GDPR Data Processing Addendum

Last updated: July 11, 2018

This Data Processing Addendum ("DPA") is an agreement between Embleema ("EMBLEEMA," "we," "us," or "our") and you ("Customer", "user" or "you").

1. Data Processing.

1.1 **Scope and Roles.** This DPA applies when Customer Data is processed by EMBLEEMA. In this context, EMBLEEMA will act as "processor" and "controller" to Customer who may act as "controller" with respect to Customer Data (as each term is defined in the GDPR).

1.2 **Customer Controls.** The Services provide Customer with a number of controls, including security features and functionalities, that Customer may use to retrieve, correct, delete or restrict Customer Data.

1.3 Details of Data Processing.

1.3.1 **Subject matter.** The subject matter of the data processing under this DPA is Customer Data.

1.3.2 **Duration.** As between EMBLEEMA and Customer, the duration of the data processing under this DPA is determined by Customer.

1.3.3 **Purpose.** The purpose of the data processing under this DPA is the provision of the Services initiated by Customer from time to time.

1.3.4 **Nature of the processing:** Compute, storage and such other Services as described in the Documentation and initiated by Customer from time to time.

1.3.5 **Type of Customer Data:** Customer Data uploaded to the Services under Customer's EMBLEEMA accounts.

1.4 **Categories of data subjects.** The data subjects may include Customer's customers, employers, suppliers and end-users.

1.5 **Compliance with LAW**. Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this DPA, including the GDPR.

2. Customer Instructions. The parties agree that this DPA constitute Customer's documented instructions regarding EMBLEEMA's processing of Customer Data ("**Documented Instructions**"). EMBLEEMA will process Customer Data only in accordance with Documented Instructions. Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between EMBLEEMA and Customer, including agreement on any additional fees payable by Customer to EMBLEEMA for

carrying out such instructions. Customer is entitled to terminate this DPA and the Agreement if EMBLEEMA declines to follow instructions requested by Customer that are outside the scope of, or changed from, those given or agreed to be given in this DPA.

3. Confidentiality of Customer Data. EMBLEEMA will not access or use, or disclose to any third party, any Customer Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If a governmental body sends EMBLEEMA a demand for Customer Data, EMBLEEMA will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, EMBLEEMA may provide Customer's basic contact information to the government body. If compelled to disclose Customer Data to a government body, then EMBLEEMA will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless EMBLEEMA is legally prohibited from doing so. If the Standard Contractual Clauses apply, nothing in this Section 3 varies or modifies the Standard Contractual Clauses.

4. Confidentiality Obligations of EMBLEEMA Personnel. EMBLEEMA restricts its personnel from processing Customer Data without authorization by EMBLEEMA as described in the EMBLEEMA Security Standards. EMBLEEMA imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.

5. Security of Data Processing

5.1 EMBLEEMA has implemented and will maintain the technical and organizational measures for the EMBLEEMA Network as described in the EMBLEEMA Security Standards and this Section. In particular, EMBLEEMA has implemented and will maintain the following technical and organizational measures:

(i) security of the EMBLEEMA Network;

(ii) physical security of the facilities;

(iii) measures to control access rights for EMBLEEMA employees and contractors in relation to the EMBLEEMA Network; and

(iv) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by EMBLEEMA.

6. Security Breach Notification.

6.1 **Security Incident.** EMBLEEMA will (a) notify Customer of a Security Incident without undue delay after becoming aware of the Security Incident, and b) take reasonable steps to mitigate the effects and to minimise any damage resulting from the Security Incident.

6.2 **Unsuccessful Security Incidents.** Customer agrees that:

(i) An unsuccessful Security Incident is one that results in no unauthorized access to Customer Data or to any of EMBLEEMA's equipment or facilities

storing Customer Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents; and EMBLEEMA's obligation to report or respond to a Security Incident is not and will not be construed as an acknowledgement by EMBLEEMA of any fault or liability of EMBLEEMA with respect to the Security Incident.

