Data Processing Agreement V1.5

Last updated: 21. february 2024

The Customer at Inspectly ApS
("The Data Controller")

and

Inspectly ApS
VAT no. DK-33954883
Lægårdsvej 24
8520 Lystrup
Denmark
("The Data Processor")

The Data Controller and Data Processor are individually denominated as "Party" and collectively as "Parties"

1. Background and purpose

1.1. The Data Controller has entered a contract (hereafter "Subscription") with the Data Processor, wherein the Data Processor processes personal information on behalf of the Data Controller. The purpose of the Subscription is to give the Data Controller the opportunity to register and edit information pertaining to quality assurance and quality control, including but not limited to, change orders, notes, project documents, images, etc. relevant to the Data Controller's enterprise, and registered/uploaded by the Data Controller.

1.2. The Data Processor handles personal information on behalf of the Data Controller's employees, so far as they are in contact with the Data Processor. The information handled are, first name, last name, phone/mobile number as well as email addresses. This information is also collected for persons who receive invoices, newsletters, operational news as well as commercial news. Further, the Data Processor handles the following types of data in relation to the Data Controllers usage of the provided platform; text, images, locations and other information relevant to the usage of the system – per instruction from the Data Controller. The parties have estimated the business relationship to be of a character as to let the Data Processor process/store personal information on behalf of the Data Controller due to, among others,

a) The Data Controller instructs the Data Processor on the purpose of the Data Processor's service as well as the auxiliary aids to be used by the Data Processor in relation to this task, as set out in Annex 1 and 2
b) The data controller is responsible for ensuring that the processing of personal data complies with the General Data Protection Regulation, data protection provisions in other EU law, or national laws of the member states, and these provisions.
c) The data controller is responsible for, among other things, ensuring that there is a legal basis for the processing of personal data, as instructed to be carried out by the data processor.
d) The Data Processor has no independent interest in collecting personal information, only collecting and processing information on behalf of the Data Controller, as set out in the instructions.
e) The Data Controller can require the Data Processor to cease the processing of personal information as well as compel the deletion of stored personal information, as set out in article 11.

f) The processing of personal information is carried out through the use of a technical solution, invented by the Data Processor (hereafter “the system”)

g) The Data Processor undertakes tasks that could, in principle, be carried out by the Data Controller

1.3. The purpose of the Data Processing Agreement is to ensure the Data Processors 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 (GDPR)).

1.4. The Data Processing Agreement sets out the rights and obligations applicable when the Data Processor handles and processes personal information on behalf of the Data Controller. The Data Controller can, via the system, login and see the processed information.

1.5. The Data Processing Agreement includes Annex 1 and 2. The annexes function as an integrated part of the Data Processing Agreement. The Data Processing Agreement follows the conditions for the termination of the Subscription, as laid out in article 1.1. as well as the associated General Business Conditions (hereafter “Trading Conditions”).

1.6. The Trading Conditions are generally applicable in relation to the Data Processing Agreement. In case of doubt or conflicting cases, the Data Processing Agreement takes precedence, unless otherwise stated in the Data Processing Agreement.

1.7. The Data Processing Agreement, with annexes, is to be stored in written form, as well as electronically by the Parties.

2. Instruction

2.1. The Data Processor can handle and process personal information as laid out in written instructions by the Data Controller, unless other requirements are made by EU-law or member states national law, under which the Data Processor is obligated. In this case, the Data Processor notified the Data Controller of their legal rights prior to processing, unless applicable law prohibits such a notification due to public safety concerns, as laid out in the GDPR article 28(3)(d).

2.2. This Data Processing Agreement, including annexes, serve as the instruction at the time of signing. Potential future modifications shall be agreed upon in written form.

2.3. The Data Processor will immediately notify the Data Controller in the case an instruction, by the Data Controller, is contrary to the GDPR or other data protection regulations in EU-law or the law of member states, under which the Data Processor is obligated.

2.4. If not otherwise specified in the Data Processing Agreement, the Data Processor reserves the right to use all relevant aids, including IT-systems, to meet the obligations of the Data Processor as laid out in the Data Processing Agreement.

3. Generally concerning procedural security

3.1. If not otherwise specified in the Data Processing Agreement, the Data Processor reserves the right to use all relevant aids, including IT-systems, to meet the obligations of the Data Processor as laid out in the Data Processing Agreement. The Data Processor shall continuously strive to implement all required processes, as laid out in article 32 of the GDPR.

