agree upon in writing from time to time.

"**Services Agreement**" has the meaning set forth in the Preamble.

"**Subprocessor**" means a third party engaged by Service Provider to assist with the provision of the Services which involves the processing of Customer Data, including, without limitation, Cloud Service Providers.

"**Term**" is the term of the Services Agreement.

2. **RELATIONSHIP WITH SERVICES AGREEMENT.** For the avoidance of doubt, unless there is any conflict or inconsistency between the provisions in the Services Agreement and this Data Processing Agreement (in which case, to the extent this Data Processing Agreement requires additional, more stringent, or more protective obligations, the provisions of this Data Processing Agreement take precedence), all other provisions of the Services Agreement apply.

3. **STATUS OF PARTIES.** Service Provider is the Processor of Customer Data and Customer is the Controller of Customer Data under this Data Processing Agreement. Service Provider shall not assume any responsibility for determining the purposes for which Customer Data shall be processed.

4. **SCOPE OF DATA PROCESSING.**

4.1. All Parties shall comply with their applicable obligations under Data Privacy Laws.

4.2. The subject-matter of the data processing to be carried out by the Service Provider is: Myndbend Process Manager for Zendesk or any other Services or applications that may be provided by Service Provider under the Services Agreement.

4.3. The duration of the data processing to be carried out by the Service Provider shall be for the Term stated in the Services Agreement.

4.4. The nature of the data processing to be carried out by the Service Provider is: Service Provider will be accessing Customer's Zendesk instance via the Zendesk API for the purposes of providing the Services.

4.5. The purpose of the data processing is: Service Provider will be retrieving ticket data, and related user data, from Customer's Zendesk instance in order to create new tickets and post updates to tickets.

4.6. The type of personal data involved in the data processing is: Service Provider retrieves the full ticket data from a specific ticket request which may include personal information stored in custom fields. However, Service Provider does not use or store such personal information.

4.7. The categories of Data Subjects involved in the data processing are: the Data Subjects will ultimately depend on data stored in Zendesk, provided, however, that the normally-expected Data Subjects would be Customer's end-users and customers that create tickets within Customer's Zendesk instance.

5. PROCESSOR OBLIGATIONS.

5.1. The Service Provider shall process Customer Data on behalf of Customer exclusively and only in accordance with the instructions received from Customer.

5.2. In the event Service Provider is required under any Applicable Law to process Customer Data in excess of Customer's documented instructions, Service Provider shall immediately notify Customer of such a requirement, unless such Applicable Law prohibits such notification on important grounds of public interest.

5.3. Service Provider will not perform their obligations under the Services Agreement and this Data Processing Agreement in such a way as to cause Customer to breach any obligation under applicable Data Privacy Laws.

5.4. Service Provider shall co-operate in good faith with any third party that Customer engages to provide services to Customer where the third party is required to access Customer Data.

5.5. Upon Customer's request, the Service Provider will promptly co-operate with Customer to enable Customer to: (a) comply with all requests of access, rectification, and/or deletion of Customer Data arising from a Data Subject; (b) enforce rights of Data Subjects under the Data Privacy Law; and/or (c) comply with all requests from a supervisory authority, including but not limited to in the event of an investigation.

5.6. Service Provider shall provide all reasonable assistance to Customer where Customer carries out a data privacy impact assessment relating to Customer Data.

5.7. The Service Provider shall promptly notify Customer and shall respond without unreasonable delay to all inquiries from Customer regarding:

(a) the Service Provider's Processing of the Customer Data;

(b) any request Service Provider receives from a Data Subject regarding that Data Subject's Personal Data where it is Customer Data, provided, however, that the Service Provider shall obtain specific prior written consent and instructions from Customer prior to responding to the Data Subject;

(c) any request, complaint, or communication relating to Customer's obligations under Data Privacy Laws (including from data protection authorities and/or supervisory authorities) provided, however, that the Service Provider shall obtain specific written consent and instructions from Customer prior to responding to such request, complaint, or communication.

5.8. Any data collected pursuant to data analytics or monitoring carried out by Service Provider in connection with the provision of the Services or otherwise connected with Customer's use of the Services may include Personal Data, which Customer hereby authorizes Service Provider to use solely in accordance with carrying out its obligations under the Services Agreement or this Data Processing Agreement.

