This is ConnectMyApps' standard Data Processing Agreement template. It applies where ConnectMyApps processes personal data on behalf of a customer and forms part of the applicable agreement between ConnectMyApps and that customer.

Schedule B: Data Processing Agreement

This data processing agreement (**"The Agreement**") was entered into between [company name] a company with organisation number [org. no], having its registered address at [address] ("The Customer" or" Data Controller") and ConnectMyApps AS, a company that is subject to Norwegian law, with organisation number 913 244 990 ("The Provider" or " Data Processor").

The companies are referred to as "party" or "parties".

1. Introduction

1.1 The Data Processor will provide services to the Data Controller according to the ConnectMyApps Master Services Agreement between the parties entered into on [date] ("The Master Agreement"). Implementation of the services according to the Master Agreement could involve the Data Processor receiving personal data from and handling personal data on behalf of the Data Controller. Such services may include the integration, transfer, synchronisation, automation, or processing of data between ConnectMyApps and other third-party software applications, systems, platforms, or services used by the Data Controller. This Agreement is applicable to the extent that the Data Processor processes personal data.

1.2 In the Agreement, the terms "personal data", "data processor", "data controller", "registered" and "handling" shall have the same meaning as in the Personal Privacy legislation (as defined below).

1.3 In the event of any contradiction between the Master Agreement and the Agreement concerning the processing of personal data, this Agreement shall take precedence.

2. The content of this agreement and scope of processing

2.1 The purpose of the Agreement

This Agreement governs the rights and obligations under applicable personal privacy legislation in connection with the Data Processor's processing of personal data on behalf of the Data Controller. The Agreement shall ensure that the personal data is handled in accordance with the EU Privacy Protection Regulation (2016/679) ("GDPR") and the at all times applicable national legislation relating to privacy protection under the Governing Law as set out in the Master Agreement, including legislation that implements or supplements GDPR (collectively named "Personal Privacy Legislation").

2.2 The Data Controller's right to administer the processing

The Data Controller determines the purpose of the processing and provides instructions to the Data Processor. The Data Processor and its subcontractors shall only process personal data on Data

Controller's behalf upon written instructions from the Data Controller, and in accordance with this Agreement, unless otherwise stated in applicable legislation. The Data Processor must inform the Data Controller immediately if the Data Processor believes that an instruction conflicts with Personal Privacy Legislation.

2.3 The scope and purpose of the processing

The scope and purpose of the Data Processor's processing of personal data on behalf of the Data Controller is related to the provision of services described in detail in the Master Agreement, or in relevant Statement of Work (SoW). Such services may include facilitating integrations, data transfers, workflow automation, or interoperability between the Data Controller's systems and third-party applications, platforms, or services selected or authorised by the Data Controller.

2.4 Categories of personal data that are registered

The handling involves the processing of Personal Data relating to the Data Controller's customers, partners, employees or similar, depending on the Data Controller's specific use of the services as stated in the Master Agreement and as described in more detail in Appendix 1.

3. Rights and Obligations

3.1 General

The Parties shall comply with applicable Personal Privacy Legislation, regardless of the type of treatment (manual or automatic).

In the event of a conflict between the requirements of this Agreement and Personal Privacy Legislation, the latter has precedence.

3.2 The Data Controller's Rights and Obligations

(a) The Data Controller will provide the Data Processor with written instructions for the handling of personal data. If the Data Controller gives instructions to a subcontractor appointed in accordance with point 4, the Data Controller will inform the Data Processor accordingly. The Data Processor cannot be held responsible for the processing carried out by a subcontractor as a result of instructions from the Data Controller, and that results in breach of this Agreement, the Master Agreement or Personal Privacy Legislation.

(b) The Data Controller verifies that personal data is handled for legitimate and objective purposes, and that the Data Processor does not handle personal data to a greater extent than is necessary for its purpose.

(c) The Data Controller is responsible for there being a valid legal basis for the processing at the time when the personal data is transferred to the Data Processor. On request, the Data Controller will provide a written account and/or documentation for the legal basis for the processing.

(d) The Data Processor confirms that the registered persons that have supplied personal data have been properly notified and informed of the processing of their personal data.

3.3 The Data Processor's rights and obligations

(a) The Data Processor should only handle the personal data on behalf of the Data Controller and in accordance with written instructions from the Data Controller. The Data Processor cannot process other personal data than what is necessary to provide the services according to the Master Agreement. This may include the temporary processing, transformation, or routing of personal data through third-party systems, applications, or services that form part of the Data Controller's configured integrations or workflows.

(b) Unless otherwise agreed or provided by applicable law, the Data Controller will be entitled to require access to personal data processed by the Data Processor on behalf of the Data Controller. The Data Processor will assist the Data Controller in fulfilling the Data Controller's obligation to respond to requests that the registered persons file to exercise their rights as set out in Personal Privacy Legislation, including the right to access, correction, erasure, limitation, or objection to the processing, as well as to be provided with their own personal data in an appropriate and common format. The Data Processor is to be compensated for such assistance, by further agreement between the parties. If the Data Processor or Subcontractor (as defined below in Appendix 2) receives a request from a registered person regarding the processing of his or her personal data, the Data Processor should forward the request to the Data Controller, unless the Data Processor, according to applicable law or the Data Controller's instructions, can deal with the request.

(c) If the Data Processor or a Subcontractor receives a request from the relevant supervisory authority for access to, or information about, the registered personal data or processing under this Agreement, the Data Processor should notify the Data Controller, unless such notification is forbidden by law, or the Data Processor can handle the request according to the applicable legislation or the Data Controller's instructions.

(d) The Data Processor will assist the Data Controller in the conduct of a personal privacy consequence analysis if the Data Controller is obliged to undertake such an analysis. The Data Controller will cover the costs inflicted on the Data Processor as a result of its assistance.

(e) The Data Processor should not store the personal data longer than necessary in order to provide the services described in the Master Agreement, unless required by the Data Controller or applicable legislation. Processed personal data will be deleted automatically after 30 days.

(f) The Data Processor will ensure that employees are informed of the obligations in this Agreement, particularly in respect of security and protection of personal data.

4. Use of Subcontractors

4.1 The Data Processor should not appoint any other Data Processor ("Subcontractor") without prior written notification to the Data Controller. The Data Processor may engage additional Subcontractors where reasonably required to provide or support the services, including cloud infrastructure providers, integration platforms, analytics tools, support systems, or other technical service providers, provided that the Data Controller retains the right to object on reasonable grounds.

4.2 The Data Processor will inform the Data Controller of any changes or additions of Subcontractors, and the Data Controller has the right to oppose such changes.

4.3 The Data Processor will ensure that Subcontractors are subject to the same rights and obligations as the Data Processor in accordance with this Agreement and Personal Privacy Legislation by written agreement, including that the Subcontractor should provide adequate guarantees that technical and organizational measures are carried out that meet the requirements of Personal Privacy Legislation. The Data Controller and the relevant supervisory authorities should be provided with the access and information that is necessary for verification in connection with this. The Data Processor will be responsible to the Data Controller for ensuring that Subcontractors fulfil their obligations.

5. Personal data transfer

5.1 The transfer to, disclosure or access to personal data from countries outside the EU/EEA ("third countries") can only occur by prior written approval of the Data Controller and using the EU standard terms of use or based on any other legal basis for such transfer or disclosure.

