EFFECT IO

STANDARD DATA PROCESSING AGREEMENT

This data processing agreement ("**DPA**"), dated 13.01.2022 is between:

(1) _____ (customer name) a company incorporated under the laws of _____ with registration number _____ (the "**Data Controller**"); and

(2) **Effect IO AS,** a company incorporated under the laws of Norway with registration number NO912416585 (the "**Data Processor**")

(each individually referred to as a "**Party**" and both referred as "**Parties**").

1. INTRODUCTION

1.1 The Data Processor's fulfilment of the Data Processing Agreement entered into by the Parties (the "**Agreement**") will involve Processing of Personal Data subject to statutory provisions and obligations under relevant Privacy Laws (as defined in Clause 3).

1.2 For purposes of this DPA, the terms "Personal Data", "Processor", "Controller", "Data Subjects" and "Processing" shall have the meaning set out in Regulation EU 2016/679.

1.3 This DPA governs the Parties' rights and obligations with regard to all Processing of Personal Data on behalf of the Data Controller under the Agreement in order to ensure that all Processing is conducted in compliance with applicable privacy and data protection legislation.

1.4 The parties acknowledge that Effect IO will act as a Data Controller and that the Effect IO customer will act as a Data Processor with respect to the Processing of Personal Data under this DPA, or the role as applies under applicable legislation.

2. SUBJECT MATTER OF THIS AGREEMENT AND EXTENT OF THE DATA PROCESSING

2.1 Purpose

The purpose of the Processing of Personal Data is for the Data Processor to render Services to the Data Controller in accordance with the Agreement, and that all rules, regulations and operating procedures agreed between the parties are complied with. Reference is made to the specifications of the Services in Schedule 2 of the Agreement.

2.2 The Controller's right to manage the processing

The Data Controller shall have the full power of disposition regarding the Personal Data. The Data Processor shall perform the Processing only on and as per the documented, legitimate and reasonable instructions from the Data Controller, and in accordance with the Agreement, unless required to do otherwise by law. In the latter case the Data Processor shall inform the Data Controller of such deviating legal requirement (provided that the laws do not prohibit such notification).

The Data Processor

a) will not acquire any rights in or to the Personal Data;
b) will not use the Personal Data for any purpose other than those covered in the instructions from the Data Controller; and
c) will not disclose the Personal Data to Third Parties without the prior written approval of the Data Controller, unless required to do so by law.

2.3 Processing activities

The Data Processor will in agreement with Data Controller point out one or more administrator that can access the Data Controller's setup and data in order to carry out support services. This includes, but is not limited to, the following processing activities:

- Identification of information of the Data Controller's projects, respondents and client companies
- Identification of the Data Controller users
- Identification of users and respondent's technical setup in scope of using the service

The processing activities will take place as long as the Services are provided under the Agreement and storing of Personal Data to the extent permissible under the DPA and applicable law.

2.4 The types of personal data that will be processed

The following overview lists the categories of Data Subjects which are encompassed by the processing, what types of Personal Data is to be processed and if any special categories of Personal Data will be part of the processing are listed in Annex 1.

In addition to the Personal Data and categories listed in Annex 1, the Data Processor will only process other relevant Personal Data that is strictly in order to perform the services as described in the DPA.

3. RIGHTS AND OBLIGATIONS

3.1 General

The Parties will comply with all laws and regulations in force from time to time, collectively referred to as "Privacy Laws", and regardless of the type of processing (manual or automatic). This includes, but is not limited to:

(a) all national and local laws, as well as all applicable rules, regulations, directives and governmental requirements relating in any way to processing of Personal Data;

(b) the General Data Protection Regulation (Regulation EU 2016/679).

To the extent there is a conflict between the requirements of this DPA and mandatory Privacy Laws, the mandatory requirements of such Privacy Laws will prevail.

3.2 Rights and obligations of the Data Controller

The Data Controller shall:

(a) Ensure that appropriate technical and organisational measures are in place for the data processing to be performed in accordance with Privacy Laws

(b) give the Data Processor documented instructions on the Processing, which instructions shall comply with the Agreement and applicable law;

(c) have the right and obligation to specify the purpose and means of Processing of Personal Data;

(d) represent that all the data subjects of the Personal Data have been provided with appropriate notices and information and establish and maintain for the relevant term the necessary legal grounds for processing the Personal Data;

(e) confirm that it has provided the Data Processor with all necessary information in order for the Data Processor to perform the Processing in compliance with law.

3.3 Rights and obligations for the Data Processor

The Data Processor assumes the following obligations:

(a) Advise the Data Controller regarding appropriate technical and organisational measures required for the fulfilment of the Data Controller's obligations under Privacy Laws and relevant for this DPA.

(b) To process the Personal Data only on behalf of Data Controller, and in accordance with the instructions provided by Data Controller, and not for any other purposes. If the Data Processor cannot provide such compliance for whatever reasons, the Data Processor agrees to inform promptly the Data Controller of its inability to comply, in which case the Data Controller is entitled to suspend the transfer of data. The Data Processor will treat as strictly confidential any Personal Data provided by Data Controller whenever access to such data is required to render the Services.

(c) Apply the necessary security measures in accordance with applicable laws and regulations on data protection in force from time to time and in general, implement the appropriate safety, technical and organizational measures to safeguard the Personal Data from unauthorized or unlawful amendments, access to, processing or accidental loss, destruction or damage;

(d) Ensure that each of its personnel are made aware of its obligations under this DPA with regard to the security and protection of the Personal Data and take all reasonable steps to ensure the reliability of any of its personnel who have access to the Personal Data.

(e) Taking into account the nature of the Processing, the Data Processor will co-operate as requested by the Data Controller by providing reasonable assistance and information to the Data Controller to allow the Data Controller to perform its obligations under the Privacy Laws and, in particular, the obligation to provide Data Subjects access to Personal Data and other rights that Data Subjects may have, such as the right to rectification, deletion and restriction. The same applies where the Data Controller is required to deal or comply with any assessment, enquiry, notice

or investigation by a data protection supervisory authority within scope of the Agreement and this DPA.

(f) In the event that the Data Processor or the Data Controller receives a request from a data protection supervisory authority relevant to this DPA, to provide to the Data Controller and the data protection supervisory authority a written description of the data protection measures established by the Data Processor and any of its Subcontractors, in order to demonstrate that the processing operations are in compliance with Privacy Laws.

(g) The Data Processor will not retain Personal Data for longer than is necessary to perform the Services described in the Agreement unless otherwise required by the Data Controller, including in the Data Controller's records retention policies or other requirements. The Data Processor will not correct, delete or lock Personal Data without a corresponding instruction of the Data Controller, unless required by law.

4. USE OF SUB-DATA PROCESSORS

4.1 The Data Processor shall not sub-contract any of the Processing assigned to him by the Data Controller to any other entity without the express, prior written consent of the Data Controller, such consent not to be unreasonably withheld. By signing of this DPA, the Data Controller has accepted the sub-data processors listed in Annex 2.

4.2 Any third party Processing Personal Data on behalf of the Data Processor shall be subject to the same rights and obligations as those imposed on the Data Processor pursuant to this DPA. If any third party processor fails to fulfil its data protection obligations, the Data Processor shall remain liable to the Data Controller for the performance of that other processor's obligations in accordance with section 17 of the Agreement. The limitation of liability applies correspondingly; see section 10 of this DPA.

5. TRANSFER OF PERSONAL DATA

5.1 The Data Processor will only transfer Personal Data out of the territory of the member states of the European Union, the European Economic Area, or other countries which the European Commission has found to guarantee an adequate level of data protection (collectively, the "Approved Jurisdictions") with the Data Controller's prior written consent.

