DATA PROCESSOR AGREEMENT

This data processor agreement (the "Agreement") in entered into between:

[Name of the data controller]
Company registration number: [insert]
[Address]
[Country]
(the "Data Controller")

and

Outlay ApS
Company registration number: 25 70 55 64
Turbinevej 10
5000 Middelfart, Denmark
(the "Data Processor")

(separately referred to as a "Party" and collectively the "Parties")

regarding the Data Processor's processing of personal data on behalf of the Data Controller.

1. Processing of personal data

1.1 This Agreement has been entered into in connection with the Parties' execution of the software as a service agreement (the "Main Agreement").

1.2 The types of personal data which the Data Processor shall process under and in connection with the Main Agreement referred to in clause 1.1 are listed in Appendix 1. The processing activities concerns the data subjects listed in Appendix 1.

1.3 The Data Controller is entitled to delete and/or add additional types of personal data/data subjects to the above lists by forwarding an updated Appendix 1 to the Data Processor.

2. Purpose and instructions

2.1 The Data Processor may only process the personal data for purposes which are necessary in order to fulfill the obligations set out in the Main Agreement.

2.2 The Data Processor is only entitled to process the personal data, including transfer the personal data to a third country or an international organisation in accordance with the Data Controller's instructions, unless such processing or transfer is required pursuant to applicable legislation. In such case, the Data Processor shall inform the Data Controller of such legal requirement before the processing/transfer unless the law prohibits such information on important grounds of public interest.

2.3 The Data Controller hereby instructs the Data Processor to carry out the below listed processing activities with respect to the personal data comprised by clause 1.2:

- Collection
- Registration
- Organizing
- Systematizing
- Storing
- Adapting or altering
- Rediscovery
- Searching
- Use
- Disclosure by transmission
- Communicating or any kind of making available
- Compilation or interfacing
- Restricting
- Deletion or destruction

2.4 The Data Processor shall immediately inform the Data Controller if, in the Data Processor's opinion, any instruction infringes applicable data protection legislation regarding processing of personal data, including the EU General Data Protection Regulation 2016/679 (GDPR).

3. Obligations of the Data Processor

3.1 All processing by the Data Processor of the personal data governed by this Agreement must be in accordance with instructions prepared by the Data Controller, and the Data Processor is, furthermore, obliged to comply with any applicable data protection legislation at the time in question.

3.2 The Data Processor must take all necessary technical and organisational security measures, including any additional measures, required to ensure that the personal data specified in clause 1.2 is not accidentally or unlawfully destroyed, lost or impaired or brought to the knowledge of unauthorised third parties, abused or otherwise processed in a manner which is contrary to applicable data protection legislation. Thus, the Data Processor must, among other things,

- introduce login and password procedures and set up and maintain a firewall and antivirus software;
- ensure that only employees with a work related purpose have access to the personal data;
- store data storage media securely so that it is not accessible to third parties;

- implement appropriate technical measures to limit the risk of unauthorised access to systems containing personal data and/or installation of harmful code. The Data Processor shall have formal procedures to ensure that security systems are kept up-to-date at all times;

- ensure that suitable restrictions for physical access is introduced. Such access control mechanisms may include systems for physical access control, locks, airlocks, security staff and surveillance equipment;

- ensure that only high-quality hardware and software, which is regularly updated is used;

- ensure that tests and waste material are destroyed in accordance with data protection requirements on the specific instruction of the Data Controller. In particular cases, to be determined by the Data Controller, such tests and waste material must be stored or returned;

- prepare and implement formal processes for handling breaches of data security, including notification to the Data Controller in accordance with the Agreement;

- ensure that employees receive proper training, adequate instructions and guidelines on the processing of the personal data. The Data Processor must ensure that the employees involved with the processing of the personal data are familiar with the security requirements;

- monitor that the Data Processor's organisation complies with relevant legal requirements, policies and procedures.

3.3 The Data Processor must ensure that employees authorised to process the personal data have committed themselves to confidentiality or are under appropriate statutory obligation of confidentiality.

3.4 If so requested by the Data Controller, the Data Processor shall make available to the Data Controller all information necessary to demonstrate that the Data Processor complies with the requirements of the applicable data protection legislation, and the obligations under this Agreement, including the implementation of necessary technical and organisational security measures.

3.5 If the Data Processor processes the personal data in another EU/EEA member state other than Denmark, the Data Processor must comply with any and all legislation concerning security measures in that member state.

3.6 The Data Processor must notify the Data Controller immediately where there is an interruption in operation, a suspicion that data protection rules have been breached or other irregularities in connection with the processing of the personal data occur. In case of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the personal

data transmitted, stored or otherwise processed, the Data Processor shall inform the Data Controller hereof immediately and no later than 12 hours from the discovery of the breach. If requested by the Data Controller, the Data Processor shall assist the Data Controller in relation to clarifying the scope of the security breach, including preparation of any required notification to the supervisory authority and/or data subjects.

3.7 Upon the request of the Data Controller, the Data Processor is obliged to assist the Data Controller in relation to completion of data protection impact assessments, including potential prior consultations with the supervisory authority, taking into account the nature of processing and the information available to the Data Processor.

