

Data processing agreement

FieldTechie ApS · Version 2026-10-14

Translation of the Danish pack. The Danish version prevails.

What is this?

When you use FieldTechie, we store and process personal data for you: your employees, your customers, and the people who appear in your jobs. You decide what happens to that data. We may only do what you ask us to.

Article 28 of the GDPR requires this to be set out in a written agreement. This is that agreement.

What is in the pack

Part	What it is
Parties (next page)	Who the agreement is between. Our details are filled in; your fields are blank
The Clauses	Datatilsynet's own standard text (March 2024), word for word. We have not changed a comma
Appendix A	Which personal data we process, about whom, and for how long
Appendix B	The sub-processors we use, and what they can reach
Appendix C	Your instruction to us, and the security measures we have
Appendix D	What the parties agree beyond that

Why Datatilsynet's text? The Danish supervisory authority adopted it as standard contractual clauses. If we use it unchanged, neither you nor your adviser needs to review the contract text itself. What is worth reading is the appendices — and we have written those as concretely as we can.

The short version

- **Where is your data?** At Scaleway in Paris. The database is yours alone, not shared.
- **Who else touches it?** The four companies in Appendix B. Maps and address search come from

Google, and so do push notifications — it says so there, and we do not claim everything stays in the EU.

- **Who at FieldTechie can see it?** Today one person, and only for operation and support.
- **If something goes wrong:** we tell you within 24 hours of discovering it. You then have 72 hours to notify the authority.
- **If you leave:** you can view everything and export lists for 30 days, and on request we send you a complete copy of all your data. After that we delete all of it within 60 days and confirm it in writing.
- **Deletion means deletion.** We do not just mark data as deleted.

What do you need to do?

- **Accepting at signup?** The agreement is made when you tick the subscription terms. We record the time, the version and who accepted. You do not have to sign anything.
- **Want a signed copy?** Fill in your fields on the next page and we will send it for signature.
- **Do your own employees need to know anything?** Yes. If you use GPS tracking or time registration, it is you who must inform your employees. We are happy to help with the wording.

Questions? Write to privacy@fieldtechie.com. You will get an answer from a person who helped build the system.

Standard Contractual Clauses

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

The data controller (the customer)

Name

Company reg. no.

Address

Postcode and city

Country

Contact person for the agreement

Name

Position

Telephone

Email

(the data controller)

and

The data processor

Name FieldTechie ApS

Company reg. no. 46686721

Address Mispelvej 1

Postcode and city 9500 Hobro

Country Denmark

Contact person for the agreement

Name Lars Søgaard Jensen

Position Managing Director

Email privacy@fieldtechie.com

(the data processor)

each a 'party'; together 'the parties'

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

Commencement

The agreement takes effect when the data controller accepts the subscription terms and the accompanying data processing agreement at signup, or when both parties have signed below.

	The data controller	The data processor
Name	Lars Søgaard Jensen	
Position	Managing Director	
Date		
Signature		

This sheet reproduces the standard text's front page word for word, with the parties filled in. It replaces the standard text's front page with its blank party fields, just as Appendices A–D at the back replace the blank appendix forms. The Clauses on the following pages are reproduced unchanged. The contact-person and signature fields in the Clauses are completed on this sheet.

Changelog

CHANGE	VERSION
1.1.	Clauses 9.2. and 10.4., (<i>Corrected cross-references</i>).
1.2	Clause 7.6 (<i>now made optional and amended wording</i>)

1. Table of Contents

2. Preamble.....	3
3. The rights and obligations of the data controller.....	3
4. The data processor acts according to instructions.....	4
5. Confidentiality.....	4
6. Security of processing.....	4
7. Use of sub-processors.....	5
8. Transfer of data to third countries or international organisations.....	6
9. Assistance to the data controller.....	7
10. Notification of personal data breach.....	8
11. Erasure and return of data.....	8
12. Audit and inspection.....	9
13. The parties' agreement on other terms.....	9
14. Commencement and termination.....	9
15. Data controller and data processor contacts/contact points.....	10
Appendix A Information about the processing.....	11
Appendix B Authorised sub-processors.....	12
Appendix C Instruction pertaining to the use of personal data.....	13
Appendix D The parties' terms of agreement on other subjects.....	18

2. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.
2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 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. In the context of the provision of NAME OF SERVICE, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.
4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.
5. Four appendices are attached to the Clauses and form an integral part of the Clauses.
6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.
7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.
8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.
9. Appendix D contains provisions for other activities which are not covered by the Clauses.
10. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.
11. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State¹ data protection provisions and the Clauses.
2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

¹ References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.
2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

[NOTE: THE PARTIES SHOULD FORESEE AND CONSIDER CONSEQUENCES WHICH MAY ARISE FROM ANY POTENTIALLY UNLAWFUL INSTRUCTIONS GIVEN BY THE DATA CONTROLLER AND REGULATE THIS IN AN AGREEMENT BETWEEN THE PARTIES.]

5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.
2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

1. Article 32 GDPR stipulates that, taking into account the state of the art, the 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, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

- a. Pseudonymisation and encryption of personal data;
- b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

- c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
 - d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.
 3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).
2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior [CHOICE 1] specific written authorisation / [CHOICE 2] general written authorisation of the data controller.
3. [OPTION 1 SPECIFIC PRIOR AUTHORISATION] The data processor shall engage sub-processors solely with the specific prior authorisation of the data controller. The data processor shall submit the request for specific authorisation at least [SPECIFY TIME PERIOD] prior to the engagement of the concerned sub-processor. The list of sub-processors already authorised by the data controller can be found in Appendix B.

[OPTION 2 GENERAL WRITTEN AUTHORISATION] The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least [SPECIFY TIME PERIOD] in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.
4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract

or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.
6. **[OPTIONAL]** The processor shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the processor has factually disappeared, ceased to exist in law or has become insolvent – the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.
7. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.
2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.
3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:
 - a. transfer personal data to a data controller or a data processor in a third country or in an international organization
 - b. transfer the processing of personal data to a sub-processor in a third country
 - c. have the personal data processed in by the data processor in a third country
4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the data controller

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

- a. the right to be informed when collecting personal data from the data subject
 - b. the right to be informed when personal data have not been obtained from the data subject
 - c. the right of access by the data subject
 - d. the right to rectification
 - e. the right to erasure ('the right to be forgotten')
 - f. the right to restriction of processing
 - g. notification obligation regarding rectification or erasure of personal data or restriction of processing
 - h. the right to data portability
 - i. the right to object
 - j. the right not to be subject to a decision based solely on automated processing, including profiling
2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:
 - a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, **[PLEASE INDICATE THE COMPETENT SA]**, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;
 - b. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;
 - c. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);
 - d. the data controller's obligation to consult the competent supervisory authority, **[PLEASE INDICATE THE COMPETENT SA]**, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.
2. The data processor's notification to the data controller shall, if possible, take place within [NUMBER OF HOURS] after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.
3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:
 - a. The nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - b. the likely consequences of the personal data breach;
 - c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation [OPTION 1] to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so / [OPTION 2] to return all the personal data to the data controller and delete existing copies unless Union or Member State law requires storage of the personal data.
2. [OPTIONAL] The following EU or Member State law applicable to the data processor requires storage of the personal data after the termination of the provision of personal data processing services:
 - a. [...]

The data processor commits to exclusively process the personal data for the purposes and duration provided for by this law and under the strict applicable conditions.

12. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.
2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.
3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

13. The parties' agreement on other terms

1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

1. The Clauses shall become effective on the date of both parties' signature.
2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.
3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.
4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.
5. Signature

On behalf of the data controller

Name	[NAME]
Position	[POSITION]
Date	[DATE]
Signature	[SIGNATURE]

On behalf of the data processor

Name	[NAME]
------	--------

Position	[POSITION]
Date	[DATE]
Signature	[SIGNATURE]

15. Data controller and data processor contacts/contact points

1. The parties may contact each other using the following contacts/contact points:
2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Name	[NAME]
Position	[POSITION]
Telephone	[TELEPHONE]
E-mail	[E-MAIL]

Name	[NAME]
Position	[POSITION]
Telephone	[TELEPHONE]
E-mail	[E-MAIL]

Appendix A — Information about the processing

The processing is one processing activity: providing the FieldTechie service to the data controller.

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

To provide the FieldTechie service to the data controller under the subscription terms, including to:

- plan, dispatch and document the data controller's service work;
- register working time and absence;
- communicate with the data controller's employees and customers;
- invoice, and exchange data with the accounting and payroll systems the data controller connects;
- provide support, and operate, secure and back up the service.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

- **Collection:**
 - data is entered by the data controller's users or imported from files;
 - the mobile app records GPS positions while a tracking session is active, as well as photos and signatures;
 - data is received from systems the data controller connects.
- **Storage** at Scaleway in Paris (fr-par): in a separate database per data controller, in object storage and in backups, see Appendix C.2.
- **Organisation, search and display** for the data controller's users, according to roles and permissions.
- **Automated use:**
 - scheduling suggestions and route calculation with a routing engine the data processor runs itself;
 - scoring of technicians as suggestions to a dispatcher;
 - automatic deletion after retention periods.

No automated decisions are taken about data subjects.

- **Disclosure on the data controller's instruction or configuration:**
- SMS and email messages to the data controller's customers;
- push notifications to the data controller's users;
- webhooks and exports to systems the data controller connects.
- **Erasure:** data is permanently deleted, not merely marked as deleted.
- **Access by the data processor's staff** only for support and operation (see Appendix C).

A.3. The processing includes the following types of personal data about data subjects:

1. Identity and contact details:

- name, email, phone number and postal address;
- job title, company and department;
- employee or contact number.

For contact persons and employees also, where the data controller fills them in, date of birth and social-media profile addresses. In addition, employees' next of kin (name, relationship and contact details).

1. User account and login:

- username, email and user identifier;
- encrypted password and one-time-password secret;
- sessions and login events, including IP address (kept 30 days, see Appendix C.4);
- registered devices and push tokens;
- user settings, roles and permissions;
- seat type and activation periods.

1. Planning and performance of work:

- assigned jobs and appointments with planned and actual arrival, start and end times;
- routes;
- working-hour schedules and on-call duty;
- qualifications;
- cost and bill rates;
- tools issued;
- scores for assignment suggestions.

1. **Working time and absence:**

- time entries with notes;
- timesheets and approvals;
- absence requests with the reason the user writes.

1. **Location:**

- GPS positions (coordinates, accuracy, altitude, speed and heading) recorded by the mobile app while the employee is clocked in and the data controller has switched tracking on;
- last known position;
- tracking-session information (device model, operating system, distance travelled, battery level);
- GPS information in photos, unless removed;
- coordinates of service addresses.

1. **Communication:**

- chat messages including edits;
- channel membership and read status;
- case messages and internal messages;
- in-app notifications;
- messages to the data controller's customers (the recipient's phone number or email, content and delivery status);
- consent to and opt-out from messages.

1. **Documentation:**

- photos and files;
- checklist answers;
- handwritten signatures with the signer's name and role;
- notes and free-text fields, including fields the data controller creates;
- service history;
- imported files.

1. **Commercial data about sole traders:**

- invoices and payments;
- company registration and VAT number;
- bank details.

1. **Technical data and audit trail:**

- log of who changed what, with previous and new values;
- copies of records in technical messages (webhooks, jobs, imports);
- links to identifiers in connected systems;
- application logs.

Data concerning health. The service is delivered with absence types for sickness, medical appointments, parental leave, and family or medical leave. The data controller can change these types. When absence of such a type is registered for an employee, data concerning that employee's health is processed (Article 9 GDPR). The service does not ask for diagnoses or causes of illness. If a payroll system is connected, the absence type, date and hours are transferred to it on the data controller's instruction.

Other special categories and criminal offences. The service has no fields for other special categories of personal data, e.g. trade-union membership, or for data relating to criminal convictions and offences (Article 10).

National identification numbers (CPR). The data processor does not store national identification numbers. The service has no field for one, and only employee number, name and email are read from connected payroll systems. Employees are matched on employee number. The only exception: the organisation number of a Swedish sole trader (enskild firma) is the owner's personal identity number and can be registered as a customer's registration number.

Free text, custom fields and photos. The data processor cannot technically prevent users from entering special categories of data or identification numbers in free-text fields, custom fields, chat or photos. The data controller instructs its users not to do so (see Appendix C).

