

Turbine Room Ltd

Kalliosuontie 19

36200 Kangasala

Finland

VAT ID: FI26208758

www.firstofficer.io

FirstOfficer Data Processing Agreement

This Data Processing Agreement (“DPA”) amends and forms part of a contract of service with Turbine Room Ltd (“FirstOfficer”, “Processor”) together with Terms of Service that can be found on FirstOfficer’s website (<https://www.firstofficer.io/terms>). This agreement shall reflect the Parties’ agreement with regard to the Processing of Personal Data.

In the course of providing the Services to the Controller, FirstOfficer may process Personal Data on behalf of Controller and Parties agree to comply with the following provision with respect to any Personal Data, each acting reasonably and in good faith.

How to execute this DPA

This DPA has been pre-signed on behalf of FirstOfficer. Please fill in your company information and sign the agreement in our [self-service DPA page](#).

This DPA will become legally binding upon FirstOfficer’s receipt of the validly completed and signed DPA.

How this DPA applies

If the Controller signing this DPA is a customer of FirstOfficer, this DPA is an addendum to the Terms of Service and is legally binding.

If the Controller signing this DPA is not a customer of FirstOfficer at the date of the signature, this DPA is not valid and legally binding.

If you have any questions about this DPA, please email to: dpo@firstofficer.io

Executive Summary

This agreement is made so that you can be sure that FirstOfficer processes your

customers' Personal Data in GDPR compliant way. It also explains what data is processed, how and where.

Please see clause 2.4.4 to find out what Personal Data FirstOfficer collects about your customers.

Please see clause 9.1. to find out the Sub-Processors that FirstOfficer uses to physically store your customers' Personal Data.

Please go to www.firstofficer.io/legal/gdpr/data-partners to see a full listing of Sub-Processors and ancillary services that FirstOfficer uses.

Parties

SAMPLE COMPANY LTD , incorporated and registered in DE with company registration number 111111-11111-111111111 and having its registered office at 1111 SAMPLE STREET, (“Controller”, “Customer”)

Turbine Room Ltd, incorporated and registered in Finland with company registration number 2620875-8 and having its registered office at Kalliosuontie 19, 36200 Kangasala, Finland, (“Processor”, “FirstOfficer”)

This Agreement is entered into force between Turbine Room Ltd and SAMPLE COMPANY LTD and shall be effective on the date both parties execute this DPA (“Effective Date”).

Recitals

WHEREAS the Parties have agreed that:

The Controller will act as the sole data controller of the Personal Data;

It may be necessary for the Processor to Process certain Personal Data on behalf of the Controller in order for the Processor to perform the Services;

The provision of the Services under the Processor's Terms of Services may qualify as Processing as per Data Protection Laws and Regulations and GDPR;

This DPA shall render any and all other previous agreements entered into force between the Controller and the Processor in relation to data protection, before the date of this DPA, null and void.

Definitions

Controller means the Party which, alone or jointly with others, determines the

purposes and means of the processing of personal data.

Data Protection Laws and Regulations 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 the Agreement.

Data Subject means the identified or identifiable person to whom Personal Data relates as defined under GDPR.

DPA means this agreement.

GDPR means the 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 repealing Directive 95/46/EC (General Data Protection Directive).

Personal Data means “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”, as defined in the GDPR.

Processor means the Party which processes Personal Data on behalf of the Controller.

Processing means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Purpose means the performance of the Services by the Processor and the associated Processing of Personal Data as defined in clause 2.2.2.

Services means any product or service provided by Turbine Room Ltd to Customer pursuant to the DPA.

Terms of Service means the legal agreement between the Controller as the customer and the Processor that governs the Controller’s right to use the FirstOfficer site and Services.

2. Processing of Personal Data

2.1 Appointment

2.1.1 The Processor is appointed by the Controller to process such Personal Data for and on behalf of the Controller as is necessary to provide the Services, and as may subsequently be agreed to by the Parties in writing. Any such subsequent agreement shall be subject to the provisions of this DPA.

2.2 The Controller shall process Personal Data in accordance with Data Protection Laws and Regulations. For the avoidance of doubt, the Controller's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations and the Processor reserves the right to refuse such instructions if not in compliance with the Data Protection Laws and Regulations.

2.3 The Controller shall have sole responsibility for the accuracy, quality and legality of Personal Data and the means by which it acquires the Personal Data.

2.2 Purpose of Processing

2.2.1 The Processor shall process the Personal Data it receives from the Customer solely for the purposes of the processing operations as set out in the following and for no other purpose except with the express written consent of the Customer.

