Standard Contractual Clauses

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

between

Company		
VAT		
Address		
Zip / City		
Country		

(the data controller)

and

COMAsystem ApS
VAT DK 33 86 52 79
Transformervej 14
DK 2860 Søborg
Danmark

(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.

References to "Member State" in these provisions shall be understood as a reference to "EEA Member States".

Table of Contents

1. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

3. In the context of the provision of COMAsystem, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

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

5. Four appendices are attached to the Clauses and form an integral part of the Clauses.

6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

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

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

11. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

2. 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 data protection provisions and the Clauses.

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

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

3. The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

4. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

5. Security of processing

1. Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

   a. Pseudonymisation and encryption of personal data;
   b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
   c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
   d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data

processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by inter alia providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

   If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

6. Use of sub-processors

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

2. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

3. The data processor shall engage sub-processors solely with the specific prior authorisation of the data controller. The data processor shall submit the request for specific authorisation at least one month prior to the engagement of the concerned sub-processor. The list of sub-processors already authorised by the data controller can be found in Appendix B.

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

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

5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

6. The processor shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the processor has factually disappeared, ceased to exist in law or has become insolvent – the controller shall have the right to terminate the sub-processor contract and to instruct the sub-

processor to erase or return the personal data.

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.

7. Transfer of data to third countries or international organisations

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

2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

   a. transfer personal data to a data controller or a data processor in a third country or in an international organization
   b. transfer the processing of personal data to a sub-processor in a third country
   c. have the personal data processed in by the data processor 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 tool 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 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.

8. Assistance to the data controller

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

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

   a. the right to be informed when collecting personal data from the data subject
   b. the right to be informed when personal data have not been obtained from the data subject
   c. the right of access by the data subject
   d. the right to rectification
   e. the right to erasure ('the right to be forgotten')
   f. the right to restriction of processing

g. notification obligation regarding rectification or erasure of personal data or restriction of processing
h. the right to data portability
i. the right to object
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, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

   a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, The Danish Data Protection Agency, Carl Jacobsens Vej 35, DK-2500 Valby, (+45) 33 19 32 00, dt@datatilsynet.dk, 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, Carl Jacobsens Vej 35, DK-2500 Valby, (+45) 33 19 32 00, dt@datatilsynet.dk, 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 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.

9. 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 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.

10. Erasure and return of data

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.

11. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

12. 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.

13. 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
   a. On behalf of the data controller - see last page of this document.
   b. On behalf of the data processor - see last page of this document.

14. 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.

Name:	Christian Richter-Pedersen
Position:	CEO
Telephone:	(+45) 69 15 99 60
Email:	crp@comasystem.eu

The data processor's contact person is stated on the purchase invoice from COMAsystem.

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 data processor is responsible for storing and processing the customer's contract data, which includes personally identifiable information.

The data processor handles the customer's contract files and documents, including information entered into the system by the data controller. The data processor sends email notifications according to the data provided by the data controller in the system.

Under no circumstances may the data processor share the customer's information with any third parties other than the sub-processors specifically mentioned in this agreement, except in the case of external legal claims arising from EU law or national law of member states to which the data processor is subject.

The data processor may not use and/or process the customer's data for other purposes.

The processing may in the future include additional system functionalities, including automated analyses or assistant features, to the extent that such functionalities are an integrated part of the system's services.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly per-tain to (the nature of the processing):

- Receiving and storing files and associated metadata provided by the data controller.
- Enabling the data controller to create new contracts and documents based on the data provided by the data controller.
- Generating reports and summaries compiled from data provided by the data controller.

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

While it is outside the influence of the Data processor to which data the Data con-troller enters into the system, the Data processors operates under the assumption that any kind of personal and personal identifiable data could be processed.

