DATA PROCESSING AGREEMENT (DPA)

This Data Processing Agreement with appendices (the "**Agreement**") has been entered between:

The **Controller**
You ("**Controller**"); and

The **Processor**
ftrack AB, Reg. No. 5568813769 ("**Processor**"),

The parties are jointly referred to as the "**Parties**", each being a "**Party**".

1. BACKGROUND

The Agreement refers to the Personal Data Processed under the ftrack ABs Terms of Service entered into by the Parties regarding the Processor's products for project management, production tracking and media reviews (The "**Terms**"), as a result of which the Processor processes personal data on behalf of the Controller.

In the event of any conflict with the Terms, this Agreement shall prevail.

The agreement contains the following appendices:

- Appendix 1 - List of sub-processors
- Appendix 2 - Technical and organisational security measures
- Appendix 3 - Contact details

2. DEFINITIONS

The terms used in this Agreement shall have the same meaning as ascribed to them in Article 4 of the GDPR.

"**Applicable Law**" refers to the legislation applicable to the processing of Personal data under the Agreement, including the GDPR, supplementary national legislation, as well as practices, guidelines and recommendations issued by a Supervisory Authority.

"**Controller**" means the company / organisation that decides for what purposes and in what way Personal data is to be processed and is responsible for the processing of Personal data in accordance with applicable data protection legislation.

"**GDPR**" refers to 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 movement of such data, and repealing Directive 95/46/EC.

"**Data Subject**" means the natural person whose Personal data is processed.

"**Personal Data**" means any kind of information that can be derived from an identifiable natural person (in the Agreement, "Personal data" is used synonymously with "personal data for which the Controller is responsible and that is processed by the Processor on behalf of the Controller").

"**Processing**" means any operation or set of operations which is performed on Personal data, *e.g.* storage, modification, reading, handover and similar.

"**Processor**" means the company / organisation that processes Personal data on behalf of the controller and can therefore only process the Personal data according to the instructions of the controller and Applicable law.

"**Supervisory Authority**" means Swedish or EU authority, such as the Swedish Data Protection Authority, or another supervisory authority which on the basis of law has the authority to conduct supervisory activities over the Controllers operation.

Unless otherwise defined herein, all capitalised terms (definitions) used in this Agreement shall have the same meaning as ascribed to them in the Terms.

3. INTRODUCTION

This Agreement concerns the processing of Personal Data that the Processor performs on behalf of the Controller. It has been drawn up to meet the requirements set out in Article 28 (3) of 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 ("**GDPR**"). According to this provision, the Processing of Personal Data by the Processor on behalf of the Controller shall be governed by a contract.

4. DESCRIPTION OF PROCESSING

4.1 Categories of Data Subjects

The Controller directs the Processor to process data that identifies the Controllers':

- Users

4.2 Categories of Personal Data

- Name
- E-mail
- IP Address

4.3 Source

The processor is processing Personal Data that:

- The Controller’s employees enter into the Service
- The Controller collects from the data subject
- The Processor collects from the data subject on behalf of the Controller

4.4 The purpose of the processing of Personal Data (the "Purpose")

- Register user accounts for the Service

4.5 Processing of Personal data

- Organization and Structuring
- Storage
- Alteration
- Erasure and destruction

5. SPECIFIC UNDERTAKING OF THE PROCESSOR

5.1 The Processor undertakes to consider and observe the principles for processing Personal Data set out in Article 5 of the GDPR in connection with each and every Processing.

5.2 By entering into this Agreement, the Processor guarantees that the Controller does not need to take any additional measure to ensure that the Processor meets the requirements for expertise, reliability and resources to carry out the technical and organisational measures required by Applicable law.

5.3 The Processor undertakes to only process Personal Data in accordance with the Agreement, the purposes set out in the Terms, the Controller’s documented instructions and Applicable Law.

5.4 Upon the Controller’s request, the Processor shall a) (by using the appropriate technical and organisational measures) assist the Controller in its duty to respond to the request for the exercise of the rights of Data Subjects and b) with regards to the type of processing and available information, carry out Data Protection Impact Assessments (DPIA) and participate in consultations with Supervisory Authorities in accordance with Applicable Law.

5.5 If the Processor violates Applicable Law by independently determining the purposes and means of the Processing (*e.g.* processing the Personal Data for purposes other than the Purpose), the Processor shall be regarded as the controller for the new Processing. To clarify, any new Processing shall not affect the Processing made in accordance with this Agreement.