A.4. Processing includes the following categories of data subject:

1. The data controller's users: owner, office staff, dispatchers and managers.
2. The data controller's technicians and other field staff, including apprentices and subcontractors' staff with access to the service.
3. Contact persons at the data controller's customers.
4. Private customers and occupants at the addresses where service is performed, and sole traders among the data controller's customers and suppliers.
5. Other persons appearing in the data: employees' next of kin, signers, invited users, and persons in photos or free text.

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

Processing lasts for as long as the data controller's subscription runs, including the trial period. After that it continues until the personal data has been erased or returned under Clause 11 and Appendix C (read-only access and export of lists for 30 days and a complete copy on request, deletion no later than 60 days after termination, and backups expiring within a further 14 days, see Appendix C.4).

Appendix B — Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

Name	Registration no.	Address	Description of processing
Scaleway SAS	RCS Paris 433 115 904	8 rue de la Ville-l'Évêque, 75008 Paris, France	Hosting of the entire service in Paris (fr-par): servers, databases and backups, object storage, cache, networking, email sending, logs and secrets. Covers all types of personal data in Appendix A. Processing takes place in the EU.
Google LLC (Firebase Cloud Messaging)	Delaware limited liability company, USA	1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	Delivery of push notifications to the mobile app: the device push token and the notification's title and text. May be processed outside the EU; transfer basis: the EU-US Data Privacy Framework (Google LLC is certified) and, as a fallback, the European Commission's standard contractual clauses in Firebase's data processing terms. Retention: a notification that cannot be delivered at once is held for up to 28 days and then discarded. On Android a device's registration expires after 270 days without use; Google keeps the app installation's identifier until it is deleted and then removes it within 180 days.
Functional Software, Inc. (Sentry)	Delaware corporation, USA	45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA	Error and crash reports from the mobile app: device and app information, and the context of the error. User identity is not sent. Data is stored in Sentry's EU region; transfer basis: the EU-US Data Privacy Framework (Sentry is certified) and, as a fallback, the European Commission's standard contractual clauses in Sentry's data processing addendum. Retention: crash reports are deleted after at most 90 days.
ONLINECITY.IO ApS (GatewayAPI)	CVR 27364276	Buchwaldsgade 50, 5000 Odense C,	Sending SMS to the data controller's customers: the recipient's phone number and the message text.

Name	Registration no.	Address	Description of processing
		Denmark	Processing takes place in the EU. Retention: after 30 days the message text, the sender and the last four digits of the phone number are anonymised. An SMS charged in error is kept for 6 months to settle the refund and then fully anonymised.

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

Not sub-processors: systems the data controller connects itself (e.g. accounting and payroll systems, and webhooks) are the data controller's own. The data processor sends data to them only on the data controller's instruction. Software the data processor runs itself at Scaleway (user management, message queue, route calculation) is not a sub-processor. DNS for the data processor's domains is provided by Cloudflare, Inc. Traffic to the service does not pass through Cloudflare, and Cloudflare does not process the data controller's personal data.

Recipient that is not a sub-processor: **Google Ireland Limited** (Google Maps Platform), 368047 (Ireland), Gordon House, Barrow Street, Dublin 4, Ireland. When the data controller's users use maps and address search, Google receives:

- **for address suggestions and lookups:** the address the user types, sent from the data processor's server;
- **for maps and map images:** the user's IP address, the map area shown and, in map images, the coordinates or address of a customer's location, loaded in the user's browser.

Google processes this data as an **independent controller** under Google's own terms (Google Maps Platform and Google's Controller-Controller Data Protection Terms), not on the data processor's instructions, and is therefore not a sub-processor. The data may be processed outside the EU. Transfer basis: the European Commission's standard contractual clauses (Module 1, controller to controller) in Google's terms, and the EU-US Data Privacy Framework.

B.2. Prior notice for the authorisation of sub-processors

The data controller gives a general prior written authorisation (Clause 7.3).

Notice. The data processor gives at least **30 days'** notice of any intended addition or replacement of sub-processors before the change takes effect. Notice is sent by email to the data controller's owner and billing contact, and published on the data processor's list of sub-processors.

Objection. Within the notice period the data controller may object on reasonable data-protection grounds. If the change nevertheless goes ahead, the data controller may terminate the affected service free of charge before the change takes effect.

