

Standard Contractual Clauses

For the purposes of Article 28(3) and (4) of Regulation 2016/679 (the GDPR) and the sub-processors processing of personal data on behalf of the data processor

between

Garuda A/S, Ledelse & Udvikling
CVR-nummer: 68 75 56 11
Voldbjergvej 14, 2. sal
8240 Risskov
Danmark

(the data processor)

and

A Bigger Boat
CVR: 38684906
Haslegårdsvej 8-12, D37
8210 Aarhus V
Denmark

(the sub-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

1. Table of Contents	2
2. Preamble	3
3. The rights and obligations of the data processor.....	3
4. The sub-processor acts according to instructions	4
5. Confidentiality	4
6. Security of processing	4
7. Use of other sub-processors	5
8. Transfer of data to third countries or international organisations	6
9. Assistance to the data controller	7
10. Notification of personal data breach	8
11. Erasure and return of data.....	8
12. Audit and inspection	9
13. The parties' agreement on other terms	9
14. Commencement and termination	9
15. Data processor and sub-processor contacts/contact points	10
Appendix A Information about the processing	11
Appendix B Authorised sub-processors.....	12
Appendix C Instruction pertaining to the use of personal data	13
Appendix D The parties' terms of agreement on other subjects	17

2. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the sub-processor, when processing personal data on behalf of the data processor.
2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) cf. Article 28 (4) 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 Autosspots, the sub-processor will process personal data on behalf of the data processor 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 processor's conditions for the sub-processor's use of other sub-processors and a list of sub-processors authorised by the data processor.
8. Appendix C contains the data processors instructions with regards to the sub-processors processing of personal data, the minimum security measures to be implemented by the sub-processor and how audits of the sub-processors and any other 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 sub-processor from obligations to which the sub-processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3. The rights and obligations of the data processor

1. The data processor is responsible for ensuring that the sub-processor is imposed the same obligations as the data processor is imposed pursuant to the data processor agreement entered into between the data processor and the data controller, which regulates the data processor's processing of personal data on behalf of the data controller cf. Article 28 (3), as well as the Data Protection Regulation (see GDPR Article 28), data protection provisions set under other Union law or the national law of the Member States and these Provisions.

2. The data controller shall ensure that the sub-processor has appropriate technical and organizational measures so that the processing meets the requirements of this Regulation and the data processor agreement entered into by the data processor and the data controller.
3. The data processor shall be responsible, among other, for ensuring that the processing of personal data, which the sub-processor is instructed to perform, has a legal basis.

4. The sub-processor acts according to instructions

1. The sub-processor shall process personal data only on documented instructions from the data processor, unless required to do so by Union or Member State law to which the sub-processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data processor 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. As it is the data controller, who decides for what purposes and with what aids the personal data may be processed, cf. the GDPR Article 4, no. 7, the data processor's instructions reflects the instructions that the data processor has received pursuant to the data processor agreement entered into between the data processor and the data controller, which regulate the data processor's processing of personal data on behalf of the data controller, cf. Article. 28 (3). The purpose of this sub-data processor agreement is exactly to impose the same obligations to the sub-processor as the data processor is imposed by the GDPR. 28, cf. Article. 28 (4).
3. The sub-processor shall immediately inform the data processor if instructions given by the data processor, in the opinion of the sub-processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

1. The sub-processor shall only grant access to the personal data being processed on behalf of the data processor to persons under the sub-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 sub-processor shall at the request of the data processor demonstrate that the concerned persons under the sub-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. This obligation is imposed on the sub-processor to the same extent as it is imposed on the data processor pursuant to this sub-data processor agreement, as prescribed in the GDPR Article 28 (4).

The data processor 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. Furthermore, the sub-processor shall assist the data processor in ensuring compliance with the data controller's obligations pursuant to Article. 32 GDPR, by *inter alia* providing the data processor with information concerning the technical and organisational measures already implemented by the sub-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. This information is made available for the data processor to pass on to the data controller.

