itm8®

Segura Security Services

Standalone

Sub-Processing Agreement

Table of Contents

Introduction to the Sub-Processor Agreement

This sub-processor agreement is drafted in accordance with the Danish Data Protection Agency's Standard Contractual Clauses.

The sub-processor agreement sets out the rights and obligations that apply when a sub-processor is entrusted with processing personal data on behalf of a data processor.

The sub-processor agreement is designed to ensure the parties' compliance with Article 28 of the European Parliament and Council Regulation (EU) 2016/679 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 (the General Data Protection Regulation), which imposes specific requirements on the content of a data processing agreement.

The sub-processor's processing of personal data for the data processor is carried out to fulfil the parties' agreement on services from the sub-processor to the data processor, which the data processor uses in its deliveries to customers. The sub-processor thus acts as another data processor (sub-processor) in accordance with Article 28(4) of the General Data Protection Regulation.

The purpose of the sub-processor agreement is to impose the same data protection obligations on the sub-processor as those imposed on the data processor in its agreement with the data controller.

All terms used in this sub-processor agreement shall be understood in accordance with the General Data Protection Regulation.

The parties agree that where the sub-processor agreement refers to "the data controller," it shall be understood as "the data processor," and where the sub-processor agreement refers to "the data processor," it shall be understood as "the sub-processor."

Data Processing Agreement

1. Standard Contractual Clauses

Pursuant to Article 28(3) of the General Data Protection Regulation (EU) 2016/679 for the purpose of the data processor's processing of personal data

between

MT4 Tecnologia Ltda.
Rua Joaquim Antunes, 767
São Paulo – SP, 05415-012
Brazil
(hereinafter the " data processor")

and

itm8 A/S
27001092
Dalgasplads 7B,1.sal
7400 Herning
Denmark

(hereinafter the " data controller ")

each referred to as a "party" and collectively as the "parties"

the following Standard Contractual Clauses (the "Clauses") have been agreed in order to comply with the General Data Protection Regulation and to ensure the protection of privacy and fundamental rights and freedoms of individuals.

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 Clauses of services comprised by the parties' agreement(s) regarding IT Services (the "Service Agreement", the "Service" and/or the "Services"), the data processor will process personal data on behalf of the data controller in accordance with the Clauses. The Clauses may cover the data processor's processing activities under several independent Service agreements entered into between the parties.

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

5. 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.

6. 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.

7. 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.

8. Appendix D contains supplemental the Clauses.

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

10. 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 essential 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.

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

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 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 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 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 as a deviation in Appendix D.8. 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 organizational 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, 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, 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 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.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so or 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 in the parties' agreement regarding the data processor's provision of the Services ("Services Agreement") or in Appendix D, agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

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

2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. The Clauses shall apply for the duration of the provision of personal data processing Services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

4. If the provision of personal data processing Services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

11. Signature
On behalf of the data controller

Name Rene Jeppesen
Position Partner, Commercial Strategy, Advisory & Solutions
Date: 7/30/2025

Signature Signed by: Rene Jeppesen 32CB3DC9EF1C4D2...

On behalf of the data processor

Name Henrique Calidonna Stabelin
Position Manager Compliance

Signature DocuSigned by: Henrique Calidonna Stabelin 6C8D8AAEC1B14B4...

15. Data controller and data processor contacts

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

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

Data controller		Data processor	
Name:	Henrique Calidonna Stabelin	Name:	Compliance & Security

Email:	hstabelin@segura.security | dataprivacy@segura.security	Email:	gdpr@itm8.com
Phone:	+55 (11) 957785633	Phone:	+45 7026 2988

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

The purpose of the processing is to provide hosting operation services as specified in the main agreement.

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)

The data processor provides hosting, maintenance and development of security services.

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

Types of personal data specified below:

- Name
- Address
- Zip Code
- Phone number
- Cell phone number
- Email address
- Business data (company, title, contact info)

A.4. The processing includes the following categories of data subjects

Categories of data subjects, identified or identifiable natural persons comprised by the data processor's processing:

- Employees
- The data controller's own customers

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 data processor's processing of personal data on behalf of the data controller is performed when the parties' Service Agreement comes into force and will continue until the Service Agreement is terminated.

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/address	Company number	Location of processing	Description of processing
Google Cloud Platform datacenter – Frankfurt – Germany		EU	Cloud infrastructure and platform services (GCP) used for data storage, computing, and processing

The list of sub-processors used at the time of contracting is inserted in the above table and will be adjusted in case of acquisition or changes in services.

After commencement of the Clauses, the data processor can use other sub-processors. The data controller will be informed of changes in data processors used upon purchase of new services or data processor changes to services. In addition, an appendix of currently used sub-processors can be provided upon request.

The procedure for the data processor's notice regarding planned changes in terms of addition or replacement of sub-processors is described in clause B.2.

B2. Notice for approval of sub-processors

The data processor's notification of any planned changes regarding the addition or replacement of sub-processors must be received by the data controller at least 90 days before the implementation or change takes effect.