3.2. Article 32 prescribes fitting technical and organisational measures to ensure a security level appropriate to the risks connected to the possession of personal information, taking into consideration

a) The current level
b) Implementation costs

3.2.1. The character, extent, context, and reason pertaining to the process (taking into consideration the category of personal information, as laid out in Annex 1)

3.2.2. Risk of varying degrees of severity and probability pertaining to the rights of physical persons and their fundamental freedoms.

3.3. The Data Processor, will in all instances regarding the aforementioned, implement the level of security as laid out in article 4-7, as a minimum.

3.4. The Parties agree that these guarantees are satisfactory at the moment of commencement of this Data Processing Agreement, while acknowledging that the Data Processor implements further procedures internally.

4. Physical security

4.1. The data processor processes data at its own company address and, if applicable, at the employees' home addresses (see also Appendix 1).

4.2. The Data Processor evaluates and implements the security of physical locations, including the safety of the building and access are monitored via surveillance system outside of opening hours.

5. Organisational security

5.1. The Data Processor ensures access to the personal information, processed on behalf of the Data Controller, only by authorized personnel. Access to the information is to be terminated immediately if the authorization is rescinded or expires.

5.2. Only persons necessary to fulfil the obligation of the Data Processor to the Data Controller can be authorized.

5.3. The Data Processor ensures that persons authorized to handle personal information on behalf of the Data Controller have been obliged to professional privacy and/or have signed appropriate confidentiality agreements, as set out by applicable law. The Data Processor further ensures persons authorized comply with the Data Processing Agreement.

5.4. The data processor continuously verifies that only the relevant individuals within the data processor have access to process personal data.

5.5. The data processor must be able to demonstrate that the individuals subject to the data processor's instructions are bound by the confidentiality obligation mentioned above.

All employees are made aware of and obliged to follow internal procedures regarding the handling of security breaches.

6. Technical security

6.1. The Data Processor exclusively makes use of high-quality hardware and software, which is regularly updated, including anti-malware software and firewalls.

6.2. All communication to and from the System takes place encrypted (HTTPS) and supports a 256/128-bit TLS connection. Further, communication happens only through the application of an SSL certificate.

6.3. Access to the internal IT-systems of the Data Processor is protected by login-information ensuring non-authorized access cannot be given. The Data Processor regularly changes internal access codes to the System containing the personal information of the Data Controller.

6.4. For the purpose of integration of the System with the Data Controller's IT-systems, the Data Processor receives the necessary passwords and access information. The Data Processor securely stores this information until the Subscription is terminated by one of the Parties. Concurrently with the termination, the Data Controller is encouraged to change the access information.

7. Notification of personal data breach

7.1. The Data Processor notifies without unnecessary delays, and if possible, within 72 hours the Data Controller when the Data Processor has become aware of the occurrence of a personal data breach. This includes personal data breaches at potential sub-data processors.

7.2. A personal data breach includes any breach with the potential to accidental or illegal destruction, loss, change, unauthorized communication of or access to personal data processed on behalf of the Data Controller ("Security breach")

7.3. The Data Processor shall keep and update a record of all security breaches. The record shall, at minimum, contain the factual circumstances regarding the Security breach, the consequences and any measures implemented to mitigate future damages.

8. Usage of sub-Data Processors

8.1. The Data Processor shall live up to the conditions as laid out in the GDPR article 28(2)(4) when using sub-Data Processors.

8.2. The Parties agree that the Data Processor generally has the right to use sub-processors, as laid out in Annex 2, where already approved sub-processors are also listed.

8.3. The Data Processor requires the sub-processor to employ at least the same data protection measures as the ones listed in this Data Processing Agreement. This is done through contract or

other legal document to ensure the sub-processor is, at all time, compliant with the technical and organisational requirements as laid out in the GDPR or other applicable regulations.

8.4. If the sub-processor is not compliant with the data protection measures, the Data Processor remains fully responsible to the Data Controller for the for the fulfilment of the sub-processor's obligations.

9. Transfer of data to third countries or international organisations

9.1. The data processor exclusively employs approved sub-processors, including regarding the transfer (transfer, disclosure, and internal use) of personal data to third countries or international organizations, unless exceptions to this are met in the General Data Protection Regulation and/or other relevant applicable regulations.