6. Information security

6.1 The Data Processor will implement appropriate organisational and technical measures as set forth in the Personal Privacy Legislation and/or as imposed by the relevant supervisory authority to ensure adequate information security in order to achieve a suitable level of security. The Data Processor should evaluate the appropriate level of security and take action to safeguard the requirements to confidentiality, integrity and accessibility that correspond to the risk that the processing of personal data represents, including the risk of illegal destruction, loss, alteration, unauthorised disclosure, and access to personal data that is transmitted, stored, or otherwise processed. Upon request from the Data Controller, the Data Processor will provide information on relevant security measures taken by the Data Processor, in accordance with the Personal Privacy Legislation, to demonstrate compliance with the requirements set out in GDPR article 32. The Data Controller should maintain the level of security referred to above when the Data Processor exercises its services in the Data Controller’s technical environment.

6.2 All transfer of personal data between the parties or between the Data Processor and a third party must be carried out using adequate security measures, or as agreed between the parties.

6.3 The Data Processor will provide the necessary training to personnel with access to the personal data or information system regarding privacy protection, security and security requirements covered in this agreement.

7. Notification of security breach

7.1 If a personal data breach and/or other IT security breach ("Security Breaches") is detected, or if there is reason to believe that such has occurred, then the Data Processor shall notify the Data Controller without undue delay after becoming aware of such Security Breach. The Data Controller is responsible for reporting Security Breaches to the relevant supervisory authority.

7.2 The notification to the Data Controller should contain the information that is required according to Privacy Protection Legislation, including an adequate overview of the impact of the breach on the services, together with the corrective measures to be taken by the Data Processor.

7.3 The Data Processor will provide reasonable assistance so that the Data Controller can fulfil its obligations to provide comprehensive information to the relevant supervisory authority and the registered persons.

7.4 The Data Processor should execute the necessary and advisable corrective actions. The Data Processor will also cooperate with the Data Controller to prevent, minimise the consequences of, or correct Security Breaches.

8. Security checks and audit

8.1 The Data Controller and relevant supervisory authority have the right to carry out audits, including inspection of personal data that is being processed, systems used for this purpose, technical and organisational security measures, and Subcontractors.

The Data Controller has the right to conduct such an audit once a year. The audit should be limited to an assessment of whether the Data Processor meets its obligations in accordance with this Agreement. If the Data Controller appoints an external auditor to carry out the audit, the external auditor should not be a competitor of the Data Processor. Well in advance, the parties should agree to the timing and other details related to the implementation of such audits. The audit should not include access to information about third parties. Both Parties' representatives or external auditors participating in the audit will be subject to the duty of confidentiality in respect of the other Party.

8.2 The Data Controller will cover all expenses connected with the audit, and the Data Processor is entitled to compensation for all expenses incurred with the audit, including compensation to the Data Processor for reasonable elapsed time for Data Processor and its employees in respect of assistance during the audit. The Data Processor will nevertheless cover such costs if an audit discloses significant failure to comply with the obligations according to the Agreement or Personal Privacy Legislation.

9. Duty of confidentiality

9.1 The Data Processor, its Subcontractors, and others that perform services on behalf of the Data Processor and have access to personal data are subject to the duty of confidentiality and must comply with the duty of confidentiality in connection with the processing of personal data and security documentation in accordance with applicable Personal Privacy Legislation.

9.2 The Data Processor will ensure that all those acting on behalf of the Data Processor are subject to such duty of confidentiality and are informed of what their confidentiality obligations imply.

9.3 In the case of an order from public authorities for disclosure of personal data, the Data Processor will notify the Data Controller, unless otherwise provided by applicable legislation.

9.4 The Data Controller and representatives of the Data Controller, including external auditors who participate in the audits (see Section 8) or receive information from the Data Processor in accordance with this Agreement, are subject to the duty of confidentiality, unless otherwise provided by applicable legislation.

9.5 The duty of confidentiality also applies after the Agreement has been terminated. Employees or others who resign from their positions will be imposed the duty of confidentiality, also after termination of employment.

10. Limitation of liability

10.1 Neither party shall be liable to the other party for any indirect loss or consequential damages of any kind (including, but not limited to, losses resulting from interruption of operations, loss of data, loss of earnings or similar) notwithstanding any liability basis, whether by contract, fault-based liability, product liability or otherwise, even if the party is advised of the possibility of such damages (collectively referred to as "indirect loss").

10.2 Neither party shall be liable to the other party for;

a) failures or delays that lie beyond the reasonable control of the party, including general internet or line delays, power failures or machine malfunctions; or

b) failure caused by the other party's systems or actions, negligence, or omissions, which will be solely the party's responsibility.

10.3 The total and maximum liability for each twelve (12) month period, for either party to the other party during or in accordance with the Data Processing Agreement, should under no circumstances exceed an amount equivalent to the total amount paid (excluding VAT) for the Service under the Agreement over the twelve (12) months preceding the wrongful act.

10.4 The foregoing limitations will not apply to damages caused by fraud, gross negligence, or deliberate intent.

11. Agreement terms and termination

11.1 This agreement is valid from the date it is signed and until the Master Agreement expires, or until the obligations of the Data Processor to provide services in accordance with the Master Agreement are terminated, except for the provisions which continue to apply.

11.2 Upon termination of this Agreement, the Data Controller may require the return of personal data from the Data Processor (only data stored in backups) for a period of one month. The Data Processor should provide reasonable assistance in returning the personal data in a readable, accessible, and commercially sensible file format. The Data Controller will cover the Data Processor’s reasonable expenses associated with the return of personal data. After the return period, the Data Processor may delete the personal data without further notice, unless the agreement between the Data Processor and the Data Controller, or legislation require that the personal data be stored.

11.3 With respect to personal data stored on backup servers, this data should be erased in accordance with ordinary routines and industry standards.

11.4 On request from the Data Controller, the Data Processor should provide the Data Controller with written confirmation that all of the stated personal data has been returned or erased, unless otherwise provided by applicable legislation.

12. Applicable law and legal venue

12.1 The Agreement is subject to Norwegian law.

12.2 Both parties hereto submit to the exclusive jurisdiction of the courts of Norway for all disputes arising out of or in connection with this Agreement, with Oslo, Norway as their exclusive legal venue.

***

Appendix 1: Processing and the categories of personal data to be processed

The provision of the service may involve the processing of personal data and the Data Controller's customers, employees or other persons through their business applications and systems, depending on the Data Controller's specific use of services as described in the Master Agreement.

Processing may include the following categories of personal data, depending on the Data Controller's specific use of services as described in the Master Agreement;

a) General personal data, including name, telephone number, address, title, birth- and national insurance number, salary, email, information on education and training etc.

b) The content of email communication between employees or between customers or between employees and customers.

c) Special categories of personal data, including information that reveals racial or ethnic origin, political and religious standpoint, health information and union membership.

Appendix 2: Approved subcontractors

Data Processor has the following subcontractors:

Amazon Web Services
Technical platform for our cloud services: EU
ConnectMyApps uses AWS to run our platform and provide our cloud services. We store data on your account with us, and data on your connected applications and workflows.

Microsoft Azure
Technical platform for our cloud services: EU
ConnectMyApps uses Azure to run our platform and provide our cloud services. We may store data on your account with us, and data on your connected applications and workflows.

Amesto Group
Parent company of ConnectMyApps AS: EEA / EU
ConnectMyApps uses Amesto to handle invoicing and other client account management processes for our cloud-services. They maintain invoicing records in Norway. Amesto Group provide overall IT support and management of our Microsoft Office 365 platform.

Hubspot MAT provider
ConnectMyApps utilises HubSpot as a provider for marketing automation and email distribution services. HubSpot ensures that all data is processed and stored in compliance with applicable regulations, with data being maintained within the EU.

Overviu
Helpdesk software: Norway
ConnectMyApps uses Overviu for managing projects and for managing support tickets.

The Data Processor may from time to time appoint additional subcontractors in accordance with Section 4 of this Agreement where necessary for the delivery, support, or improvement of the services, including infrastructure, integration, analytics, security, support, or communications providers.