DATA PROCESSING AGREEMENT

VERSION 4.0 FEBRUARY 2024

CompuSoft A/S

Sunekaer 9

5471 Soendersoe

Denmark

VAT DK21774774

Standard Contractual Clauses

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

between

«COMPANY»
CVR «COMPANYCVR»
«COMPANYADRESS»
«COMPANYZIPCITY»
«COMPANYCOUNTRY»

(the data controller)

and

CompuSoft A/S
VAT DK21774774
Sunekaer 9
DK-5471 Soendersoe
Denmark

(the data processor)

Each a 'party'; together 'the parties'

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1. TABLE OF CONTENTS

2. PREAMBLE

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

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

3. In the context of the provision of the data processor's IT service booking and payment system as specified in CompuSoft's TERMS AND CONDITIONS for hosting ("**Main Agreement**"), 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 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 or any sub-processors are to be performed.

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

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

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

3. THE RIGHTS AND OBLIGATIONS OF THE DATA CONTROLLER

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

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

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

4. THE DATA PROCESSOR ACTS ACCORDING TO INSTRUCTIONS

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

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

5. CONFIDENTIALITY

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need-to-know basis. The list of persons to whom access has been granted shall be kept under periodic

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

review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

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

6. SECURITY OF PROCESSING

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

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

   a. Pseudonymisation and encryption of personal data
   b. The ability to ensure 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 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 in order to engage another processor (a sub-processor).

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

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

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

8. TRANSFER OF DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

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 data processor in a third country or in an international organisation
    b. Transfer the processing of personal data to a sub-processor in a third country
    c. Have the personal data processed 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.

9. ASSISTANCE TO THE DATA CONTROLLER

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

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

    a. The right to be informed when collecting personal data from the data subject
    b. The right to be informed when personal data have not been obtained from the data subject

c. The right of access by the data subject
d. The right to rectification
e. The right to erasure ('the right to be forgotten')
f. The right to restriction of processing
g. Notification obligation regarding retification 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, 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 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 12 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 D 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 return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data.

2. The following EU or Member State law applicable to the data processor requires storage of the personal data after the termination of the provision of personal data processing services:

    a. Arkivloven (Danish Archives Act) – Legislative Decree no. 1201 of 28/09/2016

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

12. AUDIT AND INSPECTION

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

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

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

13. THE PARTIES' AGREEMENT ON OTHER TERMS

1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g., liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. COMMENCEMENT AND TERMINATION

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

2. Both parties shall be entitled to require the Clauses renegotiated if changes in 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	«PERSONSIGNATURETEXT»
Position	«PERSONPOSITION»
Telephone	«PERSONPHONENUMBER»
Email	«PERSONEMAIL»

Date and signature: «PERSONSIGNATUREDATE»

On behalf of the data processor

Name	Thomas Traberg-Larsen
Position	CEO
Telephone	+45 63186318
Email	TTL@COMPUSOFT.COM

Date and signature: «CSSIGNATUREDATE»

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.

Name	«PERSONSIGNATURETEXT»
Position	«PERSONPOSITION»
Telephone	«PERSONPHONENUMBER»
Email	«PERSONEMAIL»

Navn	Thomas Traberg-Larsen
Position	CEO
Telephone	+45 63186318
Email	TTL@COMPUSOFT.COM

APPENDIX A INFORMATION ABOUT THE PROCESSING

CompuSoft A/S offers as a data processor a number of IT services, including hosting, bookings, and payment ("**the System"**). The processing is further described below.

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

The purposes are to give the data controller's employees access to a system that can assist them in managing the customer's bookings and tickets, and in this context, collecting payments and issuing invoices, providing technical support, troubleshooting, and maintaining the System, as well as protecting against fraud, unauthorised actions, and security breaches.

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):

Collection, registration, organisation, structuring, storage, adaptation, or modification of personal data in accordance with the instructions of the data controller.

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

General personal data (cf. Article 6 GDPR):

☐General personal data:

Costumers and guests: Name, address, postcode, city, nationality, telephone number, card details, correspondence, content in free-text fields, purchased products, email address, and in certain instances social security number for governmental and municipal customers. In addition, any registered period of stay, number of people, age, and gender.

Employees: Name, address, telephone number, and email address.

Sensitive personal data (cf. Article 9 GDPR):

☐Race or ethnic origin

☐Political beliefs

☐Religious beliefs

☐Philosophical beliefs

☐Trade union affiliation

☐Genetic data

☐Biometric data

☐Health information, including abuse of medication, drugs, alcohol, etc.