9.2. In the event of a transfer to a third country, the Data Controller, without charge, assists the Data Processor in entering into necessary agreements, or the Data Controller authorizes the Data Processor to enter into the required agreements on behalf of and at the expense of the Data Controller.

9.3. The Data Controller must be notified before any non-instructed transfers to third countries, unless notification is not permitted.

10. Assistance for the Data Controller

10.1. The Data Processor assists the Data Controller with the fulfilment of the Data Controllers obligations to comply with requests regarding the exercise of the rights of data subjects, as laid out in chapter 3 of the GDPR, taking into account the nature of the request.

10.2. The Data Processor assists the Data Controller to ensure compliance of the Data Controllers obligations as laid out in article 32-36 of the GDPR, taking into account the nature of the request and the information available to the Data Processor, as laid out in article 28(3)(f) of the GDPR

10.3. The Parties agree to the financial compensation laid out in article 12 of the Data Processing.

11. Deletion

11.1. The Data Processor does not delete the personal information, or other information, belonging to the Data Controller during the period of Subscription, unless instructed to do so by the Data Controller.

11.2. The deletion of all forms of data by the Data Processor, and any sub-processors, commences maximally 30 days after the termination of Subscription and without further notification. Early deletion can happen if requested by the Data Controller.

11.3. At termination of the Subscription, the Data Processor is obliged to transfer back or delete all personal information to the Data Controller, as well as delete all copies of the data, unless EU-law or other applicable regulations require the Data Processor to keep records of the data. Requests for the deletion of data must be issued in a timely manner, so as to be effectuated by the date of Subscription termination.

12. Monitoring and revision

12.1. The Data Processor makes available all data necessary to certify the Data Controller's compliance with article 28 of the GDPR, upon request.

12.2. The Data Processor provides for and assists with revisions and inspections carried out by the Data Controller or an independent expert (e.g accountant or IT specialist) authorized by the Data Controller.

12.3. The Data Processor shall be required to obtain a yearly recognised report from an independent expert regarding the Data Processor's compliance of this Data Processing Agreement, including annexes, if requested by the Data Controller. The costs related to the obtainment of the report shall be borne by the Data Controller and the Data Processor has the right to receive a copy of the report. In the event a report has been obtained within 12 months prior, the Data Processor reserves the right to offer this report to the Data Controller in lieu of a new report

12.4. The Data Controller, a representative of the Data Controller or a relevant supervisory authority has upon presentation of sufficient identification have the right of access to inspections, including physical inspection, of the Data Processor's premises, when requested by the Data Controller.

12.5. Inspections must be requested in a timely manner and no less than 30 days prior to the date of inspection. In conjunction with the inspection request, the Data Controller must submit a detailed plan defining the scope of the inspection, including the time and date of the inspection. The Data

Processor is obligated to make available necessary resources for the Data Controller to complete the inspection.

12.6. Any loss or expense incurred in relation to inspections or revisions, including time spent, are to be borne by the Data Controller and will include time spent by the Data Processor.

12.7. The abovementioned also applies in instances where the Data Controller requests documents or other material from the Data Processor for the purpose of inspecting the Data Processor's compliance with the Data Processing Agreement.

13. Breach of contract

13.1. Remedies for breaches of contract are regulated in accordance with the Trading Conditions, as laid out in section 1.6.

14. Liability and limitations of liability

14.1. The Parties are liable in accordance with the rules and regulations of established law, with the exceptions laid out in the section below.

14.2. The Parties renounce any liability for indirect or consequential loss, including but not limited to, operating losses, loss of goodwill, loss of savings, interest and income, including expenses to compensate for lost income due to loss of data.

14.3. The Parties liability for all cumulative claims in relation to this Data Processing Agreement are limited to due payments related to the principal supply for 6 months immediately preceding the harmful incident.

14.4. If however, the Data Processing Agreement has entered into force less than 6 months prior to the incident, the compensation is calculated as the cost of the principal supply for the period the Data Processing Agreement has been in force, divided by the number of months the Data Processing agreement has been in force and multiplied by 6.

14.5. The following are not subject to the limitations of liability, as set out in section 14:

14.5.1. Loss or damage, caused by any negligent or reckless act or omission by the other Party

14.5.2. Expenses, including resources spent when fulfilling a Party's obligation towards regulatory authorities or fines imposed by regulatory authorities or a court of law, in so far as these are the product of gross negligence or omission of another Party's actions.