Appendix C — Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

- **Providing the service.** The data processor provides the FieldTechie service as described in Appendix A and the subscription terms. This covers storing, displaying and processing the personal data that the data controller's users enter, import or record through the mobile app.
- **Disclosure.** Personal data is disclosed only to the systems, recipients and channels that the data controller itself connects or enables in the service, e.g. accounting and payroll systems, webhooks, and SMS and email messages to customers.
- **Support and operation.** The data processor accesses the personal data only where necessary for operation, security and troubleshooting, or when the data controller requests support.
- **The data controller's responsibilities.** The data controller instructs its users not to record special categories of data or national identification numbers in free-text fields, custom fields, chat or photos (see Appendix A.3). The data controller informs its employees about GPS tracking and time registration.

C.2. Security of processing

The level of security shall take into account that the processing is an ordinary business service with two elevated elements:

- **Location data** about the data controller's employees (GPS positions and routes).
- **Absence types** that can reveal health.

The processing does not involve a large volume of special categories of personal data. A **normal level of security, with increased protection of location, absence and access data**, is therefore established.

The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

The data processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

Pseudonymisation and encryption

- **Separation per customer.** Each data controller's data is stored in a separate database with its own database role.
- **Encryption of credentials.** Credentials for databases, connected systems and webhooks are encrypted in the application with AES-256-GCM.
- **Keys.** The keys are held in Scaleway Secret Manager and are available only to the production servers.

Confidentiality, integrity, availability and resilience

- **Access control.** Users' access is controlled by roles and permissions per action and data type. Every request is tied to the customer from the user's membership, looked up on the server. A customer id in the request is not accepted.
- **Automated tests.** Customer separation is covered by automated tests run on every change.
- **Operation.** The service runs behind a load balancer with health checks. Messages between the service's components are stored before they are sent, so an outage delays them without losing them.

Restoring availability after an incident

- **Backups.** The databases are backed up automatically once a day as a snapshot of the whole database server, so every data controller's database is included. Each copy is kept for **14 days** at Scaleway in Paris (fr-par). Restoring a single data controller's database follows a written procedure that has been tested.

Regular testing and evaluation

- **Tests.** Automated tests of security-critical functions (customer separation, cookies, CORS, HTTPS) run on every change. Only tested versions can be deployed.
- **Secrets in code.** The code is scanned for secrets on every change.
- **Vulnerabilities and updates.** Dependencies are scanned for known vulnerabilities on an ongoing basis, and operating systems and containers are updated regularly.
- **Evaluation.** The measures in this appendix are reviewed at least once a year, and when the service changes materially.

Access to data online

- **Login.** Users log in through the data processor's own login service (Keycloak):
 - passwords of at least 12 characters;
 - lockout after repeated failed attempts;
 - email verification;
 - access tokens valid for 5 minutes.
- **Two-factor authentication** is offered to all users. The data controller is encouraged to require it for owners and administrators.
- **The data processor's staff.** Staff with administrative access must use two-factor authentication. Administrative access is not open to the internet and happens only over encrypted connections from approved addresses.

Protection of data during transmission

- **Encryption.** All traffic between users and the service is encrypted with TLS, and HTTP is redirected to HTTPS.
- **Email.** Emails are sent encrypted to the email service.
- **Internal network.** Internal traffic between the service's servers runs inside Scaleway's private network, which is not reachable from the internet.
- **Database.** The connection to the database is encrypted, and the database's certificate is verified.
- **Webhooks.** Webhooks are sent over HTTPS only and signed. Addresses in private networks are refused.

Protection of data during storage

- **Encryption at rest.** The databases are encrypted at rest at Scaleway.
- **Credentials** are additionally encrypted in the application (see above).
- **Deletion.** Data is permanently deleted, not merely marked as deleted.
- **The mobile app.** Login credentials are kept in the device's secure storage. Data the app stores for offline use is not encrypted beyond the device's own encryption. The data controller ensures devices are protected by a screen lock.

Physical security of locations

Processing takes place exclusively in Scaleway's data centres in the Paris region (fr-par). Physical security is Scaleway's responsibility under its sub-processor agreement. The data processor keeps no personal data on its own premises.

Home/remote working

The data processor's staff work from home and remote workplaces. Access to the production environment happens only over encrypted connections and personal accounts protected by two-factor authentication. Personal data is not copied to staff devices, except where support for a specific case requires it, and is deleted afterwards. Workstations with access have encrypted disks and an automatic screen lock.

Logging

- **Changes.** All changes to the data controller's data are logged with user, time, and previous and new values.
- **Login and administration.** Login events and administrative events in the login service are kept for 30 days.
- **Application logs** are kept for up to 31 days, centrally in Scaleway Cockpit in Paris.
- **Viewing.** Who has *read* which data is not logged.

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

- **Data-subject requests (self-service).** The data controller's users can themselves view, correct and delete data about data subjects in the service.
- **What the data processor deletes or extracts.** Data that cannot be handled by self-service, the data processor deletes or extracts within **10 working days** of a written request from the data controller. This covers copies in logs, technical messages and imports.
- **Charges.** The assistance is free of charge unless requests are manifestly excessive.
- **Impact assessments and prior consultation.** The data processor provides Appendices A–C and its security description, including a template impact assessment for location tracking. The data processor answers reasonable questions within **10 working days**.
- **Personal data breaches.** The data processor notifies the data controller without undue delay and no later than **24 hours** after becoming aware of the breach, see Clause 10.2, with the information known at the time, and supplements it as the investigation proceeds.

C.4. Storage period/erasure procedures

During the subscription, personal data is stored until the data controller deletes it, with the following automatic erasure:

- **Chat messages:** 24 months by default. The data controller can change the period.
- **Raw GPS positions:** 90 days by default. The data controller can change the period.
- **Change log:** 24 months.
- **Webhook deliveries and events:** 30 and 90 days.
- **Login and administrative events** in the login service: 30 days.
- **Application logs:** 31 days.
- **Backups:** 14 days.

Upon termination of the provision of personal data processing services, the data processor returns the personal data and then deletes existing copies, under Clause 11.1:

- **Export.** The service remains available in read-only mode for **30 days** after termination, so the data controller can view all data and export lists itself. On the data controller's request within those 30 days, the data processor provides a **complete copy of all data, including files**, in a commonly used, machine-readable format, no later than 10 working days after the request and always before the deletion.
- **Deletion.** After that, the data controller's database, files, users and user accounts are deleted within a further **30 days**. Everything is therefore gone from production systems no later than 60 days after termination.
- **Backups.** Deleted data disappears from backups as they expire, no later than **14 days** after deletion.
- **Confirmation.** The data processor confirms the deletion in writing on request.
- **Copies at sub-processors.** Copies held by sub-processors (SMS, push notifications and crash reports) are deleted under the retention periods in Appendix B.
- **Trial period.** A trial that does not continue as a subscription is deleted 30 days after the end of the following 14-day read-only period. The data controller is warned twice by email beforehand.

This applies unless the data controller – after accepting the Clauses – has modified its original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

The data processor's own records. The data processor's own records about the data controller as a customer are processed by the data processor as a controller and are not covered by Clause 11:

- **Invoices, credit notes and payments:** kept for 5 years after the end of the financial year under the Danish Bookkeeping Act.
- **Evidence of acceptance of the agreement:** kept for 5 years after termination.

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorisation:

- **Scaleway SAS:** data centres in the Paris region (fr-par), France. Hosting of the entire service, including backups.
- **The data processor's staff:** home and remote workplaces in Denmark. Administration and support, see C.2.
- **Other sub-processors** as listed in Appendix B, for the processing described there.

C.6. Instruction on the transfer of personal data to third countries

The data controller instructs the data processor to transfer personal data to third countries in the following cases, and only to the extent described in Appendix B:

- **Push notifications:** Google (Firebase Cloud Messaging).
- **Maps and address search:** disclosure to Google Maps Platform when users use maps and address search. Google receives the data as an independent controller (Appendix B, recipient that is not a sub-processor) and transfers it under Google's own terms: the European Commission's standard contractual clauses, Module 1 (controller to controller), and the EU-US Data Privacy Framework. Maps are loaded in the user's browser.
- **Error reports from the mobile app:** Sentry, only where data cannot be kept in Sentry's EU region.

Legal basis for the transfer (Chapter V GDPR):

- **Primary basis:** the European Commission's adequacy decision for the EU-US Data Privacy Framework (Article 45), for recipients that are certified.
- **Supplementary basis:** the European Commission's standard contractual clauses (Article 46(2) (c)) in the sub-processors' terms.

If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled

within the framework of the Clauses to perform such transfer.