2.2.2 FirstOfficer is a SaaS financial metrics and analytics service. The purpose of processing the Personal Data is to provide end-user specific financial information and metrics to the Customer.

2.3 Duration

2.3.1 This DPA shall commence on the date this DPA is entered into and shall continue in full force and effect until the termination of the Purpose, or for as long as the Processor is required to Process the Personal Data under Data Protection Laws and Regulations.

2.4 Data Processing

2.4.1 The data processed under this Agreement will be hosted within the European Economic Area (EEA). The Processor may access the data from the USA in order to provide the Services. Such transfer of data is subject to the Controller guaranteeing appropriate safeguards through the Privacy Shield mechanism.

2.4.2 Any transfer of data, other than as set out in clause 2.4.1, to a country which is not a member of the EEA requires the prior consent of the Controller and is subject to compliance with the special requirements on transfers of personal data to countries outside the EEA

2.4.3 The Data Subjects affected by the Processing of their Personal Data under this Agreement includes end-users of the Controller's websites.

2.4.4 Depending on how the Controller chooses to use FirstOfficer and connected payment gateways (e.g. Stripe), the Processing of Personal Data may cover the following types/categories of data.

For Controller's end-users:

- Name
- Email
- Country
- Internal identification numbers (e.g. Stripe customer id, internal Team ID)
- Description that may or may not contain online identifying information (e.g. Description field from Stripe, description given through FirstOfficer API)
- Financial data

3. The obligations of the Processor

3.1 The Processor shall comply with Data Protection Laws and Regulations when carrying out this DPA. The processor ensures compliancy with the following requirements:

The Processor entrusts only such legal or natural persons with the Processing under this DPA who have given an undertaking to maintain confidentiality and have been informed of any data protection requirements relevant to their work;

The Processor shall promptly notify the Controller and provide the Controller with reasonable co-operation if it receives any complaint, notice or communication which relates to the Processing of the Controller's Personal Data under this DPA or to the Controller's compliance with Data Protection Laws and Regulations;

The Processor and any person acting under its authority shall process the Personal Data in accordance with the Processor's Terms of Service and on documented instructions from the Controller, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to so do by Union or Member state law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest;

The Processor shall implement appropriate technical and organisational measures (taking into account costs of implementation and the nature, scope and purposes of Processing) to ensure a level of security appropriate to the risk against unauthorised or unlawful Processing of Personal Data, and ensure the security of such data at all times;

The Processor shall cooperate, on request, with the supervisory authority in performance of its tasks;

The Processor will assist the Controller (at the Controller's expense) by providing all reasonable assistance to the Controller, having regard to the nature of processing, in order to assist the Controller to comply with its obligation to respond to requests from Data Subjects to exercise their rights under Data Protection Laws and Regulations, or if the Controller is subject to an inspection by the supervisory authority;

With effect from 25 May 2018, upon the Controller's request and at the Controller's expense, the Processor shall provide the Controller with reasonable cooperation and assistance needed to fulfil the Controller's obligation under GDPR to carry out a data protection impact assessment related to the Controller's use of the Services, to the extent that the Controller does not otherwise have access to the relevant information, and to the extent such information is available to the Processor;

4. Monitoring rights of the Controller

4.1 The Controller has the right, after consultation with the Processor, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. The Processor agrees to contribute to such inspections and reserves the right to invoice the Controller for any reasonable costs incurred by the Processor in contributing to such inspections.

4.2 The Processor shall ensure that the Controller is able to verify compliance with the obligations of the Processor in accordance with Data Protection Laws and Regulations. The Processor undertakes to provide to the Controller all necessary information on request within a reasonable timeframe

5. Notification of security breaches by the Processor

5.1 The Processor shall:

Notify the Controller without undue delay and, where feasible, not later than 72 hours after having become aware of any accidental, unauthorised or unlawful Processing or disclosure of, or access to, Personal Data ("Security Breach") and promptly provide the Controller with all relevant information in this regard;

Take appropriate measures to secure the data and limit any possible detrimental effect on the Data Subjects;

Ensure an appropriate level of protection through technical and organisational measures that take into account the circumstances and purposes of Processing as well as the projected probability and severity of a possible infringement of Data

Protection Laws and Regulations as a result of security vulnerabilities;

Cooperate with the Controller and provide the Controller with any information which the Controller may reasonably request relating to the Security Breach. The Processor shall investigate the Security Breach and shall identify, prevent and make reasonable efforts to mitigate the effects of any such Security Breach and, with the Controller's prior agreement, to carry out any recovery or other action necessary to remedy the Security Breach;

6. Authority of the Controller to issue instructions

6.1 The Personal Data may only be handled under the terms of this DPA, in alignment with the Terms of Service, and under the instructions issued by the Controller. The Controller retains a general right of instruction as to the nature, scope and method of data processing, which may be supplemented with additional written instructions. The Processor may only pass on information to 3rd parties or to the Data Subject with the prior written consent of the Controller.

