CHRISTENSEN KJÆRULFF
REVISION | REGNSKAB | RÅDGIVNING

Appendix 1 – Data Processing Agreement

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

between

[CLIENT]

(the data controller)

and

Christensen Kjærulff Statsautoriseret Revisionsaktieselskab
CVR: 15915641
Østbanegade 123
2100 København Ø
Danmark

(the data processor)

each a 'party'; together 'the parties'

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

1. Table of Contents

2. Preamble

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

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

3. In the context of the provision of the data processor's services as described in the general terms and conditions, 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.

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.

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

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.

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.

7. At the commencement of this Data Processing Agreement, the data controller has approved the use of sub-processors. A list of the sub-processors engaged by the data processor is available upon request from the data 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 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 breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

    b. Name and contact details of the Data Protection Officer (DPO)

    c. the likely consequences of the personal data breach;

    d. 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.

5. Likewise, sub-processors are required to notify the data processor without undue delay in accordance with clause 10.3.

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. This Data Processing Agreement is attached as an appendix to the engagement letter covering the agreed service. By signing the engagement letter, the Data Processing Agreement shall be deemed accepted, and its provisions shall enter into force on the date of signature by both parties.

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.

Appendix A Information about the processing

The data processor may provide the following services which involve the processing of personal data on behalf of the data controller:

- Bookkeeping services
- Payroll accounting services
- Compilation of financial statements and/or tax reports

This appendix describes the data processor's processing of personal data in relation to the services agreed between the parties. Only the sub-appendices corresponding to the specific service(s) agreed upon by the parties shall apply.

Sub-appendix A.1 – Bookkeeping Services

A.1.1. Purpose of the data processor's processing of personal data on behalf of the data controller

The purpose of the processing is to ensure the data controller's compliance with bookkeeping legislation.

A.1.2. The data processor's processing of personal data on behalf of the data controller primarily concerns (the nature of the processing)

The data processor assists with bookkeeping for the data controller, thereby gaining access to and systematically registering accounting records which may contain personal data.

A.1.3. The processing includes the following categories of personal data concerning the data subjects

- Contact details such as name, email address, and physical address
- Organisational details such as job title, position, and workplace
- Financial information such as account numbers, salary, and pension contributions
- National identification numbers (CPR-numre)
- Information regarding trade union membership

The types of personal data processed vary depending on the data controller's accounting material, including accounting documents.

A.1.4. The processing includes the following categories of data subjects

- Employees of the data controller
- Customers of the data controller
- Suppliers and business partners of the data controller
- Other associates of the data controller

A.1.5. 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 shall commence following the entry into force of these provisions and will continue for the duration of the engagement letter between the parties.

Sub-appendix A.2 – Payroll Accounting Services

A.2.1. Purpose of the data processor's processing of personal data on behalf of the data controller

The purpose of the processing is to ensure accurate and timely salary payments by the data controller, and to ensure compliance with applicable tax and bookkeeping legislation related to salary disbursement.

A.2.2. The data processor's processing of personal data on behalf of the data controller primarily concerns (the nature of the processing)

The data processor assists with payroll services for the data controller, gaining access to, collecting, verifying, and organising personal data required for calculating salary, deductions, etc., and carries out the calculation and payment of salaries on behalf of the data controller.

A.2.3. The processing includes the following categories of personal data concerning the data subjects

- Contact details such as name, email address, and physical address
- Organisational details such as job title, position, and workplace
- Financial information such as account numbers, salary, and pension contributions
- National identification numbers (CPR)
- Information regarding trade union membership

The types of personal data processed vary depending on the data controller's accounting material, including accounting documents.

A.2.4. The processing includes the following categories of data subjects

- Employees of the data controller

A.2.5. 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 shall commence following the entry into force of these provisions and will continue for the duration of the engagement letter between the parties.

Sub-appendix A.3 – Compilation of financial statements and/or tax reports without auditor's report

A.3.1. Purpose of the data processor's processing of personal data on behalf of the data controller

The purpose of the processing is to ensure the data controller's compliance with the Danish Financial Statements Act (Årsregnskabsloven) and tax legislation.

A.3.2. The data processor's processing of personal data on behalf of the data controller primarily concerns (the nature of the processing)

The data processor assists with compilation of financial statements and/or tax reports, gaining access to and reviewing relevant accounting material which may include personal data.

