Standard Contractual Clauses

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

between

[NAME]
CVR [CVR-NO]
[ADDRESS]
[POSTCODE AND CITY]
[COUNTRY]

(the Data Controller)

and

Fischer & Kerrn A/S
CVR 24237087
Amagerfælledvej 106
2300 København S
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 delivery of the CONCIERGE BOOKING software, 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.

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 above-mentioned 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

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

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 specific written authorisation 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 30 days prior to the engagement of the concerned sub-processor. The list of sub-processors already authorised by the Data Controller can be found in Appendix B.

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

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

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

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

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

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 Danish Data Protection Agency or other competent supervisory authority, 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 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 4 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, 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.

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

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

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

5. Signature

   On behalf of the Data Controller

   Name
   Position
   Date

   Signature

   On behalf of the Data Processor

Name	Henrik Fehrn
Position	Sales Director, CEO
Date	
Signature	

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
   Position
   Telephone
   E-mail

Name	Henrik Fehrn
Position	Sales Director, CEO
Telephone	+45 25600933
E-mail	hfe@fischerkerrn.dk

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:

Fischer & Kerrn processes personal data on behalf of the Data Controller for the purpose of providing software for the registration and processing of meetings, guests and orders for goods/services.

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):

Fischer & Kerrn collects and stores personal data on behalf of the Data Controller in order for the Data Controller to be able to:

- inform meeting participants/guests about upcoming meetings/visits
- efficiently planning the booking of the Data Controller's resources (premises, equipment, etc.).
- extract a history of which meeting participants/guests have visited the Data Controller's locations
- make settlement of ordered goods/services to the right person

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

The following personal data is collected and stored:

- Name
- Email
- Telephone
- Place of employment (company)

The following information, which may be of particular interest and which may potentially relate to individuals, is collected and stored:

- Ordered goods/services/resources
- Comments on orders about allergies, preferences, etc.

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

The following categories of data subjects are covered by the processing:

- Employees
- Business contacts and guests, including customers, suppliers and business partners

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:

A.5.1. This Agreement shall come into force upon signature by both Parties.

A.5.2. Unless otherwise agreed in writing, the Agreement remains in force for as long as the Data Processor processes data on behalf of the Data Controller or until the termination of the Agreement (the later of the two events).

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
Microsoft West Europe The Netherlands		Evert van de Beekstraat 354, 1118 CZ Luchthaven Schiphol, Noord-Holland, Netherlands	Datacenter located in The Netherlands

The Data Controller shall on the commencement of the Clauses authorise the use of the abovementioned 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

Not relevant.

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:

- Collects personal data about employees, business associates and guests.
- Stores personal data about employees, business contacts and guests for as long as the Data Controller deems it relevant in relation to requests for statistics and reporting options
- Makes personal data available to the Data Controller in connection with its reporting and processing of the personal data.
- Deletes personal data at the request of the Data Controller.

C.2. Security of processing

The general security of processing in order to prevent information from being accidentally or illegally destroyed, lost, impaired, disclosed to unauthorized persons, misused or otherwise processed in violation of the rules and regulations in force at any given time for the processing of personal data is maintained through the Data Processor's organizational, administrative and IT security measures.

The Data Processor determines the security level for all processing operations according to the highest level of the Data Processor.

The Data Processor is then entitled and obliged to make decisions on which technical and organizational security measures must be implemented in order to establish the necessary (and agreed) level of security.

However, the Data Processor must – in all circumstances and as a minimum – implement the following measures, which have been agreed with the Data Controller:

C.2.1. Access management and authorization

- Access to personal data is isolated to users with a work-related need for it.
- There are formalised procedures for restricting users' access to personal data, as well as procedures for following up that users' access to personal data is in accordance with their work-related needs.
- When the work-related need is no longer present, the users' access is closed.

