DATA PROCESSING AGREEMENT

TDC Erhverv SOC Services

Ver. 1.2

Standard Contractual Clauses

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

between

Customer
(the data controller)

and

TDC Erhverv A/S
CVR 40 07 52 91
Teglholmsgade 1
2450 København SV
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 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 as outlined in Appendix A (Information about the processing) 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

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

and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

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

6 Security of processing

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

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

   a. Pseudonymisation and encryption of personal data;

   b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

   c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

   d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data

controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7 Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

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

3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 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 in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

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

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

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

6. The processor shall, where feasible, 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 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 including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

   b. the likely consequences of the personal data breach;

c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11 Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to return all the personal data to the data controller and delete existing copies unless Union or Member State law requires storage of the personal data.

12 Audit and inspection

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

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

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

13 The parties' agreement on other terms

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

14 Commencement and termination

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

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

The provisions form part of the Main Agreement and must therefore not be signed.

15 Data controller and data processor contacts/contact points

1. The parties are obliged to continuously inform each other of changes regarding contact persons.

2. The data processor's data protection officer: dpo@nuuday.dk

   NB: In case of a data breach **outside normal working hours** (08.00 – 16.00), please contact Network Operations Center (NOC) via telephone: 70709212.

3. The data controller's contact persons are represented in the main agreement.

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:

TDC Erhverv offers a number of SOC Services, which involve the processing of personal data. The SOC services which include processing of personal data are Incident response, Log Management, and Managed Detection and Response (MDR). MDR can either be delivered on TDC Erhverv's hosted platform in Denmark or by making use of the customer's Microsoft Sentinel tenant. Regardless of whether the customer enters into an agreement on Incident response, Log Management, MDR based on TDC Erhverv's hosted platform or MDR based on the customer's Microsoft Sentinel tenant, TDC Erhverv processes personal data in the same way. This data processing agreement reflects TDC Erhverv's processing in relation to all SOC Services, where processing of personal data is included.

- **Incident response**
  With incident response TDC Erhverv might collect data from the customer's infrastructure for investigation purposes. The data is stored in TDC Erhverv's own data center in Denmark on encrypted hard drives on TDC Erhverv's premises, accessible only by the analysts working on the incident.
  In this connection, TDC Erhverv does not engage sub-processors.

- **Log Management (based on TDC Erhverv's hosted platform)**
  With Log Management, TDC Erhverv collects logs from devices located in the customer's infrastructure and stores these in TDC Erhverv's data center.
  In this connection, TDC Erhverv does not engage sub-processors.

- **MDR (based on TDC Erhverv's hosted platform)**
  With MDR, TDC Erhverv analyzes logs and reacts to suspicious activity in the customer's infrastructure. This MDR solution is based on logs collected by the Log Management service above.
  In this connection, TDC Erhverv does not engage sub-processors.

- **MDR (based on the customer's Microsoft Sentinel tenant)**
  TDC Erhverv is granted access to the customer's Microsoft Sentinel tenant.
  TDC Erhverv analyzes logs and reacts to suspicious activity in the customer's infrastructure. This solution is based on logs from the customer's infrastructure, and where logs are stored in the customer's own Microsoft Sentinel tenant in Microsoft Azure.
  In this connection, Microsoft is a direct data processor for the customer and thus not a sub-data processor for TDC Erhverv.

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):

TDC Erhverv Security Operations Center (SOC) monitors customers' infrastructure 24/7/365 for security incidents. All SOC analysts are security cleared by FE and PET, and the SOC is ISO 27001 certified as part of the certification of TDC Erhverv.

- **Incident response**
  Preparedness service
  Initial analysis and assessment of malicious activity / security incident
  Collection of data from customer's infrastructure
  Data is stored on Danish ground
  Identification, containment and eradication of incident
  Debriefing of customer at end of incident handling
  General recommendation on how to recover to trusted state
  Semi-annual status meetings and reports

- **Log Management**
  Collection of logs from the customer's infrastructure
  Logs are stored on Danish ground
  Parsing of logs into one unified format to enable correlation of information across logs
  Standard log retention time is 6 months
  Customer access to data through portal

- **Managed Detection and Response (MDR)**
  Built on top of Log Management service or Microsoft Sentinel
  Log based security alerting
  Alert rules reflecting current threat picture
  Alert handling, either manually by SOC analysts or automatically
  Identification, containment and eradication of security incidents
  Threat hunting for proactive identification of malicious activity based on latest threat intelligence
  Forensics for collection of digital evidence
  Monthly and quarterly reports

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

The data processor does not determine the type of personal data included in the services. It is the responsibility of the data controller to determine which categories of personal data are processed.

Typically, the SOC Services will include the following types of personal data:

- Name
- Address

- Email
- Telephone number
- Free text
- Username
- IP address
- IP packet content
- User activity (only for Incident response)

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

- Customers of the data controller
- Employees of the data controller
- Third parties

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

Until termination of the Main contract between the Customer and TDC Erhverv.

