Bryntum AB

Data Processing Agreement

This Data Processing Agreement (“DPA”) reflects the requirements of the European Data Protection Regulation (“GDPR”) and comes into effect on May 25, 2018.

1. Introduction

This DPA is an amendment to the Terms of Service ("Agreement") between Bryntum AB ("BAB") and the Customer (“Customer”). Capitalized terms not defined in this DPA are defined in the general Terms of Service. The parties agree that with regard to the Processing of Personal Data, Customer is the Data Controller, BAB is a Data Processor and that BAB will engage Subprocessors as part of providing the Service to Customer, as set forth in Section 5.

2. Definitions

2.1. **Data Protection Laws** means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under this DPA.

2.2. **Personal Data** means any information that identifies a natural person.

2.3. **Special Data** means sensitive Personal Data as defined by GDPR which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life, unique identity of a person by processing biometric or genetic data and criminal convictions and offences.

3. Responsibilities of BAB

3.1. By entering into this DPA, the Customer is instructing BAB to process Personal Data; (a) for the purpose of providing the Service offered by BAB, i.e. trouble shooting of web application software errors, (b) in a manner that complies with Data Protection Laws, (c) to fulfil its duties under the terms of the Agreement, (d) as outlined in this DPA.

3.2. To the best of BAB’s knowledge, there is no legislation that prevents BAB from following the instructions set forth in 3.1. In case BAB is notified of the contrary, BAB shall notify Customer about any instructions or Data Processing that violates Data Protection Laws.

3.3. BAB warrants that it will treat Personal Data as confidential information and shall implement adequate security measures and use established industry best practices to protect the Personal Data.

3.4. BAB will reasonably assist Customer with fulfilling its obligations as Data Controller, to respond to requests from its end users exercising their rights to their Personal Data, to the extent BAB is legally permitted to do so. Such rights include correcting, deleting or otherwise accessing the

Personal Data. Any cost arising out of this assistance shall be borne fully by Customer. The cost of BAB's assistance is based on BAB's current hourly rate for such work.

4. Responsibilities of Customer

4.1. By entering into this DPA, Customer confirms that by using the Service provided by BAB, Customer will not violate Data Protection Laws as part of processing Personal Data.

4.2. Customer warrants that it is legally authorized to process and share the Personal Data with BAB (including any Subprocessors engaged by BAB).

4.3. Customer acknowledges that it bears sole responsibility for the correctness, integrity and content of the Personal data submitted to BAB.

4.4. Customer warrants that it complies with all regulatory requirements and obligations set forth by relevant authorities in relation to the processing of Personal Data.

4.5. Customer warrants that it has fulfilled its duties under the Data Protection Laws and that it has notified relevant authorities about Customer's processing of Personal Data.

4.6. Customer explicitly agrees to not transfer any Special Data as defined in this DPA to BAB. If a transfer of Special Data is made, BAB cannot be held accountable for any wrongful processing of such Special Data.

4.7. Customer shall maintain an up to date register of the types and categories of Personal Data it processes.

5. Subprocessors; Data transfer

5.1. By entering into this DPA, Customer consents to BAB's use of Subprocessors and also acknowledges that BAB may add, remove or replace any such listed Subprocessor at its discretion. BAB warrants that the Subprocessors engaged meet the same requirements as BAB does in its role as Data Processor as set forth in this DPA.

5.2. The current list of Subprocessors with access to the Personal Data are documented at https://therootcause.io/privacy-policy/

5.3. Customer may at any request a detailed description of the subprocessors used by BAB in providing the Service.

5.4. If a BAB Subprocessor is located outside the European Economic Area, BAB shall ensure that any involved data transfer complies with the Data Protection Laws. Customer hereby authorizes BAB to transfer Personal Data outside the European Economic Area and to enter into standard agreements for data processing with its Subprocessors, and to transfer Personal Data in accordance with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks.

6. Security

6.1. BAB shall perform organizational and technical measures, as described in Appendix A, to guarantee an adequate security level, taking into account cost of implementation relative to the risk of the data processing and the types of Personal Data processed.