☐A natural person's sexual relationship or sexual orientation

Personal data pertaining to criminal convictions and offences (cf. Article 10 GDPR):

☐Criminal convictions

☐Offences

Data pertaining to social security number (cf. Article 11 GDPR):

☐Social security numbers (in special cases, and solely when the data controller is a municipality or government organisation and only to the extent that it is necessary for the data controller for the purpose of collecting payments)

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

- Costumers, potential customers, and guests
- Employees.

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:

Until the agreement is terminated.

APPENDIX B AUTHORISED SUB-PROCESSORS

B.1. Approved sub-processors

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

NAME	CVR	ADDRESS	DESCRIPTION OF PROCESSING
Cloudflare Inc.		101 Townsend Street, San Francisco, California, 94107 USA. Support access can be done from the U.S. ClaudFlare Inc. is certified under the EU-U.S. Data Privacy Framework. However, the information is stored solely through European data centers in Copenhagen, Frankfurt, Amsterdam, Hamburg, and Oslo.	Cloudflare is a content delivery network (CDN) and cybersecurity company that provides website optimisation, DDoS protection, and other security features to improve the performance of the System and protect against online threats. Cloudflare provides a number of security features that help protect the System against cyberattacks. Cloudflare's firewall blocks malicious traffic, while its SSL certificate encrypts web traffic to protect user data. Cloudflare's DNS services help protect against DNS attacks, while its browser isolation technology helps protect against malware and other threats.

The data controller shall on the commencement of the Clauses authorize the use of abovementioned sub-processors 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.

Personal data may only be stored in the locations indicated in the form above and at the following addresses via the data processor:

- Sunekaer 9 | DK-5471 Soendersoe
- Anderupvej 16 | DK-5270 Odense N

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

The data processor shall submit the request for a specific authorization at least two months before the use of the relevant sub-processor.

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's tasks according to the Main Agreement.

The data processor shall process the personal data on behalf of the data controller in accordance with the written instructions from the data controller and solely for the purpose specified in the data processing agreement. The instructions exhaustively include the following:

- Delivering the System
- Collection, storage, and handling of the personal data in accordance with the data controller's instructions and applicable data protection legislation
- Ensuring the confidentiality, integrity, and availability of the personal data through appropriate technical and organisational security measure
- Erasure or return of the personal data according to the instructions of the data controller at the termination of the data processing agreement
- Reporting any security breaches, unauthorized access, or leaks of the personal data to the data controller within a reasonable time after discover
- Anonymising information for the following purposes:
    - Developing, optimising, and analysing the System
    - Compiling and publishing statistics, reports, and calculations related to the System
    - Sharing and selling anonymous data to third parties.

The data processor guarantees that data is exclusively processed in completely and irrevocably anonymised form, making it impossible for the data processor and other individuals to deduce which data is related to which natural persons.

C.2. Security of processing

The data processor shall implement the following measures that have been agreed upon with the data controller:

General security measures

The data processor shall maintain a formal, well-implemented and professional information security management system based on legal requirements and good data processing practices. The data

processor shall determine and implement internal policies and regulations that are adequate and reflect the actual conditions. In addition, the data processor shall maintain procedures for regular testing, assessment, and evaluation of the technical and organisational measures that the data processor has implemented to secure the personal data. The data processor ensures:

- Penetration testing (vulnerability scanning) from both the LAN and WAN side
- Systematic patching/updating of software (OS, etc.)
- Monitoring of critical systems, providing notifications if one or more systems do not behave as expected
- Independent backup solutions
- The data centers are securely locked - and equipped with camera surveillance
- Automatic fire extinguishing systems are activated in the data centers
- Redundant cooling systems have been installed in our data centers
- Two independent emergency power systems are available
- Encryption
- Implementation of IT security policy
- Network monitoring
- Data mirroring
- 24/7 support
- Security incident management (breakdown procedures)
- Logging of network activity
- Separation of account and rights.

Handling of personal data

Documents and data (including mobile storage devices) containing personal data are processed to maintain confidentiality, integrity, availability, and robustness to ensure that they are not lost or fall into the wrong hands as well as to prevent the harmful effects such breaches may have on registered persons.

Instruction of employees, etc.

The data processor ensures that employees and any business partners are constantly aware of and have sufficient training and instruction about the purpose of the data processing, policies, work practices, and about their duty of confidentiality.

Access control and administration of user access

Only employees who have a work-related need to process personal data in relation to the Main Agreement shall be created as users with access to the data controller's personal data. Only those persons authorized by the authorized person to do so may have access to the personal data. The data processor shall without undue delay cancel authorizations (including access) for users who no longer have a work-related need for authorization.

A list of authorized employees is kept, indicating which type of access the authorization covers. The list of authorized employees is regularly updated in accordance with good data processing practices. If the data controller requests the list, the list shall be made available without undue delay.

