Data processing agreement

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

Version 21.12 (year, month)

between:

NAME

CVR:

ADDRESS

POSTCODE AND CITY

COUNTRY

(the data controller)

and

Livehouse A/S

CVR: 35038574

Galoche Allé 14

4600 Køge

Denmark

(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.

CONTENT

2 PREAMBLE

2.1 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.

2.2 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).

2.3 In the context of the provision of the processing activities described in Annex A, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

2.4 The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

2.5 Five appendices are attached to the Clauses and form an integral part of the Clauses.

2.6 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.

2.7 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.

2.8 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.

2.9 Appendix D contains provisions for other activities which are not covered by the Clauses.

2.10 Appendix E contains an Affidavit. This affidavit is used upon termination of this Agreement.

2.11 The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

2.12 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

3.1 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 data protection provisions and the Clauses.

3.2 The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

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

4 THE DATA PROCESSOR ACTS ACCORDING TO INSTRUCTIONS

4.1 The data processor shall process personal data only on documented instructions from the data controller, and only to the extent necessary for the Data Processor to fulfil the obligations under the Main Agreement and the Data Processor Agreement, 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.

The Data Processing Agreement is part of the Data Controller's instruction to the Data Processor. The Data Processor Process the personal data on behalf of the Data Controller and may not process personal data covered by the Data Processing Agreement for its own purposes.

4.2 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.

4.3 The Data Processor shall comply with legal obligations imposed on the Data Processor by the Danish Data Protection law or any other law imposed on the Data Processor.

5 CONFIDENTIALITY

5.1 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.

5.2 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

6.1 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.

The data controller's minimum requirements for the security measures of the data processor are set out in Annex C.18.2.

6.2 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.

6.3 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.

6.4 If subsequently – in the assessment of the data controller – mitigation of the identified risks requires 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

7.1 The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

7.2 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.

7.3 The data processor has the data controller's general authorisation to engage 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 90 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.

7.4 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.

7.5 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.

7.6 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.

7.7 If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8 TRANSFER OF DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

8.1 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.

8.2 In case transfers to other third countries or international organisations are required under EU or member state law and in case the data processor shall comply with such law, 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.

8.3 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 organisation
b. transfer the processing of personal data to a sub-processor in a third country
c. have the personal data processed in by the data processor in a third country

8.4 The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.18.6.

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

9 ASSISTANCE TO THE DATA CONTROLLER

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

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

a. the right to be informed when collecting personal data from the data subject
b. the right to be informed when personal data have not been obtained from the data subject
c. the right of access by the data subject
d. the right to rectification
e. the right to erasure ('the right to be forgotten')
f. the right to restriction of processing
g. notification obligation regarding rectification or erasure of personal data or restriction of processing
h. the right to data portability
i. the right to object
j. the right not to be subject to a decision based solely on automated processing, including profiling

9.2 In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, considering 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, 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);
d. the data controller's obligation to consult the competent supervisory authority, 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.

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

10 NOTIFICATION OF PERSONAL DATA BREACH

10.1 In case of any personal data breach or suspicion of data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller accordingly.

10.2 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.

10.3 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.

10.4 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 DELETION AND RETURN OF DATA

11.1 On termination of the provision of personal data processing services, the data processor shall be under obligation to return all the personal data to the data controller and delete existing copies unless Union or Member State law requires storage of the personal data.

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

11.2 The data processor shall fulfill Clause 11.1 by using the Affidavit in Appendix E.

12 AUDIT AND INSPECTION

12.1 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.

12.2 Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C, Clause 18.7. and 18.8.

12.3 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

13.1 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 da-ta subject and the protection afforded by the GDPR.

14 COMMENCEMENT AND TERMINATION

14.1 The Clauses shall become effective on the date of both parties' signature.

14.2 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.

14.3 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.

14.4 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, Clause 18.4., the Clauses may be terminated by written notice by either party.

