FastTrack Software

San Francisco, Chicago
Wisconsin, New York

United Kingdom, Germany
Denmark, Sweden, Norway

Phone (US)
262-299-4606

Phone (UK)
(0) 20 3808 8747

Email
sales@fasttracksoftware.com

Data Processing Agreement

Processing in accordance with Article 28 General Data Protection Regulation (GDPR)

Agreement

between

The Data Controller

[Your Company name goes here]

and

The Data Processor

FastTrack Software Aps
Niels Jernes Vej 10
9220 Aalborg
Denmark

Version 4.2
Effective date: February 25th, 2021

PREFACE

This Data Processing Agreement applies to all customers. The Data Processing Agreement is static and thus not subject to negotiation.

1. BACKGROUND, PURPOSE AND SCOPE

1.1 This Data Processing Agreement ("Agreement") is a supplement to the Terms & Conditions and is effective as of the date of acceptance. Archived PDF copies of both agreements, signed by FastTrack Software's CEO, issued to

you, are legally binding at any time in the future. Such PDF copies can be downloaded at https://www.adminbyrequest.com/trustcenter. FastTrack Software reserves the right at any time to adjust or make changes within both agreements. Any changes must be accepted by the Customer. If the Customer cannot agree to the changes, the Customer has 180 days to discontinue the use of the SaaS Product, in which term existing Agreements are valid.

1.2 This Agreement has been formed in accordance with the European General Data Protection Regulation (Regulation 2016/679 EU). This means that whether The Data Controller's data is being stored within the EU or outside the EU borders, all data which is being processed or stored by The Data Processor is being processed and protected in accordance with the European General Data Protection Regulation.

1.3 This Agreement is in effect as long as the Data Controller has an active subscription of the principal service with the Data Processor.

2. PERSONAL DATA THAT FALLS WITHIN THE SCOPE OF THE AGREEMENT

2.1 This Agreement and the instructions associated therewith comprise all types of personal data described in Appendix 1 of the Agreement.

2.2 Personal data to which is being processed in accordance with this Agreement is being processed by the Data Processor or sub-processors in accordance with the EU General Data Protection Regulation at all time as described in sections 3 and 4.

3. PERSONAL DATA STORED IN EUROPEAN DATACENTERS

3.1 Any personal data processed in the context of the activities of an establishment of the Data Controller in the Union – regardless of whether the processing takes places in the Union or not – will be stored on a datacenter within the Union. Access to the datacenter is only to be given to the Data Controller – if the Data Controller is registered within the Union – and the Data Processor.

3.2 The Data Processor will implement appropriate and necessary technical and organizational security measures throughout all Datacenters within the EU against the accidental destruction, loss or impairment of personal data and shall ensure that the data will not be disclosed to any unauthorized person and are not misused or otherwise processed in contravention of the law.

3.3 The Data Controller's data will be processed and stored in accordance with the EU General Data Protection Regulation and in accordance with the provisions of this Agreement.

4. PERSONAL DATA STORED IN NON-EUROPEAN DATACENTERS

4.1 Any personal data processed in the context of the activities of an establishment of the Data Controller outside the Union (e.g. Australia, USA, Asia etc.) will be stored on a datacenter located in the continent in which the processing takes place. Local data is hereby and always stored and processed locally or nationally. Access to the datacenters is only to be given to the Data Controller – if the Data Controller is registered within the continent or location of the processing – and the Data Processor.

4.2 The Data Processor will implement appropriate and necessary technical and organizational security measures throughout all Datacenters worldwide against the accidental destruction, loss or impairment of personal data and shall ensure that the data is not disclosed to any unauthorized person and is not misused or otherwise processed in contravention of the law.

4.3 The Data Controller's data will be processed and stored in accordance with the EU General Data Protection Regulation and in accordance with the provisions of this Agreement regardless of whether the processing is located within the Union or not.

5. DUTIES OF THE DATA PROCESSOR

5.1 The Data Processor shall comply with the General Data Protection Regulation (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) and the legal instruments associated therewith as well as the national legislation derived from these.

5.2 The Data Processor undertakes to implement and comply with all technical and organizational measures as described in Appendix 3 to the Agreement.

5.3 The Data Controller shall be informed immediately of any inspections and measures conducted by the Supervisory Authority, insofar as they relate to this Agreement. This will also apply if the Data Processor is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, Administrative Rule or Regulation regarding the processing of personal data in connection with the processing of this Agreement.

5.4 Insofar as the Data Controller is subject to an inspection by the Supervisory Authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the Order or Contract data processing by the Data Processor, the Data Processor shall make every effort to support the Data Controller.

5.5 The Data Processor has the duty to assist the Data Controller with regard to the Data Controller's obligation to provide information to the Data Subject concerned and to immediately provide the Data Controller with all relevant information in this regard.