Appendix C – Instruction pertaining to the use of personal data

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

The processing of personal data by the data processor on behalf of the data controller shall be carried out in accordance with the Service Agreement concluded between the data controller and the data processor.

The data processor bases its management system for information security on the principles in the ISO 27001 security framework and has implemented the relevant controls defined by this standard. In addition, the data processor has implemented a management system for secure processing of personal data.

These controls are managed in an ISMS system for ISO 27001, and a PIMS system for GDPR. Thereby, controls are documented on an ongoing basis, and findings from internal audits are used for ongoing improvements.

The data processor is also audited once every year where an ISAE 3402 statement is made in terms of operation, hosting and support, as well as an ISAE 3000 statement. In addition, the data processor maintains and updates an ISO 27001:2022 certification.

The most recent statements and certificates are always available here https://legal.itm8.com.

The data controller has instructed the data processor in processing data on the basis of the Services agreed and on the basis of the instructions below.

C.1.1 Hosting and operation

If Hosting and operation has been selected as a processing activity in the table in Appendix A.1., the following applies:

Storage and backup and any related processing activities required in connection with the supply of the agreed services or required to comply with a request or instructions from the data controller. Processing operations carried out by the data processor include:

- Backup and backup controls.
- Patch Management.
- Operation and maintenance of systems and infrastructure.
- Virus scanning and follow-up on virus alerts.
- Installations and configurations.
- Handling of monitoring alarms.
- Documentation of assets, procedures and controls.

C.1.2 Support

If support has been selected as a processing activity in the table in Appendix A.1., the following applies:

Data processing is performed in accordance with services related to the support services provided for in the parties' Service Agreement or specific cases initiated by the data controller.

C.1.3 Consultancy services

If consultancy services have been selected as a processing activity in the table in Appendix A.1., the following applies:

Data processing can only be based on specifically agreed consultancy projects.

C.1.4 Database administration

If database administration has been selected as a processing activity in the table in Appendix A.1., the following applies:

Data processing is performed in accordance with services related to the Database Administration service provided for in the parties' Service Agreement or specific cases initiated by the data controller.

C.1.5 Configuration and development

If configuration and development have been selected as a service in the table in Appendix A.1., the following applies:

Data processing is performed in accordance with the tasks agreed with the data controller.

C.1.6 Hosting and maintenance of application services

If hosting and maintenance of application services have been selected as a processing activity in the table in Appendix A.1., the following applies:

The data processor's processing of personal data on behalf of the data controller takes place as part of the delivery of the agreed application services to the data controller, which is further specified in the Service Agreement concluded between the parties, including:

- Backup.
- Support.
- Hosting.
- Operation and maintenance.
- Configuration.
- Updates.
- Documentation.

and related processing activities which are necessary in connection with the provision of Services or which are necessary to fulfil a request or instruction from the data controller.

C.1.7 Security services

If security services have been selected as a processing activity in the table in Appendix A.1., the following applies:

The data processor's processing of personal data on behalf of the data controller takes place as part of the delivery of the selected security services to the data controller, which are further specified in the Service Agreement concluded between the parties, including:

- Monitoring.
- Configuration.
- Reporting.
- Maintenance.
- Documentation.

C.2. Security of processing

The security level must reflect a generally high level of security, which reflects the types of personal data being processed.

Furthermore, the security level must reflect the specific agreed services in the Service Agreement.

The data processor implements and carries out appropriate technical and organizational measures to ensure a security level that matches the risks associated with the processing activities the data processor performs for the data controller.

The technical and organizational measures are determined considering the current technical level, implementation costs, the nature, scope, context, and purpose of the processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.

When assessing what security level is appropriate, particular consideration is given to the risks posed by processing, especially accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed.

The data processor is then entitled and obliged to make decisions about which technical and organizational security measures must be implemented to establish the necessary (and agreed) security level.

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

- User authentication with multiple-factor authentication, whenever available, and access management.
- Encryption to protect sensitive data.
- Hardening process at different application levels (reviewed periodically), indicated by the organizations NIST (National Institute of Standards and Technology) and CIS (Center for Internet Security).
- Vulnerability management and frequent security assessments in the form of Pentest.
- DLP (Data Loss Prevention), DRP (Disaster Recovery Plan) and BCP (Business Continuity Plan), reviewed annually.
- Updated antivirus with appropriate security settings.
- Networks configured with department segmentation and logically isolated.
- Backup and restore procedures for critical systems for data availability.
- Physical and virtual servers with updated and adequate security parameters.
- Physical access process with several security controls, making unauthorized access to storage locations difficult.

- Properly functioning firewalls, with regular reviews of configurations and security standards.
- The solution's monitoring includes an intrusion detection, access blocking and notification system.
- Policies, procedures and processes reviewed annually.
- Internal and external audits.