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

- Employees of the data controller
- Customers
- Suppliers

Appendix B - Authorised sub-processors

B.1 Approved sub-processors

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

NAME	VAT	ADDRESS	DESCRIPTION OF PROCESSING
Unit IT A/S	15660945	Strandvejen 7 DK-5500 Middelfart	Backup
Addo Sign | twoday	29973334	Gærtorvet 1-5 DK-1799 Copenhagaen V **Data locations:** IT Relation Nygårdsvej 5A, DK-2100 Copenhagen Cloud Factory Vestergade 4, DK-6800 Varde	Digital Signatur
Myra Security GmbH		Landsberger Straße 187 80687 München Tyskland **Datacenter co-location:** noris network AG, Deutschherrnstraße 15-19 90429 Nürnberg, Deutschland Digital Realty Germany GmbH (vormals Interxion), Weismüllerstraße 19 60314 Frankfurt/Main, Deutschland Digital Realty Austria GmbH (vormals Interxion), Louis-Häflinger Gasse 10 1210 Wien, Österreich Digital Realty Switzerland GmbH (vormals Interxion) Sägereistraße 35, 8152 Glattbrugg, Schweiz Equinix Kleyerstrasse 90 - 60326 Frankfurt/Main, Deutschland Equinix Science Park 610 - 1098 XH Amsterdam, Niederlande Equinix Aleje Jerozolimskie 65/79 00-697 Warschau, Polen IPB Internet Provider in Berlin GmbH Lützowstraße 106, 10785 Berlin Deutschland The datacenter providers (Digital Realty and Equinix) solely deliver physical co-location infrastructure (power, cooling and facilities) without access to systems, networks or personal data. All processing is carried out exclusively by Myra.	Web Application Firewall
Scaleway SAS	FR 35 433115904	**Datacenter Colocations:** Op Core* EU (France)	AI inference Quantum computing Web service

The data controller shall on the commencement of the Clauses authorise the use of the above mentioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

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 may only handle and store the data controller's contract files and documents, as well as information entered into the system by the data controller.
- The data processor shall send e-mail notifications according to the dates and information specified by the data controller in the system.
- Under no circumstances may the data processor share the customer's data with other third parties without the explicit permission of the data controller. If there is a requirement from EU law or the national law of the Member States to which the Data Processor is subject, this must be respected.
- The data processor must be aware that the processing must be in accordance with the GDPR rules and all relevant legislation to which the data processor is subject.
- The data processor may not use or process the Customer's data for purposes other than those described above.

C.2 Security of processing

The level of security shall take into account:
The processing may include personal data subject to Article 9 of the GDPR on "special categories of personal data," for which a "high" level of security should be established.

The data processor is therefore authorized and obligated to make decisions regarding the technical and organizational security measures to be implemented to establish the necessary (and agreed upon) level of security.

However, the data processor must – in any case and at a minimum – implement the following measures, as agreed with the data controller:

- **Risk Assessment**
  The data processor must perform a risk assessment and then implement appropriate technical and organizational measures to address identified risks.

- **Expertise and Resources**
  The data processor must provide sufficient expertise, reliability, and resources to implement appropriate technical and organizational measures to meet the requirements for processing personal data under applicable data protection law.

- **Information Security Policy**
  The data processor must ensure that there is a management-approved information security policy.

- **Organization of Information Security**
  The data processor must ensure that information security is a focus within the organization, with clearly defined roles and responsibilities.

  Furthermore, the data processor's access to the data controller's data must be secured through contracts, confidentiality agreements, and ensuring the separation of functions to minimize errors and misuse of data.

- **Employee Security**
  The data processor must have a process in place for ensuring that employees and consultants are aware of their responsibilities concerning information security.

  The data processor must ensure employee awareness of obligations during employment, and this training must be maintained throughout the duration of the employment. The data processor must conduct awareness training for anyone performing work for the data processor who has access to personal data covered by these provisions. This training must be maintained throughout the duration of their employment.

  The data processor must ensure that any person performing work for the data processor, who has access to personal data covered by these provisions, processes this

- **Asset Management**
  The data processor must ensure ownership of critical assets and keep documentation up to date.

- **Access Control**
  The data processor must have a documented access management process and ensure that access is only granted based on a work-related need.

  The data processor must have defined procedures for creating, closing, and continuously reviewing assigned rights based on the principle of work-related need, as well as decisions about role separation.

  The data processor must have procedures in place for secure login to minimize the possibilities for unauthorized access to systems and applications.

- **Cryptography**
  The data processor must ensure encryption with up-to-date encryption levels for communication over open networks and between systems, and ensure that key management is carried out according to a documented process.

- **Physical Security and Environmental Security**
  The data processor must organize and establish physical protection against natural disasters, malicious attacks, or accidents at the data processor's physical locations.

  The data processor must also ensure protection against unauthorized access to the data processor's physical locations through access control processes for all individuals with access.

- **Operational Security**
  The data processor must ensure that operational procedures are documented and maintained. At a minimum, the following procedures must be included:
  - Malware protection
  - firewall
  - backup
  - Logging and monitoring
  - Management of operational software
  - Vulnerability management
  - ongoing security updates

- **Communication Security**
  The data processor must ensure that networks are managed and controlled to protect information. The data processor must ensure that the data controller's data, communicated internally and externally, is processed legally, ethically, and commercially correct throughout its lifecycle.

  The data processor must ensure that the data controller's data, communicated internally and externally, is processed correctly according to legal, ethical, and business standards throughout its lifecycle. Additionally, access to the network must be protected.

