Data Processing Agreement

pursuant to Article 28(3) of Regulation 2016/679 (GDPR) for the purposes of the processing of personal data by the processor;

between the Customer who subscribes to a Cloud-based version of ReportLoq

Name:
CVR:
Address:
Postal code. and city:
Country:

hereinafter referred to as "the data controller"

and

Olicem A/S
CVR 39958708
Majsmarken 1,
9500 Hobro
Denmark

hereinafter referred to as the "Data Processor"

each of which is a "party" and together constitutes the "parties"

HAVE AGREED on the following Standard Contractual Clauses (the Clauses) in order to comply with the General Data Protection Regulation and to ensure the protection of privacy and the fundamental rights and freedoms of natural persons;

Last updated 15 September 2025

Content

1 Preamble

1. These Clauses set out the rights and obligations of the data processor when it carries out the processing of personal data on behalf of the data controller.

2. These provisions are designed to ensure that the parties comply with Article 28(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

3. In connection with the provision of cloud-based versions of ReportLoq, the data processor processes personal data on behalf of the data controller in accordance with these Regulations.

4. The provisions shall prevail over any corresponding provisions in other agreements between the parties.

5. There are four annexes to these Regulations, and the Annexes form an integral part of the Regulations.

6. Appendix A contains further information on the processing of personal data, including the purpose and nature of the processing, the type of personal data, the categories of data subjects and the duration of the processing.

7. Appendix B contains the Data Controller's terms and conditions for the Data Processor's use of sub-processors and a list of sub-processors that the Data Controller has approved the use of.

8. Appendix C contains the Data Controller's instructions with regard to the Data Processor's processing of personal data, a description of the security measures that the Data Processor must implement as a minimum, and how the Data Processor and any sub-processors are supervised.

9. Annex D contains provisions relating to other activities not covered by the Regulations.

10. The provisions and their annexes must be kept in writing, including electronically, by both parties.

11. These Terms do not release the Data Processor from obligations imposed on the Data Processor under the General Data Protection Regulation or any other legislation.

2 Rights and obligations of the controller

1. The Data Controller is responsible for ensuring that the processing of personal data is carried out in accordance with the General Data Protection Regulation (see Article 24 of the Regulation), data protection provisions in other EU or Member States[1]' national law and these Provisions.

[1] References to "Member State" in this provision shall be understood as a reference to "EEA Member States".

2. The data controller has the right and duty to make decisions about the purpose(s) and means for which personal data may be processed.

3. The data controller is responsible for, among other things, ensuring that there is a legal basis for the processing of personal data that the data processor is instructed to undertake.

3 The data processor acts according to instructions

1. The data processor may only process personal data on documented instructions from the data controller, unless this is required by EU law or the national law of the Member States to which the data processor is subject. This instruction must be specified in Appendices A and C. Subsequent instructions may also be given by the data controller while personal data is being processed, but the instruction must always be documented and stored in writing, including electronically, together with these Regulations.

2. The processor shall immediately inform the controller if an instruction in its opinion is contrary to this Regulation or data protection provisions of other Union or Member State law.

4 Confidentiality

1. The Processor may only grant access to Personal Data processed on behalf of the Controller, to persons who are subject to the Processor's instructional powers, who have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality, and only to the extent necessary. The list of persons who have been granted access must be reviewed on an ongoing basis. On the basis of this review, access to personal data may be closed if access is no longer necessary and the personal data must then no longer be accessible to these persons.

2. At the request of the data controller, the data processor must be able to demonstrate that the persons in question, who are subject to the data processor's instructional powers, are subject to the above-mentioned duty of confidentiality.

5 Processing safety

1. Article 32 of the GDPR states that the controller and the data processor, taking into account the current state of the art, the implementation costs and the nature, scope, context and purpose of the processing in question, as well as the risks of varying probability and severity to the rights and freedoms of natural persons, shall implement appropriate technical and organisational measures to ensure a level of protection appropriate to these risks.