6. SCOPE MODIFICATIONS.

6.1. In the event that changes in Data Privacy Laws require modifications to the Services, the Parties shall use commercially reasonable efforts to comply with such requirements. If such changes in Data Privacy Laws require structural changes to the Services such that the provision of the Services would otherwise be in breach of such Data Privacy Laws unless such changes are performed, the Parties will discuss in good faith Service Provider's ability to comply and will negotiate and revise the Services accordingly.

6.2. In the event that a Party's compliance with Data Privacy Laws requires the imposition of certain additional contractual obligations under this Data Processing Agreement, such Party shall notify the other Party and both Parties shall in good faith seek to amend this Data Processing Agreement in order to address the requirements under Data Privacy Laws.

6.3. Customer shall notify Service Provider of any faults or irregularities in relation to this Data Processing Agreement that it detects in the provision of the Services. If the notification provided by Customer under this Section 6.3 necessitates a change of the Services, Service Provider shall use all commercially reasonable efforts to coordinate such changes with Customer before they are implemented.

7. SECURITY MEASURES.

7.1. The Service Provider shall take and implement appropriate technical and organizational security and confidentiality measures and regularly update them to ensure a level of security appropriate to the risk to Customer Data. Service Provider shall undertake commercially-reasonable efforts to protect Customer Data against any actual or threatened unauthorized use, modification, loss, compromise, destruction, or disclosure of, or access to, Customer Data ("**Security Incident**").

7.2. Such measures implemented in Section 7.1 shall require the Service Provider to have regard to industry standards and costs of implementation as well as taking into account the nature, scope, context, and purposes of the Processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals.

7.3. The Parties agree and acknowledge that Customer is relying upon Service Provider's skill and knowledge in order to assess what is "appropriate" to protect Customer Data against unauthorized or unlawful processing and against including, but not limited to, accidental loss, destruction, damage, alteration, or disclosure.

7.4. The Service Provider shall implement and maintain policies and procedures to detect and respond to Security Incidents.

7.5. The Service Provider shall protect all Customer Data that is likely to be transferred via the Internet by encryption measures reasonably designed to ensure confidentiality.

8. CONFIDENTIALITY.

8.1. Service Provider represents and warrants that:

(a) all persons who have access to Customer Data shall maintain its confidentiality and keep current with any special data protection, data security, and confidentiality requirements arising from the Services Agreement or this Data Processing Agreement. Service Provider shall furthermore require their employees and contractors to adhere to the confidentiality obligations set out in the Services Agreement and shall document such employees' and contractors' obligation in writing; and

(b) all persons involved in the processing of Customer Data shall, no less than once annually, and prior to exposure to Personal Data, attend adequate training in the care, protection, and handling of Personal Data.

8.2. Service Provider shall require that the obligation of confidentiality on the respective persons shall continue beyond, and survive termination or expiration of, the Services Agreement or this Data Processing Agreement. Service Provider shall require that the obligation of confidentiality shall continue after the employment or contractual relationships with the respective person ends.

8.3. Service Provider shall keep Customer Data logically separate, with adequate logical separate security controls, from other data and information held by Service Provider.

8.4. The Service Provider shall, without undue delay, notify Customer in writing of any request received from a third party public authority including a law enforcement agency or government agency for disclosure of the Customer Data unless otherwise legally prohibited (such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation). Such notification shall set out (a) the scope of the request, (b) the reason for the request, and (c) the form of the disclosure requested, in so far as Service Provider are able to describe such aspects. Where Service Provider is legally prohibited from notifying Customer, Service Provider shall use reasonable efforts to request the third party public authority to direct the request directly to Customer. Unless prohibited by law, Service Provider shall not respond to a request received under this Section 8.4 unless and until it receives written instructions from Customer.