3.8 At least annually, the Data Processor must have its processing of personal data reviewed by an independent third party in order to document, that the Data Processor complies with the requirements of the applicable data protection legislation, including the implementation of necessary technical and organisational security measures. If the Data Processor does not provide the Data Controller with this documentation, the Data Controller is entitled to have the Data Processor's processing of personal data revised by an independent third party at the Data Processor's expense. In addition, the Data Processor shall allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.

3.9 If the Data Processor, or another data processor which processes the personal data in accordance with clause 4 below, receives a request for access to the personal data from a data subject or his/her agent, or a data subject objects to processing of his/her personal data, or a data subjects exercises any other rights, the Data Processor must immediately send such request and/or objection to the Data Controller, for the Data Controller's further processing thereof, unless the Data Processor is entitled to handle such request itself. If requested by the Data Controller, the Data Processor shall assist the Data Controller in answering such requests and/or objections.

4. Use of sub-processors

4.1 The Data Processor is not entitled to engage another data processor (sub-processor) for the processing of the personal data governed by this Agreement without prior specific authorisation from the Data Controller to this effect.

4.2 Before making the personal data available to a sub-processor, the Data Processor must ensure that the same data protection obligations as set out in this Agreement are imposed on such sub-processor by way of a written sub-processor agreement. The Data Processor shall, in its own name, enter into such sub-processor agreements. The Data Processor shall remain fully liable to the Data Controller for the performance of any sub-processor's obligations.

4.3 If the personal data is made available to foreign sub-processors, it must be stated in the sub-processor agreement that the data protection legislation applicable in the Data Controller's country applies to such foreign sub-processors. Furthermore, if the receiving sub-processor is established within the EU/EEA, it must be stated that the receiving EU/EEA country's specific statutory requirements regarding data processors, e.g. concerning demands for notification to national authorities, must be complied with.

4.4 If the sub-processor authorised by the Data Controller under clause 4.1 processes the personal data in a country which is not considered to provide an adequate level of data protection and the sub-processor is not certified under the Privacy Shield Framework or a similar certification mechanism, the Data Processor must enter into standard agreements in accordance with Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under the European Parliament and the Council's Directive 95/46/EC ("Standard Contractual Clauses").

4.5 The Data Controller hereby authorises the Data Processor to enter into Model Clauses with sub-processors outside the EU/EEA on behalf of and in the name of the Data Controller, provided, however, that the Data Controller has authorised the transfer in accordance with clause 4.1 above.

4.6 At the time of the signature of this Agreement, the Data Processor engages the sub-processors listed in Appendix 2.

5. Amendments

5.1 In the event of amendments to the applicable data protection legislation, the Data Controller is entitled to amend the instructions set out in this Agreement by giving 2 (two) weeks' written notice when forwarding the new written instructions to the Data Processor. The Data Processor must however, at all times, comply with the applicable data protection legislation.

6. Liability

6.1 The Data Processor shall indemnify the Data Controller against any claims, costs (including reasonable expenses for legal services), loss, liability, fines, expenses or damages incurred by the Data Controller as a result of the Data Processor's breach of this Agreement, including breach of the applicable legislation on the protection of personal data.

7. Effective date and termination

7.1 This Agreement becomes effective on the date of signing hereof.

7.2 **Alternative 1:** Termination of the separately concluded Main Agreement between the Data Controller and the Data Processor will result in the termination of this Agreement. However, the Data Processor remains subject to the obligations stipulated in this Agreement, as long as the Data Processor processes the personal data on behalf of the Data Controller.

7.3 In the event of the termination of the Agreement, the Data Controller is entitled to determine whether the personal data must be returned on a media format of the Data Controller's choice or the personal data must be deleted by the Data Processor.

8. Governing law and jurisdiction

8.1 This Agreement is subject to Danish law.

8.2 Any claim or dispute arising from or in connection with this Agreement must be settled by a competent court of first instance in same jurisdiction as stated in the main agreement.

9. Signatures

9.1 The Agreement is signed in duplicate original copies, each Party receiving one copy.

On behalf of the Data Controller:

_____
Name:
Date and place:

On behalf of the Data Processor:

_____
Name:
Date and place:

Appendix 1
Types of personal data and data subjects

Types of personal data:

- Name,
- Address,
- Phone number,
- E-mail address,
- Contact information
- Payment and bank information

Data subjects:

- Employees
- Former employees
- Clients B2B
- Clients B2C

Appendix 2
Sub-processors

Keepers ApS, cvr. 36079886
Keepers IT ApS, cvr 38317121
WeCode ApS, cvr. 37496510
Penneo ApS, cvr. 35633766
Microsoft Ireland Operations Ltd
Dropbox International Unlimited Company
Teamwork.com, Ltd
Recurly
Amazon Web Services
Dibs

Location(s) for processing personal data

The data processing is carried out on the following location(s):

Turbinevej 10, 5000 Middelfart
Dronningens Tværgade, 9, 1. sal, 1302 København K