DATA PROCESSING AGREEMENT

Standard Contractual Clauses

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

between

Name:

Address:

ZIP code & City:

Country:

Company Registration No.:

(the data controller)

and

Relewise ApS
Trindsøvej 8, 1st floor
8000 Aarhus C
Danmark
CVR: 41311290

(the data processor)

each party'; together 'the parties'

HAVE AGREED on the following Contractual Clauses (the Clauses) 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. These 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 regarding 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 services to recommend, search and target content and products (see appendix A.1), the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

4. These 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 authorized 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. These 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 owns any data provided to and processed by the Data Processor.

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

3. The data controller has the right and obligation to make decisions about the purposes and means of the processing of any data, such as personal data.

4. The data controller shall be responsible, among others 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

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by European Union or Member State law to which the processor is subject to. 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.

   The platform allows for extensions, such as built-in user profile as well as other entities. Here including new data attributes that can be used for dynamic filtering and relevance impact. The data controller is therefore required to ensure that data containing personal data are not categorized outside the data categories which is already established by the Clauses (See Appendix A.4) If the data processor discovers and assesses that extended data does not comply with the above, the data controller is immediately notified and the data controller pays the data processor separately, after time and material has passed to handle the fulfillment of the rights of the data subjects..

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 people to whom access has been granted shall be kept under periodic review. Based on 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 of the Data Protection Regulation states that the data controller and the data processor, taking into account the current technical level, the implementation costs and the nature, scope, context and purpose of the processing in question, as

well as the risks of varying probability and seriousness for physical rights and freedoms of individuals, implements appropriate technical and organizational measures to ensure a level of protection appropriate to these risks.

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. This includes the following:

a. Pseudonymization and encryption of personal data, here especially regarding the data processors relation to sub-data processor(s). See Appendix B.1.

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 procedure for regularly testing, assessing and evaluating the effectiveness of technical and organizational 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 the 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 organizational 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 in GDPR.

   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

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

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfillment of the Clauses without a prior general written authorization of the data controller.

   The data processor has the data controller's general authorization for the use 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). This objection must be made within 21 days from the data controller have received the notification of changes. Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorized by the data controller can be found in Appendix B.

3. When 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 organizational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

   The data processor is therefore responsible for requiring that the sub-processor at least comply with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

4. 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 the data controller gives 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.

5. The data processor must, in his agreement with the sub-processor, include the data controller as a beneficiary third party in the event of the data processor's bankruptcy, so that the data controller can enter into the data processor's rights and assert them against sub-processors, such as e.g. enables the data controller to instruct the sub-processor to delete or return the personal data

6. 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 fulfillment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – 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 organizations

1. Any transfer of personal data to third countries or international organizations by the data processor shall only occur based on documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

2. In case of transfers to third countries or international organizations, where the data processor has not been instructed to perform by the data controller. It is required under EU or Member State law to which the data processor is subject, that 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 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.

c. process the personal data in a third country.

4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer basis under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

5. The Clauses shall not be confused with standard Data Protection Clauses as referred to in Article 46(2)(C) and (d) GDPR, and these Clauses cannot be relied upon by the parties as a transfer basis under Chapter V GDPR.

9. Assistance to the data controller

1. Considering the nature of data processing, the data processor shall assist the data controller by appropriate technical and organizational measures, insofar as this is possible. And in the fulfillment 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.

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore consider the nature of the data processing and the information available to the data processor, and 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. It is the data controller’s obligation to communicate without undue delay 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. It is 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. It is 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.

3. The parties shall define in Appendix C the appropriate technical and organizational 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

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 24 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 breach 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.

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 of damage, if 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.

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.

5. Signature

On behalf of the data controller

Name

Title

Phone

Email

Date and signature ______________________________

On behalf of the data processor

Name	Brian Holmgård Kristensen
Title	CPO
Phone	+45 51270774
Email	bhk@relewise.com

Date and signature ______________________________

15. Data controller and data processor contacts/contact points

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

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

Data controller:

Name

Title

Telephone

Email

Data processor:

Name	Brian Holmgård Kristensen
Title	CPO
Telephone	+45 51270774
Email	bhk@relewise.com

Appendix A Information about the processing

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

The processing of personal data is used to be able to search, to recommend and target products and other content on the data controller's website, emails, mobile services, trading platforms, search engines, social media and other web-related services, as well as on non-digital contact points for storing data, including product and personal data, as well as the use of algorithms on this data, as referred to in the "Customer Agreement", which is concluded as a separate written agreement from the Clauses.