6.2 The Processor will only accept instructions via electronically communicated text in writing or in text form. The Processor must not use the data for any other purpose and shall not disclose the data to third parties without the Controller's written authority. No copies or duplicates may be produced without the knowledge of the Controller. This does not apply to backup copies (which may be kept for 35 days) where these are required to assure proper data Processing, or to any Processing required to comply with Data Protection Laws and Regulations.

6.3 The Processor shall inform the Controller immediately if it believes that following the instructions would result in infringement of law. The Processor may then postpone the execution of the relevant instruction until it is confirmed or changed by the Controller.

7. Deletion of Personal Data

7.1 Within a reasonable period (which shall not exceed 30 days) of termination of the Purpose or when requested by the Controller, the Processor must delete all Personal Data in compliance with Data Protection Laws and Regulations unless Union or Member State Law requires storage of the Personal Data. The same applies to any test data. The proof of deletion shall be presented upon request.

7.2 Electronic documentation intended as proof of proper data Processing and fulfilment of EU VAT obligations must be kept by the Processor beyond the termination of the Purpose. The Processor may hand such documentation over to the Controller after expiry of the DPA, upon request by the Controller.

8. Indemnification

Indemnity and liability provisions are as set out in the Terms of Service.

9. Sub-Processing

9.1 The Controller agrees to the commissioning of the following sub-processors on the condition of a contractual agreement in accordance with applicable Data Protection Laws and Regulations:

Sub-Processor: Heroku, Salesforce.com, Inc

Country: US

DB Location: Heroku's "EU Region" (currently Ireland)

Service: Infrastructure, Secure Cloud Service Platform for Database Storage

Sub-Processor: Amazon Web Services, Inc

Country: US

Storage Location: Ireland

Service: S3 File Storage for data export

9.2 "Sub-Processing", in the meaning of this DPA, does not include ancillary services, such as telecommunication services, postal or transport services, maintenance and user support services or legal and administrative services, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data Processing equipment. The Processor shall be obliged to make appropriate and legally binding contractual arrangements to ensure the protection and the security of the Controller's data, even in the case of outsourced ancillary services to Sub-Processors.

9.3 The Controller grants the Processor general authorisation to engage Sub-Processors to provide the Services provided that the Processor and Sub-Processor enter into a contract on terms that guarantee that any Processing will meet the requirements of Data Protection Laws and Regulations and the Processor will keep the Controller informed of any intended changes to Sub-Processors giving the Controller an opportunity to object in writing or text form within 10 business days. The Controller shall not unreasonably object to any sub-processor engaged in accordance with this clause.

9.4 If the Sub-Processor provides the agreed service outside the EU/EEA, the

Processor shall ensure compliancy with Data Protection Laws and Regulations.

9.5 The Processor shall be liable to the Controller for the performance of Sub-Processor's obligations.

9.6 The Processor will disclose the list of used Sub-Processors at:
www.firstofficer.io/legal/gdpr/data-partners.

10. Miscellaneous

10.1 Any dispute or claim, including non-contractual disputes or claims, arising out of this DPA or in connection with it or its subject matter or formation shall be governed by and interpreted in accordance with the law of Finland. The courts of Finland have jurisdiction to settle any such dispute or claim. Finland is a Member State of European Union and is committed to GDPR.

10.2 If any variation is required to this DPA as a result of a change in the Data Protection Laws and Regulations, then either Party may provide written notice to the other party of that change in law. The Parties will discuss and negotiate in good faith any necessary variations to this DPA. The parties will promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the relevant requirements.

10.3 Clauses and other headings in this DPA are for convenience of reference only and shall not constitute a part or otherwise affect the meaning or interpretation of this DPA.

10.4 The provisions of this DPA are severable. If any phrase, clause or provision is invalid or unenforceable, the rest of the DPA shall remain in full force and effect.

10.5 The provisions of this DPA shall endure to the benefit or and shall be binding upon the Parties and their respective successors and assigns.

[Followed by Signature Page]

The Parties' authorised signatories have duly executed this DPA Apr 01 2020:

Turbine Room Ltd



Signature:

Print Name: Jaana Kulmala

Title: CEO, Data Privacy Officer

Date: May 6, 2018

SAMPLE COMPANY LTD



Signature:

Print Name: Sample M. Sampleson

Title: Chief Executive Sample

Date: Apr 01 2020