14.5 Signature

On behalf of the data controller

Name

Position

Telephone number

E-mail

Signature _____

On behalf of the data processor

Name

Position

Telephone number

E-mail

Signature _____

15 DATA CONTROLLER AND DATA PROCESSOR CONTACTS/CONTACT POINTS

15.1 The parties may contact each other using the following contacts/contact points:

15.2 The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Name	
Position	
Telephone number	
E-mail	

Name	René Steenfeldt
Position	CTO
Telephone number	+45 3111 6402
E-mail	RST@livehouse.com

Please add Information on 24/7-365 contact details, in case of data breach discovery

16 APPENDIX A: INFORMATION ABOUT THE PROCESSING

16.1 The purpose of the data processor's processing of personal data on behalf of the data controller is:

Provide registration facilities prior to a live-streamed virtual and hybrid event

To deliver the Livehouse Services as described in the Main Agreement. This includes provision of the software-enabled service solution, consisting of the Livehouse Streaming Platform (the "Application") and event production services (the "Production Services") facilitating the data controller's internal and external communication through streaming of virtual and hybrid events.

Provide a wireless system RFID to identify people "tags"

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

Collection of attending persons' names and e-mail address, recording of events, storage, disclosure by transmission, and erasure.

16.3 The processing includes the following types of personal data about data subjects:

Registration prior to events:
Name, title, telephone number, e-mail address, country.

Live-streamed events:
Footage of persons at the physical event

RFID:
If a person carries a tag; it is possible to track this person's location within the range of the reader systems. The data processor does not have access to a list of identifiable persons receiving a tag.

16.4 Processing includes the following categories of data subject:

Persons registered to attend a physical, virtual or hybrid event
The data controller's employees, contractors, customers, participants
End Users

RFID:
Persons carrying a tag

16.5 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 follows the term of the main agreement.

17 APPENDIX B: AUTHORISED SUB-PROCESSORS

17.1 Approved sub-processors

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

NAME	VAT REGISTRATION NUMBER	ADDRESS	DESCRIPTION OF PROCESSING
Amazon AWS	DK39009323	c/o Azets Insight A/S Lyskær 3c, 1. Tv. 2730 Herlev Denmark	Hosting
Amazon AWS	DK39009323	c/o Azets Insight A/S Lyskær 3c, 1. Tv. 2730 Herlev Denmark	CDN / stream
Jet-Stream Services b.v.	NL8523.04.778.B.01	Helperpark 290 9723 ZA Groningen The Netherlands	Stream
Hetzner Online GmbH	DE 812871812	Industriestr. 25 91710 Gunzenhausen Germany	Hosting

Processing activity: The data processor has the general approval of the controller to make use of sub-processors. Without the data controllers written approval, the data processor shall not make use of a sub-processor for a processing activity other than the one described and agreed upon.

Sub-processor: The data processor shall inform the controller of any planned changes concerning the addition or replacement of other sub-processors, thereby allowing the controller to object to such changes. If the controller objects to the changes, the data controller shall notify the data processor within 30 days of receipt of the notification. The controller may object only if the controller has reasonable and concrete reasons for doing so.

17.2 Notice for approval of sub-processors:
Request for change of a sub-processor must be notified 90 days prior to substitution by data processor to the data controller. Data controller must notify within 30 days of receipt of notice whether the sub-processor can be approved.

In the absence of agreement on a change in the use of the sub-processor, the parties shall, by negotiation, try to reach an agreement. If this is not possible, this Agreement may be terminated in accordance with the rules on termination.

18 APPENDIX C: INSTRUCTION PERTAINING TO THE USE OF PERSONAL DATA

18.1 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:

Performance of Livehouse services, including personal data collection, storage, transmission, erasure, and other activities as necessary to provide the Livehouse Services.