5.6 The Data Processor has the duty to assist the Data Controller with regards to the Data Controller's obligation to comply with the legal rights of the Data Subjects without undue delay.

5.7 The Data Processor is obliged to notify the Data Controller without undue delay if a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person. (Article 34 Paragraph 1)

5.8 The Data Processor will be responsible – on the basis of a sub-processor agreement – for requiring that the sub-processor at least comply with the obligations to which the Data Processor is subject pursuant to the requirements of the General Data Protection Regulation and this Data Processing Agreement and its associated appendices.

5.9 The Data Processor must support the Data Controller with regards to prior consultation of the Supervisory Authority.

5.10 The Data Processor shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that processing within his area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.

5.11 In the case of a personal data breach, the Data Processor's notification to the Data Controller shall take place within 24 hours after the Data Processor has discovered the breach to enable the Data Controller to comply with his obligation, if applicable, to report the breach to the supervisory authority within 72 hours.

5.12 The Data Processor shall assist the Data Controller in ensuring compliance with Article 35 relating to data protection impact assessments.

6. INSTRUCTIONS

6.1 The scope of the tasks that shall be provided and supported by the Data Processor means that there shall be different forms of processing of personal data. The different forms of processing of personal data are described in Appendix 1 of the Agreement.

6.2 Where an instruction, in the Data Processor's opinion, clashes with the General Data Protection Regulation, the Data Processor shall notify the Data Controller thereof.

6.3 The Data Processor shall engage in the following processing on the Data Controller's behalf: All processing shall be based on this Agreement. Data Processors may undertake all actions that are necessary for complying with the Agreement. The Data Processor may not disclose information to third parties without the Data Controller's consent. The data may not be used for profiling or integration with other data.

6.4 The categories of data subjects that the personal data refer to are primarily the Data Controller's users and employees.

6.5 Data that is subject to EU Data Protection Laws must not be transferred outside the European Union. This includes Microsoft Support that is not allowed to access data in the European Union from outside the European Union.

7. USE OF SUB-PROCESSORS

7.1 If necessary, the Data Processor may use sub-processors through subcontracting.

7.2 Subcontracting for the purpose of this Agreement is to be understood as services which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment.

7.3 The Data Processor currently uses the sub-processors identified in Appendix 2 of the Agreement for the technical provision of services.

7.4 On entering into this Agreement, the Data Controller accepts that the Data Processor is entitled to change its sub-processor provided that a) a new sub-processor, if any, meets the corresponding terms and conditions as laid out in section 7 on the current sub-processor and that b) the Data Controller is notified by the Data Processor of the identity of the new sub-processor or replacement of Sub-Data Processors no later than 90 days before the beginning of processing of personal data by such a second sub-processor, if any, for whom the Data Controller shall act as data controller.

7.5 The Data Controller may, within 30 days after being notified of the engagement of a new subprocessor, object by terminating the Agreement immediately upon written notice to the Data Processor. This termination right is the Data Controller's sole and exclusive remedy, if the Data Controller objects to a new subprocessor.

7.6 The transfer of personal data from the Data Processor to the subprocessor and the subcontractor's commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved.

7.7 Sub-processors shall work under the Data Processor's instructions. The Data Processor shall enter into a written data processing agreement with the sub-processor, which ensures that the sub-processor meets the same requirements placed on the Data Processor by the Data Controller in accordance with the Agreement.

8. PROCESSING AND DISCLOSURE OF PERSONAL DATA

8.1 The Data Controller guarantees to have the requisite legal authority to process personal data that falls within the scope of this Agreement.

8.2 The Data Processor may not disclose data to third parties without the Data Controller's written consent unless such disclosure follows from the legislation or from a binding request from a court instance or a data protection authority or is stipulated herein.

9. SECURITY

9.1 The Data Processor shall take appropriate technical and organizational security measures against the accidental destruction, loss or impairment of personal data and shall ensure that the data is not disclosed to any unauthorized person and is not misused or otherwise processed in contravention of the law.

9.2 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Data Processor shall in relation to the Client Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

9.3 In assessing the appropriate level of security, Data Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

10. RIGHT OF SUPERVISION

10.1 The Data Processor shall, at the Data Controller's request, provide the Data Controller with sufficient documentation to ensure that the Data Processor has taken the necessary technical and organizational security measures.

10.2 To the extent the Data Controller also wants such information to extend to the processing provided by sub-processors, notice of this shall be given to the Data Processor. The Data Processor shall subsequently procure sufficient information from the sub-processor.

10.3 The Data Controller has the right, after consultation with the Data Processor, at the cost of the Data Controller, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. The aim of such an inspection, will be to ensure that the Data Processor is in compliance of this Agreement in business operations by means of random checks, which are ordinarily to be announced in good time.