15. Revisions

15.1. The Data Processor can, without incurring any expenses and with at least 30 days of notification, make changes to the Data Processing Agreement.

16. Duration and termination

16.1. The Data Processing Agreement can be replaced by another valid Data Processing Agreement. The Data Processing Agreement cannot be terminated or repealed separately from the Subscription during the period of Subscription.

16.2. Notwithstanding the termination of the Data Processing Agreement, the agreement's article 5(3), 11, 14 and 17 continue to be in effect after the Data Processing Agreement has come to an end.

16.3. The duration of the data processing agreement extends from the conclusion of the agreement until the termination of the subscription.

16.4. The Data Processer can continue to handle and process personal information for up to three months after the termination of the Data Processing Agreement in where such processing is necessary to fulfil legal obligations, as laid out in article 11(2). Concurrently, the Data Processor is entitled to allow personal information to remain a part of regular back-up procedures.

16.5. The Data Processors processing will for the period be considered to take place in accordance with the instructions of the Data Processing Agreement.

17. Disputes

17.1. Handling of disputes related to the Data Processing Agreement follow the regulations laid out in the Trading Conditions.

17.2. Insofar as nothing else is agreed upon, the Data Processing Agreement is subject to Danish law and the Parties are entitled to resolve any disputes arising from the Data Processing Agreement in an ordinary court of law. Aarhus Byret is the chosen jurisdiction at first instance.

Annex 1

(Information regarding processing and handling)

The processing involves a small amount of personal data covered by Article 9 of the General Data Protection Regulation but does not include the processing of "special categories of personal data," hence pseudonymization and encryption of personal data are not performed.

The data processor exclusively employs the latest encryption standards and SSL during the transmission of personal data. To access data, the data controller must be authenticated through our OAuth authentication server, ensuring the relationship between the client and the server.
Data is stored solely on Microsoft Azure servers, and the terms for this are outlined in the sub-processor's data processing agreement.

The data processor logs personal information during logins, but since location and/or IP addresses are not logged, this is not considered a risk concerning sensitive information. Location is only logged when the user creates photo registrations in the system, but as it is assumed the user is at a workplace in this case, it is also not deemed a risk.

Databehandler's employees are not allowed to log in on publicly accessible networks during possible remote work. In all data processing outside the company's physical location, logging occurs on the company's internal systems or Azure servers via an IP address at the office through a VPN connection.

1. Purpose

1.1. The purpose of the Subscription is the documentation of quality control/quality assurance, task management, supervisory notes and technical queries through project documents, images, notes, etc. This includes the dissemination of data to the Data Controller (including personal information). The data is generated by the Data Controller.

2. Processing

2.1. The Data Processor handles personal information including name, phone numbers and email. Furthermore, geo-locations are logged in relation to the creation of documentation, including time stamps. The documentation/registrations are afterwards kept and provided to the Data Controller via the System.

3. The processing includes the following personnel categories.

3.1. Employees of the Data Controller

3.2. Sub-contractors of the Data Controller

3.3. Other project related personnel set up by the Data Controller in the System.

4. Types of personal information

4.1. The Data Processor handles and stores the following personal data:

- Name (first, last)
- Phone number
- Email
- Photos/Images taken by the employees
- Time stamp and geo-location for every registration created

Annex 2

(Sub-processors)

1. General authorization

1. The Data Processor has the Data Controllers general authorization to use sub-processors in the processing and handling of data.
2. The data processor conducts annual supervision of the employed sub-processors through written information gathering, ensuring that the utilized sub-processors are subject to and comply with at least the same obligations as the data processor.
3. The Data Processor must notify the Data Controller of any planned changes regarding additions or replacements of sub-processors, giving the Data Controller the possibility to challenge such changes.
4. Such notification must be received by the Data Controller no less than 30 days before the planned changes enter into force.
5. If the Data Controller challenges the changes, the Data Controller must notify the Data Processor of such challenges within 14 days of receiving a notification of change.
6. The Data Controller alone can challenge the changes only if the Data Controller has reasonable and specific reasons for the challenge.

2. List of sub-processors at the time of the Data Processing Agreements entering into force

The data processor only uses approved sub-data processors, and the data processor can at any time, at the request of the data controller, forward a list of used approved sub-data processors including a copy of the agreement entered into with the sub-processor, along with the basis and instructions for the transfer.