   The Data Controller must assess the risks to the rights and freedoms of natural persons represented by the processing and implement measures to address these risks. Depending on their relevance, it may include:

   a. Pseudonymization and encryption of personal data

b. ability to ensure the ongoing confidentiality, integrity, availability and robustness of processing systems and services;

c. the ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident;

d. a procedure for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures to ensure the safety of treatment.

2. According to Article 32 of the Regulation, the data processor – independently of the data controller – must also assess the risks to the rights of natural persons that the processing poses and implement measures to address these risks. For the purposes of this assessment, the Controller shall make available to the Processor the necessary information to enable it to identify and assess such risks.

3. In addition, the processor must assist the controller in its compliance with the controller's obligation under Article 32 of the Regulation, by, inter alia, making available to the controller the necessary information regarding the technical and organisational security measures that the processor has already implemented pursuant to Article 32 of the Regulation, and all other information necessary for the controller's compliance with its obligation under Article 32 of the Regulation. Article 32 of the Regulation.

   If, in the opinion of the controller, addressing the identified risks requires the implementation of additional measures than the measures already implemented by the processor, the controller shall indicate the additional measures to be implemented in Appendix C.

6 Use of sub-processors

1. The data processor must meet the conditions referred to in Article 28(2) and (4) of the General Data Protection Regulation in order to make use of another data processor (a sub-processor).

2. Thus, the Data Processor may not make use of a sub-processor for the fulfilment of these Terms without the prior general written approval of the Data Controller.

3. The data processor has the data controller's general approval for the use of sub-processors. The Data Processor shall notify the Data Controller in writing of any planned changes regarding the addition or replacement of sub-processors with at least 2 weeks' notice, thereby giving the Data Controller the opportunity to object to such changes prior to the use of the sub-processor(s) in question. Longer notice for notification in connection with specific processing activities may be specified in Appendix B. The list of sub-processors that the controller has already approved is set out in Appendix B.

4. Where the Processor makes use of a sub-processor in connection with the performance of specific processing activities on behalf of the Controller, the Processor shall, by means of a contract or other legal document under Union or Member State law, impose on the Sub-processor the same data protection obligations as those set out in these Clauses, providing in particular the necessary

safeguards for: that the sub-processor will implement the technical and organisational measures in such a way that the processing complies with the requirements of these Regulations and the General Data Protection Regulation.

The Data Processor is therefore responsible for requiring the Sub-Processor to comply with the Data Processor's obligations under these Provisions and the General Data Protection Regulation as a minimum.

5. Sub-processing agreement(s) and any subsequent amendments thereto shall be sent – at the request of the Data Controller – in a copy to the Data Controller, who thereby has the opportunity to ensure that corresponding data protection obligations pursuant to these Terms are imposed on the Sub-Processor. Provisions on commercial terms that do not affect the data protection law content of the sub-processing agreement do not need to be sent to the data controller.

6. The Data Processor must include the Data Controller as a third party beneficiary in the event of the Data Processor's bankruptcy, in the event of the Data Processor's bankruptcy, so that the Data Controller can assume the Data Processor's rights and enforce them against sub-processors, e.g. enabling the Data Controller to instruct the Sub-processor to delete or return the personal data.

7. If the sub-processor fails to fulfil its data protection obligations, the data processor remains fully liable to the controller for the fulfilment of the sub-processor's obligations. This does not affect the rights of the data subjects under the General Data Protection Regulation, in particular Articles 79 and 82 of the Regulation, vis-à-vis the data controller and the data processor, including the sub-processor.

7 Transfer to third countries or international organisations

- Any transfer of personal data to third countries or international organisations may only be carried out by the data processor on the basis of documented instructions to this effect from the data controller and must always take place in accordance with Chapter V of the General Data Protection Regulation.

- Where the transfer of personal data to third countries or international organisations for which the processor has not been instructed by the controller is required by Union or Member State law to which the processor is subject, the processor shall inform the controller of this legal requirement prior to processing, unless that law prohibits such notification on grounds of important public interest.

- Thus, without documented instructions from the Data Controller, the Data Processor cannot, within the framework of these Provisions:

    a. transfer personal data to a controller or processor in a third country or an international organisation;
    b. entrust the processing of personal data to a sub-processor in a third country;
    c. process the personal data in a third country;

- The controller's instructions regarding the transfer of personal data to a third country, including the possible transfer basis in Chapter V of the General Data Protection Regulation on which the transfer is based, must be stated in Appendix C.6.