A.3.3. The processing includes the following categories of personal data concerning the data subjects

- Contact details such as name, email address, and physical address
- Organisational details such as job title and workplace

- Financial information such as account numbers, salary, and pension contributions
- National identification numbers (CPR-nr)
- Information regarding trade union membership

The types of personal data processed vary depending on the data controller's accounting material, including accounting documents.

A.3.4. The processing includes the following categories of data subjects

- Employees of the data controller
- Customers of the data controller
- Suppliers and business partners of the data controller
- Other associates of the data controller

A.3.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. The processing has the following duration

The processing shall commence following the entry into force of these provisions and will continue for the duration of the engagement letter between the parties.

Appendix B – Authorised sub-processors

B.1. Approved sub-processors

By signing the engagement letter and thereby accepting this data processing agreement with its appendices, the data controller has approved that the data processor may use sub-processors.

A list of the sub-processors engaged by the data processor is available upon request from the data processor.

Copenhagen, January 2026

CHRISTENSEN kJÆRULFF

STATSAUTORISERET REVISIONSAKTIESELSKAB
CVR NR. 15915641

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 shall carry out the processing of personal data as described in sections A.1.2., A.2.2., and/or A.3.2. above.

C.2. Security of processing
The level of security shall take into account:

The processing involves personal data that, under data protection legislation, enjoys special protection, including information such as national identification numbers (CPR), bank account details, and potentially trade union membership. The processing also includes personal data concerning employees who are considered a vulnerable group of data subjects. Therefore, a "high" level of security must be established.

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 neces-sary (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:
:

General Security Measures
The data processor shall ensure that:

- All employees with access to personal data have committed to confidentiality concerning personal data and processing activities, and that such confidentiality remains in effect after the termination of cooperation between the parties and the employee's employment with the data processor.
- All such employees are subject to internal IT security and data protection policies.
- All such employees receive continuous training in IT security and data protection.
- The implemented security measures are regularly tested and evaluated.

Where the data controller has approved the use of sub-processors providing systems, platforms, or hosting services, the data processor shall also ensure that:

- The systems used for processing personal data are developed based on data security principles and best practices in data protection.

Physical Security Measures
The data processor shall ensure that:

- Physical locations where personal data is processed are secured with burglary protection and electronic surveillance.
- Access to such physical locations is only granted through personal key cards or similar access control measures.
- Visitors are not allowed unsupervised access to these locations.

Encryption of Personal Data
The data processor shall ensure that:

- All transmission of sensitive and confidential personal data takes place via an adequately encrypted connection.
- Equipment used for processing personal data is encrypted.

Where the data controller has approved the use of sub-processors providing systems, platforms, or hosting services, the data processor shall also ensure that:

- Personal data is encrypted at rest in accordance with best practices.
- Encryption keys are strong and stored securely with identity-based access controls and access control policies.

Ensuring Continuous Confidentiality, Integrity, Availability, and Resilience of processing systems and services
The data processor shall ensure that:

- Only authorized employees of the data processor have access to personal data.
- Such employees only access personal data as necessary for the performance of their duties.
- Equipment provided to employees for work purposes is secured with access control mechanisms.
- All employees have unique usernames and passwords.
- Password policies based on best practices are implemented.
- VPN or equivalent solutions with multi-factor authentication are used for remote access to personal data, including in connection with remote work.
- Employees are required to maintain access control and ensure that passwords remain personal and confidential.
- Procedures are implemented to ensure that employees lock their screens when unattended, and automatic screen locks are activated after a short period of inactivity.
- Firewalls and antivirus programs are used on all equipment involved in processing personal data, and such programs are kept up to date at all times.
- Procedures are implemented for handling requests from public authorities concerning access to personal data. These procedures must ensure that such requests are documented and made available to the data controller.

Where the data controller has approved the use of sub-processors providing systems, platforms, or hosting services, the data processor shall also ensure that:

- Effective backups are established and subject to regular spot checks.
- Procedures are implemented to protect against harmful incidents affecting operational equipment.
- Procedures are implemented to prevent the destruction, loss, alteration, or unauthorized disclosure of personal data stored on electronic and physical media.
- Operating servers only run necessary services and ports and are continuously updated for security.

Logging
Where the data controller has approved the use of sub-processors providing systems, platforms, or hosting services, the data processor shall ensure that: all access to and processing of personal data is logged and random checks are performed to ensure proper logging of access and processing activities.

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:

Assistance pursuant to Clause 9.1
If the data processor receives requests concerning data subject rights in relation to the data controller's personal data, the data processor must, without undue delay, forward such requests to the data controller via an encrypted connection.