18.2 Security of processing

The level of security shall take into account the nature, scope, context and purposes of the processing activity as well as the risk for the rights and freedoms of natural persons

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

Information security at the data processor is based on the standard ISO / IEC 27001 Information technology – Security techniques.
The standard includes the Statement of Applicability (SOA), which forms part of the data processor's Information Security Management System (ISMS). SOA constitutes of policies, procedures, processes, organisational decision-making processes and activities in the following information security control areas

- Organisation of information security
- Human Resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance

Information security
The data processor has implemented policies, controls and processes that cover the information security areas described below:

- Confidentiality
  Ensure that unauthorized persons cannot access data that may be misused to the detriment of the data controller's customers, business associates and employees.
- Integrity
  Ensure that systems contain accurate and complete information.
- Accessibility
  Ensure that relevant information and systems are accessible and reliable.

18.3 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 organizational measures:

The data processor shall maintain its current technical and organizational measures to facilitate compliance with Clause 9.1 and 9.2.

18.4 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 and 11.2., 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.

18.5 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 authorization:

- AWS Frankfurt and Ireland
- Hetzner, Germany
- Jet-Stream, The Netherlands
- Livehouse A/S, Denmark

18.6 Instruction on the transfer of personal data to third countries

The data processor shall use the modernized Standard Contractual Clauses (issued June 2021) as transfer tool for contracts entered into after 27 September 2021.

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.

18.7 Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor.

Pursuant to Article 28, the data processor shall make all information available to the controller in order to demonstrate compliance with the General Data Protection Regulation and this Agreement. In addition, the data processor shall allow the data controller or auditor appointed by the data controller to perform audits in accordance with Article 28(3)(h) of the General Data Protection Regulation.

Every year in Q2 the data processor supplies audits to the standards ISAE3000 and ISAE 3402 to the data controller. These audits are signed by an independent auditor. The audits cover the previous year and demonstrates compliance with the General Data Protection Regulation and with the provisions of the Danish Data Protection Act. First audit report shall be type I; whereas the following years shall be type II.

It is agreed between the Parties that the declaration may be applied in accordance with these provisions:

The audits shall be forwarded without undue delay to the controller for information. The controller may challenge the framework and/or method in an audit and may, in such cases, request a new independent assessment under different frameworks and/or using another method at the data controller's expense.

The controller may, on the basis of the results of the internal audit, request the data processor to take further security measures to ensure compliance with the General Data Protection Regulation, data protection provisions of other EU law or the national law of the Member States and these Provisions.

In addition, the controller or a representative of the controller shall have access to inspections, including physical inspections, to the locations 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.

Any costs incurred by the controller in connection with a physical inspection shall be carried by the controller. However, the data processor is obliged to allocate the resources (mainly the time) necessary for the controller to carry out such inspections.

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

In accordance with ISO27001 – supplier relationships – the data processor requests audit reports, inspection reports from the sub-contractors and makes this information available to the data controller on request.

The data processor shall facilitate to the extent commercially practicable, the data controller, or its authorized third-party representative subject to an appropriate confidentiality agreement, to conduct an audit or inspection during regular business hours. The data controller shall carry cost incurred from third parties or the sub-processor.

19 APPENDIX D: THE PARTIES' TERMS OF AGREEMENT ON OTHER SUBJECTS

N/A

20 APPENDIX E: AFFIDAVIT REGARDING DELETION OF DATA UPON TERMINATION OF AGREEMENT

Master data

This declaration is issued by Livehouse A/S:

VAT registration number: 35038574

I, the undersigned, solemnly declare on behalf of the company - and

1. confirm that data processed under this Agreement were deleted in accordance with point 11.1 of the Agreement;
2. confirm that data were deleted as per the below date.
3. confirm that deletion was executed, and that data are not anonymised or otherwise stored without legal basis.
4. Allow the data controller to audit the accuracy of this declaration with us, and our relevant sub-processors. Such control can be started by the data controller no later than 90 days after receipt of this declaration. Any costs from third parties shall be carried by the data controller.

Name: Title:

Signature: _____ Date:

Deletion

The date of data deletion: