Data Processing Agreement V2.0

Last updated 1 August 2025

This Data Processing Agreement is entered into between

The Customer at Inspectly ApS
(the **Data Controller**)

and

Inspectly ApS
CVR No.: 33954883
Lægårdsvej 24
8520 Lystrup
(the **Data Processor**),

who are each a "Party" and together the "Parties". The Parties have agreed on the following standard contractual provisions (the **Clauses**) with a view to complying with the General Data Protection Regulation and ensuring the protection of privacy and the fundamental rights and freedoms of natural persons as part of the subscription agreement (the **"Subscription"**). Processing is carried out via Inspectly's technical solution (the **"System"**).

The Agreement follows the Danish Data Protection Agency's template and applicable data protection law.

1. Preamble

1. These Clauses set out the Data Processor's rights and obligations when processing personal data on behalf of the Data Controller.

2. The Clauses are designed to ensure the Parties' compliance with Article 28(3) of Regulation (EU) 2016/679 of 27 April 2016 (the General Data Protection Regulation, **GDPR**).

3. In providing the System – a technical solution developed by the Data Processor – the Data Processor processes personal data on behalf of the Data Controller in accordance with these Clauses. The purpose of the solution is to support the Data Controller's quality work, including documentation in the form of notes, photos, project-related material and other data relevant to that purpose.

4. The Clauses take precedence over any corresponding provisions in other agreements between the Parties, including Inspectly's General Terms and Conditions, unless otherwise expressly stated in this Agreement.

5. Four appendices accompany these Clauses and form an integral part of them:

6. **Appendix A** contains details of the processing of personal data, including the purpose and nature of the processing, types of personal data, categories of data subjects and the duration of the processing. This includes, among other things, personal data relating to users of the System (name, contact details, texts, photos, locations and similar data submitted through the System on the Data Controller's instructions).

7. **Appendix B** contains the Data Controller's conditions for the Data Processor's use of sub-processors and the option to obtain, at any time, a list of the sub-processors whose use the Data Controller has approved.

8. **Appendix C** contains the Data Controller's instructions regarding the Data Processor's processing of personal data, a description of the minimum security measures to be

implemented by the Data Processor, and how supervision of the Data Processor and any sub-processors is conducted.

9. **Appendix D** contains provisions regarding other activities not covered by the Clauses.

10. The Clauses and the Appendices must be kept in writing, including electronically, by both Parties.

11. These Clauses do not relieve the Data Processor of any obligations imposed upon it by the GDPR or any other legislation.

2. The Data Controller's rights and obligations

1. The Data Controller is responsible for ensuring that the processing of personal data takes place in accordance with the GDPR (see Article 24), data-protection provisions in other EU law or Member State national law, and these Clauses.

2. The Data Controller has the right and the obligation to decide for which purpose(s) and by which means personal data may be processed.

3. The Data Controller is responsible, inter alia, for ensuring that there is a legal basis for the processing of personal data that the Data Processor is instructed to carry out.

3. The Data Processor acts on instructions

1. The Data Processor may only process personal data on documented instructions from the Data Controller, unless required to do so by EU law or Member State national law to which the Data Processor is subject. In such a case, the Data Processor shall inform the Data Controller of that legal requirement before processing, unless that law prohibits such notification on important grounds of public interest.

2. This Data Processing Agreement, including the Appendices, constitutes the instructions at the time of signature. Changes to the instructions must be made in writing and documented.

3. The Data Processor shall notify the Data Controller without undue delay if, in the Data Processor's opinion, an instruction infringes the GDPR or other applicable data-protection legislation.

4. Unless otherwise stated in this Agreement, the Data Processor is entitled to use relevant tools, including its own IT systems, to perform the processing.

4. Confidentiality

1. The Data Processor may only grant access to personal data 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 to the extent necessary. The list of persons granted access shall be reviewed on an ongoing basis. Based on this review, access to personal data may be revoked if it is no longer necessary, and the personal data shall no longer be available to those persons.

2. At the Data Controller's request, the Data Processor shall be able to demonstrate that the persons under its authority are subject to the above confidentiality obligations.

5. Security of processing

1. The Data Processor shall implement the technical and organisational security measures required by Article 32 of the GDPR.

2. The measures must ensure a level of security appropriate to the risk, taking into account:

a. the state of the art,

b. the costs of implementation,

c. the nature, scope, context and purposes of processing, and

d. the risks of varying likelihood and severity for the rights and freedoms of natural persons.