- These Clauses are not to be confused with standard contractual clauses within the meaning of Article 46(2)(c) and (d) of the GDPR and these Clauses cannot constitute a basis for the transfer of personal data within the meaning of Chapter V of the GDPR.

8 Assistance to the data controller

1. The data processor, taking into account the nature of the processing, assists the data controller as far as possible by means of appropriate technical and organisational measures in fulfilling the data controller's obligation to respond to requests for the exercise of the data subjects' rights as laid down in Chapter III of the General Data Protection Regulation.

   This means that the data processor must, as far as possible, assist the data controller in connection with the data controller's compliance with:

   a. the duty to provide information when collecting personal data from the data subject;
   b. the duty to provide information if personal data has not been collected from the data subject;
   c. The right of access
   d. the right to rectification;
   e. the right to erasure (the 'right to be forgotten');
   f. the right to restriction of processing;
   g. the duty to notify in connection with the 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 Processor's obligation to assist the Controller in accordance with Clause 6.3., the Processor shall further assist, taking into account the nature of the Processing and the information available to the Processor, the Controller with:

   1. the obligation of the controller to notify the competent supervisory authority of the country in which the controller is established without undue delay and if possible within 72 hours of becoming aware of it, to the competent supervisory authority of the country in which the controller is established, unless it is unlikely that the personal data breach poses a risk to the rights or freedoms of natural persons;

   2. the obligation of the controller to notify the data subject without undue delay of any personal data breach when the breach is likely to result in a high risk to the rights and freedoms of natural persons;

3. the obligation of the controller to carry out, prior to processing, an analysis of the impact of the proposed processing activities on the protection of personal data (an impact assessment);

4. the obligation of the controller to consult the competent supervisory authority of the country in which the controller is established prior to processing, where a data protection impact assessment shows that the processing would lead to a high risk in the absence of measures taken by the controller to mitigate the risk.

3. The Parties shall specify in Appendix C the necessary technical and organisational measures by which the Data Processor shall assist the Data Controller and to what extent and extent. This applies to the obligations arising from Clauses 9.1 and 9.2.

9 Notification of personal data breaches

1. The data processor notifies the data controller without undue delay after becoming aware that a personal data breach has occurred.

2. If possible, the data processor's notification to the data controller must take place no later than 48 hours after the data controller has become aware of the breach, so that the data controller can comply with its obligation to report the personal data breach to the competent supervisory authority, cf. Article 33 of the General Data Protection Regulation.

3. In accordance with Clause 9.2.a, the Processor shall assist the Controller in notifying the Competent Supervisory Authority of the breach. This means that the processor must assist in providing the following information, which according to Article 33(3) must appear in the controller's notification of the breach to the competent supervisory authority:

   a. the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects affected, as well as the categories and approximate number of personal data data data breaches affected;

   b. the likely consequences of the personal data breach;

   c. the measures taken or proposed by the controller to address the personal data breach, including, where applicable, measures to limit its potential adverse effects.

4. The Parties shall specify in Annex C the information that the processor must provide in the context of its assistance to the controller in its obligation to notify personal data breaches to the competent supervisory authority.

10 Deletion and return of information

1. Upon termination of the services relating to the processing of personal data, the Data Processor is obliged to delete all personal data that has been processed on behalf of the Data Controller and

confirm to the Data Controller that the data have been deleted, unless Union or Member State law provides for the storage of the Personal Data.

11 Audit, including inspection

1. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with Article 28 of the General Data Protection Regulation and these Provisions and shall enable and contribute to audits, including inspections, by the Data Controller or another auditor authorised by the Data Controller.

2. The procedures for the controller's audits, including inspections, with the processor and sub-processors are set out in more detail in Appendix C.7. and C.8.

3. The Data Processor is obliged to provide supervisory authorities that have access to the Data Controller's or the Data Processor's facilities, or representatives acting on behalf of the supervisory authority, access to the Data Processor's physical facilities in return for proper identification.

