Likvido GDPR Contract - Standard Contractual Clauses

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

between

CLIENT

(the data controller)

and

LIKVIDO APS
FREDERIKSSUNDSVEJ 62, BAGHUSET, 1. + 2. Floor
2400 KØBENHAVN NV
CVR 39270765

(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.

1. Table of Contents

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 Likvido's services which appears on Likvido's general terms of trade 2.2, 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 State[1] 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.

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.

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

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.

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 general written authorisation of the data controller.

3. 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 30 days 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. The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.

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

    a. have the personal data processed in by the data processor in a third country

2. 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.

3. 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
    a. the right not to be subject to a decision based solely on automated processing, including profiling

1. 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, in Denmark, the Danish Data Protection Agency, 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);

    a. the data controller's obligation to consult the competent supervisory authority, in Denmark, the Danish Data Protection Agency, 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.

2. 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.
3.

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 48 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 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 to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so unless Union or Member State law requires storage of the personal data.

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 with Likvido's Terms of Trade which is considered a main agreement to the Regulations.

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.

Appendix A Information about the processing

The data processor is a software company that has developed a tool for electronic invoicing, debtor and creditor management, and further offer assistance with bookkeeping.

The purpose of the cooperation between the parties is that the data controller wishes to use the data processor's systems and services to optimize its debtor management. With a profile, the data controller can use the services and services covered by Likvido's general trading conditions section 2.2 where Likvido acts as data processor.

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

The purpose of processing personal data is the management of debtor management, credit management and bookkeeping.

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):

Storage and systematization of invoices and payments on the basis of the data controller's payment requirements to business and private customers.

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

Name, address, email address, telephone number, payment information, possibly customer-specific number, type of customers and similar personal information that may appear on a regular invoice.

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

The data controller's business and private customers.

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:

The duration of the processing follows the data controller's subscription with the data processor.

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:
https://da.likvido.com/underdatabehandlere

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors in the link 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.

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

30 days.

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:

The purpose of processing personal data is the management of debtor management, credit management and bookkeeping.

C.2. Security of processing

The level of security shall take into account:

It is crucial for the level of security that this is ordinary personal information that is invoiced. The nature and general distribution of the information thus speaks in favor of a security risk, which is 3 on a scale from 1-5. This is because it is mainly ordinary personal data, which is only of a private nature for the data controller's private customers. The fact that reminder letters are sent out for unpaid bills does not reveal the solvency of the data subjects and therefore information about reminders is not considered particularly confidential, which could have led to a different risk assessment.

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:

[DESCRIBE REQUIREMENTS FOR PSEUDONYMISATION AND ENCRYPTION OF PERSONAL DATA]

No pseudonymization requirements have been agreed due to the nature of the data processing as described above.

[DESCRIBE REQUIREMENTS FOR ENSURING ONGOING CONFIDENTIALITY, INTEGRITY, AVAILABILITY AND RESILIENCE OF PROCESSING SYSTEMS AND SERVICES]

The data processor's systems are protected by the following technical security measures to meet the requirements of the GDPR regarding the confidentiality, integrity, availability and robustness of processing systems and services:

Encryption (https: //)
Network segmentation
Backup
System monitoring
Internal rights management

[DESCRIBE REQUIREMENTS FOR THE ABILITY TO RESTORE THE AVAILABILITY AND ACCESS TO PERSONAL DATA IN A TIMELY MANNER IN THE EVENT OF A PHYSICAL OR TECHNICAL INCIDENT]

At least once a year, the data processor conducts a self-audit or external assistance a test, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure processing security.

[DESCRIBE REQUIREMENTS FOR PROCESSES FOR REGULARLY TESTING, ASSESSING AND EVALUATING THE EFFECTIVENESS OF TECHNICAL AND ORGANISATIONAL MEASURES FOR ENSURING THE SECURITY OF THE PROCESSING]

Any access to the system for the data processor and the data controller requires a password. When creating user profiles, Captcha is used to prevent access to robots.

[DESCRIBE REQUIREMENTS FOR ACCESS TO DATA ONLINE]

The data processor protects personal information via encryption during transmission.