5.2 If required by applicable legislation, the Data Processor shall enter into relevant contractual arrangements with required parties (including with the Data Controller itself or any of the Data Controller's Affiliates) for the lawful transfer of Personal Data from the Approved Jurisdiction to third countries.

6. INFORMATION SECURITY

6.1 The Data Processor will implement planned, systematic, organisational and technical measures to ensure satisfactory information security with regard to confidentiality, integrity and availability in connection with the information security provisions in applicable Privacy Laws, and to protect against accidental or unlawful destruction, loss, alteration or unauthorized disclosure of and access to Personal Data (hereinafter "Personal Data Breach").

6.2 Further, the Data Processor will maintain and implement a written information security program that includes appropriate administrative, technical and physical safeguards and other security measures designed to:

(a) protect the security and confidentiality of Personal Data;

(b) protect against any anticipated threats or hazards to the security and integrity of Personal Data; and

(c) protect against any Personal Data Breach and unauthorized access to, acquisition of, or use of the data processing equipment used to process Personal Data

6.3 The Data Processor will adopt all reasonable recommendations the Data Controller makes concerning data security measures, programs and procedures to ensure ongoing compliance with this DPA and applicable law.

7. PERSONAL DATA BREACH AND NOTIFICATION

7.1 The Data Processor shall promptly notify the Data Controller upon becoming aware of a Personal Data Breach, and in no event shall such notice be given later than 48 hours after the breach occurred. Such notice will summarize in reasonable detail the effect of the breach on the Services, and the corrective action to be taken by the Data Processor.

7.2 The Data Processor will promptly take necessary and advisable corrective actions, and will cooperate with the Data Controller to prevent, mitigate or rectify such Personal Data Breach**.**

8. SECURITY AUDITS

8.1 The Data Processor will comply with reasonable requests made in writing by the Data Controller to audit the Data Processor's Processing activities necessary to enable the Data Controller to verify that the Data Processor is complying with its obligations under this DPA and Privacy Laws.

8.2 The Data Controller is obligated to use external auditors who are not competitors of the Data Processor, to conduct such an audit. The Parties shall agree well in advance on the time and other details relating to the conduct of such audits.

8.3 The Data Processor shall immediately inform the Data Controller if, in the Data Processor's opinion, an instruction given in relation to an audit infringes this Privacy Laws.

8.4 The audit shall be conducted in such a manner that the Data Processor's undertakings towards third parties or authorities are in no way jeopardized. All the Data Controller's representatives or external auditors participating in the Audit shall execute customary confidentiality undertakings towards the Data Processor.

8.5 The Data Controller shall bear all audit expenses, and compensate the Data Processor for any and all costs incurred as a result of the audit; provided, however, that if the audit reveals material deficiencies in the Data Processor's performance, the Data Processor shall bear its own costs for the audit.

9. CONFIDENTIALITY

9.1 The Data Processor shall (i) keep any Personal Data received from the Data Controller confidential, (ii) ensure that persons authorized to process the Personal Data have committed themselves to confidentiality, and (iii) ensure that Personal Data is not disclosed to third parties without the Data Controller's prior written consent, unless the Data Processor is obliged by mandatory law or decree to disclose such information.

9.2 In case data subjects or governmental authorities make a request concerning Personal Data, the Data Processor shall, as soon as reasonably possible, inform the Data Controller about such requests prior to providing any response or taking other action concerning the Personal Data, or, in case any applicable authority prescribes an immediate response, as soon as reasonably possible thereafter unless the Supplier is prohibited by mandatory law or authority order to disclose such information.

9.3 All the Data Controller's representatives, including any external auditors, participating in audits (see section 8) or receiving information from the Data Processor in accordance with this DPA, shall keep the information confidential unless by law required to inform authorities or the Data Subjects.

10. LIABILITY

10.1 In the event of breach of this DPA, or obligations according to applicable Privacy Laws, the relevant provisions regarding breach in the Agreement shall apply. The limitations of liability set out under the Agreement shall apply also to this DPA**.**

10.2 The Data Processor shall notify the Data Controller without undue delay if it is or is likely to become unable to comply with any of its obligations under this DPA.