5.6 If there is a conflict between the Controller's instructions and Applicable law, the Processor has the right to refrain from complying with such instructions. The Processor shall inform the Controller immediately if it considers that the instructions provided by the Controller are incomplete, inadequate or incorrect.

6. SPECIFIC UNDERTAKINGS OF THE CONTROLLER

6.1 The Controller determines the purpose and means for the Processing of the Personal data. The Controller has full ownership and the formal control of the Personal Data Processed by the Processor.

6.2 The Controller is responsible to the Data Subject for the Processing of the Personal data.

6.3 The Controller is responsible for ensuring that the Personal Data is accurate and up to date.

7. PERSONAL DATA BREACH

7.1 In the event of a situation leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed ("**Personal Data Breach**"), the Processor shall, without undue delay, and no later than eight (8) hours after having become aware of the Personal Data Breach, notify the Controller by sending a written notice to the address provided in appendix 3. The information shall, to the extent that it is available to the Processor, contain the following at least:

- A description of the circumstances surrounding the Personal Data Breach
- A description of the nature of the Personal Data Breach, and, if possible, the categories and approximate number of Data Subjects affected and the categories and approximate number of Personal Data concerned
- A description of the likely consequences of the Personal Data Breach
- A description of the measures taken or proposed to address the Personal Data Breach, and, where appropriate, measures to mitigate its potential adverse effects
- Contact information to the Data Protection Officer or other contact person who can provide more information to the Controller

7.2 If it is not possible for the Processor to provide all the information at once, the information may be provided in installments without undue delay.

8. AUDIT RIGHTS

8.1 Upon the Controller's request, the Processor shall give access to all information necessary to show that the Processor's obligations under Applicable Law and this Agreement have been fulfilled.

8.2 If the information provided in accordance with the previous paragraph cannot reasonably demonstrate that the Processor's obligations under Applicable law have been fulfilled, the Controller is entitled to carry out physical audits.

8.3 The Processor shall enable and contribute to audits and inspections carried out by the Controller or by an impartial third party appointed by the Controller. The Controller shall notify the Processor in writing of the planned audit at least ten (10) business days in advance.

8.4 The audit shall be carried out:

- During normal business hours
- After the Controller has ensured that the person conducting the review is subject to a confidentiality agreement appropriate in relation to the Personal Data and information to be reviewed
- In accordance with the Processor's internal policies and security procedures

8.5 Each party is responsible for its own costs incurred in connection with an audit performed.

8.6 In the event of any additional audits within one (1) year of a performed audit, the Controller shall be responsible for all costs incurred as a result of such audit(s).

9. SUB-PROCESSOR

9.1 The Processor may not appoint a sub-processor without first informing the Controller. Accordingly, the Processor shall inform the Controller if it intends to appoint a sub-processor (or replace an existing sub-processor) at least five (5) business days in advance.

9.2 If there is a reasonable reason for the Controller to object to the appointment of a sub-processor the parties shall endeavour to find a suitable alternative. Should the parties fail to find a suitable alternative, the Controller has the right to terminate this Agreement and (if applicable) the Terms.

9.3 When engaging a sub-processor, the Processor shall ensure that the sub-processor comply with the Processor's obligations in the Agreement by entering into a contract or other legal act (the "**Sub-processor agreement**"). The foregoing shall be particularly observed in respect of the Processor's obligation to provide sufficient guarantees regarding implementing appropriate technical and organisational measures as required to comply with Applicable Law.

9.4 The Controller is always entitled to a copy of the Sub-processor agreement (strictly commercial information may be edited).

9.5 The Processor must keep an updated record of the sub-processors. The record shall be made available to the Controller upon request.

9.6 Processor shall be exclusively responsible towards the Controller if the sub-processor fails to, or omits from, fulfilling its obligations under the Sub-processor agreement.

10. RECORD OF PROCESSING AND DATA PROTECTION OFFICER

10.1 The Processor undertakes to keep a written record of the processing of Personal Data according to Article 30 (2) of the GDPR. The record shall be available to the Controller upon request.

10.2 If the Processing or the nature of the Controller's business requires the Controller to appoint a Data Protection Officer in accordance with Article 37 of the GDPR, the Data Protection Officer's contact details shall be included in the appendix 3.

11. CONTACT WITH SUPERVISORY AUTHORITY AND THE DATA SUBJECT

11.1 The Processor shall promptly inform the Controller of all contact it may have with the Data Subject, a Supervisory authority or any other third party concerning the Personal Data that the Processor is Processing.