[DESCRIBE REQUIREMENTS FOR THE PROTECTION OF DATA DURING TRANSMISSION]

All employees of the data processor are subject to confidentiality via the employment agreement with the data processor.

All data processor employees must use security-approved IT equipment using a personal password.

[DESCRIBE REQUIREMENTS FOR THE PROTECTION OF DATA DURING STORAGE]

The physical framework of the data processor is protected by locking.

[DESCRIBE REQUIREMENTS FOR THE USE OF HOME/REMOTE WORKING]

The data processor follows internal procedures for processing personal data using remote or home workstations. The data processor uses VPN access for remote access.

[DESCRIBE REQUIREMENTS FOR LOGGING]

No logging requirements have been agreed due to the nature of the data processing as described above.

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:

When answering inquiries from data subjects, it is a fixed procedure for the data processor to inform the data controller of the inquiry. All correspondence is gathered at the data processor in order to ensure a professional and uniform procedure.

In the event of a security breach, it is a fixed procedure for the data processor to keep its own event log for events. This log is shared with the data controller to the extent that there are no conflicting legal interests between the parties. All correspondence is gathered in order to ensure a professional and uniform procedure.

C.4. Storage period/erasure procedures

Upon termination of the provision of personal data processing services, the data processor shall either delete or return the personal data in accordance with Clause 11.1., unless the data controller – after the signature of the contract – has modified the data controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

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:

See Appendix B.

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

The Data Controller grants with the Regulations its general approval for the use of sub-processors, including sub-processors located in third countries, to the extent that the use of sub-processors takes place pursuant to Section 7 of the Regulations and the EU Commission's standard contract for the transfer of personal data to third countries. The permission is conditional on the sub-processor in a third country only being allowed to access the data processor's systems via VPN or equivalent access with the same security standard.

[STATE THE LEGAL BASIS FOR TRANSFER PURSUANT TO CHAPTER V GDPR]

The basis for the transfer is Article 46 (1) of the GDPR. 2, letter c on the EU Commission's standard contract.

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, of the processing of personal data being performed by the data processor

[DESCRIBE PROCEDURES FOR THE DATA CONTROLLER'S AUDITS, INCLUDING INSPECTIONS, OF THE PROCESSING OF PERSONAL DATA BY THE DATA PROCESSOR]

The data processor shall at minimum once a year at The Data Processor's expense obtain an auditor's report from an independent third party concerning the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The parties have agreed that the following types of auditor's reports may be used in compliance with the Clauses:

ISO 27001
ISAE 3000
ISAE 3402
Lawyer's statement on GDPR compliance

The auditor's report shall without undue delay be submitted and made available on the data processor's website and/or be sent to the data controller for information. The data controller may contest the scope and/or methodology of the auditor's report and may in such cases request a new audit/inspection under a revised scope and/or different methodology. In this case, the data controller liable for the costs of the auditor's report.

Based on the results of such an audit, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data controller or the data controller's representative shall in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the data processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the data controller deems it required."

The data controller's costs, if applicable, relating to physical inspection shall be defrayed by the data controller. The data processor shall, however, be under obligation to set aside the resources (mainly time) required for the data controller to be able to perform the inspection. Any expenses of the data processor in connection with the data controller's physical inspection shall be borne by the data controller to the extent that the data processor can objectively account for the financial consequences of the physical inspection. Both parties are obliged to carry out a physical inspection with the least possible inconvenience to the operation of the parties.

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

The data controller shall once a year obtain a statement of assurance regarding the sub - data controller's compliance with the Data Protection Regulation, data protection provisions of other Union or national law of the Member States and these Regulations.

Audit statements obtained on this basis are included as part of the data processor's own audit statement in order to document the data processor's relevant investigations of the sub - data processors that have been contracted in accordance with the general instructions in Section 7.3.

The parties agree that the audit statement for sub-processors in third countries, insofar as they work as independent consultants for the data processor, is not covered by the requirement to submit an independent audit statement, as the consultants access the data processor's systems and thus the data processor's audit statement.

Appendix D The parties' terms of agreement on other subjects

DKK 1.500 / an hour