

Data processing agreement for personal data in your uploaded Content

1. Background and purpose

This personal data processing agreement (“Data Processing Agreement”) regulates the processing of personal data included in Content uploaded by Favo’s customers while using the PinToMind web service. All words and expressions used herein shall have the same meaning as defined in the Terms of Service.

The purpose of the Data Processing Agreement is to regulate rights and obligations under the Act of 15 June 2018 no. 38 relating to the processing of personal data, and 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 (GDPR).

When you as a customer of Favo upload Content that includes personal data, you will be considered the data controller for such personal data under the relevant data protection law, and you or the company you sign up for are therefore referred to as the “Data Controller” in the following.

In so far as Content includes personal data, i) Favo will be data processor of such data; (ii) the Data Controller will comply with its obligations as a data controller under the relevant data protection legislation; and (iii) Favo will comply with its obligations as a processor under these terms. The Data Processing Agreement only applies as far as Favo actually processes personal data as part of the Content. Other data Included in the Content that Favo may process is not regulated by these terms.

Favo will only process the type of personal data that a Data Controller provides to Favo via the PinToMind web service, and regarding the types of individuals that the Data Controller provides to Favo.

The Data Controller shall ensure that there is adequate basis for processing the personal data, including obtaining consent from the data subject to the extent required by applicable privacy regulations.

2. Favo’s general obligations

Favo shall only process personal data it may access as part of fulfilling its contractual obligations to the Data Controller. Favo has no right to hand over personal data to unauthorized third parties.

Favo shall follow the procedures and instructions for the processing of personal data that the Data Controller has laid out, and to the extent necessary to comply with applicable law. This includes but is not limited to instructions provided by the Data Controller as part of operating the PinToMind service.

The Data Controller shall only provide Favo with instructions that are in accordance with current applicable law. Favo is obliged to inform the Data Controller if Favo believes that a given instruction is not in accordance with applicable law. Favo will in accordance with GDPR article 28 (h) make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in said article and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.

Upon a Data Controller's request, Favo is obliged to provide necessary assistance for the Data Controller to access the data processed on behalf of the Data Controller.

Favo has a duty of confidentiality regarding personal data that it has access to in accordance with the Data Processing Agreement. This also applies after the Agreement with the Data Controller is terminated. Favo shall ensure that persons authorized to process personal data on behalf of Favo are subject to confidentiality by law or contract.

Favo shall, considering the nature of the processing, as far as possible and with appropriate technical and organizational means, assist the Data Controller in answering the data subject's requests for fulfillment of the data subject's rights under the applicable data protection law.

Favo shall, to the extent to which it is relevant to the contractual relationship, considering which personal data is available to it and the nature of the processing, assist the Data Controller in complying with the information security requirements, requirements for notifications to the Norwegian Data Protection Authority and the data subjects, as well as impact assessments, pursuant to Articles 32-36 of the GDPR.

Favo will comply with the requirements for security measures under the Personal Data Act and the Personal Data Regulation, including particularly the Personal Data Act Section 13-15 with regulations, as well as Article 32 of the GDPR.

Any assistance from Favo required by a Data Controller under this Section 2, or corresponding legislation regarding personal data, shall be compensated according to the applicable hourly rates agreed between the parties, or, if no hourly rates are agreed upon, by the current regular and reasonable fees for such services.

3. Location of personal data

Favo is based in Norway and will mainly access your data in Norway from our regular place of business. Favo uses sub-processors located outside of Norway and the EU/EEA, listed in the next section.

The Content may be made available for our employees in countries outside the EU/EEA, and temporarily stored in a country where employees, sub-processors or their agents are located or have facilities, including in countries outside the EU/EEA.

If personal data is transferred outside the EU/EEA, we only do so based on approved basis for transfer, such as EU's approved standard clauses (SCC), in addition to any further security measures necessary for ensuring a level of security equivalent to the level of the EU/EEA.

4. Use of sub-processors

Favo uses the following sub-contractors and data processors ("Sub-processors") for processing your Content:

- Brightbox Systems Ltd ("**Brightbox**"), where we store our servers and databases. Most of the contents of the solution are stored here; such as information regarding accounts, screens, displays, users, screen contents, as well as images uploaded by users. External content, such as calendar data, is stored temporarily and processed for screen displays. Data is processed and stored in the United Kingdom. The United Kingdom is subject to the [Commission's adequacy decision of 28 June 2021](#), which ensures an equivalent level of protection to that guaranteed in the EU/EEA. Favo has a data processing agreement with Brightbox through the [standard terms](#).
- PowerOffice AS ("**PowerOffice**"), which we use for invoicing and accounting. Here we store company information, invoice information and any information regarding the customer's contact person(s). This service is not used for customers who opt for card payments. Data is processed and stored in Europe. Favo has a data processing agreement with PowerOffice through the [standard terms](#), as well as a separate privacy and security agreement.
- Stripe, Inc. ("**Stripe**"), which we use for card payments. Information on cards, card holders, invoicing and transactions is stored here. The service is only used for customers who choose card payments. Stripe is an American company, and data is processed and stored in the US. Favo has entered into a data processing agreement with Stripe and ensured adequate basis for the data transfer (SCC). Stripe has provided documentation showing implementation of several organizational and technical security measures, including encryption and appendices which explicitly address the American intelligence legislation. Stripe writes that it is highly unlikely that they will be instructed by the American government to reveal information. If the Data Controller does not wish to approve Stripe as a sub-processor, this may be solved by not opting for card payments.
- Peaberry Software, Inc. ("**Customer.io**"), which we use for distribution of information and newsletters by e-mail. Here we store users' contact information, language and which roles they have in the solution. Customer.io is an American company which processes and stores data in Europe. Favo has entered into a data processing agreement with Customer.io and ensured adequate basis for the data transfer (SCC). The personal data processed by Customer.io is limited to contact information and account information and is therefore not very sensitive. In addition, Customer.io has implemented a number of security measures, including encryption.
- Sveve AS ("**Sveve**"), which we use to send SMS with a code for two-factor authentication, for users who have activated this. Mobile number and current message are transferred to Sveve. Data is processed and stored in Europe. Favo has a data processing agreement with Sveve.
- Microsoft Ireland Operations, Ltd. ("**Microsoft Azure**"), which we use for storage of images, videos, display backgrounds, logos etc. This is primarily data which does not include any personal information. Microsoft Azure is an American company with a subsidiary in Ireland and server location in Norway. Favo has entered into a data processing agreement with

Microsoft Azure and ensured adequate basis for the data transfer (SCC). The data processing agreement states that Microsoft Azure may in certain cases process data outside the EU. Based on the nature of the processed information and the implemented security measures, we view the risk of any significant privacy protection consequences resulting from sporadic data processing in the US to be extremely low.

- Elasticsearch, Inc.-General ("**Elastic**"), which we use for performance and error analysis; data which is described as stored and processed by other services, will be logged and analyzed by Elastic. Favo has entered into a data processing agreement with Elastic. Logs are stored for up to 30 days and are continually deleted. Data is stored and processed in Europe.

Favo shall only use Sub-processors for processing personal data that are authorized by the Data Controller. The Data Controller hereby authorizes appointment of the above-mentioned Sub-processors, the terms of use or the privacy statement, and accepts that Favo may change its Sub-processors at its own discretion. The Data Controller shall be notified of such changes of Sub-processors through the updating of these terms or through a notification on our website. The Data Controller may object to such appointment by written notice to Favo, and Favo may in such case choose to terminate the Data Processing Agreement upon written notice to the Data Controller if the Data Controller does not accept the new Sub-processor.

Anyone who, on behalf of Favo, carries out assignments in which the personal data in question is processed, shall be subject to the same obligations to Favo, pursuant to this Data Processing Agreement.

5. Data correction and deletion

Through the services Favo delivers, the Data Controller will be provided with the ability to correct, block, export and delete Content in a manner consistent with the functionality of the PinToMind web service and the Agreement.

During the Term, Favo will make available to the Data Controller the Content in a manner consistent with the functionality of the PinToMind web service and in accordance with this Data Processing Agreement. To the extent the Data Controller, in its use and administration of the PinToMind web service does not have the ability to amend or delete Content (as required by applicable law), or migrate Content to another system or service provider, Favo will, at the Data Controller's reasonable expense, comply with any reasonable requests from the Data Controller to assist in facilitating such actions to the extent Favo is legally permitted to do so and has reasonable access to the relevant Content. Content that is deleted by the Data Controller shall be deleted by Favo within reasonable time, and no later than 2 months.

6. Term

This Data Processing Agreement applies between the parties as long as Favo processes personal data as a data processor on behalf of the Data Controller.

In case of breach of this Data Processing Agreement or the Personal Data Act, the Data Controller may request that Favo stop further processing of the data with immediate effect.

7. Termination

Upon termination of the Data Processing Agreement, Favo shall upon instruction from the Data Controller delete or properly destroy all documents, data, floppy disks, CDs, etc. containing personal data covered by this Data Processing Agreement as laid out in section 6 above.

The above applies only if nothing else follows from an explicit agreement between the parties or applicable law, such as an obligation to store data for specific purposes.

8. Breach of contract

Upon breach of this Data Processing Agreement, the regulation on indemnification, liability and limitation of liability in the Agreement shall apply.

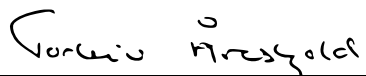
9. Contact information

Any communication regarding this Data Processing Agreement can be directed at Favo's data protection officer by e-mail support@pintomind.com.

**Signed for and behalf of Data
Controller (customer)**

**Signed for and behalf of Data
Processor (Favo AS)**

Signature of authorized person



Signature of authorized person

Name of company or organization

Name of company
Favo AS

Date

Date
May 10, 2023

Location

Location
Ølensvåg, Norway

Send a copy of the signed document to Favo via e-mail to support@pintomind.com