- **Acquisition, Development, Maintenance, and Disposal of Systems**
  The data processor must ensure that security requirements for acquisition, development, maintenance, and disposal are integrated into solutions, and that the requirements of the Data Protection Regulation for data protection by design and by default are adhered to.

- **Changes to Systems**
  The data processor must ensure that changes to IT systems follow a documented change process with appropriate approvals and testing.

  The data processor must ensure that development, testing, and operational systems are kept separate, and that capacity and performance are monitored and managed.

- **Supplier Relationships**
  The data processor must at least impose the same security requirements on subprocessors and other subcontractors that engage with the data processor and ensure compliance with these.

- **Handling of Information Security Breaches**
  The data processor must register and assess information security incidents and report them to the data controller without undue delay. The data processor must develop procedures for collecting evidence in the event of information security incidents.

- **Information Security Aspects of Emergency, Contingency, and Recovery Management**
  The data processor must have developed contingency plans defining how systems or services are to be restored in a timely manner. These contingency plans must be tested annually or whenever there are major changes.

- **Compliance**
  The data processor must continuously check if systems and services meet the requirements of the data processor's security requirements, as well as the effectiveness and capacity of these security measures to ensure ongoing confidentiality, integrity, availability, and resilience of systems and services.

  The data processor must provide an annual ISAE 3000 type II auditor's report.

C.3 Assistance to the data controller

The data processor must ensure that the data controller is notified without undue delay of any request from a data subject regarding the exercise of their rights, received by the data processor. The data processor is not entitled to respond to requests from a data subject regarding the exercise of their rights under applicable data protection law.

The data processor shall provide the data controller with the necessary assistance as required in

accordance with Provisions 9.1 and 9.2, without receiving compensation for the time spent by the data processor.

The data processor must ensure that tools for data extraction are available so that the data processor can provide data to the data controller.

C.4 Storage period/erasure procedures

Personal data is retained for as long as the data controller has their individual account in the provided system. Upon deletion of any entity, the data will exist in the data processor's backup for up to 180 days, after which they are automatically and irrevocably deleted.

Upon termination of the service regarding the processing of personal data, the data processor must either delete or return the personal data in accordance with provision 11.1, unless the data controller – after signing these provisions – has changed their original choice. Such changes must be documented and kept in writing, including electronically, in connection with the provisions.

C.5 Processing location

Processing of the personal data under the Clauses is solely performed at locations listed in Appendix B.1

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

The data processor has not been instructed to transfer personal data to third countries or international organizations.

If the data controller does not provide a documented instruction regarding the transfer of personal data to a third country in these provisions or subsequently, the data processor is not entitled to make such transfers under these provisions.

The data processor does not use transfers to third countries in connection with the processing.

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 annually, at its own expense, obtain an ISAE 3000 type II from an independent third party regarding the data processor's compliance with the Data Protection Regulation, data protection provisions in other EU law or national law of the member states, and these provisions.

The parties agree that the following types of audit report can be used in accordance with these provisions:

ISAE 3000 type II for COMAsystem ApS
The audit report shall be promptly submitted to the data controller for information. The data controller may contest the scope and/or method of the audit report and, in such cases, may request a new audit report under different terms and/or using a different method.

Based on the results of the audit report, the data controller is entitled to request the implementation of additional measures to ensure compliance with the Data Protection Regulation, data protection provisions in other EU law or national law of the member states, and these provisions.

The data controller or a representative of the data controller also has access to conduct inspections, including physical inspections, at the locations where the data processor performs 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.

The data controller's potential expenses related to an inspection are borne by the data controller. However, the data processor is obligated to allocate the resources (mainly time) necessary for the data controller to conduct their inspection. Any expenses of the data processor related to an inspection are borne by the data processor itself and are not the responsibility of the data controller.

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

The data processor or a representative of the data processor conducts an inspection by either (i) reviewing audit reports, (ii) sending a questionnaire to the sub-processor, which the sub-processor must answer, and/or (iii) conducting a planned physical inspection of the locations from which the sub-processor processes personal data, including physical locations and systems used for or in connection with the processing, in order to determine the sub-processor's compliance with the Data Protection Regulation, data protection provisions in other EU law or national law of the member states, and these provisions.

In addition to the planned inspection, the data processor may conduct an unplanned inspection of the sub-processor when the data processor (or the data controller) deems it necessary.

Documentation of and results from inspections must be promptly sent to the data controller for information. The data controller may contest the scope and/or method of the inspection and may, in such cases, request the conduct of a new inspection under different terms and/or using a different method.

Based on the results of the inspection, the data controller is entitled to request the implementation of additional measures to ensure compliance with the Data Protection Regulation, data protection provisions in other EU law or national law of the member states, and these provisions.