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):

All data is collected and received from the data controller, via API integration, from which registration, storage and processing are subsequently systematically and automatically carried out by the platform of the data processor, with which the platform subsequently enables the data controller to query relevant and personalized recommendations and searches. For this, the following types of processing are performed: recovery, search, use, juxtaposition, interconnection, encryption, restriction, and deletion.

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

- Default data attributes
  - Profile ID (also known as AuthenticatedId)
  - Alternative Profile ID (also known as TemporaryId)
  - Identifiers (Optional – additional IDs to recognize a user)
  - Email (Optional)
  - Other keys for user identification (Such as Customer Number – Optional)
  - Behavior pattern (product views, category views, shopping cart content, placing orders, viewing content, and interaction with recommendations and search)
  - Classifications (for example, UserType=B2B)
- In addition, additional attributes can be stored optionally, and thus any other personal data defined by the data controller can be processed.
  - The data controller commits to ensure that these additional attributes may not be used to store personally identifiable data.
- The data controller commits to ensure that any classification or contained data attribute is not used to store personally identifiable data.
- All personal data, including "Profile ID", "Alternative Profile ID", "Identifiers" and/or Email are generally optional, and the data processor can continue to provide a limited range of functions, even if only anonymous data is used.
- The data processor alone decides the data, which is stored on users to Relewise, here including the use of IDs (see "Standard data attributes") to recognize users and finally the use of pseudonymized IDs.
- If the data subject invokes the right to restriction of processing, it is the responsibility of the controller to ensure that "Profile ID", "Alternative Profile ID", "Identifiers", "Email" and/or other personal identifiable information are not included. The data processor will thus treat this customer anonymously.
- It is the responsibility of the data controller to ensure that unnecessary personal data is not included. The data processor can advise on what information is necessary to enable the provision of the very services that the data controller wishes to use.

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

The data subjects whose personal data may be processed are natural persons who interact with the data controller via any digital channel or platform in which the data controller integrates the Relewise platform, including — but not limited to — websites, apps, mobile or desktop applications, email systems, in-store systems, or other connected interfaces.

All personal data pertaining to these data subjects that is processed under this Agreement is classified as ordinary (non-sensitive) personal data.

Because the Relewise platform permits the data controller to extend and store additional attributes on a user profile, the data controller must ensure that no data falling outside the scope of ordinary personal data — such as special categories of personal data under Article 9(1) GDPR, or data relating to criminal convictions under Article 10 — are transmitted to the data processor. The controller remains solely responsible for verifying that any attribute it adds is compliant with this requirement.

The parties may agree in writing to extend the personal data covered by the Clauses.

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 processing is not limited in time and thus lasts until the "Customer Agreement" between the parties is terminated.

Appendix B Authorized sub-processors

B.1. Approved sub-processors

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

NAME	DESCRIPTION OF PROCESSING
Microsoft Ireland Operations Ltd. (Microsoft Azure)	Provision and operation of Microsoft Azure cloud services and resources that Relewise deploys inside Microsoft's EU Data Boundary (i.e., Azure data centers located in the EU/EEA/EFTA). Microsoft hosts, stores, transmits and otherwise processes personal data solely on Relewise's documented instructions and in accordance with the Microsoft Online Services Data Protection Addendum.

The data controller shall at the commencement of the Clauses authorize the use of the above-mentioned sub-processor for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorization – 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.

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 data processor is instructed to process personal data only (see Appendix A.3) for the purpose described in Appendix A.

C.2. Security of processing

The level of security shall consider:

The security of processing is considered an integral part of the provisions of the data processing agreement. The processing security must reflect the following:

Setting up access to data containing personal data is thus limited and granulated to only authorized employees, who can access this data, and at the same time the data processor is subject to confidentiality with respect to personal data and must ensure that the employees are subject to confidentiality obligations. The obligation of confidentiality shall also apply after the expiry of the Clauses.

The data processor is then entitled and obliged to make decisions, and implement these, on the technical and organizational security measures to establish the necessary (and agreed) level of security.

However, the data processor shall, in any case and at least, implement the following measures agreed with the controller:

See Appendix A.3, the data processor receives a pseudo-anonymized "Profile ID" and "Alternative Profile ID", which thus ensures that only by means of supplementary information stored separately with the data controller that personal data, with the data processor, can be used to assign to an identified or identifiable natural person.

The data processor processes and converts received data in real time and then persists inferred data in a non-standard (binary) format containing measures related to fault tolerance, restoring, and maintaining integrity.

