

DATA PROCESSING AGREEMENT

This data processing agreement ("**The Agreement**") was entered into on the date signed by the Customer on page 9 of the Agreement between

- (1) **The Customer**, as per the details signed on Page 7 of the Agreement ("**The Customer**" or "**Data Controller**") and
- (2) **ConnectMyApps AS**, a company that is subject to Norwegian law, with organization 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 Terms & Conditions 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 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**") from the time this enters into force and the at all times applicable national legislation relating to privacy protection, including legislation that implements or supplements GDPR (collectively named "**Personal Privacy Legislation**")

The Agreement will ensure that personal data is handled in accordance with Personal Privacy Legislation and is not used in an illegal manner or ends up in the possession of unauthorized persons

2.2 The Data Controller's right to administer the processing

The Data Controller determines the purpose of the processing and provides instructions. The Data Processor, its subcontractors, and others that, on behalf of the Data Processor, perform assignments and have access to personal data will carry out processing solely on behalf of the Data Controller and in accordance with this Agreement and 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 is in conflict with Personal Privacy Legislation.

2.3 The purpose of the data processing

The Agreement applies to the Data Processor's processing of personal data on behalf of the Data Controller. The purpose of processing personal data is that the Data Processor should provide services to the Data Controller in accordance with the Master Agreement, and that all rules and routines that the parties have agreed, are followed.

2.4 The scope 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.

2.5 Categories of personal data that are registered

The handling involves the processing of Personal Data relating to the Data Controller's customers or employees, 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 their 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
- (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 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) 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 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. The Data Processor will not correct, erase or lock personal data without instructions from the Data Controller, unless required by legislation
- (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 permission of the Data Controller
- 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 this connection. 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, 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 organizational 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, unauthorized disclosure and access to personal data that is transmitted, stored or otherwise processed. Upon request from the Data Controller, the Data Processor will provide documentation on security strategy and security measures. 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 Upon request, the Data Processor will provide documentation of technical and organizational measures implemented to ensure an adequate level of security. To the extent that the Data Processor has access to these, descriptions of any security measures that any Subcontractors have implemented also apply.

6.4 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 Breaches of personal data security and other security breaches ("Security Breaches") should be treated as deviations. If any deviation is detected, or if there is reason to believe that a deviation has occurred, then the Data Processor should notify the Data Controller without undue delay. 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 Processor will provide the Data Controller, upon request, with documentation on technical and organisational measures that have been carried out to ensure a suitable level of security, along with other information necessary to document that the Data Processor meets its obligations in accordance with this Agreement and the Personal Privacy Legislation

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 organizational 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 other customers that the Data Processor holds, or information about how the Data Processor implements security measures. All the Data Processor's representatives or external auditors participating in the audit will be subject to the duty of confidentiality in respect of the Data Processor.

- 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. RESPONSIBILITY

- 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 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,

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 or employees through applications, files and databases including but not limited to ERP, CRM, e-commerce and/or HRS information 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, email, information on education 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

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 Any dispute or claim arising out of this Agreement should be resolved by Oslo District Court.

This Agreement is in 2 – two originals, one to each of the parties.

On behalf of the Data Controller

On behalf of the Data Processor

.....
(name)

Luke Buckley
(name)

.....
(job title)

CEO
(job title)

.....
(company name)

ConnectMyApps AS
(company name)


.....
(company number)

913 244 990
(company number)

.....
(place and date)

Oslo, Norway, 24 May 2018
(place and date)

.....
(signature)


(signature)

Appendix 2: Approved subcontractors

Data Processor has the following subcontractors

Daxx Soft BV
Zaandijkeweg 8, 1521AX WORMERVEER, Netherlands
Registration number 34278628
Perform integration development services

Amesto Group AS
Smeltingen 1, 0195, Oslo, Norway
Org nr 979 482 639
Perform invoicing services