If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the sub-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 other sub-processors

1. The sub-processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (another sub-processor).
2. The sub-processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data processor.
3. The sub-processor has the data processor's general authorisation for the engagement of sub-processors. The sub-processor shall inform in writing the data processor 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 processor can be found in Appendix B.

4. Where the sub-processor engages another sub-processor for carrying out specific processing activities on behalf of the data processor, 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 sub-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 processors request – be submitted to the data processor, thereby giving the data processor 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 processor.
6. The sub-processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the sub-processor – the data processor 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 sub-processor, e.g. enabling the data processor to instruct the sub-processor to delete or return the personal data.
7. If the sub-processor does not fulfil their data protection obligations, the sub-processor shall remain fully liable to the data processor 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 Article 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

1. Any transfer of personal data to third countries or international organisations by the sub-processor shall only occur on the basis of documented instructions from the data processor and shall always take place in compliance with Chapter V in the GDPR.
2. In case transfers to third countries or international organisations, which the sub-processor has not been instructed to perform by the data processor, is required under EU or Member State law to which the sub-processor is subject, the sub-processor shall inform the data processor 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 processor, the sub-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
 - c. have the personal data processed in by the data processor in a third country
4. The data processors instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V in the 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 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 in the GDPR.

9. Assistance to the data controller

1. Taking into account the nature of the processing, the sub-processor shall assist the data processor 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 sub-processor shall, insofar as this is possible, assist the data processor in the data processors assistance to 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 sub-processors obligation to assist the data processor pursuant to Clause 6.3., the sub-processor shall furthermore, taking into account the nature of the processing and the information available to the sub-processor, assist the data processor when assisting 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.
3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the sub-processor is required to assist the data processor 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 sub-processor shall, without undue delay after having become aware of it, notify the data processor of the personal data breach.
- 2. The sub-processor's notification to the data processor shall, if possible, take place within 48 hours after the sub-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 sub-processor shall assist the data processor in the data processors assist to data controller in notifying the personal data breach to the competent supervisory authority, meaning that the sub-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 sub-processor when assisting the data processor in 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 sub-processor shall be under obligation to delete all personal data processed on behalf of

the data processor and certify to the data processor that it has done so unless Union or Member State law requires storage of the personal data.

12. Audit and inspection

1. The sub-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 processor or another auditor mandated by the data processor and data controller.
2. Procedures applicable to the data processor's audits, including inspections, of the sub-processor and other sub-processors are specified in appendices C.7. and C.8.
3. The sub-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 sub-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.
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 processor 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 processor

Name Rasmus Hall Mortensen
Position CEO

Date

Signature



On behalf of the sub-processor

Name	Jonas Kvist Jensen
Position	CEO
Date	
Signature	

15. Data processor and sub-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.

On behalf of the data processor

Name	Søren Skou Jessen
Position	GDPR Compliance Consultant
Telephone	+45 29365164
E-mail	ssj@garuda.dk

On behalf of the sub-processor

6/1/2021

Name	Jonas Kvist Jensen
Position	CEO
Telephone	+45 42646809
E-mail	jonas@abiggerboat.dk



Appendix A Information about the processing

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

Processing of the data controller's personal data is done with the aim to generate template based promotional video content.

A.2. The subprocessors processing of personal data on behalf of the data processor shall mainly pertain to (the nature of the processing):

The data processor processes data by general operation and delivery of the services under the main agreement, including by hosting, viewing, organizing, receiving, forwarding, structuring, customizing, implementing, searching, processing, storing, transferring, recovering, deleting, limiting, maintaining, troubleshooting, and other services related to providing the service.

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

Company names, addresses, phone numbers, various images supplied by the companies, job titles, job descriptions, promotional te

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

- Employees
- Customers

A.5. The subprocessors processing of personal data on behalf of the data processor may be performed when the Clauses commence. Processing has the following duration:

The processing is not limited in time and lasts until the agreement between the parties on the delivery of the data processor's service to the data controller is terminated or repealed by one of the parties.

Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data processor authorises the engagement of the following sub-processors:

NAME	CVR	ADDRESS	DESCRIPTION OF PROCESSING
Hetzner	DE812871812	Industriestr. 25, 91710 Gunzenhausen, Germany	Hosting of web an database servers The processing of data by Hetzner is contractually required to take place according to the standard sub- data processor agreement, attached to this Annex B as attachment B.1
Google Commerce Limited	DK12686765	Gordon House, Barrow Street, Dublin 4, Ireland	API Location services based on addresses The processing of data by Google is contractually required to take place according to the standard sub- data processor agreement, attached to this Annex B as attachment B.2

Attachment B.1-B.2 as referred to above in this Appendix B can be obtained upon request sent to jonas@abiggerboat.dk

The data processor shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. The sub-processor shall not be entitled – without the data processors 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

Cf. 7.3

Appendix C Instruction pertaining to the use of personal data

Appendix A

C.1. The subject of/instruction for the processing

The sub-processors processing of personal data on behalf of the data processor shall be carried out by the sub-processor performing the following:

The data processor processes data by general operation and delivery of the services under the main agreement, including by hosting, viewing, organizing, receiving, forwarding, structuring, customizing, implementing, searching, processing, storing, transferring, recovering, deleting, limiting, maintaining, troubleshooting, and other services related to providing the service.

C.2. Security of processing

The level of security shall take into account that the processing concerns non-sensitive personal data about a limited number of data subjects in well-known IT systems.

The purpose of the security measures implemented by the data processor is to ensure:

- **Confidentiality:** Ensuring that personal data is accessible only to those authorized to process the personal data.
- **Integrity:** Safeguarding the accuracy and completeness of information and processing methods.
- **Availability:** Ensuring that authorized users have access to Services, information and associated assets when required.

Organisation of Information Security

The data processor ensures, inter alia, that:

- Security issues are reviewed and progressed.
- Security risk assessments are performed on a regular basis.
- Effectiveness of Information Security is monitored.

Human Resource Security

The data processor ensures, inter alia, that:

- All employees and contractors work in accordance with all policies and procedures which includes information security specific requirements.

Access Control

The data processor ensures, inter alia, that:

- Employees, contractors, suppliers and anyone else follow a number of controls and procedures, which exist to limit access to confidential information.
- An access control policy is in place.

Physical and Environmental Security

The data processor ensures, inter alia, that controls and procedures exist to ensure adequate physical security, including:

- Building and individual alarm systems.
- Restricted access to the building and further restricted access within it.
- Secure lockers, drawers, storage and safes.
- Clear desk and clear screen policy.

Operations Security

The data processor ensures, inter alia, that:

- Operations are managed by multiple coherent Information Security policies and Change Management processes to ensure correct and secure operations of information processing facilities.

Communications Security

The data processor ensures, inter alia, that:

- Communication is controlled and managed by established procedures and guidelines.
- Information Security Steering Group is established to ensure appropriate security measures and processes.

System Acquisition, Development and Maintenance

The data processor ensures, inter alia, that:

- Development policy provides guidelines to ensure processes, technical environments and processes for developing and implementing systems through secure coding and development practices.
- Information Security requirements for mitigating the risks associated with any supplier's access to the data processor's assets is documented.
- An Information Security policy for supplier relationships has been prepared and implemented.

Information Security Incident Management

The data processor ensures, inter alia, that:

- Security incidents are maintained, updated and monitored.
- Procedures for breach, GDPR and Security Incident Management has been prepared and implemented.

Compliance

The data processor shall implement appropriate technical and organisational measures to protect personal data against the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed by the data processor. In particular the data processor shall implement measures ensuring that:

- Anyone managing and handling personal data understands that they are contractually obliged to follow good data protection practice.
- Anyone managing and handling personal data is appropriately instructed to do so.
- Everyone managing and handling personal data is appropriately supervised.

C.3. Assistance to the data controller

The sub-processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data processor in their assist of the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

The rights of the data subject, cf. 9.1.

- The sub-processor must assist in observing the data subjects' rights by e.g. being able to provide insight into, delete, limit and correct information, and ensure that the sub-processor's sub-processors also is able to do so.
- The sub-processor must assist in fulfilling the data subjects' rights without any undue delay
- The sub-processor must have a procedure for how they process requests from a data subject about their rights.