Thus, the data processor can recover lost, corrupt, or infected data at any time, for the sole purpose of continuing to provide the service to the data controller.

The data processor formalizes written procedures requiring:

- processing of personal data only when there is an instruction.
- the data controller is informed in cases where the processing of personal data is deemed to be in breach of the law.
- that agreed security measures be put in place for the processing of personal data in accordance with the Clauses.
- access to personal data is limited to users with work-related needs.

An ongoing assessment of whether the procedures should be updated is carried out on an ongoing basis, and at least once a year.

Personal data transmitted to the data processor via the API, the data from data controller to data processor, is only transmitted encrypted. Personal data transmitted from the data processor to the data controller, also via the API, is also always encrypted. Other forms of transmission of personal data between the parties, which are not via the API, must also be exclusively encrypted.

In accordance with Appendix B.1, data is stored at from approved sub-processors, where data is stored in the data processor's own binary format, which is not readable to anyone other than the data processor himself, without special technical insight and competence. In addition, data backups are stored for future recovery in case of data loss. These backups are stored for 30 days with the same approved sub-processor.

In the event of errors, these are logged and stored with the same sub-processor as the other data. The logging is stored solely for the purpose of quickly recreating and correcting any errors and is automatically deleted after 30 days.

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 organizational measures:

- Assist the data controller with documentation that applicable personal data legislation is being complied with in accordance with paragraph 12.

The data controller shall pay the data processor separately and after time and materials to handle the duty of assistance and the fulfillment of the data subject's rights.

- In addition, the data processor shall assist, by means of technical measures, via the API and through the management system, in fulfilling the data controller's obligation to respond to requests for the exercise of the data subjects' rights, as laid down in Chapter 3 of the Data Protection Regulation.

C.4. Storage period/erasure procedures

The duration of the retention of personal data is not limited in time and thus lasts until the "Customer Agreement" between the parties is terminated or ends.

Upon termination of the service relating to the processing of personal data, the data processor deletes the personal data in accordance with provision 11.1, unless, after the signature of these provisions, the data controller has changed the data controller's original choice. Such changes shall be documented and kept in writing, including electronically, in conjunction with the Clauses.

C.5. Data 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:

- All personal data is processed exclusively within Microsoft Azure data centers that are part of Microsoft's "EU Data Boundary", i.e. located in EU Member States or in the EEA/EFTA countries (Iceland, Liechtenstein, Norway).

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

The data controller agrees that the data processor uses Microsoft Azure data centers that fall within Microsoft's "EU Data Boundary" (i.e., facilities situated in EU Member States or the EEA/EFTA countries) – and that the data processor may transfer personal data to a third country (outside the EU/EEA/EFTA) or an international organization only if the sub-processor has provided the necessary guarantees, etc., as specified in Chapter 5, Article 46 of the Personal Data Regulation. Here include by applying the standard contractual clauses adopted by the European Commission, or provided that the European Commission has established that: the third country or international organization concerned has an adequate level of protection or that the data processor has secured another legal basis for transmission. However, with the proviso that the data processor ensures compliance with applicable legal practice regarding third country transfers.

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.

The data processor shall, within a reasonable time and without undue delay, at the request of the data controller and at the expense of the data controller, obtain a statement of assurance from an independent third party concerning the data processor's compliance with the Data Protection Regulation, data protection provisions of other EU law or the national law of the Member States and these Clauses.

It is agreed between the Parties that the following types of statement of assurance may be used in accordance with these Provisions:

The following declarations are approved by the parties:
ISAE3000, ISO27701/ISO27001 certificate, SOC2 or similar. declarations. If the data processor cannot produce such a declaration, then the data controller can request the data processor to complete a corresponding questionnaire, which is completed at the data controller's own expense.

The statement of assurance shall be forwarded without undue delay to the data controller for information. The data controller may challenge the framework and/or methodology of the declaration and may, in such cases, request a new statement of assurance under a different framework and/or using another method.

Based on the findings of the statement of assurance, the data controller is entitled to request the implementation of further measures to ensure compliance with the Data Protection Regulation, data protection provisions of other EU law or the national law of the Member States and these Clauses.

In addition, the data controller or a representative of the data controller shall have access to inspections, including physical inspections, with 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. Such inspections may be carried out whenever the data controller deems it necessary.

Appendix D The parties' terms of agreement on other subjects

This agreement is subject to Danish law, and any disputes arising from it shall be resolved in accordance with Danish law.

The Clauses shall be signed in duplicate, each of which shall constitute an original.