C.7. Procedures for the data controller's audits, including inspections

- **Yearly statement.** Once a year, free of charge, the data processor sends the data controller a written statement from its management. The statement covers compliance with the Clauses and Appendix C, together with an overview of the security measures and changes since the previous statement.
- **Questionnaire.** The data processor also answers one security questionnaire from the data controller per year, free of charge.
- **Further audits.** The data controller may in addition carry out an audit or inspection at its own expense. The following applies:
 - it is announced at least **30 days** in advance and takes place during normal business hours under confidentiality;
 - it is carried out remotely unless the data controller gives reasons for more;
 - it gives no access to other customers' data.
- **Data centres.** Physical inspection of the data centres is not possible. It is covered by the sub-processor's certifications, see C.8.
- **Out of scope.** Auditor's reports under ISAE 3000/3402 and ISO 27001 certification of the data processor are not part of the agreement.
- **Contesting.** The data controller may contest the scope and methodology of the statement and request further information.

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

- **Yearly review.** Once a year, the data processor reviews each sub-processor's published certifications and audit reports, and changes to its data processing agreement.
- **Summary.** On request, the data processor sends a summary to the data controller.
- **No physical inspection.** The data processor does not carry out physical inspections at the sub-processors, all of which provide standardised services.

Appendix D — The parties' terms of agreement on other subjects

D.1 Relationship to the subscription terms

These Clauses govern the processing of personal data. Everything else — price, payment, term, termination, availability and liability — follows the subscription terms, to which the Clauses are an appendix.

In case of conflict about the processing of personal data, the Clauses and their appendices prevail over the subscription terms.

D.2 Conclusion and evidence

The agreement is entered into when the data controller accepts the subscription terms and the accompanying data processing agreement when creating its account.

The data processor records and retains **the time, the accepted version of each document, and who accepted**. The data controller may at any time obtain a copy of that record and of the accepted documents.

A separately signed copy may be agreed and does not change the content of the agreement.

D.3 Changes to the Clauses and the appendices

- **Notice.** The data processor gives at least **30 days'** notice of changes before they take effect, by email to the data controller's owner and contact person.
- **Exception.** Changes that merely reproduce changes in legislation or in Datatilsynet's standard text may be made without notice. The data controller is informed.
- **Objection.** The data controller may object before the change takes effect, on reasonable data-protection grounds. If the parties cannot agree, the data controller may terminate the subscription free of charge before the change takes effect.
- **Sub-processors** are notified under Appendix B.2.

D.4 Optional clauses the parties have not agreed

- **Clause 7.6** (the data controller as third-party beneficiary in the data processor's contracts with

sub-processors) **has not been agreed**. The data processor's sub-processors provide standardised services on their own terms, which cannot be amended for an individual customer.

D.5 Language

The Clauses and the appendices exist in Danish and English. **The Danish version prevails** in case of discrepancy. The English version is a translation for readers who do not read Danish.

D.6 Contact

Enquiries about this agreement, about data-subject requests and about personal data breaches are sent to the data processor's contact person on the front page. The data controller informs the data processor of changes to its own contact person.

D.7 Fields and choices in the Clauses

The Clauses are the Danish Data Protection Agency's standard text and are reproduced unchanged. The fields and choices in the text are completed as follows:

- **Clause 2.3** [NAME OF SERVICE]: the service **FieldTechie**, see Appendix A.
- **Clauses 7.2–7.3** [CHOICE 1] / [CHOICE 2]: **Option 2**, general written authorisation. The notice period [SPECIFY TIME PERIOD] is **30 days**, see Appendix B.2.
- **Clause 7.6** [OPTIONAL]: not agreed, see D.4.
- **Clause 9.2** [PLEASE INDICATE THE COMPETENT SA]: **the Danish Data Protection Agency (Datatilsynet)**.
- **Clause 10.2** [NUMBER OF HOURS]: **24 hours**, see Appendix C.3.
- **Clause 11.1** [OPTION 1] / [OPTION 2]: **Option 2**: the data processor returns the personal data and then deletes existing copies, see Appendix C.4.
- **Clause 11.2** [OPTIONAL]: **none**. Neither EU law nor Danish law requires the data processor to keep the data controller's personal data after termination.
- **Clauses 14 and 15** (signature and contact persons): completed on the parties sheet at the front of the agreement.