Data breach and incidents, cf. 9.2.

Notice of a breach or an incident must be completed as soon as possible within the 24-hour deadline, at no extra cost.

Information to be sent:

- Facts about the breach (time, place, cause)
- When the breach started, when it was discovered, and when the breach was stopped
- The nature of the data breach, including whether there has been a breach of confidentiality, integrity and accessibility
- The categories and the approximate number of data subjects affected, if possible
- The categories of personal information, if possible.
- Name and contact information of the contact point where further information can be obtained
- A description of the likely consequences of the breach
- A description of the measures taken or proposed to be taken as part of the handling of the breach, and the possible harmful effects of the breach

C.4. Storage period/erasure procedures

Personal data is stored until termination of cooperation between Garuda and A Biggger Boat after which the personal data is automatically erased by the sub-processor.

Upon termination of the provision of personal data processing services, the sub-processor shall either delete or return the personal data in accordance with Clause 11.1., unless the data processor – 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:

The place of the data processor's place of business or within the data regions mentioned in Annex B, section B.1.

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

Any transfer of personal data to third countries or international organizations can only be done to a secure third country, on a validly EU commission standard contractual clauses.

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 subprocessor 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 sub-processor shall within a 12 month period at the subprocessors expense obtain an inspection report concerning the sub-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 inspection reports may be used in compliance with the Clauses:

The inspection report shall without undue delay be submitted to the data processor for information. The data processor may contest the scope and/or methodology of the report and

may in such cases request a new audit/inspection under a revised scope and/or different methodology.

Based on the results of such an audit/inspection, the data processor 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 processor or the data processors 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 processor deems it required."

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

The data processor must annually, at its own expense, obtain an auditor's statement from an independent third party or an audit report on the sub-processor's compliance with the GDPR, data protection provisions of other EU or national law of the Member States.

Documentation of such inspections is sent to the data controller for information without undue delay.

Appendix D The parties' terms of agreement on other subjects

D.1. Default and disputes

Defaults and disputes are regulated in the Main Agreement. In the event that the Main Agreement does not take a stand on this, the general law of contract of the applicable court shall apply to the Agreement.

Regulation of dispute resolution, including choice of law and venue, in the Main Agreement also applies to the Agreement, as if the Agreement were an integrated part thereof. In the event that the Main Agreement does not take a stand on this, the following provisions shall apply to the Agreement.

The agreement is subject to Danish law with the exception of:

- a) Rules leading to the application of another law than Danish law and
- b) United Nations Convention on International Trade in Goods (CISG)

In the event of a disagreement in connection with the Agreement, the parties shall, with a positive, cooperative and responsible attitude, seek to enter into negotiations with a mediator with the intention of resolving the dispute. If necessary, the negotiations must be made at the executive level of the parties' organizations.

If the parties are unable to reach a settlement by negotiation, the parties are entitled to demand that the dispute be settled definitively by litigation in courts. The court in Aarhus has been chosen as the venue. However, the referral rules of the Danish Administration of Justice Act (retsplejeloven) to the High Court and the Maritime and Commercial Court continue to apply.

Prima facie, it is considered a material breach, if the sub-processor does not comply with the obligations in the Sub-processor Agreement, the current legislation regarding data protection and the requirements in the documents that make up annexes to the Sub-processor Agreement.

D.2. Compensation and insurance

Compensation and insurance issues are regulated in the Main Agreement. In the event that the Main Agreement does not take a stand on this, the sub-processor is liable for damages in accordance with the general rules of Danish law in the event of a breach of the Sub-processor Agreement. If the Data processor is made liable by a third party for the sub-processor's and / or any sub-processor's non-compliance with the Sub-processor Agreement, including the Sub-processor Agreement's annexes, and / or violation of applicable data protection legislation, the Sub-processor shall indemnify the Data processor for all costs, fees, expenses, which the Data processor has incurred or incurred as a result thereof.