C.3 Assistance to the data controller

As far as possible – and within the scale and extent specified below – the data processor shall assist the data controller in accordance with Clause 9.1 and 9.2 by implementing the following technical and organisational measures:

At the specific request of the data controller, the data processor shall, as far as possible and taking into account the nature of the processing, assist the data controller with appropriate technical and organisational measures, in the fulfilment of the data controller's obligations to respond to requests for the exercise of the data subjects' rights pursuant to the General Data Protection Regulation.

If a data subject makes a request to the data processor to exercise its rights, the data processor shall notify the data controller without undue delay.

Taking into account the nature of the processing and the information available to the data processor, the data processor shall also, upon specific request, assist the data controller in ensuring compliance with the obligations of the data controller in relation to:

- Implementation of appropriate technical and organisational measures.
- Security breaches.
- Notification of a personal data breach to the data subject.
- Conducting impact assessments.
- Prior consultation of the supervisory authorities.

C.4 Storage period/erasure procedures

The data controller itself disposes personal data processed by the data processor on behalf of the data controller. Thus, personal data made available for the data processor's processing will be stored until erased by the data controller or until termination of the Services relating to processing of personal data.

Upon deletion of personal data in the data controller's systems, these personal data will be deleted in the data processor's backup system based on the agreed retention period (backup history) for each system.

At the request of the data controller, the data processor will assist with erasure or return of personal data as further instructed by the data controller.

C.5 Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorisation:

Personal data is processed exclusively on Google Cloud Platform (GCP) infrastructure, operated by Google Cloud EMEA Limited, headquartered in Dublin, Ireland. Data is stored and processed in data centers located in the customer's region.

C.6 Instruction for transfer of personal data to third countries

The data controller has authorised and thereby instructed the data processor to transfer personal data to a third country as further specified below. In addition, by subsequent written notification or agreement the data controller can provide instructions or specific consent pertaining to the transfer of personal data to a third country.

If the data controller does not in the Clauses or subsequently provides documented instructions pretraining 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.6.1 General approval of transfer of personal data to secure third countries

With these Clauses, the data controller provides a general and prior approval (instructions) for the data processor to transfer personal data to third countries if the European Commission has laid down that the third country/the relevant area/the relevant sector has a sufficient level of protection.

For transfers to organisations in the United States that are certified under the EU-U.S. Data Privacy Framework ("DPF"), the Controller also provides by the Provisions its general and prior approval (instruction) for the Data Processor to make transfers of personal data to these organisations. The Data Processor is at any time obliged to ensure that the sub-processors used have the required certification.

C.6.2 Approval of transfer to specific recipients of personal data in third countries

The data controller instructs the data processor to use the following sub-processor(s) where transfers of personal data to third countries take place:

Name	Company number	Description of processing	Transfer to a third country

When entering into the Clauses, the data controller has given consent to the use of the above sub-processor(s) and instructed on the transfer of personal data to third countries for the provision of the Services.

If the European Commission's Standard Contractual Clauses ("SCC") for the transfer of personal data to a third country are used as the transfer basis, the data processor and/or any sub-processor shall be entitled to enter into such SCCs with the relevant sub-processor.

In the event that the European Commission produces new SCCs after the conclusion of the Service Agreement, the data processor is authorised to replace, update and apply the SCCs in force at any time.

The contents of this instruction and/or the Clauses shall not be deemed to modify the contents of the SCCs.

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 controller has the right and obligation under Articles 24 and 28 of the General Data Protection Regulation to supervise the data processor's processing of personal data on behalf of the data controller. The data controller's supervision of the data processor can be carried out by performing one of the following actions:

- Self-assessment based on documents made available by the data processor to the data controller,
- Written supervision, or
- Physical inspections.

At the request of the data controller, the data processor must, at its own expense, obtain an audit statement/inspection report from an independent third party regarding the data processor's compliance with the General Data Protection Regulation, data protection provisions in other EU law, or national law of the Member States and these Provisions.

The parties agree that one or more of the following statements/certifications, for example, can be used in accordance with these Provisions:

- ISAE 3402 type 2 statement
- ISAE 3000 statement
- ISO 27001 certification
- SOC 2 report

The documentation is sent without undue delay to the data controller for information. The data controller may challenge the scope and/or method of the statement and may, in such cases, request a new audit statement under different frameworks and/or using another method.

Based on the results of the statement/report, the data controller is entitled to request the implementation of additional measures to ensure compliance with the General 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 carry out inspections, including physical inspections, of the locations from which the data processor processes personal data, including physical locations and systems used for or in connection with

the processing. Such inspections can be carried out whenever the data controller deems it necessary.

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

The data processor carries out audits, including inspections, of sub-processors' processing of personal data based on the data processor's risk assessment and considering the specific processing activities. This can be done through self-assessment of audit statements and similar (where possible), written supervision, or physical inspection, or a combination thereof.

At the request of the data controller, the data controller can obtain further information about which control measures have been initiated and carried out concerning the individual sub-processors.

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

D.1 In general

In relation to the data processor's processing of personal data on behalf of the data controller, the parties have agreed on the following additional terms.

In the event of any inconsistency between the Provisions and the terms set out in this Appendix D, Appendix D shall prevail.