At the termination of the service, the employees' access is closed.

The data processor shall use secure identification and authorization technologies, e.g., passwords, biometrics, or the like. The authentication methods used shall comply with the latest guidance from the Danish Agency for Digital Government and good practices in the field.

Control of rejected access attempts

Based on a risk-based approach, the data processor registers rejected access attempts and blocks further attempts after a fixed number of consecutive rejected access attempts.

The data processor shall also maintain procedures which ensure timely follow-up of all rejected access attempts, where follow-up is necessary to prevent breaches of personal data security and harmful effects for registered persons.

Change management

The data processor shall have formal change management procedures in place to ensure that any change is properly authorised, tested, and approved prior to implementation.

Operational interruptions

The data processor shall have documented contingency procedures that ensure the re-establishment of services without undue delay in the event of operational interruptions in accordance with the Main Agreement.

External communication links

The data processor has appropriate technical measures to protect systems and networks as well as to limit the risk of unauthorized access and/or installation of malicious code.

To the extent that it is a requirement pursuant to applicable legislation, good data processing practices, or is otherwise covered by the Main Agreement, the data processor uses encryption technologies and other similar measures.

Ad hoc and home workplaces

If the data processor carries out data processing from ad hoc and/or home workplaces, the data processor shall ensure that these meet the security requirements in this Data Processing Agreement with appendices, other legislation, and the Danish Data Protection Agency's instructions in this regard.

The data processor shall, among other things, fulfill and be able to document the following:

- Description of the encrypted connection used between the ad hoc workplace and the data processor's/data controller's network.
- The data processors internal instructions to its own employees regarding afd hoc and home workplaces.

In addition, if it is possible, the data processor shall use two-factor authentication.

Disposal of equipment

The data processor shall have formal processes to ensure that personal data is effectively deleted before disposal of electronic equipment.

C.3 Assistance to the data controller

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

a. The obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks associated with the processing
b. The obligation to report a breach of personal data to the supervisory authority (the Danish Data Protection Agency) without undue delay and, if possible, no later than 72 hours after

the data controller has become aware of the breach, unless it is unlikely that the breach of personal data security entails a risk for natural persons' rights or freedoms

c. The obligation to – without undue delay – notify the data subject(s) of a breach of personal data security when such a breach is likely to entail a high risk for the rights and freedoms of natural persons
d. The obligation to carry out a data protection impact assessment if a type of processing is likely to entail a high risk for the rights and freedoms of natural persons
e. The obligation to consult the supervisory authority (the Danish Data Protection Agency) before processing, if any analysis regarding data protection shows that the processing will lead to high risk in the absence of measures taken by the data controller to limit the risk.

C.4 Storage period/erasure procedures

The personal data is stored by the data processor until the data controller requests that the data be deleted or returned or as long as there is a factual basis for storage.

Upon termination of the provision of personal data processing services, the data processor shall either delete or return the personal data in accordance with Clause 11.1, unless the data controller – after the signature of the contract – has modified the data controller's original choice. Such modifications 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 those specified in Appendix B without the data controller's prior written authorization.

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

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 review its internal security measures at least once a year.

The data processor shall, at its own expense, obtain a statement or another form of audit from an independent third party concerning the data processor's compliance with this data processing agreement and its appendices.

The statement or the audit result shall be sent promptly after obtaining it for information to the data controller.

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

APPENDIX D THE PARTIES' TERMS OF AGREEMENT ON OTHER SUBJECTS

D.1. Notification of breach of personal data security

In accordance with point 10 of the data processing agreement, the data processor shall notify the data controller without undue delay after becoming aware that a breach of personal data security has occurred. The data processor's notification to the data controller shall, if possible, take place no later than 12 hours after the data processor has become aware of the breach.

The data processor's notification to the data controller shall contain information on the following:

- Description of the breach and the reason for the breach
- Date and time of the start of the breach
- Data and time of the discovery of the breach
- Total duration of the breach
- Listing of the type of personal data affected by the breach (e.g., name, social security number, information on finances, etc.)
- Number of registered (persons) affected by the breach
- Description of the likely consequences/damaging effects of the breach
- Description of the measures taken to stop or limit the breach, including data and time
- Information on whether the affected registered (persons) have been notified of the breach and how they may have been notified
- Name *and* contact information of the data protection officer or other point of contact where further information can be obtained
- Any other information that is necessary for the data controller to comply with his obligation to report the beach of personal data security to the competent supervisory authority, cf. Article 33 GDPR.

The data processor shall also assist the data controller in providing the above information in connection with the data controller's obligation to report breaches of personal data security to the competent supervisory authority.

END