9. SECURITY INCIDENT NOTIFICATION OBLIGATIONS.

9.1. In the event of a Security Incident arising during the performance of the Services by the Service Provider, the Service Provider shall, at its own cost:

(a) notify Customer about the Security Incident without undue delay and at least within forty-eight (48) hours of Service Provider becoming aware of the Security Incident;

(b) as part of the notification under Section 9.1(a) provide a description of the Security Incident including the nature of the Security Incident;

(c) promptly begin a full investigation into the circumstances surrounding the Security Incident;

(d) after investigating the causes of such Security Incident, take such actions as may be necessary or reasonably expected by Customer to minimize the effects of the Security Incident; and

(e) take all actions as may be required by Data Privacy Laws;

9.2. Service Provider shall make any information referred to under Section 9.1 available to Customer on request. All such information shall be considered the Confidential Information of Service Provider.

9.3. In the event of a Security Incident, each Party shall use all reasonable efforts in good faith to mitigate any reputational and brand damage to the other affected Party.

9.4. Subject to Applicable Law, Service Provider will promptly notify Customer in writing if any Customer Data stored or maintained by Service Provider are at risk due to third-party actions (such as attachment or seizure), due to insolvency proceedings or other occurrences. In such cases, subject to Applicable Law, Service Provider will also inform creditors without delay of the fact that the assets in question are the property of Customer and consist of Customer Data that are processed on behalf of Customer.

10. INTERNATIONAL DATA TRANSFERS. Service Provider shall process Customer Data solely on servers belonging to Service Provider in the United States of America. Except as set out under this Data Processing Agreement or as authorized by Customer in writing, Service Provider shall not transfer or make Customer Data available or accessible in any other jurisdiction or to any other party.

11. RETURN AND DESTRUCTION.

11.1. Without prejudice to any obligations under this Section 11, following termination or expiration of the Services Agreement for whatever reason, Service Provider shall cease processing Customer Data and shall require that all Subprocessors cease processing Customer Data.

11.2. Upon termination or expiration of the Services Agreement for whatever reason, Service Provider shall: (a) provide Customer with the opportunity to retrieve Customer Data; and/or (b) provide Customer on request with Customer Data including all copies and back-ups.

11.3. Following termination or expiration of the Services Agreement for whatever reason and having received written confirmation from Customer, Service Provider shall securely, irrevocably, and/or irretrievably sanitize the Customer Data in accordance with Appendix A of the National Institute of Science and Technology Special Publication 800-88, and Service Provider shall certify to Customer, in writing, that Service Provider has complied with their obligations to delete Customer Data especially from all production, testing, development, and backup systems and media.

11.4. To the extent feasible, Service Provider shall archive documentation that is evidence of proper Customer Data processing beyond termination or expiration of the Services Agreement and continuing for any period of time in which Service Provider retains Customer Data.

11.5. For the avoidance of doubt, Service Provider may retain Customer Data where strictly required to store such data under Applicable Law.

12. TERMINATION. The rights of termination for cause as set out in the Services Agreement remain unaffected. The termination or expiration of the Services Agreement for any reason shall cause termination of this Data Processing Agreement.

13. MISCELLANEOUS.

13.1. **Amendment.** This Data Processing Agreement may not be amended or modified except in writing signed by authorized representatives of both Parties.

13.2. **Severability.** If any provision in this Data Processing Agreement is determined to be ineffective or void by any court or body of competent jurisdiction or by virtue of any legislation to which it is subject, it shall be ineffective or void to that extent only and the validity and enforceability of the remaining provisions of the Data Processing Agreement and the Services Agreement shall not be affected. The Parties shall promptly and in good faith replace the ineffective or void provision with a lawful provision that reflects the business purpose of the ineffective or void provision. The Parties shall similarly promptly and in good faith add any necessary appropriate

provision where such a provision is found to be missing by any court or body of competent jurisdiction or by virtue of any legislation to which this Data Processing Agreement is subject.

13.3. **Governing Law.** Notwithstanding anything to the contrary in the Services Agreement, this Data Processing Agreement shall be governed by and construed in accordance with the national law that applies to the Service Provider.

13.4. **Headings.** The headings in this Data Processing Agreement are for reference only and shall not affect the interpretation of this Data Processing Agreement.

IN WITNESS WHEREOF, the Parties have caused their respective duly authorized representatives to execute this Data Processing Agreement, which is effective as of the Effective Date.

Customer	**Service Provider**
Signature: _____	Signature: _____
Printed Name: _____	Printed Name: _____
Title: _____	Title: _____
Date: _____	Date: _____