12 The parties' agreement on other matters

1. The Parties may agree on other provisions relating to the Service regarding the processing of personal data, e.g. liability for damages, as long as these other provisions do not directly or indirectly conflict with the Provisions or impair the fundamental rights and freedoms of the data subject under the General Data Protection Regulation.

13 Entry into force and termination

1. The provisions shall enter into force on the date of signature by both parties.

2. Either party may request that the Terms be renegotiated if legislative amendments or inexpediencies in the Terms give rise to this.

3. The provisions apply for the duration of the service relating to the processing of personal data. During this period, the Terms cannot be terminated unless other provisions governing the provision of the service regarding the processing of personal data are agreed between the parties.

4. If the provision of the services relating to the processing of personal data ceases and the personal data is deleted or returned to the Data Controller in accordance with Clause 11.1 and Appendix C.4, the Clauses may be terminated with written notice by either party.

14 Signature

1. Signature

On behalf of the Data Controller

Name
Position
Telephone number
Email
Signature

On behalf of the data processor

Name	Kenneth Vindum
Position	Director
Phone number	+45 40 35 88 35
E-mail	kvin@olicem.com

Signature

Kenneth Vindum

15 Contact persons at the data controller and the data processor

5. The parties can contact each other via the contact persons below.
6. The parties are obliged to inform each other on an ongoing basis of changes regarding contact persons.

At the data processor

Name
Position
Telephone number
Email

At the data processor

Name	Kenneth Vindum
Position	Director
Phone number	+45 40 35 88 35
E-mail	kvin@olicem.com

Appendix A - Information about the processing

A.1. The purpose of the processing of personal data by the data processor on behalf of the controller

The purpose of the data processor's processing of personal data on behalf of the data controller is to make the "ReportLoq" service available to the data controller.

A.2. The processing of personal data by the Data Processor on behalf of the Data Controller is primarily concerned with (the nature of the processing)

In ReportLoq, users are registered for access control. For **form-based login**, the username (email) and a **password hash (Argon2id) are stored**; the password itself is not stored. Security **logs** are kept of login attempts (including IP and time) and **application audit trails** of significant user actions.

For **OAuth2/OIDC login** (e.g. Microsoft Entra ID), **only the email/identifier** is stored to link the user's account in ReportLoq; **Passwords are not stored** for these users.

All data is stored at Amazon Web Services in an EU data center (currently Frankfurt). Access for Olicem's staff is restricted according to "least privilege".

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

"ReportLoq" stores environmental measurements in a cloud-based platform. Sensitive personal information includes:

- Name
- Email address
- Password hash (Argon2id with unique salt embedded in the hash) for users with form-based login
- Login metadata: IP address and time of login attempt
- Audit trail for user actions in ReportLoq

A.4. The processing includes the following categories of data subjects

Regarding the users of the system:

- User information for login
- User behavior for use in audit trails

A.5. The processing of personal data by the Data Processor on behalf of the Data Controller may commence after the entry into force of these Regulations. The duration of the treatment is as follows

The data processor's processing of personal data on behalf of the data controller continues as long as the data controller makes use of ReportLoq. At the end of the subscription agreement, personal data of the type "User information" will be deleted after 7 days.

Appendix B - Sub-processors

B.1. Approved sub-processors

At the entry into force of the Regulations, the Data Controller has approved the use of the following sub-processors

NAME	CVR	ADDRESS	DESCRIPTION OF TREATMENT
WEBCRM A/S	DK25189558	Lyngbyvej 2 2100 Copenhagen Ø	Sending out newsletters based on valid consent
Amazon Web Services	DK39009323	Ørestads Boulevard 73 2300 Copenhagen S	Data hosting
Olicem A/S	DK39958708	Cornmark 1 9500 Hobro	Operations, support and development

At the entry into force of the Regulations, the Data Controller has approved the use of the above-mentioned sub-processors for the described processing activity. The Data Processor may not – without the written consent of the Data Controller – make use of a sub-processor for a processing activity other than the one described and agreed upon or make use of another sub-processor for this processing activity.

B.2. Notice for approval of sub-processors

See clause 7.3.