The data processor shall assist the data controller in ensuring compliance with its obligations to fulfill data subject requests within the deadlines set forth in the General Data Protection Regulation. The data processor shall be entitled to remuneration for such assistance, based on its applicable hourly rates.

Assistance pursuant to Clause 9.2
In accordance with Clause 9.2 of these Provisions and Section 10, the data processor shall—taking into account the nature of the processing and the information available to the Processor—assist the data controller in notifying the supervisory authority of a personal data breach by providing the following information:

a. A description of the incident, including its physical location.
b. A timeline of events including the start, detection, and (expected) end of the incident.
c. The nature of the personal data breach, including any involved technologies, categories of data and data subjects, and the estimated number of affected data subjects and, where possible, the approximate number of personal data records concerned.
d. A general assessment of the likely consequences for the data subjects.

e. A description of the measures taken by the data processor and/or proposed by the data controller to address the incident and mitigate its adverse effects.
f. Information on whether the notification is final, or if further information will be provided, and how.
g. Details on where the data controller can obtain further information.

If it is not possible to provide all of the above information at once, it shall be delivered step-by-step without undue delay as soon as the data processor is able to obtain it.

The data processor is obligated to actively contribute to ensuring that the data controller receives sufficient information to comply with any obligation to notify the competent supervisory authority and the affected data subjects of the personal data breach.

Notification of a personal data breach, along with the above information, must be submitted in writing via email marked as "high priority" to the data controller.

The data processor must not make any public statements or disclosures to third parties about the personal data breach without prior written agreement from the data controller.

Provided that neither the data processor nor any sub-processor was the direct cause of the breach, the data processor shall be entitled to remuneration for assistance in handling the breach, based on its applicable hourly rates.

C.4. Storage period/erasure procedures
The data controller is solely responsible for deleting personal data that is processed within the data controller's own systems.

Any personal data that may be processed by the data processor in systems provided by the data processor as part of the service agreed in the engagement letter shall be deleted upon request from the data controller.

Upon termination of the service involving 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 provisions—has changed the original choice. Such changes must be documented and stored in writing, including in electronic form, together with these 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:

- The address(es) of the data controller
- The address(es) of the data processor
- The address(es) of approved sub-processors

Employees of the data processor are permitted to process personal data while working remotely, provided that the security of processing as described in Appendix C is maintained.

C.6. Instruction on the transfer of personal data to third countries
The processing of personal data covered by these Provisions may not take place in locations outside the EU/EEA without the prior approval of the data controller. The data controller's approval of sub-processors established outside the EU/EEA shall be considered as such approval.

The data processor shall ensure that any transfer of personal data to recipients outside the EU/EEA is based on either an adequacy decision by the European Commission or a valid transfer mechanism in accordance with Article 46 of the General Data Protection Regulation.

If the data controller does not, within these Provisions or subsequently, provide documented instructions regarding the transfer of personal data to a third country, the data processor shall not be entitled to perform such transfers within the scope of these Provisions.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

At the request of the data controller, the data processor shall participate in audits or inspections carried out by the data controller or the data controller's representative concerning the processing of personal data—for example, in the form of on-site inspections or by responding to a questionnaire. The data processor shall be entitled to remuneration for its participation in such audits, based on its applicable hourly rates.

Based on the results of the audit, the data controller shall be entitled to request the implementation of additional measures in order to ensure compliance with the General Data Protection Regulation, other applicable EU legislation, or national law, as well as these Provisions. The data controller shall bear all costs related to the acquisition, implementation, and operation of such additional measures.

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

The data processor is obligated to supervise any sub-processors by obtaining audit statements, conducting on-site inspections, or using questionnaires.

The results of such audits shall be submitted to the data controller upon request. The data controller may dispute the scope and/or methodology of the audit and, in such cases, request a new audit to be conducted under different conditions and/or using a different method. The data controller shall bear all costs associated with such new audits, and the data processor shall be entitled to remuneration in accordance with its applicable hourly rate.

Based on the results of the audit, the data controller shall be entitled to request the implementation of additional measures to ensure compliance with the General Data Protection Regulation, data protection provisions under other EU legislation, or national law of the Member States, as well as with these Provisions. The data controller shall bear all costs related to the procurement, implementation, and operation of such additional measures.

Appendix D The parties' terms of agreement on other subjects

D.1. Liability
The liability of the parties shall be governed by the data processor's general terms and conditions.

D.2. Governing Law and Jurisdiction
The provisions regarding governing law and jurisdiction set out in the data processor's general terms and conditions shall apply to these Provisions.