6.3 **Communication.** Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's contacts by any means EMBLEEMA selects, including via email. It is Customer's sole responsibility to ensure Customer maintains accurate contact information on the EMBLEEMA management console and secure transmission at all times.

7. EMBLEEMA Certifications and Audits.

EMBLEEMA ISO-Certification and SOC Reports. In addition to the information contained in this DPA, upon Customer's request, and provided that the parties have an applicable NDA in place, EMBLEEMA will make available the following documents and information: the System and Organization Controls (SOC) 1 Report, the System and Organization Controls (SOC) 2 Report and the System and Organization Controls (SOC) 3 Report (or the reports or other documentation describing the controls implemented by EMBLEEMA that replace or are substantially equivalent to the SOC 1, SOC 2 and SOC 3).

7.1 **EMBLEEMA Audits.** EMBLEEMA uses external auditors like securitymetrics.com to verify the adequacy of its security measures, including the security of the physical data centers from which EMBLEEMA provides the Services. This audit: (a) will be performed at least annually; (b) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001; (c) will be performed by independent third party security professionals at EMBLEEMA's selection and expense; and (d) will result in the generation of an audit report ("**Report**"), which will be EMBLEEMA's Confidential Information.

7.2 **Audit Reports.** At Customer's written request, and provided that the parties have an applicable NDA in place, EMBLEEMA will provide Customer with a copy of the Report so that Customer can reasonably verify EMBLEEMA's compliance with its obligations under this DPA.

8. Transfers of Personal Data.

8.1 **Application of Standard Contractual Clauses.** The Standard Contractual Clauses will apply to Customer Data that is transferred outside the EEA, either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR). The Standard Contractual Clauses will not apply to Customer Data that is not transferred, either directly or via onward transfer, outside the EEA. Notwithstanding the foregoing, the Standard Contractual Clauses (or obligations the same as those under the Standard Contractual Clauses) will not apply if

EMBLEEMA has adopted Binding Corporate Rules for Processors or an alternative recognized compliance standard for the lawful transfer of personal data (as defined in the GDPR) outside the EEA.

9. **Termination of the DPA.** This DPA shall continue in force until the termination of the Agreement (the "**Termination Date**").

10. **Return or Deletion of Customer Data**. The Services provide Customer with controls that Customer may use to retrieve or delete Customer Data as described in the Documentation. Up to the Termination Date, Customer will continue to have the ability to retrieve or delete Customer Data in accordance with this Section. For 90 days following the Termination Date, Customer may retrieve or delete any remaining Customer Data from the Services, subject to the terms and conditions set out in the Agreement, unless prohibited by law or the order of a governmental or regulatory body or it could subject EMBLEEMA or its Affiliates to liability. No later than the end of this 90 day period, Customer will close all EMBLEEMA accounts. EMBLEEMA will delete Customer Data when requested by Customer by using the Service controls provided for this purpose by EMBLEEMA.

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

12. **Definitions.** Unless otherwise defined in the Agreement, all Capitalized terms used in this DPA will have the meanings given to them below:

"**EMBLEEMA Network**" means EMBLEEMA's data center facilities, servers, networking equipment, and host software systems (e.g., virtual firewalls) that are within EMBLEEMA's control and are used to provide the Services.

"**EMBLEEMA Security Standards**" means the security standards attached to the Agreement, or if none are attached to the Agreement, attached to this DPA as Annex 1.

"**Customer**" means you or the entity you represent.

"**Customer Data**" means the "personal data" (as defined in the GDPR) that is uploaded to the Services under Customer's EMBLEEMA accounts.

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

"**GDPR**" means Regulation 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

"**processing**" has the meaning given to it in the GDPR and "process", "processes" and "processed" will be interpreted accordingly.

"**Security Incident**" means a breach of EMBLEEMA's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data.

"Standard Contractual Clauses" means Annex 2, attached to and forming part of this

DPA pursuant to the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC.