Standard Contractual Clauses

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

between

the Customer (as defined in the "main agreement")

(the data controller)

and

IntraManager A/S
CVR 33966458
Helgavej 26
5230 Odense M
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 system "IntraManager Work" and "IntraManager Board", 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.

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.

---

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

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 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 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.

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 general written authorisation of the data controller.

3. 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 fourteen (14) 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.

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. 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 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.

9. 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, 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 forty-eight (48) hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's

obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

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.

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 data controller and delete existing copies unless Union or Member State law requires storage of the personal data.

12. Audit and inspection

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

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

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.

15. Data controller and data processor contacts/contact points

1. The parties may contact each other using the contacts/contact points listed in the "main agreement".

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

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:

That the data controller can use the systems "IntraManager Work" and "IntraManager Board" owned and managed by the data processor to collect and process information about the data controller's customers and/or employees.

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):

That the data processor makes the systems "IntraManager Work" and "IntraManager Board" available to the data controller and thereby hosts, displays, organises, receives, retrieves, shares, structures, adapts, implements, searches, processes, stores, restores, deletes, restricts, logs, supports and troubleshoots personal data about the data controller's customers and/or employees on its servers.

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

IntraManager Board:
Name, email address, customer number/-name.

IntraManager Work:
Name, email address, customer number/-name phone number, address, social security number, employee number, customer number and bank details.

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

- Data controller's customers
- Data controller's 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:

The processing is not limited in time and lasts until the Clauses are terminated or cancelled by one of the parties.

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	CVR	ADDRESS	DESCRIPTION OF PROCESSING
Amazon Web Services EMEA SARL (AWS Europe)	B 186284	38 Avenue John F. Kennedy L-1855 Luxembourg Luxembourg (Data location: Greenhills Road, Tymon North, Dublin, Ireland)	AWS is used for hosting the solution, including storage and processing of data, and thus all data is processed in the platform, including the data controller's personal data. Data is stored encrypted. AWS is contractually obliged to carry out this data processing within the data region EU-WEST (Ireland), and thus within the EU/EEA. The data processor does not use a support agreement with AWS, as this does not have the same level of security.
Elastic AS	NO 994 812 564	Postboka 539 1373 Asker Norway	Elastic Cloud is used for server management at AWS. Elastic Cloud complies with the provisions of SOC 2 & 3. Elastic is certified with ISO 27001, 27017, 27018, ISAE 3000, etc. (https://www.elastic.co/trust/security-and-compliance)

NAME	CVR	ADDRESS	DESCRIPTION OF PROCESSING
inMobile ApS	31426472	Axel Kiers Vej 18 L 8270 Højbjerg Denmark	SMS Gateway (**Note**: This sub-processor is only used if the data controller opts in for the data processor's service for system SMS)
Criipto ApS	35142207	Dronninggårds Alle 136 2840 Holte Denmark	MitID broker (**Note**: This sub-processor is only used if the data controller opts in the processor's service for digital signing with MitID)

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.

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

Within fourteen (14) days of receiving a request from the data processor to add or replace a sub-processor, the data controller must submit an objection against the selection and use of the sub-processor in question to the data processor. Otherwise, the selected sub-processor is deemed to be authorised by the data controller.

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's processing of personal data on behalf of the data controller takes place by the data processor performing the following: general IT operations, including hosting, displaying, organising, receiving, retrieving, sharing, structuring, adapting, implementing, searching, processing, storing, restoring, deleting, restricting, logging, support and troubleshooting and other IT services associated with the data processor's delivery of the software platform to the data controller in accordance with the subscription agreement entered into between the parties for the data processor's software solutions.

C.2. Security of processing

The level of security shall take into account:

Since the data processor's software enables the data controller to upload and otherwise add data to the platform, the data processor will potentially process an unknown amount of personal data and unknown categories of personal data and data subjects. Therefore, the data processor has chosen to implement a general security level reflecting the fact that a large amount of personal data and all types of categories of personal data and data subjects may be processed.

The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

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

Information security
The data processor has implemented policies, controls and processes that cover the information security areas described below:
- Confidentiality: Ensure that unauthorised persons cannot gain access to data that could be misused to the detriment of the data processor's customers, business partners and employees.
- Integrity: Ensure that systems contain accurate and complete information.
- Availability: Ensure that relevant information and systems are available and stable.

Instruction
There are written procedures in place that require that personal data may only be processed when instructions are in place. There is an ongoing – and at least once a year – assessment of whether the procedures need to be updated. The data processor only carries out the processing of personal data that appears in the instructions from the data controller.

Physical security
The data processor shall maintain physical security measures to secure the premises used for the processing of personal data, including the storage of personal data covered by these Clauses against unauthorised access and manipulation.

The data processor shall have appropriate physical measures in place to limit the risk of any unauthorised access to premises where personal data is processed. The data processor shall also, where necessary, evaluate and improve the effectiveness of such measures. Ensure that the level of physical security is at all times appropriate to the current threat landscape and the sensitivity and volume of personal data covered by these Clauses.

Communication connections and encryption
The data processor has appropriate technical measures to protect systems and networks, including the protection of data during transmission and access via the Internet and to limit the risk of unauthorised access and/or installation of malicious code.

The data processor uses appropriate encryption technologies and other equivalent measures in accordance with legal requirements, approved standards for encryption of classified information and good data processing practices.

To the extent required by applicable national and international legislation, standards for encryption of classified information or good data processing practice, the data processor shall use encryption technologies and other equivalent measures.

Transmission of sensitive and confidential information over the Internet is protected by encryption. Technological solutions for encryption are available and enabled. Firewall only allows encrypted data traffic. Formalised procedures are in place to ensure that the transmission of sensitive and confidential information over the Internet is protected by strong encryption based on a recognised algorithm.

Encryption keys are managed on behalf of the data controller and under the control of the data processor so that sub-processors or others do not have access to customer data in clear text. The data processor is obliged to encrypt personal data processed on behalf of the data controller in the data processor's application prior to any transfer of personal data to sub-processors specified in section B.1.

Firewall or similar technical measures
External access to systems and databases used for processing personal data is made through a VPN. There must be administrative access to maintain firewall configuration and rulesets.

Antivirus
Antivirus software is installed for the systems and databases used to process personal data and is regularly updated.

Backups
The data processor must have internal contingency procedures that ensure the restoration of services without undue delay in the event of operational interruptions in accordance with the "main agreement". The data processor ensures backup.

Configuration files and data must be backed up in a continuous sequence so that relevant data can be restored. The backups are stored in such a way that they are not accidentally or illegally (e.g. by fire, flood, accident, theft or similar) destroyed, lost, deteriorated, disclosed to unauthorised persons, misused or otherwise processed in violation of the rules and regulations in force at any time for the processing of personal data.

Backups must be stored physically separate from primary data and in a security-approved data centre.

The data processor uses a redundant environment to ensure access and continuous operation of the software solution. The data processor ensures that backups are stored in their full length.

Use of home/remote workstations
If data processing is carried out from ad hoc and/or home workstations, the data processor must ensure that these fulfil the security requirements in these Clauses with appendices and other legislation.

Among other things, the data processor must fulfil the following:
- That an encrypted connection is used between the ad hoc workplace and the data processor's/data controller's network.
- The data processor has internal instructions for its own employees regarding ad hoc and home workplaces.

In addition, the data processor must, if technically possible, use 2-factor authentication.

Logging
1. There are formalised procedures for setting up logging of user activities in systems, databases and networks used for the processing and transmission of personal data.
2. The data processor ensures that the scope of the security log is defined based on a risk assessment performed by the data processor.
3. The data processor ensures that there is enough space for the security logs to be stored for the period.
4. The data processor ensures that regular random checks are carried out to ensure that the security logs contain what is expected.
5. The data processor balances the security log deletion deadlines between the possibility of analysing cyber-attacks, supporting investigations and the protection of the rights and freedoms of natural persons.
6. The data processor ensures that collected information about user activity in logs is protected against deletion and manipulation.
7. The data processor shall ensure that logging of user activities in systems, databases and networks used for the processing and transmission of personal data is configured and activated.
8. Data processor ensures logging in all environments where personal data is processed.
9. Activities performed by system administrators and others with special rights.
10. Changes to logging setups, including deactivation of logging.
11. Changes to system rights for users.
12. Failed attempts to log on to systems, databases and networks.

User administration
The data processor ensures that the solution supports appropriate user administration. The data controller is ensured the possibility of using automatic or manual user administration.

The solution supports the creation, periodic review and cancellation of users. The data controller can perform these functions alone, but the data processor can assist with this if deemed necessary and within a reasonable scope.

Instruction of employees

The data processor shall ensure that employees are at all times aware of and have adequate training and instruction on the purposes of data processing, policies, work procedures and their duty of confidentiality.

An information security policy is in place, which the management has reviewed and approved within the past year. The information security policy has been communicated to relevant stakeholders, including the data processor's employees.

The information security policy generally fulfils the requirements for security measures and processing security in data processing agreements.

There are formalised procedures in place to ensure verification of the data processor's employees in connection with hiring.

Employees have signed a confidentiality agreement when hired. Employees have been introduced to:
- The information security policy.
- Data processing procedures and other relevant information.

Procedures are in place to ensure that resigned employees' rights are deactivated or terminated upon resignation and that assets such as access cards, PC, mobile phone etc. are confiscated.

