Edison Law Advokater
CVR 32515754
% SingularityU Nordic
Titangade 11
2200 København N
Denmark
Responsible partner: *Kristian Holte*

DATA PROCESSING AGREEMENT

Forecast ApS	**Customer name**
Frederiksborggade 20 B, 1. floor	Address
DK-1360 Copenhagen K	Postal code
CVR/VAT: 38019651	CVR/VAT:
Denmark	Country
(“Processor”)	(“Controller”)

(Referred to individually as a "Party" or collectively as the "Parties".)

have entered into the following Data Processing Agreement (“DPA”):

1. INSTRUCTIONS ON DATA PROCESSING

1.1 Subject to this DPA, the Processor processes the categories of personal data stated in sections 2.3, 2.5.2 and 2.6 on behalf of and on the instruction of the Controller.

1.2 The Processor may process personal data without the explicit consent of the Controller if required under EU law and/or Danish law. The Processor informs the Controller hereof before the processing occurs, unless prohibited by law.

1.3 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.

2. PERSONAL DATA AND DATA PROCESSING

2.1 The DPA forms part of the company's Terms of Service ("Customer Agreement") entered into between the Processor and the Controller. 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").

2.2 "Personal data" means any information relating to an identified or identifiable natural person, in accordance with art. 4(1) of regulation (EU) 2016/679 of 27 April 2016 ("General Data Protection Regulation").

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

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

2.4 The Processor does not process personal identification numbers or special categories of personal data about Data Subjects, cf. art. 9 and 10 of the General Data Protection Regulation.

2.5.1 The Processor provides a cloud based Professional Service Automation ("PSA") software platform 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 Platform constitutes a resource, project management and reporting suite of tools. The purposes for which the platform can be used are listed in section 2.5.2 of the DPA.

2.5.2 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

2.6 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

2.7 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.

3. STORAGE OF DATA

3.1 Personal data is stored on behalf of the Processor on servers at the Processor's sub-processors in the EU and the USA.

3.2 By their signature to this DPA, the Controller approves by way of explicit consent to the transfer of personal data to the USA for storage purposes. The Processor is liable to procure the legal foundation of the transfer of personal data prior to the transfer taking place, such as the "European Commission's Standard Contractual Clauses for transfer of personal data to third countries" or the "EU - USA Privacy Shield Framework".

3.3 The Processor is obliged to inform the Controller in writing if the Processor finds an instruction of the Controller to be in violation of the General Data Protection Regulation or other data protection legislation in EU law or member state law.

3.4 The Processor must inform the Controller of any change of supplier of server hosting prior to the change and give the Controller the option to object.

4. PROCESSOR'S OBLIGATIONS

4.1 The Processor processes personal data in accordance with applicable Danish data protection legislation, including the General Data Protection Regulation, when it enters into force in Denmark on 25 May 2018.

4.2 The Processor processes personal data only on instruction 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.

4.3 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.

4.4 At the expiry of the contract period of the Customer Agreement and at the Controller's option, the Processor shall 1) erase or 2) return to the Controller all personal data and remove existing copies. The Processor shall erase personal data from all IT systems when so instructed by the Controller and future storage no longer serves a legitimate purpose.

4.5 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.

4.6 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.

4.7 The Processor shall, to the extent possible, assist the Controller in complying with the Controller's obligation to respond to Data Subjects' exercise of a their rights in accordance with chapter 3 of the General Data Protection Regulation. 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. THE CONTROLLER'S OBLIGATIONS

5.1 The Controller warrants that the processing of personal data in accordance with the Processor's instructions is legal. This includes the collection and use of legal consent in accordance with the law. 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 illegal collection of consent.

5.2 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.

5.3 The Controller is required to ensure that any third-parties acting on behalf of the Controller comply with the same obligations as the Controller. The Controller is required to ensure that no actions be taken that may compromise the Processor's processing of personal data without the prior approval of the Processor.

6. MUTUAL REPORTING OBLIGATIONS

6.1 The Processor shall forward to the Controller any third-party inquiries regarding the content of data originating from the Controller's systems or Data Subjects.

6.2 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.

6.3 If there is any suspicion, or an incident indicating, that a personal data breach has occured, this shall be immediately reported to the other Party.

6.4 In case a personal data breach has occured, the Processor shall immediately notify the Controller who in turn notifies the Danish Data Protection Agency (Datatilsynet) of the violation within 72 hours of the Processor having been notified of the breach, unless it is unlikely that the personal data breach endangers Data Subjects' rights or rights of freedoms.

7. SUB-PROCESSING

7.1 The Processor is authorised to use sub-processors without further written permission from the Controller. 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, allowing the Controller to object to the appointment of the sub-processor in question. A list of the Processor's sub-processors as at 2 April 2018 is attached as Annex A.

7.2 The Processor shall notify the Controller in writing of any planned major additions or replacements of sub-processors no later than one month prior to the changes taking effect.

7.3 Having received notice, the Controller has the right to make legitimate objections to the appointment of the new sub-processor. In that case, the Processor is entitled to terminate all agreements with the Controller, according to which the Processor processes personal data for the Controller, giving one month's notice.

7.4 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 General Data Protection Regulation be satisfied.

8. DURATION AND TERMINATION

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. Danish law applies to the DPA, including issues as to its existence and validity. Danish international private law designating foreign law does not apply.

.o0o.

SIGNATURES

Date:	Date:
On behalf of the **Processor**	On behalf of the **Controller**
_____	_____
Dennis Kayser, CEO	Name, title

Annex A:

List of Sub-processors

Vendor	Security standards
Amazon Web Service	ISO 27001, 27017 and 27018 SOC 1, 2 and 3
HubSpot	Hosting partially at Amazon Web Service which has the following security codes: ISO 27001, 27017 and 27018 SOC 1, 2 and 3 And hosting partially on the Google Cloud Platform which has the following security codes: ISO 27001, 27017 and 27018 SOC 2 and 3