C.2.2. Maintaining safety measures

- Data is stored in the Azure Data Centre and can only be accessed by selected employees and only if there is an actual operational need for this. The starting point is that access to data is not possible other than through the software, which also runs in the Azure Data Centre, and that access must therefore be opened up as needed, e.g. due to support or operational problems. It is logged when this access is opened.
- Remote access to machines where the software is run in Azure Datacenter is only possible for selected employees, only from Fischer & Kerrn's work network (via IP restriction) and only when this access is enabled.

- Customers' data is stored in different databases and a given customer's instance of the software runs in isolation from other customers' instances of the software. Thus, there are no software processes and/or databases that process or store data from multiple customers simultaneously.
- The technical and organizational security measures put in place are described at all times in the annual statement of assurance for the general IT controls for the relevant systems.
- The established technical measures are continuously tested by vulnerability scans and penetration tests. These are carried out by the Data Controller.

C.2.2.1. Instruction of employees

- The Data Processor instructs the relevant employees on the purpose and workflows of the data processing.

C.2.2.2. Professional secrecy

- The Data Processor's employees are subject to a duty of confidentiality during and after their employment with the Data Processor.

C.2.2.3. Physical security

- Physical access security has been established so that only authorized persons can gain physical access to premises in which personal data is stored and processed.

C.2.2.4. Network and communication security

- External access to systems and databases used for the processing of personal data is done through a secured firewall.
- Effective encryption is used when transmitting confidential and sensitive personal data via the internet and by e-mail.
- Internal networks are segmented to ensure limited access to systems and databases used for the processing of personal data.
- Network traffic is monitored.

C.2.2.5. Operating procedures and responsibilities

- Antivirus has been installed for the systems and databases used for the processing of personal data, which is continuously updated.
- Logging has been established in systems, databases and networks for the following conditions:
    - Activities performed by system administrators and others with special privileges.
    - Security incidents include:
        - Changes to log setups, including disabling logging.
        - Changes to System Rights for Users.
        - Failed attempts to log-on to systems, databases and networks.
- Log information is protected from manipulation and technical errors and is reviewed on an ongoing basis.
- Data and configuration are continuously (in real time) duplicated to several servers, so that data exists in at least three copies at all times.
- Data backups and configuration can be done to secure against disaster scenarios where all real-time copies of data are lost. The frequency of such

backup is made by agreement with the customer, as the frequency is determined according to how long data loss is acceptable. Testing of restoration of data from backup in the event of a disaster scenario is also done by agreement with the customer, and the frequency is also determined according to how long data loss is acceptable.

- Personal data used for development, testing or the like is always in anonymized form.
- Changes to systems, databases and networks follow established procedures that ensure maintenance with relevant updates and patches, including security patches.
- For the systems and databases used for the processing of personal data, system monitoring with alarms has been established.
-

C.2.2.6. Disaster plan

- The description in C.2.2.5 describes how the system can be restored after being unavailable for a period of time.

C.3. Assistance to the Data Controller

The Data Processor shall ensure that the Data Processor's systems and internal processes are designed in such a way that enables the Data Processor to assist the Data Controller in safeguarding the rights of the data subjects in cases where the Data Controller is unable to do so without the Data Processor's participation and in cases where the Data Processor has been instructed in advance to safeguard one or more of the data subjects' rights on behalf of the Data Controller.

The Data Processor will, in cases where possible and relevant in relation to the processing in question, ensure that the Data Processor's systems are designed in a way that makes it possible for the Data Controller to safeguard the rights of the data subjects directly in the Data Processor's systems so that the Data Processor's assistance will not be required.

If the Data Processor receives an enquiry from a data subject whose personal data the Data Processor processes on behalf of the Data Controller, the Data Processor will contact the Data Controller to be instructed on how to handle such an enquiry, unless the Data Processor has been instructed in advance to handle such an enquiry. Such instructions shall be included in this section.