11. TERM AND TERMINATION OF THE AGREEMENT

11.1 This DPA shall be effective from the date of signature and until the Agreement expires, or until the Data Processor's obligations in relation to the performance of Services in accordance with the Agreement is otherwise terminated, except for those provisions in the Agreement and this DPA that continues to apply after such termination.

11.2 Once this Agreement is terminated, and no later than three months after termination of this Agreement, all Personal Data, the documents, data media and all the means where the Personal Data were recorded must be handed back to the Data Controller or destroyed/deleted in accordance with data protection regulations after prior instruction of the Data Controller. If the Data Controller finds that it is not reasonably and practical to hand back, the Personal Data shall be destroyed/deleted by the Data Processor. With regard to Personal Data stored on back up servers, the data shall be deleted in accordance with ordinary routines and industry standards.

11.3 The Data Processor shall provide to the Data Controller a written declaration whereby the Data Processor warrants that all data mentioned above has been returned or deleted according to the Data Controller's instructions, including any

copies or backup, unless any Privacy Laws requires storage of the personal data.

12. DISPUTE AND JURISDICTION

12.1 This Agreement shall be governed by and construed in accordance with the provisions set out in Agreement, save for mandatory provisions in applicable Privacy Laws.

12.2 Any dispute arising out of this DPA shall be resolved in accordance with the provisions as set out in the Agreement.

On behalf of Data Controller	Data Processor (Effect IO)
_____ (signature)	_____ Frode Jakhelln Laugen
Date:	Date: 13.01.2022

Annex 1: The types of personal data that will be processed

The list below is general, as each survey will have unique data that will be saved for every respondent.

Categories of Data Subjects	**Type of Personal Data**	**Special categories of Personal Data etc.**
Tenant company user (Effect IO's customer, Data controller company)	Email, name, user name, gender, phone number, job title, IP address	
Client company user (client of Effect IO's tenant customer)	Email, name, user name, gender, phone number, job title, IP address	
Respondent	Email, name, gender, phone number, IP address Survey responses	Which data the respondents answers to surveys is controlled by configuration made by Data Controller. It is Data Controllers responsibility that these data are following the relevant laws
Report user	Email, name, phone number, IP address and accessible reports	

In addition to the Personal Data and categories listed above, the Data Processor will only process other relevant Personal Data that is strictly required in order to perform the services as described in the DPA.

Annex 2: Approved Sub-processors

The Data Controller has accepted the following sub-processors:

Data is stored within the European Union with one exception. The following are the companies' relevant office addresses. We have signed a direct DPA with Postmarkapp to be compliant after Schrems II ruling.

Name	Address	Scope
Amazon Web Services	Domagkstraße 28, 80807 München Germany	**Data center (servers, database)** All application data is stored here. We are using Frankfurt as default site and Stockholm region as backup site.
Postmarkapp	Wildbit 1800 JFK Blvd., Suite 300 #96864 Philadelphia, PA 19103United States	**Email delivery services** Email addresses, names, email content and links are stored here
N-IX	157 Archbishop St Valletta, VLT 1440 Malta	**Programming services** Do not store data. Can access production setup on request, for custom development purposes
GatewayAPI	CC/ Online City Danneskiold-Samsøes Allé 41 1434 København K Denmark	**SMS provider** Phone number, SMS text and links are stored here
Tripletex	Karenslyst allé 56 0277 Oslo Norway	**Accounting software** Invoices and information regarding Effect IO's customer invoices. Name and email of payment contact.
Gerhard & sønn	Schweigaards gate 34E 0191 Oslo Norway	**Accountant** Gets access to information regarding Effect IO's customer invoices. Name and email of payment contact.

Changelog

01.06.2021: Mailgun was replaced with Postmarkapp

13.01.2022: Removed Datadog and Freshdesk as sub-processors. Added AWS Stockholm region as backup site for disaster recovery.