Forecast

Last update: 1st August 2022

FORECAST DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") is an exhibit to the Terms of Service (the "Customer Agreement") between Forecast (the "Processor") and Customer (the "Controller") and sets forth the obligations of the parties with regard to the Processing of Personal Data pursuant to such Agreement.

1. PREAMBLE AND DEFINITIONS

1.1 This DPA sets out the rights and obligations of the Controller and the Processor, when processing personal data on behalf of the Controller.

1.2 This DPA has been designed to ensure the Parties' compliance with Article28(3) of 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).

1.3 This DPA shall take priority over any similar provisions contained in other agreements between the parties.

1.4 "Applicable Data Protection Law" means the General Data Protection Regulation (EU 2016/679) ("EU GDPR"); the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "UK GDPR") and the UK Data Protection Act 2018 ("DPA 2018").

1.5 "Controller", "Processor", "Data Subject", "Sub-processor" "personal data," "processing", "process" (and related activities such as collection, storage, organisation, erase) have the meanings given in accordance with the EU GDPR and this DPA.

1.6 Professional Service Automation "PSA" (also "platform" and "Service") is the cloud-based software platform provided by the Processor to the Controller. The Platform constitutes a resource, project management and reporting suite of tools.

1.7 "Restricted Country" means: (i) where the EU GDPR applies, a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a country outside the UK which is not based on adequacy regulations pursuant to Section 17A of the DPA 2018; and (iii) where the Swiss Federal Act on Data Protection of June 19, 1992 applies, a country outside Switzerland which has not been recognized to provide an adequate level of protection by the Federal Data Protection and Information Commissioner.

1.8 "Restricted Transfer" means: (i) where the EU GDPR applies, a transfer of Personal Data from the European Economic Area ("EEA") to a Restricted Country; (ii) where the UK GDPR applies, a transfer of Personal Data from the UK to a Restricted Country; and (iii) where the Swiss Federal Act on Data Protection of June 19, 1992 applies, a transfer of Personal Data from Switzerland to a Restricted Country.

1.9 "User" means an individual authorized to use the Service by the Controller as a user and/or administrator as identified through a unique login, which may include employees, contractors or subcontractors, whether individual or corporate, under the terms of a contract with You.

1.10 Any request concerning this agreement shall be forwarded to legal@forecast.app

2. INSTRUCTIONS ON DATA PROCESSING

2.1 Subject to this DPA, the Processor processes the categories of personal data stated in sections 3.2 and 3.5 on behalf of and on the instruction of the Controller.

2.2 The Processor may process personal data without the explicit consent of the Controller if required under Applicable Data Protection Law. The Processor informs the Controller hereof before the processing occurs, unless prohibited by law.

2.3 The Processor may not process personal data for its own purposes. The Processor ensures that access to personal data is limited to only employees who need to access the data for the purpose of carrying out the duties they are tasked with.

3. PERSONAL DATA AND DATA PROCESSING

3.1 The DPA forms part of the company's Terms of Service ("Customer Agreement") entered into between the Processor and the Controller. In case of any difference between this DPA and Processor´s Terms of Service concerning the interpretation of this DPA, the clauses listed in this DPA shall prevail. As part of the Processor's performance of the Customer Agreement, the Processor processes on behalf of the Controller personal data concerning the Controller's employees and external consultants ("Data Subjects").

3.2 The Processor processes the following categories of personal data on Data Subjects:

- Name, phone, email address
- Data Subjects' hourly rate
- Cookie ID
- IP Address
- Any other personal data that the Controller transfers to the Processor

3.3 The Controller acknowledges that the Service is not intended or designed for the Processing of the special categories of personal data covered by articles 8, 9 and 10 of the GDPR, and agrees not to host any Sensitive Information through the Service without prior agreement with the Data Processor.

3.4 The Processor provides a PSA to the Controller. The Controller creates the Data Subjects as users on the platform or the Data Subjects create themselves as users subject to prior agreement with the Controller. The purposes for which the platform can be used are listed in section 3.5 of the DPA.

3.5 As part of the Controller's use of the Processor's software platform, the Processor processes personal data for the Controller with the following purposes:

- Overview of Data Subjects' registered time, including holidays
- Overview of Data Subjects' tasks, roles and skills
- Automatic generation of reports and insights-sharing for the Controller's clients
- Overview of resource scheduling in accordance with work-related and administrative projects, including holidays
- Project management
- Continuous improvement of the Controller's profitability and utilisation
- Delivery of accurate estimates and scope on previous and current projects based on historical data
- Other purposes necessary for the functionality of the software platform

3.6 The Processor's processing of personal data for the Controller includes the following activities:

- Storage of personal data
- Transfer of personal data to third-party providers whom the Controller has chosen to connect to the software platform
- Reception of personal data from third-party providers whom the Controller has chosen to connect to the software platform

3.7 Types of processing performed by the Processor include the following: collection, storage, organisation, internal sharing, erasure and any other form of processing that is necessary to achieve the purpose of the processing.

4. RESTRICTED TRANSFER

Where Forecast initiates a Restricted Transfer of personal data of the Controller or a User, Forecast will ensure such Restricted Transfer takes place in compliance with the Applicable Data Protection Laws.

5. PROCESSOR'S OBLIGATIONS

5.1 The Processor processes personal data in accordance with the Applicable Data Protection Law.

5.2 The Processor processes personal data only on instructions from the Controller and only in accordance with the instructions as well as any other purposes agreed between the Parties in writing. The processing of personal data shall be performed in accordance with good data processing practices.

5.3 The Processor is obliged to store personal data on behalf of the Controller and in accordance with its instructions throughout the duration of the Customer Agreement, unless the Controller instructs the Processor to store the personal data for a longer period.