C.3.1. Assistance in carrying out an impact assessment

The Data Processor's systems and internal processes are designed in such a way that the Data Processor, taking into account the nature of the processing and the information available to the Data Processor, can assist the Data Controller with its obligation to conduct an analysis of the consequences of the intended processing activities for the protection of personal data prior to the processing (an impact assessment), as well as assist the Data Controller with its obligation to consult the Danish Data Protection Agency before processing, where the impact assessment shows that the processing would lead to a high risk in the absence of measures taken by the controller to mitigate the risk.

C.3.2. Assistance in notifying breaches to the supervisory authority and notifying data subjects

The Data Processor's systems and internal processes are designed in such a way that the Data Processor can notify the Data Controller of a personal data breach without undue delay and no later than 4 hours after becoming aware of the breach. The Data Processor assists, taking into account the nature of the processing and the information available to the Data Processor, with the necessary information about the breach so that the Data Controller can fulfil its obligation to report a personal data breach without undue delay and, if possible, no later than 72 hours after it has become aware of it.

The information about the breach is sent to the Data Controller's contact person via email and is followed up by a phone call.

The Data Processor's systems and internal processes are also designed in such a way that: The Data Processor may make the necessary information available to the Data Controller so that the Data Controller can assess whether the data subjects should be notified of a personal data breach. If the Data Controller then assesses that notification of the data subjects should be made, the Data Processor shall, at the request of the Data Controller, assist in making such notification in cases where notification cannot take place without the Data Processor's involvement.

C.4. Storage period/erasure procedures

Personal data will be deleted by the Data Processor in accordance with the deletion policy provided by the Data Controller (where the Personal Data is automatically deleted by the Data Processor accordingly), to the extent that the data is stored by the Data Processor.

Upon termination of the service relating to the processing of personal data, the Data Processor shall either delete or return the Personal Data in accordance with Clause 11.1, unless the Data Controller – after signing these Terms – has changed the Data Controller's original choice. Such changes must be documented and kept in writing, including electronically, in connection with the provisions."

C.5. Processing location

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

- Fischer & Kerrn, DK
- Microsoft, Datacenter in The Netherlands.

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 make all information necessary to demonstrate compliance with Data Protection Legislation and the Data Processing Agreement available to the Data Controller and shall facilitate and contribute to audits, including inspections, conducted by the Data Controller or another auditor authorized by the Data Controller.

The following supervision has been agreed upon in the Data Processing Agreement: The Data Processor is obligated to provide an annual written status update on matters covered by the Data Processing Agreement. The status report may be shared by the Data Processor via its website or directly with the Data Controller. The status report must provide the Data Controller with sufficient opportunity to assess whether the conditions of the Data Processing Agreement are still being met. Based on the prepared status report, the Data Controller may request clarifications or additional information regarding the provided material free of charge.

The principles and recommendations in ISAE 3000 and ISAE 3402, with later amendments, may be used as a guiding framework for compliance with the requirements of the Data Processing Agreement.

The declaration will be sent to the Data Controller's contact person when the declaration is available.

The Data Controller shall have the right to once a year, with appropriate written notice and against payment of the costs thereof, to conduct an investigation of or have an independent expert carry out an investigation into whether the Data Processor has taken the said technical and organizational security measures in relation to the processing of the personal data covered by these Provisions.

The Expert shall treat any information obtained from or received from the Data Processor as confidential and may only disclose his/her conclusions to the Data Controller. The Data Processor shall receive a copy of the expert's report and be entitled to use it as documentation for other customers to the extent applicable.

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

The Data Controller may also request a copy of the appropriate audit statement from the Data Processor's sub-processors, if any. If it does not make sense to make an independent audit statement regarding a sub-processor, e.g. because the service provided by the sub-processor is of limited scope or does not present independent issues because the sub-processor only processes data in the Data Processor's own systems, the Data Processor may meet the requirement in this provision with a statement prepared by the Data Processor itself. The declaration will consist of an account of the role of the sub-processor and an overall account of the security in relation to the sub-processor's activities, as well as an assurance that the sub-processor is subject to and fulfils the same requirements as are imposed on the Data Processor under these Provisions.