10.4 The Data Processor shall ensure that the Data Controller is able to verify compliance with the obligations of the Data Processor in accordance with Article 28 of the GDPR. The Data Processor undertakes the responsibility of giving the Data Controller the necessary information on request and, in particular, to demonstrate the execution of the Technical and Organizational Measures.

11. BREACH OF PERSONAL DATA SECURITY

11.1 When the Data Processor becomes aware of a breach of personal data security, which shall be understood as a breach of security that leads to accidental or illegal destruction, loss, change, unauthorized disclosure of or access to personal data that is transmitted, stored or otherwise processed, the Data Processor is obliged to localize such a breach as well as limit the damage that has occurred to the greatest extent possible as well as to the extent it is possible to restore lost data, if any.

11.2 The Data Processor is further obliged to notify the Data Controller after it has become aware of a breach of personal data security, in the time period stated in Section 5.11. The Data Processor shall subsequently, without undue delay, to the extent possible, give the Data Controller written notice which shall contain, to the greatest extent possible:

- a) A description of the nature of the breach, including category, approximate number of data subjects concerned and personal data records.
- b) Name and contact details of the data protection officer.
- c) A description of the probable consequences of the breach.
- d) A description of the measures that have been taken or are guaranteed to be taken by the Data Processor or sub-processor in order to manage the breach, including measures for limiting its possible deleterious effects.

11.3 As long as it is not possible to submit the information specified in subsection 11.2 at once, the details can be provided step-by-step, without additional unnecessary delay.

11.4 Sub-processors are correspondingly under a duty to notify the Data Processor in accordance with subsections 11.2 and 11.3 without delay.

12. CONFIDENTIALITY OBLIGATION

12.1 The Data Processor shall keep personal data confidential and is therefore only entitled to use the personal data as part of the discharge of its rights and obligations under this Agreement.

12.2 The Data Processor shall ensure that its employees and anyone else, including sub-processors, who is authorized to process the personal data that falls within the scope of the Agreement, will be subject to a confidentiality obligation.

13. DELETION OF DATA

13.1 Copies or duplicates of the data shall never be created without the knowledge of the Data Controller, with the exception of backup copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.

13.2 After termination of the principal service, or earlier upon request by the Data Controller, at the latest upon termination of the Terms and Conditions, the Data Processor shall destroy all documents, processing and utilization results, and data sets related to the contract that has come into its possession in a data-protection compliant manner. The same applies to any and all connected test, waste, redundant and discarded material.

14. LIABILITY

14.1 Liability for violations of rules on data protection or this Agreement shall be handled in accordance with the applicable provisions of data protection law if the contractual agreements which are applied to the underlying services do not include any special provisions regarding to liability.

15. DATA PROTECTION MANAGEMENT

15.1 Appointed Data Protection Officer

Mr. Lars Sneftrup Pedersen
C/O FastTrack Software Aps

Novi Science Park
Niels Jernes Vej 10
9220 Aalborg
Denmark

15.2 Data Protection Officer contact: Please use the contact form at www.adminbyrequest.com for initial contact.

APPENDIX 1: TYPES OF PERSONAL DATA THAT FALL WITHIN THE SCOPE OF THE AGREEMENT

1.1 This Agreement and the instructions associated therewith cover all types of personal data processed by the Data Processor. Such data includes the following:

1.2 Data without personal information:

1.2.1 Administrator session data: Computer name, duration, installed and uninstalled software, UAC elevated programs and reason for administrator need

1.2.2 Inventory data (can be disabled): Basic hardware data, operating system, user and computer domain and OU, installed software, local administrator accounts, computer and user groups and current IP address

1.3 Data with personal information that cannot be disabled:

1.3.1 Portal user (administrator) name, email address and phone number (phone number mandatory only with two factor authentication)

1.4 Data with personal information that can be disabled:

1.4.1 Administrator session data: User's account name, full name, email address and phone number

1.4.2 Inventory data: Current user's email address, phone number, current account name

APPENDIX 2: SUB PROCESSORS

1.1 Sub-processors used to provision the service:

1.1.1 Microsoft Azure is used to provision the infrastructure required to run the principal service. Microsoft Azure has several datacenters around the world, such as Central US, Canada, Europe and Asia. The Data Processor only uses datacenters located within the continent of where the processing takes place. In addition to the data processing agreement mentioned in section 7.7 the Data Processor have executed an Additional Safeguards Addendum to Standard Contractual Clauses with Microsoft Azure. Microsoft Support is not allowed to access data in the European Union from outside the European Union.

1.1.2 OPSWAT MetaDefender is used for malware scanning program files. If this feature is disabled by the Data Controller, this sub-processor is not used. The Data Processor's usages of OPSWAT MetaDefender does not require processing of personal data.