Formalised procedures are in place to ensure that departing employees are made aware of the maintenance of the confidentiality agreement and general confidentiality. The employment contract contains guidelines that employees are subject to the duty of confidentiality after termination of co-operation.

The data processor provides awareness training for employees covering general IT security and processing security in relation to personal data.

The employees of the data processor are obliged to follow an internal procedure on the use of support from sub-processors used. The purpose of the procedure is to ensure the correct use of support and to prevent the use of "follow the sun"-support and thus eliminate the risk of personal data being accessed from insecure third countries.

Notification when exercising authority
A procedure has been established for notifying the data controller in the event of direct or indirect requests from authorities for disclosure of or access to data.

Disposal of equipment
The data processor must have formal processes in place to ensure effective erasure of personal data prior to the 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:

The data processor will, as far as possible, and if compliance requires the data processor's assistance, assist the data controller in fulfilling the data controller's obligation to respond to requests for the exercise of the data subjects' rights, as laid down in Chapter III of the GDPR.

As the data processor as a general rule only processes general personal data about the data controller's users of the software solution, the data processor has implemented such technical and organisational measures that allow immediate export of these users' personal data and will therefore be able to assist the data controller, just as the data controller can freely dispose of the data otherwise supplied by the data controller.

In the event of breaches and incidents, cf. clause 9.2, the data processor shall assist with the following information:
- Facts about the detected rupture (time, location, cause)
- When the breach started, when it was discovered and when the breach has stopped
- The nature of the personal data breach, including whether confidentiality, integrity and availability have been breached
- The categories and approximate number of data subjects affected, if possible
- The categories of personal data, if possible
- Name and contact details of the contact point where further information can be obtained
- Description of the likely consequences of the breach
- Description of measures taken or proposed to be taken as part of the management of the breach and its possible adverse effects.

C.4. Storage period/erasure procedures

The platform will be configured to follow deletion routines set by the data controller. However, the data controller's personal data is deleted automatically and no later than thirty (30) days after termination of the Clauses.

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 modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

C.5. Processing location

Processing of the personal data covered by the Clauses cannot, without the data controller's prior written authorisation, take place at locations other than the data processor's registered office or the locations used by the sub-processors listed in clause B.1.

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.

The data processor may not transfer personal data to or access personal data from countries outside the EU/EEA or international organisations.

If the data processor has subsequently received documented written instructions from the data controller, the data processor shall ensure that (i) such transfer is lawful, including that there is an adequate level of protection for the transfer of personal data, by entering into the EU Commission's standard contractual clauses or other lawful basis for the transfer to be initiated, (ii) all necessary authorisations have been obtained, and (iii) all necessary notifications regarding the transfer in question have been given to the relevant supervisory authority. The data processor is obliged to update the form in Annex B.1 and specify the basis for the transfer, cf. Chapter V of the GDPR.

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 provide the data controller with a self-audit report at least once (1) a year for the purpose of verifying the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data controller 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 controller 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.

In addition, the controller or a representative of the data controller shall have the right to carry out inspections, including physical inspections, of the premises from which the processor processes personal data. Such inspections may be carried out when the data controller deems it necessary but shall be organised so as to cause the least possible inconvenience to the data processor.

The data controller's costs, if applicable, relating to physical inspection shall be defrayed by the data controller. The data processor shall, however, be under obligation to set aside the resources (mainly time) required for the data controller to be able to perform the inspection.

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

The data processor shall, at its own expense, carry out annual audits of the processing of personal data entrusted to sub-processors. The audit shall relate to the sub-processor's compliance with the GDPR, data protection provisions in other EU law or Member States' national law and these Clauses.

The data processor's audit of sub-processors shall be organised in such a way that sufficient insight into and control of the sub-processors' compliance with the GDPR, data protection provisions in other EU law or Member States' law and these Clauses is achieved.

The audit may consist of obtaining an auditor's report or inspection report from an independent third party, inspections, and/or written questions. The data processor is generally free to choose the method by which sub-processors are supervised. However, the data controller may, if there are reasonable grounds to do so, challenge the framework and/or method of the audit and may in such cases request a new audit under a different framework and/or using a different method.

The data controller may – if required – elect to initiate and participate in a physical inspection of the sub-processor. This may apply if the data controller deems that the data processor's audit of the sub-processor has not provided the data controller with sufficient documentation to determine that the processing by the sub-processor is being performed according to the Clauses.

Appendix D The parties' terms of agreement on other subjects

D.1 Remuneration for the establishment of additional security measures

Any regulation/agreement between the parties on remuneration or similar in connection with the data controller's subsequent requirement for the establishment of additional security measures other than those specified in Sections 6, C.2 and C.7 will appear from the parties' "main agreement".