3. The specific security measures to be implemented by the Data Processor, at a minimum, are set out in Appendix C. This appendix specifies the agreed security level and the Data Processor's responsibility regarding technical and organisational protection of data.

4. The Data Processor may use any relevant tools, including its own IT systems, unless otherwise stated in this Agreement. In its internal procedures, the Data Processor has implemented additional security measures beyond those set out in Appendix C.

5. The Parties agree that the security level set out in this Agreement and Appendix C is sufficient at the time the Agreement is concluded.

6. Use of sub-processors

1. The Data Processor may not use another processor (a **Sub-Processor**) without the Data Controller's prior general written authorisation.

2. The Parties have agreed that the Data Processor may generally use the Sub-Processors listed on the sub-processor list and provided at any time as described in Appendix B.

3. The Data Processor has the Data Controller's general authorisation to use Sub-Processors. The Data Processor shall notify the Data Controller in writing of any planned changes concerning the addition or replacement of Sub-Processors at least 30 days in advance, thereby giving the Data Controller the opportunity to object to such changes before the relevant Sub-Processor(s) are used. The list of Sub-Processors already approved by the Data Controller can be provided at any time pursuant to Appendix B.

4. The Data Processor shall meet the requirements of Article 28(2) and (4) GDPR in order to use a Sub-Processor. This includes, inter alia, that:

a. the Sub-Processor is subject, by contract or other legal act, to at least the same data-protection obligations as those imposed by this Agreement, and

b. the requirements for technical and organisational measures in the GDPR and other applicable regulation are complied with.

5. If a Sub-Processor fails to fulfil its data-protection obligations, the Data Processor remains fully liable to the Data Controller for the performance of the Sub-Processor's obligations.

7. Transfers to third countries or international organisations

1. The Data Processor may only transfer personal data to third countries or international organisations to the extent permitted under Chapter V of the GDPR.

2. The Data Processor only uses Sub-Processors that have established a lawful transfer mechanism in accordance with the GDPR, including appropriate safeguards or adequacy decisions, unless an exception under Article 49 applies.

3. Where a transfer to a third country is to take place, the Data Controller shall, without separate remuneration, assist the Data Processor in entering into the necessary agreements, or the Data Controller may authorise the Data Processor to enter into such agreements on behalf of and at the expense of the Data Controller.

4. The Data Controller shall be notified in advance of any transfer to third countries not expressly instructed, unless such notification is prohibited by applicable law.

8. Assistance to the Data Controller

1. Taking into account the nature of the processing and the information available to the Data Processor, the Data Processor shall assist the Data Controller in fulfilling the Data Controller's obligations to respond to requests for exercising the data subjects' rights under Chapter III of the GDPR.

2. The Data Processor shall assist the Data Controller in ensuring compliance with the obligations under Articles 32–36 of the GDPR, including with regard to:

a. security of processing,

b. notification and communication of personal data breaches,

c. data protection impact assessments, and

d. prior consultation.

3. Any agreement on payment for the Data Processor's assistance under this clause appears from section 12 of this Agreement.

9. Notification of personal data breach

1. The Data Processor shall notify the Data Controller without undue delay if the Data Processor becomes aware of a personal data breach at itself or at any Sub-Processor. If possible, the notification shall be made no later than 36 hours after the Data Processor becomes aware of the breach.

2. A personal data breach means any security incident leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed on behalf of the Data Controller.

3. The notification to the Data Controller shall contain, at a minimum:

1. description of the nature of the breach, including the types of personal data affected and – where possible – the categories and approximate number of data subjects and personal data records concerned,

2. description of the likely consequences of the breach, and

3. description of the measures taken or proposed by the Data Processor to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. The Data Processor shall keep a record of all personal data breaches. The record shall at least contain information about the facts relating to the breach, its effects and the remedial action taken.

10. Deletion and return of data

1. The Data Processor may not delete personal data processed for the Data Controller during the Subscription period unless this is done on the Data Controller's instructions.

2. Upon termination of the Subscription, the Data Processor undertakes, at the Data Controller's choice, to delete all personal data or return the personal data to the Data Controller, unless storage is required under EU law or national law.

3. Deletion of personal data at the Data Processor and any Sub-Processors will as a rule take place no later than 30 days after termination of the Subscription and without prior notice. Earlier deletion may be carried out upon request.