11.2 In the event a Data Subject makes a request to the Processor regarding his / her rights in respect of the Processing, the Processor shall refer the Data Subject to the Controller.

11.3 The Processor shall allow any inspections that the Supervisory Authority may require to perform in accordance with Applicable law.

11.4 The Processor is not entitled to represent the Controller or otherwise act on behalf of the Controller in respect of the Data Subject, a Supervisory Authority or any other third party.

12. TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

12.1 The Processor shall take the appropriate organisational and technical security measures to protect and ensure that the Personal Data included in the scope of this Agreement is protected against any unauthorised or illegal access. This includes ensuring the adequate capacity, technical solutions, skills, financial and human resources, procedures and methods.

12.2 The appropriateness of the technical and organisational security measures shall be assessed taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of the Processing as well as the risks (of varying likelihood and severity) for rights and freedoms of natural persons posed by the Processing.

12.3 If the Controller assesses that the Processing operation is of high risk to the rights and freedoms of the Data subject and conducts a DPIA, the Controller shall share the results of the DPIA with the Processor to ensure that this can be taken into account in when determining what constitutes appropriate security measures.

12.4 The Processor must comply with any decisions and consultation opinions that the Supervisory Authority announces regarding measures for complying with the security requirements and all other requirements relating to the Processor under Applicable Law.

12.5 The Processor shall ensure that employees (of the Processor or their sub-contractors) are only allowed access to Personal Data to that extent necessary and that those who have access to Personal data have undertaken to respect the confidentiality of such information (*e.g.* by signing an individual non-disclosure agreement).

12.6 Only persons employed/engaged as consultants by the Processor and who have been deemed to have the adequate level of knowledge of the nature and extent of the Processing of Personal Data may process the Personal Data.

12.7 Computer equipment, storage media and other equipment used in the Processing of Personal data carried out by the Processor must be kept where/or in such manner that no unauthorised persons can access them.

12.8 The security at the Processor's facilities where Personal Data is Processed must be appropriate and secure in regards of locking equipment, functioning alarm equipment, protection against fire, water and burglary, protection against power outages and power disturbances. The equipment used to process Personal Data must have good protection against theft and events that may destroy the equipment and / or Personal Data.

13. CONTROL OVER THE PERSONAL DATA

13.1 The Processor shall ensure that Personal Data Processed is not accidentally or unlawfully destroyed, altered or corrupted. All Personal Data shall be protected against any unauthorised access during storage, transfer and other Processing.

13.2 No Personal Data may be provided to the Controller before the identity of the recipient has been duly verified.

14. TRANSFER OF DATA OUTSIDE THE EU/EEA

14.1 In the event that the Processor transfers Personal data outside the EU/EEA, the Processor ensures that the level of protection is adequate and in accordance with Applicable Law by controlling that at least one of the following requirements are fulfilled:

- The EU Commission has determined that the level of protection is adequate in the third country where the data is Processed
- The Processor has signed up to the EU Commission's standard contract clauses (SCCs) for data transfer to non-EU/EEA countries.
- The Processor has taken other appropriate safeguards prior to the transfer and that such safeguards comply with Applicable Law.

15. LIABILITY

15.1 No Party is liable for any delay or failure to perform due to extraordinary circumstances beyond the control of the Party, which the Party could not reasonably expect and which consequences the Party could not reasonably have avoided or overcome.

15.2 The Processor is liable for direct damages that arise as a result of the Processor having Processed Personal Data in violation of the Controller's instructions in accordance with the Agreement and Applicable law.

15.3 The Processor liability for direct damages be limited to SEK 50 000 SEK. The Controller is not entitled to any compensation for damages related to any Processing that has been approved by, or performed in accordance with the instructions of, the Controller.

15.4 The Processor is not obligated to pay the costs of the Controller's agent.

15.5 In no event shall the Processor be liable for any indirect or consequential damages such as lost revenue or profits, contracts, customers or business opportunities, loss of goodwill, or expected savings.

16. CONFIDENTIALITY

16.1 The Processor may not use information or other material to which it is granted access in connection with entering into this Agreement or the Terms for any other purpose than fulfilling its obligations under this Agreement or the Terms.

16.2 The Processor may not disclose information to third parties or any other unauthorised persons about the Processing of Personal data or the content of Personal Data covered by this Agreement or other information to which the Processor has been granted access as a result of, or in connection with entering into, this Agreement. This undertaking does not apply to information that the Processor is required to disclose under mandatory law.

