Data Processor Agreement

This Data Processing Agreement (the "**DPA**") is made between the Customer (the "**Data Controller**"). and Fieldly (the "**Data Processor**");

The parties listed above are hereinafter referred to as the "**Parties**" and each of them separately as a "**Party**".

1 BACKGROUND

1.1 The Parties have entered into an agreement where the Data Processor shall provide a digital project management tool specially designed and developed for the construction industry to the Data Controller (the **"Main Agreement"** or "**Terms & Conditions**").

1.2 In connection with the Data Processor's performance of its obligations under the Main Agreement, the Data Processor may from time to time and on behalf of the Data Controller process Personal Data, as further detailed in Appendix 1. In consideration hereof the Parties enter into this DPA.

2 DEFINITIONS

In this DPA, capitalized terms shall have the same meaning ascribed to them under the GDPR. In addition, the following capitalized terms shall have the meanings ascribed to them below, and references to the singular shall include the plural and vice versa.

"**Data Privacy Laws**"	means any law and regulation in force at any time concerning the processing of personal data, including but not limited to the GDPR, other European Union legislation relating to the processing of personal data, national legislation implemented under and in compliance with the GDPR and the decisions, advice, recommendations and opinions of the Supervisory Authority.
"**EU Model Clauses**"	means the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.
"**GDPR**"	means 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 and repealing Directive 95/46/EC (General Data Protection Regulation).

3 PROCESSING OF PERSONAL DATA

3.1 The Data Processor undertakes to comply with applicable Data Privacy Laws and recommendations by the Supervisory Authority or other competent authorities.

3.2 The Data Processor undertakes to only process Personal Data to the extent necessary to fulfil its undertakings under the Main Agreement, and only in accordance with the Data Controller's written instructions, Appendix 1. The Data Processor may not process the Personal Data for its own purpose(s).

3.3 The Data Processor shall immediately inform the Data Controller if the Data Processor lacks an instruction on how to process Personal Data in a particular situation or if it believes an instruction provided under this DPA infringes applicable Data Privacy Laws

3.4 If the Data Processor processes Personal Data in addition to or in violation of the Data Controller's instructions, due to being required to do so by Union or Member State law to which the Data Processor is subject, the Data Processor shall inform the Data Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

3.5 If Data Subjects, competent authorities, or any other third parties request information from the Data Processor regarding the processing of Personal Data covered by this DPA, the Data Processor shall refer such request to the Data Controller as soon as possible and no later than twenty-four (24) hours after receipt of such request. The Data Processor shall assist the Data Controller to fulfill its obligations to respond to requests from Supervisory Authorities and Data Subjects to exercise their rights under Chapter III of the GDPR.

3.6 The Data Processor shall, upon the Data Controller's request, assist the Data Controller with carrying out Data Protection Impact Assessment(s) where required under applicable Data Privacy Laws. The Data Processor shall in particular assist with:

(i) Describing the nature of the processing, including the Personal Data involved and the processing location;

(ii) Identifying and assessing risks to the rights and freedoms of Data Subjects;

(iii) Providing information on the technical and organizational measures and safeguards taken or envisaged to address the identified risks in order to ensure the protection of Personal Data processed under this DPA; and

(iv) Providing detailed information on any other parties involved in the processing of Personal Data (including information on their part of the process and their location).

3.7 Upon the Data Controller's request, the Data Processor shall assist the Data Controller with carrying out prior consultations with the Supervisory Authority, where such consultations are required under applicable Data Privacy Laws.

3.8 The Data Processor shall immediately (and in no case later than twenty-four (24) hours) upon becoming aware of a Personal Data Breach notify the Data Controller in writing thereof, providing a detailed description of the Personal Data Breach and its effects. If the Data Controller so requests, the Data Processor shall assist the Data Controller in fulfilling the Data Controller's obligations under Article 33 of the GDPR, such as:

(i) In writing provide the Data Controller with a detailed statement of the nature of the Personal Data Breach in accordance with what is stated in Article 33.3(a) in the GDPR;

(ii) In consultation with the Data Controller and at Data Processor's cost take all reasonable steps necessary to mitigate the consequences of the Personal Data Breach or (if applicable) to protect against a threatened security incident; and

(iii) As soon as practicable following the Personal Data Breach, inform the Data Controller of the remedial action(s) the Data Processor proposes to take to prevent any similar security incident occurring in the future.