The data controller may – if deemed necessary – choose to initiate and participate in a physical inspection at the sub-processor's location. This may occur if the data controller evaluates that the data processor's inspection of the sub-processor has not provided sufficient assurance that the processing by the sub-processor is in compliance with the Data Protection Regulation, data The data controller's potential participation in an inspection at the sub-processor's location does not change the fact that the data processor retains full responsibility for the sub-processor's compliance with the Data Protection Regulation, data protection provisions in other EU law or national law of the member states, and these provisions.

The data controller's potential expenses related to an inspection are borne by the data controller itself. However, the data processor and the sub-processor are obligated to allocate the resources (mainly time) necessary for the data controller to conduct its inspection. Any expenses of the data processor and the sub-processor related to an inspection are borne by the data processor and the sub-processor themselves and are not the responsibility of the data controller.

Appendix D - The parties' terms of agreement on other subjects

D.1 Roles

The data controller may be both the data controller and the data processor for the personal data that the data processor is required to process under these provisions. If the data controller acts as a data processor, the data processor acts as a sub-processor. This does not change the rights and obligations of the parties under this data processing agreement.

D.2 Compliance with Data Protection Regulations

The data processor's processing of personal data under these provisions must comply with the applicable Danish and European data protection laws, including but not limited to the Act No. 502 of May 23, 2018, on supplementary provisions to the regulation on the protection of individuals in relation to the processing of personal data and on the free exchange of such information (the Data Protection Act).

D.3 Security Measures

The data processor must, without undue delay, notify the data controller in writing of any non-compliance with the data processor's security obligations as set out in these provisions, regardless of whether this failure arises from the data processor's own actions or those of its subcontractors.

D.4 Data Breaches

The data processor must not delay notification of a personal data security breach (or suspicion thereof) due to not having full information available. In such cases, the data processor must provide the information that is available.

The data processor must not communicate about data security breaches or non-compliance with these provisions to the public or third parties without prior written agreement with the data controller regarding the content of such communication, unless the data processor is obligated to do so under the law.

D.5 The Data Protection Authority and Other Public Authorities

The data processor must, without undue delay, notify the data controller in writing of any inquiry addressed to the data processor or its subcontractors by: (i) The Data Protection Authority regarding the processing of personal data covered by these provisions, or (ii) A public authority regarding the disclosure of personal data covered by these provisions, unless informing the data controller is prohibited under EU law or the law of a member state.

The data controller is entitled to pass on information received under Appendix C, sections C.7 and C.8, to the Data Protection Authority (or other relevant authorities) upon request from the Data Protection Authority (or other relevant authorities).

D.6 Compensation

The data processor's obligations under these provisions do not give rise to a claim for separate payment to the data processor. The data processor's costs related to its subcontractors are also irrelevant to the data controller.

D.7 Liability

Notwithstanding any other agreements between the parties, the data processor shall indemnify the data controller if the data controller is faced with claims from third parties due to the data processor or its subcontractors violating applicable data protection laws. The data processor is only liable for damages if it or its subcontractors fail to meet their obligations as data processors or subprocessors

under applicable law, or if the data processor or its sub-contractors fail to follow or act contrary to the data controller's lawful and documented instructions. The indemnification obligation is not subject to any agreed limitation of liability in other agreements between the parties. However, the data processor's indemnification obligation does not apply to fines imposed on the data controller under Article 83 of the Data Protection Regulation or sanctions imposed in Denmark under Article 84 of the Data Protection Regulation.

The data controller shall indemnify the data processor if the data processor faces claims from third parties due to the data controller's violation of applicable data protection laws. The data controller is only liable for damages if it fails to meet its obligations as a data controller under applicable law. The indemnification obligation is not subject to any agreed limitation of liability in other agreements between the parties. However, the data controller's indemnification obligation does not apply to fines imposed on the data processor under Article 83 of the Data Protection Regulation or sanctions imposed in Denmark under Article 84 of the Data Protection Regulation.

D.8 Termination

If the data controller objects to planned changes regarding the addition or replacement of a sub-processor and the data processor insists on the planned change, the data controller is entitled to terminate the agreement as defined in section 2.3 of these provisions and these provisions, with effect from the end of the notice period of at least 3 months, which the data processor is obliged to give the data controller, as set out in section 7.3 of these provisions.

Termination under this section does not entitle the data processor to any additional payment.

D.9 Precedence

In the event of a conflict between these provisions and the provisions of other written or oral agreements between the parties, these provisions shall take precedence unless stricter requirements for processing security are set out in other written or oral agreements between the parties.