4. The Data Controller shall submit the request for deletion or return in good time to ensure timely completion upon termination of the Subscription.

11. Supervision and audit

1. At the Data Controller's request, the Data Processor shall make available all information necessary to demonstrate compliance with Article 28 GDPR and this Data Processing Agreement.

2. The Data Processor shall allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller. The Data Controller may also allow supervision by relevant authorities.

3. Once a year – if requested by the Data Controller – the Data Processor may prepare a management statement on compliance with the Data Processing Agreement and its appendices. The statement is prepared at the Data Controller's expense, and the Data Processor is entitled to receive a copy. If a similar statement exists from the past 12 months, it may be provided instead.

4. The Data Controller, its representative or a relevant supervisory authority is entitled to carry out supervision – including on-site supervision – at the Data Processor upon prior notice and with adequate identification.

5. Supervision must be notified with at least one month's notice. The notice shall be accompanied by a detailed plan describing the scope, duration and start date of the supervision. The Data Processor shall provide the resources necessary for efficient completion of the supervision.

6. Costs associated with supervision, including the Data Processor's internal time spent and any provision of documentation, shall be borne by the Data Controller and settled based on actual consumption.

12. Supplementary provisions

1. **Renegotiation.** Either Party may require the Clauses to be renegotiated if changes in legislation or impracticalities in the Clauses give rise to this.

2. **Term during service provision.** The Clauses apply for as long as the service involving the processing of personal data is provided. During this period, the Clauses may not be terminated unless other provisions regulating delivery of the service involving the processing of personal data are agreed between the Parties.

3. **Breach.** Regulation of breach and remedies follows the Parties' other contractual framework, including the General Terms and Conditions, cf. section 1.6 of this Agreement.

4. **Liability and limitation of liability.** The Parties are liable in accordance with the general rules of applicable law, subject to the following limitations:

a. The Parties disclaim liability for indirect losses and consequential damages, including loss of business, loss of goodwill, loss of savings, interest and revenue, including costs to recover lost revenue, and loss of data.

b. The Parties' aggregate liability under this Data Processing Agreement is limited to the total due payments for the main service in the six (6) months preceding the harmful event. If the Agreement has been in force for a shorter period than six months, the amount shall be calculated as the average monthly payment in the period multiplied by six.

1. **Changes to the Agreement.** Changes to this Data Processing Agreement may only be made in writing and by mutual agreement between the Parties. The Data Processor may propose changes with one month's notice.

2. **Term and termination.** This Data Processing Agreement applies from the time of its conclusion and until termination of the underlying Subscription, unless replaced by another valid data processing agreement. The Agreement may not be terminated separately during the term of the Subscription. Notwithstanding termination of the Agreement, the following provisions remain in force: section 5.3 (confidentiality), 11 (deletion and return), 14 (liability and limitation of liability) and 17 (disputes). The Data Processor may process personal data for up to three months after termination of the Agreement to the extent necessary for the fulfilment of statutory obligations. In the same period, data may be included in the Data Processor's customary backup procedures. Processing during this period shall continue in accordance with the instructions in this Agreement.

3. **Disputes and governing law.** Any dispute arising in connection with this Data Processing Agreement shall be handled in accordance with the Parties' applicable terms of trade. Unless otherwise agreed in writing, the Agreement is governed by Danish law. Disputes may be brought before the ordinary courts, and Aarhus City Court is agreed as the venue in the first instance.

Appendix A – Information on the processing

1. **Purpose and nature of the processing.**
   The processing takes place as part of fulfilling the agreement between the Data Controller and the Data Processor (the "Subscription") and is intended to support the Data Controller's documentation and process management in relation to quality assurance, technical enquiries, supervision, project documentation, notes, photos, etc.

The Data Processor provides a system solution in which the Data Controller enters data, including personal data. The processing includes the transfer, storage and structuring of these data in the System. The processing is carried out solely on the Data Controller's instructions.

The processing includes a small amount of personal data referred to in Article 9 of the GDPR but does not include processing of "special categories of personal data"; therefore, no pseudonymisation or encryption of personal data is carried out.

The Data Processor uses only the latest standards for encryption and SSL during transmission of personal data. To access data, the Data Controller must be authenticated through our OAuth authentication server, which secures the relationship between the client and the server.

The Data Processor logs personal data in connection with logins, but since location and/or IP addresses are not logged, this is not considered a risk in relation to sensitive personal data. Location is logged solely when the user creates photo records in the System, but as it is assumed that the user in this case is at a workplace, this is likewise not considered a risk.