5.4 Forecast shall delete customer personal data within 90 days of the termination of the Customer Agreement, unless otherwise requested in writing by the Customer to delete sooner.

5.5 The Processor trains and instructs employees in confidential processing of personal data and ensures that processing is done solely in accordance with the purposes of the DPA and the Controller's instructions. The Processor ensures that their employees have committed themselves to confidentiality with respect to all personal data and treat personal data accordingly.

5.6 The Processor has the duty to establish, implement and maintain, organisational, administrative and IT technical security measures that prevent personal data from accidentally or illegally being destroyed or lost, deteriorate or be disclosed to unauthorised persons, abused or otherwise processed in violation of the law. The Processor shall give instructions that place responsibility for, and describe processing and erasure of, personal data and operation of IT equipment. At the Controller's request, the Processor shall provide the Controller with information adequate to check whether the mentioned technical and organisational security measures are implemented.

5.7 The Processor shall, to the extent possible and taking into account the nature of the processing, assist the Controller in complying with the Controller's obligation to respond to Data Subjects' exercise of their rights in accordance with chapter 3 of the EU GDPR. The Controller is responsible for direct communication with the Data Subjects. The Controller shall put its request for the Processor's assistance in writing and strive to describe as accurately and limited as possible the activities with which the Controller is requesting the Processor's assistance.

5.8 Upon written request by Controller with a notice period of thirty (30) days to Processor, Controller is entitled to audit compliance of this Data Processing Agreement, at most once a year, at its own costs, by accessing the technical and organizational security measures of Processor in accordance with the Applicable Data Protection Law. Such audit shall be carried out by the Controller or an inspection authority composed of independent persons and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the Controller. Controller will furnish immediately after the verification or inspection to the Processor a copy of the report of such audit. Processor will cooperate with such an audit or inspection. If any audit or inspection shows that Processor does not take and implement appropriate technical and organizational security measures in accordance with the Applicable Data Protection Law, Processor and Controller shall discuss and agree to improve the technical or organizational security measures in good cooperation.

6. THE CONTROLLER'S OBLIGATIONS

6.1 The Controller shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which the Controller acquired Personal Data. This includes for the Controller to be responsible for ensuring that the collection and processing of personal data in the Services has a lawful basis in the data protection legislation. The Controller is liable to reimburse the Processor for any legal liability incurred and financial loss suffered by the Processor as a consequence of any collection of personal data that does not have a lawful basis in the data protection legislation.

6.2 The Controller must exercise good data processing practices, including securing equipment and infrastructure in such a way that this does not pose a risk to the Processor's compliance with its obligations. This applies for example to the securing of the Controller's network, endpoint protection of devices with antivirus and firewalls, structured and secure handling of user accounts and access, securing of backup and testing of the ability to recover data.

6.3 The Controller shall ensure that any third-party tools that the Controller connects to the Platform will be GDPR compliant. Controller shall apply the obligations in sections 6.1 and 6.2 of this Data Processing Agreement to Controller's use of third-party tools in connection to the Platform.

7. MUTUAL REPORTING OBLIGATIONS

7.1 The Controller shall forward to the Processor inquiries and information relating to the Processor's specific processing of data. The Processor must inform the Controller of any deviations from the given instructions regarding the processing. In particular, deviations able to compromise data accuracy must be reported.

7.2 In case a personal data breach has occurred, the Processor shall without undue delay, after becoming aware of such a breach, notify the Controller, who in turn shall notify the relevant competent authorities of the violation within 72 hours of the Controller having been notified of the breach, unless it is unlikely that the personal data breach endangers Data Subjects' rights or freedoms.

7.3 For avoidance of doubt, a Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data and should not include unsuccessful attempts or activities that do not compromise the security of Personal Data.

8. SUB-PROCESSING

8.1 The Processor is authorised to use sub-processors without further written permission from the Controller. An updated list of the Processor´s Sub-processors can be found at https://www.forecast.app/subprocessors. The Processor shall notify the Controller in writing of the identity of new sub-processors before entering into an agreement with the respective sub-processors, allowingthe Controller to reasonably object to the appointment of the sub-processor in question within 2weeks after having received notice.

8.2 With respect to Forecast's other sub-processors, Forecast will endeavor to give notice thirty (30) business days prior to any planned major additions or replacements, but will give notice no less than ten (10) business days prior to any such change. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the Controller.

8.3 Having received notice, the Controller has the right to make objections in writing and on reasonable grounds to the appointment of the new sub-processor within ten (10) business days. If no objection has been raised within this time, the Processor will deem the Controller to have authorized the new sub-processor. If the Controller refuses to consent to the Processors´ appointment of a sub-processors on reasonable grounds, then the Processor will either look for alternative solutions or not appoint the sub-processor. In case of disagreement between the Parties concerning the appointment, then either party has the right to suspend or terminate this DPA (and any other agreement between the Parties relating to the provision of services by the Processor to the Controller) without penalty for both parties.

8.4 Prior to letting the sub-processor commence processing personal data, the Processor shall enter into a written agreement with the sub-processor, making the sub-processor subject as a minimum to the obligations which the Processor is subject to under the DPA, including the obligation to implement adequate technical and organisational measures to ensure that the requirements of the Applicable Data Protection Law be satisfied.

9. DURATION AND TERMINATION

9.1 The DPA will enter into force by signing and shall remain in force until the Customer Agreement is terminated by either Party or the customer relationship terminates.

9.2 This DPA and any dispute, claim or obligation (whether contractual or non-contractual) arising out of or in connection with it, its subject matter or formation shall be governed by English law. The parties irrevocably agree that the English courts shall have exclusive jurisdiction to settle any dispute or claim (whether contractual or non-contractual) arising out of or in connection with this DPA, its subject matter or formation.