Appendix C - Instructions regarding the processing of personal data

C.1. Subject-matter/instruction of the processing

The Data Processor's processing of personal data on behalf of the Data Controller takes place by the Data Processor performing the following:

When the controller's users are created, e-mail and (for form-based login) an **Argon2id hash** of the password are stored. For OAuth2/OIDC login, **only email/identifier** is stored; no passwords are stored. The system records login attempts (IP and time) for security purposes. When the data controller logs on to www.reportloq.com and uses the system, the user's actions are recorded in the data processor's system.

Newsletters **are only sent** to users who have given **explicit consent**; consent is registered with time and version reference and can be withdrawn at any time via the unsubscribe link.

C.2. Safety of processing

The level of security must reflect:

The storage of usernames and e-mail addresses is the most sensitive thing the data processor stores. The requirements for storage are therefore not classified as being of a high level.

However, it should be mentioned that:

- **Passwords are stored solely as Argon2id hashes** with unique salt embedded in the hash (PHC format).
- All transport is protected with **TLS**; login credentials are not logged in plain text.
- The data processor's direct database access is limited to very few users and encrypted by IPSEC
- RDS backups are automatically managed and stored for generations.
- The data processor is certified under MCERTS
- All login attempts are logged (IP, time, outage) with rate limiting/lockout against brute force.
- Local servers at the Data Processor are stored in a separate locked server room
- Data Processor's employees
  - Must be logged in to company computers to access ReportLoq as administrators
  - Allowed to work from home with IPSEC encryption
  - Have encrypted computers with remote backup

C.3 Assistance to the Data Controller

The Processor shall, to the extent and extent set out below, assist the Controller in accordance with Clauses 9.1 and 9.2 by implementing such technical and organisational measures as may contribute to the Controller's ability to respond to requests for the exercise of the rights of the Data Subjects.

C.4 Storage period/deletion routine

"Personal data is stored for as long as the data controller finds that it fulfils the purpose for which the data controller has.

Upon termination of the service relating to the processing of personal data, the Data Processor shall either delete or return the Personal Data in accordance with Clause 11.1, unless the Data Controller – after signing these Terms – has changed the Data Controller's original choice. Such changes must be documented and kept in writing, including electronically, in connection with the Regulations.

C.5 Site of treatment

Processing of the personal data covered by the Regulations may not, without the prior written consent of the data controller, take place at locations other than the following:

Amazon, Germany

Olicem, Denmark

C.6 Instructions regarding the transfer of personal data to third countries

The responsible person is aware that the data processor uses a cloud-based data center at Amazon, Germany.

If the Data Controller does not provide documented instructions in these Terms or subsequently, regarding the transfer of personal data to a third country, the Data Processor shall not be entitled to carry out such transfers within the framework of these Provisions.

C.7 Procedures for the controller's audits, including inspections, with the processing of personal data entrusted to the processor

The Data Controller or a representative of the Data Controller shall annually carry out a physical inspection of the premises from which the Data Processor carries out the processing of personal data, including physical locations and systems used for or in connection with the processing, in order to determine the Data Processor's compliance with the General Data Protection Regulation, data protection provisions in other Union or Member States' national law and these Regulations.

In addition to the planned supervision, the data controller may carry out an inspection at the data processor when the data controller deems it necessary.

The Data Controller's possible expenses in connection with a physical inspection are borne by the Data Controller himself. However, the Data Processor is obliged to allocate the resources (mainly the time) necessary for the Data Controller to carry out its inspection.

Annex D - Adjustment of other matters by the parties

Regarding clause 7.3:

The Data Controller acknowledges that the Data Processor's Services are standardized, cloud-based subscription services that are made available to a large number of customers, and that the Data Processor therefore does not have the opportunity to arrange the systems offered in such a way that each customer can demand that the Data Processor may not make use of certain sub-processors that the Data Processor has otherwise approved.

On this basis, the Data Controller acknowledges that if it has objections to the Data Processor's change or choice of new sub-processors, and the Data Processor does not meet such objections, the Data Controller's sole authority is to terminate the subscription agreement with the Data Processor. The termination may take effect immediately, and neither party shall have any claims against each other in connection therewith.