It is not permitted for the Data Processor's employees to log on to publicly available networks when working from home. For any data processing outside the company's physical location, logins to the company's internal systems or Azure servers are made via an office IP address through a VPN connection.

2. **Types of personal data.**
   The data processed include, among others:

- Name
- Mobile phone number
- Email address

- Time of registration
- Location for photo records

3. **Categories of data subjects.**
   The processing concerns the following categories of data subjects:

- Employees of the Data Controller
- Subcontractors to the Data Controller
- Other project participants created by the Data Controller

4. **Duration of the processing.**
   Personal data are processed for as long as the Subscription is active and deleted no later than 30 days after its termination, cf. the provisions on deletion in the Data Processing Agreement. Processing in the period after termination takes place only to the extent necessary, e.g. to comply with legal requirements or the Data Processor's backup procedures.

Appendix B – Sub-Processors

1. **Conditions for the use of Sub-Processors.**
   The Data Processor has the Data Controller's general authorisation to use Sub-Processors in connection with the performance of this Data Processing Agreement.

The Data Processor is obliged to:

- conduct annual supervision of its Sub-Processors via written information gathering to ensure that such subcontractors comply with requirements equivalent to the obligations of this Agreement; and
- conclude written agreements with Sub-Processors ensuring that they are subject to the same data-protection obligations as the Data Processor itself.

Changes in Sub-Processors.
The Data Processor shall notify the Data Controller in writing of any planned addition or replacement of Sub-Processors at least 30 days in advance. The Data Controller may object no later than 14 days after receiving the notice, but only on reasonable and specific grounds. If no objections are received within the deadline, the change is deemed approved.

List of approved Sub-Processors.
Upon the Data Controller's request, the Data Processor shall at any time provide an up-to-

date list of current Sub-Processors, including copies of the contractual basis as well as the basis and instructions for any transfers to third countries.

Appendix C – Instructions and security measures

1. Instructions

The Data Processor may only process personal data on documented instructions from the Data Controller, cf. section 2 of the Data Processing Agreement. The processing may not be expanded or changed without a written agreement with the Data Controller.

The instructions relate to processing as part of the Subscription, including:

- registration and storage of personal data in connection with quality assurance, technical enquiries, project documentation and photo records; and transmission of such data via Inspectly's System to the Data Controller.

The instructions apply throughout the term of the Agreement and concern the data types and categories of persons specified in Appendix A. Changes to the instructions must be communicated in writing and will take effect after written confirmation from the Data Processor.

2. Technical and organisational security measures

The Data Processor has taken the following technical and organisational security measures in accordance with Article 32 GDPR:

Technical security

- All communication to and from the System takes place via encrypted connections (HTTPS, TLS 128/256-bit).
- Use of an SSL certificate.
- User access requires login via OAuth authentication.
- Internal access systems are protected by access control and continuously updated passwords.
- Backup and data storage take place exclusively on Microsoft Azure servers.
- Passwords and access information received from the Data Controller are stored securely and deleted upon termination of the Subscription.

Organisational security

- Only authorised personnel have access to personal data.
- Authorisation is removed immediately upon termination of employment or changes in job duties.
- All employees are subject to confidentiality and non-disclosure obligations.
- Internal checks are carried out to ensure that only relevant persons have access.
- Employees are trained in handling security breaches and internal procedures thereof.

Physical security

- Data processing takes place at the company's address and, where relevant, from employees' home workplaces.
- For remote work, a VPN connection is used to access the company's network.
- Access to physical premises is secured with an alarm system outside opening hours.

3. Supervision

Supervision of the Data Processor.
The Data Controller is entitled to supervise the Data Processor's compliance with this Agreement. This may be done by means of documentation, a management statement or an on-site audit. See section 12 of the Agreement.

Supervision of Sub-Processors.
The Data Processor conducts an annual written supervision of Sub-Processors and must document that they comply with the requirements of this Agreement. The Data Processor is responsible for the Sub-Processors' compliance with these requirements.

Appendix D – Other matters

At the time of entering into the Agreement, no other activities have been identified outside the purposes and instruction-based processing covered by this Data Processing Agreement.

If, in the future, the Data Processor is to carry out processing of personal data as an independent Data Controller – including as part of its own business purposes – this requires a separate written agreement with the Data Controller.