4 THE DATA CONTROLLER'S UNDERTAKINGS

4.1 The Data Controller shall provide clear and documented instructions to the Data Processor. The Data Controller may update the instructions at any time. Updated instructions shall be communicated in writing, using the form in Appendix 1.

4.2 The Data Controller is responsible for ensuring that the instructions provided to the Data Processor comply with the requirements of the Data Privacy Laws.

4.3 The Data Controller undertakes to oversee and audit the Data Processor's processing activities in accordance with the terms of this DPA.

5 SUB-PROCESSORS

5.1 The Data Processor shall notify the Data Controller in writing of the intention to engage new Sub-Processors or make changes to the already engaged Sub-Processors, giving the Data Controller at least fourteen (14) days to object to such changes. Sub-Processors approved by the Data Controller are listed in Appendix 1 (to be updated in case of changes).

5.2 The Data Processor shall ensure that any Sub-Processors approved by the Data Controller are bound by written agreements that require them to comply with corresponding data processing obligations to those contained in this DPA and that meet the requirements of Article 28(3) of the GDPR.

5.3 If the Sub-Processor fails to perform its obligations, the Data Processor shall be fully liable to the Data Controller for the due performance of the Sub-Processor's obligations.

6 TECHNICAL AND ORGANISATIONAL MEASURES

6.1 The Data Processor guarantees that it has implemented and, during the term of this DPA, will continue to implement and maintain appropriate technical and organizational measures to ensure that the Data Processor's processing of the Personal Data under this DPA meets the requirements of the Data Privacy Laws (such as Article 32 of the GDPR) and ensures that the rights of Data Subjects can be upheld. The measures implemented by the Data Processor must provide a level of security appropriate to the risk, taking into account existing technical possibilities, costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

6.2 The Data Processor shall be obliged to ensure that only personnel that directly require access to Personal Data in order to fulfil the Data Processor's obligations in accordance with this DPA have access to such information. The Data Processor shall ensure that such personnel are bound by a confidentiality obligation to the same extent as the Data Processor in accordance with this DPA and that they are informed how they may process the Personal Data.

6.3 The security measures agreed between the Parties are set out in Appendix 1. In addition, the Data Processor shall provide the Data Controller with documentation of the technical and organizational measures that are going to be or have been implemented by the Data Processor. The Data Controller may demand that additional measures are implemented from time to time.

7 DATA LOCALISATION

7.1 The Data Processor may not, without the prior written consent of the Data Controller, transfer Personal Data outside the EU/EEA. If the Data Processor wishes to transfer Personal Data outside the EU/EEA, it shall provide the Data Controller with a Data Transfer Impact Assessment ("**DTIA**"), supporting such transfer. If the Data Controller approves of the transfer, the Parties shall ensure that there is a valid transfer mechanism in place (including additional safeguards, if necessary), before the transfer commence.

7.2 If, subject to the approval of the Data Controller, the Data Processor will transfer Personal Data to a third party outside the EU/EEA, the Data Processor shall enter into the applicable EU Model Clauses with the data importer – if this is identified as the most appropriate transfer mechanism.

7.3 The Data Controller shall, at any time, have the right to revoke its consent to third country transfers in accordance with sections 7.1 - 7.2. In such event, the Data Processor shall immediately cease with transfer and shall, at the request of the Data Controller, provide written confirmation that the transfer has ceased.

8 AUDIT RIGHTS

8.1 Upon the Data Controller's request, the Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with this DPA and the Data Privacy Laws. This includes records on the Data Processor's processing of Personal Data under this DPA, as well as applicable privacy policies, sub-processing agreements, confidentiality undertakings, records of personal data breaches, and any other such information necessary for the Data Controller to verify the Data Processor's compliance with this DPA.

8.2 The Data Controller may request audit of the Data Processor's processing of Personal Data one (1) time per calendar year – unless the previous audit identified deviations from this DPA or applicable Data Privacy Laws. If so, the Data Controller may request additional audits each month until such deviations have been managed and the Data Processor provides sufficient evidence that it is in full compliance with this DPA and Data Privacy Laws.

8.3 The Data Processor will, during normal business hours and upon reasonable notice (whereby a notice period of ten (10) business days shall always be deemed reasonable), provide to the Data Controller's personnel or its hired consultants, its internal or external auditors, inspectors, and regulators reasonable access to the parts of facilities where the Data Processor is carrying out processing activities, to personnel, and to data and records (including tools and procedures) relating to the processing. The Data Controller's auditors and other representatives shall comply with the Data Processor's reasonable work rules, security requirements and standards when conducting site visits.

9 LIABILITY

Liability under this DPA shall be settled in accordance with the provisions of the Agreement.

10 CONFIDENTIALITY

10.1 The Data Processor undertakes not to disclose or reveal the Personal Data or other information received by the Data Processor as a result of this DPA, to third parties other than Sub-Processors that have been engaged in accordance with this DPA.

10.2 The obligations set out in this Section 10 do not include information disclosed in accordance with the instructions of the Data Controller or that the Data Processor is required to disclose pursuant to law, enactment, court's or other governmental authority's decision or stock exchange regulation. The Data Processor shall promptly and in writing notify the Data Controller if the Data Processor is required to disclose such information.

10.3 The confidentiality obligation in this paragraph 10 also applies after the expiration of this DPA.

11 RETURN OF DATA ETC.

Upon expiry of this DPA, the Data Processor shall, at the choice of the Data Controller, delete or return all Personal Data to the Data Controller and shall ensure that any Sub-Processor does the same, unless it is required to keep copies of the data under Union or Member State law to which the Data Processor is subject.

12 TERM

This DPA shall take effect as of the date of signing by both Parties and remain effective as long as the Data Processor processes Personal Data on behalf of the Data Controller.

13 ASSIGNMENT

Neither Party may assign its rights and/or obligations under this DPA without the prior written consent of the other Party.

14 APPLICABLE LAW

This DPA shall be governed by, construed and enforced in accordance with the laws of Sweden.

APPENDIX 1

INSTRUCTION REGARDING PROCESSING

15 INTRODUCTION

This Appendix 1 specifies the processing of Personal Data carried out by the Data Processor on behalf of the Data Controller under the DPA.

The purpose is to clarify the processing and Personal Data that is covered by the Main Agreement and to comply with the GDPR's requirements.

16 INSTRUCTIONS

<table>
<tr><td>2</td><td colspan="4">Processing</td></tr>
<tr><td>2.1</td><td>The purposes and categories of the processing</td><td colspan="3">The Personal Data are processed for the purpose of supplying the services under the Main Agreement.
The Data Processor will perform the following categories of processing:
☒ Storage
☒ Administration
☐ Access in connection with support
☐ Other _____</td></tr>
<tr><td rowspan="2">2.2</td><td rowspan="2">Categories of Data Subjects</td><td>☒ Employees, including contractors, (external consultants), temporary employees</td><td>☒ Merchant representatives</td><td>☐ Partner representatives</td></tr>
<tr><td>☒ Prospects</td><td>☒ End-customers</td><td>☒ Others</td></tr>
<tr><td rowspan="5">2.3</td><td rowspan="5">Categories of Personal Data</td><td colspan="3">☒ Payment data, such as Credit card details</td></tr>
<tr><td colspan="3">☒ Contact information, including name, telephone number, e-mail address, etc.</td></tr>
<tr><td colspan="3">☐ IT administrative data such as data related to the services provided including technical features, user names, location, contact details, communication data and metadata as well as technical events related to the services offered including system and application logs.</td></tr>
<tr><td colspan="3">☐ Security data such as security logs, facility and system surveillance data and information about security breaches.</td></tr>
<tr><td colspan="3">☒ Employee and personal data (HR) such as names, addresses, contact details, age, date of birth, personal designation, information</td></tr>
</table>