16.3 This confidentiality undertaking is valid from the date this Agreement has been duly signed by both parties and for an indefinite period in time thereafter. The Processor shall ensure that this confidentiality undertaking applies to all employees and other persons working with or on behalf of the Processor and who are authorised to process Personal Data.

17. TERM AND TERMINATION

17.1 The Agreement is valid and in force from the date that the Processor first processes Personal Data on behalf of the Controller to the date when it ceases such Processing or until this Agreement is replaced by another Data Processing Agreement.

17.2 The obligations of the Processor under the Agreement shall continue to apply, regardless of whether the Agreement has been replaced, as long as the Processor processes Personal Data on behalf of the Controller.

18. ERASURE AND RETURNING OF PERSONAL DATA

18.1 Upon the termination of the Agreement, the Processor and any sub-processor shall, at the request of the Controller, either erase or return the Personal Data processed within the scope of this Agreement.

19. GOVERNING LAW AND DISPUTES

19.1 Swedish law shall apply to these Terms.

19.2 The provision regarding disputes set out in the Terms will also apply to the Agreement.

APPENDIX 1 - EXISTING AND APPROVED SUB-PROCESSORS

Name: Amazon AWS
Service: Data storage
Website: https://aws.amazon.com/compliance/gdpr-center/
Data processed: E-mail and name
Security measures: The sub-processor has signed up to the EU Commission's standard contract clauses (SCCs) for data transfer to non-EU/EEA countries

Name: Google GCP
Service: Data processing
Website: https://cloud.google.com/security/gdpr
Data processed: E-mail, name and IP Address
Security measures: The sub-processor has taken other appropriate safeguards prior to the transfer and that such safeguards comply with applicable data protection legislation

Name: Intercom, Inc.
Service: Analysing usage of Service
Website: https://www.intercom.com/legal/privacy
Data processed: E-mail, name and IP address
Security measures: The sub-processor has taken other appropriate safeguards prior to the transfer and that such safeguards comply with applicable data protection legislation

Name: Mailchimp
Service: Email processing
Website: https://mailchimp.com/legal/data-processing-addendum/
Data processed: Email and name
Security measures: The sub-processor has taken other appropriate safeguards prior to the transfer and that such safeguards comply with applicable data protection legislation

Name: Mailgun
Service: E-mail processing
Website: https://www.mailgun.com/gdpr/
Data processed: E-mail and name
Security measures: The sub-processor has signed up to the EU Commission's standard contract clauses (SCCs) for data transfer to non-EU/EEA countries

Name: Recurly
Service: Payment Processing
Website: https://recurly.com/legal/privacy
Data processed: Name, E-mail
Security measures: The sub-processor has taken other appropriate safeguards prior to the transfer and that such safeguards comply with applicable data protection legislation

Name: Zendesk
Service: Support platform
Website: https://www.zendesk.com/company/privacy-and-data-protection/#gdpr-sub
Data processed: E-mail and name
Security measures: The sub-processor has taken other appropriate safeguards prior to the transfer and that such safeguards comply with applicable data protection legislation

Name: Orca Security
Service: Cloud Security and Compliance
Website: https://orca.security/privacy-policy/
Data processed: Orca does not process customer data as part of its service.
Security measures: The sub-processor has taken other appropriate safeguards prior to the transfer and that such safeguards comply with applicable data protection legislation

Name: Hubspot, Inc.
Service: Marketing
Website: https://legal.hubspot.com/privacy-policy
Data processed: E-mail and name
Security measures: The sub-processor has taken other appropriate safeguards prior to the transfer and that such safeguards comply with applicable data protection legislation

Name: SFDC Ireland, Ltd.
Service: Sales and Marketing
Website: https://www.salesforce.com/eu/company/privacy/
Data processed: E-mail, name and address
Security measures: The sub-processor has taken other appropriate safeguards prior to the transfer and that such safeguards comply with applicable data protection legislation

APPENDIX 2 - TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

The Processor has taken technical and organisational measures to ensure that Personal Data is processed securely and protected from loss, misuse and unauthorised access.

Technical security measures are measures implemented through technical solutions.

- Encryption
- Access control level
- Access log
- Secure network
- Back-up
- Regular security inspection
- Two-step verification

Organisational security measures are measures that are implemented in work processes and routines within the organisation.

- Internal governance document (policies/instructions)
- Login and password management
- Information security policy

APPENDIX 3 - CONTACT DETAILS

Contact Information
E-mail address: privacy@ftrack.com