6.2. BAB will promptly notify Customer after BAB becomes aware of any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unlawful access to any Customer's Personal Data that is transmitted, stored or otherwise Processed by BAB or its Subprocessors ("Security Breach"). BAB will use reasonable efforts to identify the cause of such Security Breach and shall: (a) investigate the Security Breach and provide Customer with information about the Security Breach, including if applicable, such information a Data Processor must provide to a Data Controller under Article 33(3) of the GDPR to the extent such information is reasonably available; and (b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Breach to the extent the remediation is within BAB's reasonable control. The obligations herein shall not apply to any breach that is caused by Customer or its Team Members. Notification will be sent to Customer in accordance with Section 6.4.

6.3. BAB's obligation to report or respond to a Security Breach under this Section is not and will not be construed as an acknowledgement by BAB of any fault or liability with respect to the Security Breach.

6.4. Notifications of Security Breaches will be delivered to one or more of Customer's email addresses. It is Customer's sole responsibility to ensure the email addresses entered into the Service are correct and up to date.

7. Auditing

No more often than once per year (unless required by law), upon 30 days advanced notice by Customer, BAB shall provide Customer with reasonable assistance as needed to fulfil Customer's obligation to carry out a data protection impact assessment related to Customer's use of the Service. BAB will provide such assistance upon Customer's reasonable request. In the event of an

audit, BAB reserves the right to appoint a neutral party to perform the audit. Any and all costs arising from such audit shall be borne by Customer, to the extent legally permitted.

8. Categories of Personal Data processed by BAB

8.1. The categories of Personal Data processed by BAB in connection with using the Service is documented in BAB's privacy policy at https://therootcause.io/privacy-policy/

8.2. By using the Service, Customer's Team Members and its end users are able to submit any type of data for processing by BAB, and it is therefore not possible for BAB to document which categories of Personal Data it processes.

8.3. Customer agrees to not transfer any Special Data to BAB. If a transfer of Special Data is made, BAB cannot be held accountable for any wrongful processing of such Special Data.

9. Term

The terms of this DPA are in effect during the tenure of the general Agreement.

10. Data Protection Officer

BAB has appointed a Data Protection Officer that can be reached at dpa@bryntum.com

11. Liability

In the event of a breach of the terms in this DPA, any liabilities are governed by the general Agreement between Customer and BAB.

12. Jurisdiction

This DPA shall be construed in accordance with and be governed by the substantive laws of Sweden. Any dispute, controversy or claim arising out of or in connection with the DPA, or the breach, termination or invalidity thereof, shall, with the exclusion of any other courts, be settled at the District Court of Malmö, Sweden.

Appendix A – Subprocessors

BAB's list of Subprocessors can be found as part of BAB's privacy policy. https://therootcause.io/privacy-policy/

Appendix B – Security Measures

The following Security Measures relating to the Service have been implemented by BAB.

Access Control
The servers and data center used by BAB for the Service is provided by Digital Ocean in the Netherlands, whose security measures can be found at https://www.digitalocean.com/security/gdpr/data-processing-agreement

System Access Control
The Service and any data in it may not be used without authorization.

BAB has implemented the following measures:

- Ensured that all parts of the Service that processes personal data require a password, in order to prevent unauthorized access to any Personal Data.
- The Service has a password policy that requires all users to use a strong password
- Passwords are stored in an encrypted form
- Ensured it is possible to delete a user of the Service completely
- Only members of BAB's operations team can access the Service servers
- BAB's operations team use SSH keys for any direct server access, and no standard port numbers are used.

Data Transmission Control
Personal Data may not be accessed in any way without authorization during transfer or storage.

BAB has implemented the following measures:

- All web traffic to and from the Service uses SSL and is encrypted with 2048 bit keys.

- Any internal inter-server Service traffic is encrypted using SSH

Availability Control
Personal Data shall be protected against accidental or unauthorized destruction or loss.

BAB has implemented the following measures:

- Ensured that the data of the Service is backed up on a regular basis to a separate secured server.
- Ensured that backups are encrypted and password protected

Organizational Requirements
BAB's employees and subcontractors will comply with all requirements relating to data protection.

BAB has implemented the following measures:

- Designated a data protection offer (DPO)
- All Bryntum employees and subcontractors have signed NDA agreements to maintain confidentiality
- Trained staff on data privacy and data security, and on security incident protocols