		related to the data subject's employment, including career history, sick leave, recruitment information, rehabilitation information and information about terminations, employee assessments/appraisals and competence development.			
		☒ **Website data**, such as IP address, how the visitor has interacted with the website, etc.			
		☐ Other			
2.4	**Sensitive Personal Data – if any**	☐ Racial or ethnic origin	☐ Trade union membership	☐ Data concerning a natural person's sex life or sexual orientation	☐ Political opinions
		☐ Processing of genetic data or biometric data for the purpose of uniquely identifying a natural person	☐ Personal data relating to criminal convictions and offences or thereby related security measures	☐ Religious or political beliefs	☐ Health data
2.5	**Geography**				
2.5.1	**The Personal Data will be processed (*e.g.* stored or accessed) in the following locations**	Personal Data may only be processed in ☒ Within the territory of the European Union (EU) or the European Economic Area (EEA, *i.e.* Norway, Iceland and Lichtenstein) ☐ Within EU/EEA and also transferred to the following country/-ies outside EU/EEA: _____ (in which case 2.5.2 below must also be filled in)			
2.5.2	**Personal Data will be transferred outside of the EU/EEA and an adequate level of protection:**				
	☐ Has been determined by the European Commission (Article 45(3))				
	☐ Is a result of Binding Corporate Rules (Article 46(2)(b) and Article 47)				
	☐ Is a result of an agreement regarding the EU's standard clauses, entered into by the Parties (Article 46(2)(c) and (d)				

	☐ Is a result of approved codes of conduct (Article 46(2)(e) and Article 40)
	☐ Is a result of approved certification (Article 46(2)(f) and Article 42)
	☐ Has been otherwise secured (Article 46(2)(a) and 46(3)(a) and (b))
2.6	**Erasure procedures**
2.6.1	*The processing of Personal Data may only continue for as long as there is a legal basis for the processing. When the legal basis for processing no longer exists, the processing shall stop, and erasure must take place*
2.6.2	*The Data Processor shall erase the Personal Data according to the following procedures, on condition that the Data Controller has informed the Data Processor that the legal basis for processing has expired:* ☒ When the filing period expires after 7 years: The Personal Data must then be completely erased (including back-ups). ☒ When the Data Subject requests that deletion takes place: The Personal Data must then be completely erased (including back-ups). However, erasure must not take place to the extent that a different legal basis for processing exists. ☐ When the Main Agreement expires: The Data Processor and any Sub-Processor (depending on what the Data Controller decides) shall either return all transferred Personal Data and any copies to the Data Controller or destroy all Personal Data. ☐ _____ ☐ _____
2.6.3	*At erasure, the Data Processor must be able to ensure that all Personal Data have been completely erased (albeit taking any legal requirements for archiving/filing into consideration).*

17 TECHNICAL AND ORGANISATIONAL MEASURES

17.1 The following instructions on technical and organizational measures are supplementary instructions to what is otherwise stated in the DPA and that follows from Data Privacy Laws. To avoid any uncertainty these instructions are not in any way intended to limit the Data Processor's responsibilities and obligation under the Data Privacy Laws.

17.2 To achieve an adequate level of security, the Data Processor shall take the following measures:

(i) The pseudonymisation and encryption of Personal Data when appropriate;

(ii) Physical access protection whereby computer equipment and removable data containing personal information at the Data Processor's premises shall be locked up when not under supervision in order to protect against unauthorized use, impact and theft;

(iii) A process for testing read back after Personal Data has been restored from backup copies;

(iv) Authorization control whereby access to the Personal Data is managed through a technical system from authorization control. Authorization shall be restricted to those who need the Personal Data for their work. User IDs and passwords shall be personal and may not be transferred to anyone else. There shall be procedures for allocating and removing authorizations;

(v) The ability to log access to the Personal Data. It shall be possible to follow up access to the Personal Data retrospectively through a log or similar information base. It shall be possible for the Data Processor to check the information base and report back to the Data Controller;

(vi) Secure communication whereby external data communication connections shall be protected using technical functions ensuring that the connection is authorized as well as content encryption for data in transit in communication channels outside systems controlled by the Data Processor;

(vii) A process for ensuring secure data destruction when fixed or removable storage media shall no longer be used for their purpose;

(viii) Routines for entering into confidentiality agreements with suppliers providing repair and service of equipment used to store Personal Data; and

(ix) Routines for supervising the service performed by suppliers at the premises of the Data Processor. Storage media containing the Personal Data shall be removed if supervision is not possible.

18 LIST OF SUB-PROCESSORS APPROVED BY DATA CONTROLLER

The Data Controller has approved the Sub-Processors listed below for processing under the DPA:

Name and reg. no.	Location	Types of processing
Amazon Web Services (AWS)	Sweden Germany Ireland	Hosting services
Digital Ocean	Netherlands Germany	Hosting services