APPENDIX 3: TECHNICAL AND ORGANIZATIONAL MEASURES

1. Confidentiality (Article 32 Paragraph 1 Point b GDPR)

1.1 Physical Access Control (No unauthorized access to Data Processing Facilities): Entry into facilities is granted only by documented and supervised handling of keys and rfid access cards. On access to the building, an rfid key

card must be used. Furthermore, all office rooms require a key for physical access. The combination of locks on doors and rfid key cards prevent unauthorized access by external or third party individuals. Buildings are alarmed out of business hours and facilities are video monitored. All guests must register at the reception before being granted access to the facilities.

1.2 Electronic Access Control (No unauthorized use of the Data Processing and Data Storage Systems): No part of the production environment is hosted on FastTrack Software facilities. The production environment is located in Microsoft Azure datacenters in Amsterdam and Dublin for European datacenter customers and Virginia and Washington in the United States for non-European datacenter customers. FastTrack Software Facilities contain employee computers and servers for testing purposes only. No production data exists in these facilities. Copying any data, even test data, from these facilities or the production environment is strictly forbidden.

1.3 Internal Access Control (permissions for user rights of access to and amendment of data; No unauthorized Reading, Copying, Changes or Deletions of Data within the system): All personnel access to equipment on the facilities is enforced by Active Directory accounts. Passwords are forcibly changed for all employees every 30 days. Accounts are controlled solely by the Data Protection Officer and working using credentials of other persons is strictly forbidden. Accounts are granted strictly on a "need to know" basis. No employee has access to more data than the job description warrants.

1.4 Isolation Control (The isolated Processing of Data, which is collected for differing purposes): No data collected in the Microsoft Azure production environment exists outside the production environment, except for offsite backup.

1.5 Pseudonymization (Article 32 Paragraph 1 Point a GDPR; Article 25 Paragraph 1 GDPR): Pseudonymization is an opt-in option for customers to pseudonymize ("Obfuscate") user accounts in such a way that no one can directly link an obfuscated name to an actual person. Neither the Data Processor or the Data Controller can identify the individual from an obfuscated name, if the Data Controller opts in on obfuscation.

2. Integrity (Article 32 Paragraph 1 Point b GDPR)

2.1 Data Transfer Control (No unauthorized Reading, Copying, Changes or Deletions of Data with electronic transfer or transport): Personal data in the principal service is protected against unauthorized copying to data media. No data can be accessed outside of the principal service, except for personnel with credentials assigned to the employee by the Data Protection Officer. Any access to data outside the Microsoft Azure environment is restricted by combination of IP address blocking and employee credentials. IP address access is controlled solely by the Data Protection Officer and IP address only map to internet connections registered to FastTrack Software. Any access to production data is solely for the purpose of customer support.

2.2 Data Entry Control (Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted): The principal service stores, changes or deletes any data records only as long as the system allows it. It is possible to track which user made changes to the data.

3. Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)

3.1 Availability Control (Prevention of accidental or willful destruction or loss): All data is hosted entirely on Microsoft Azure. All Microsoft Azure servers have mirrored hard drives in RAID systems and are equipped with redundant components. The database is Microsoft SQL Server and the transaction model of Azure SQL Server allows a restore at any second in time for 7 days, in case of accidental or wilful destruction or loss of data. All critical components are monitored by software monitoring special web pages designed to probe every component of the principal service. If critical parts of the principal service are not available, supervising administrators are notified immediately by email.

3.2 Rapid Recovery (Article 32 Paragraph 1 Point c GDPR): The database is Microsoft SQL Server and the transaction model of Azure SQL Server allows a restore at any second in time for 7 days. After 7 days, a daily backup can be restored, either by Microsoft or an off-site backup, which only the Data Protection Officer has access to. In case of accidental or willful loss of data, FastTrack Software can restore a database from an earlier point and has the expertise in-house to successfully merge lost data back into the production environment.

4. Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 of the GDPR; Article 25 Paragraph 1 of the GDPR)

4.1 Data Protection Management (Incident Response Management; Data Protection by Design and Default (Article 25 Paragraph 2 GDPR); Order or Contract Control): FastTrack Software has appointed the Data Protection Officer stated in section 15 of the Agreement. Any employee of FastTrack Software with access to production data for support purposes will sign a non-disclosure agreement with FastTrack Software. FastTrack Software uses Microsoft Azure, which means a standard agreement is place between FastTrack Software and Microsoft. The performance of and access to the production environment is evaluated on a scheduled monthly basis by an authorized administrator employed by FastTrack Software. The monitoring service used for Availability Control is equally tested and verified on a monthly basis by an authorized administrator.

_____

Lars Sneftrup Pedersen
CEO, FastTrack Software