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
N/A			

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, see section 7.

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 processing described under A.2 to fulfill the purposes described under A.1, where TDC Erhverv is the data processor.

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

The data processor is entitled and obliged to make decisions about which technical and organizational security measures must be implemented in order to establish the necessary (and agreed) security level. However, the data processor must - under all circumstances and as a minimum - implement the following measures (Based on technical and organizational security controls from the independent auditor's ISAE 3000 assurance report on information security and measures in accordance with the data processing agreement), which have been agreed with the data controller:

Procedures and controls that must be observed to ensure that the data processor has implemented technical measures to ensure relevant processing security.

1. There must be written procedures which contain requirements that agreed security measures are established for the processing of personal data in accordance with the agreement with the data controller.
2. There must be an ongoing – and at least once a year – assessment of whether the procedures need to be updated.
3. External access to systems and databases used for processing personal information must be through a secured firewall.
4. Access to personal data must be isolated to users with a work-related need for this.
5. System monitoring (syslog) has been established for the systems and databases used to process personal information.
6. Effective encryption must be used when transmitting confidential and sensitive personal data via the Internet and by e-mail.
7. Logging must be established in systems, databases and networks of sensitive parties:
   Activities performed by system administrators and others with special rights
   Security incidents including:
   i. Changes to logging settings, including disabling logging
   ii. Changes in system rights for users
   iii. Failed attempts to log on to systems, databases and networks
   Log information must be protected against manipulation and technical errors and reviewed on an ongoing basis.

8. Personal information used for development, testing or the like must always be (if possible) in pseudonymized or anonymized form. Use may only be made to carry out the purposes of the person responsible in accordance with the agreement and on his behalf.
9. The established technical measures must be tested continuously by vulnerability scans and penetration tests.
10. Changes to systems, databases and networks must follow established procedures which ensure maintenance with relevant updates and patches, including security patches.
11. A formalized business procedure must be established for granting and terminating user access to personal data. Users' access is reassessed regularly, including that rights can still be justified by a work-related need.
12. Access to systems and databases in which personal data is processed, which entails a high risk for those registered, must at least be done using two-factor authentication.
13. Physical access security must be established so that only authorized persons can gain physical access to premises and data centers in which personal data is stored and processed.

Procedures and controls that must be observed to ensure that the data processor has implemented organizational measures to ensure relevant processing security.

1. The data processor's management must have approved a written information security policy, which is communicated to all relevant stakeholders, including the data processor's employees. The IT security policy must be based on a completed risk assessment.
   An ongoing – and at least once a year – assessment of whether the IT security policy needs to be updated must be carried out.
2. The data processor's management must ensure that the information security policy does not conflict with concluded data processor agreements.
3. A check must be carried out on the data processor's employees in connection with employment. The inspection must include, to the extent relevant:
   - References from previous employment
   - Criminal record
   - Examination certificates
4. Upon employment, the employee must sign a confidentiality agreement. Furthermore, the employee must be introduced to the information security policy and procedures regarding data processing as well as other relevant information in connection with the employee's processing of personal data.
5. Upon resignation, the data processor must have implemented a process which ensures that the employee's rights become inactive or cease, including that assets are confiscated.
6. Upon resignation, the employee must be informed that the signed confidentiality agreement is still valid, and that the employee is subject to a general duty of confidentiality in relation to the processing of personal data carried out by the data processor for the data controller.
7. Continuous awareness training must be carried out for the data processor's employees in relation to IT security in general and processing security in relation to personal data.

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:

1. The data processor assists, considering the nature of the processing, as far as possible the data controller by means of appropriate technical and organizational measures with the fulfillment of the data controller's obligation to respond to requests for the exercise of the rights of the data subjects as laid down in the chapter of the data protection regulation III, cf. Provision 9.1. If the data controller himself is able to fulfill the data subject's rights as set out in Chapter III, and/or it requires disproportionate time, material and effort from the data processor to assist the data controller, the data controller may be invoiced by the data processor for time consumed at the standard hourly rate.
2. Regarding Provision 9.2(c): Assistance to the data controller will be provided within the framework of generally available information and documents. Any additional assistance from the data processor to the data controller must be done at the request of the data controller during a reasonable time consumption, for a reasonable time limit and at a reasonable price agreed by the parties from time to time.
3. Regarding Provisions 9.2 and 12: The data processor's assistance shall not exceed a reasonable, expected and customary extent. Assistance in addition must be provided at the request of the data controller during a reasonable time consumption, for a reasonable time limit and at a reasonable price agreed by the parties from time to time.

C.4. Storage period/erasure procedures

Personal data is stored and deleted according to instructions from the data controller.

Upon termination of the provision of personal data processing services, the data processor shall either delete or return the personal data in accordance with Clause 11.1., unless the data controller – after the signature of the contract – has modified the data controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

C.5. Processing location

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

- TDC Erhverv's (TDC Brands A/S) locations in Denmark. TDC Brands A/S headquarters are placed at Teglholmsgade 1, 2450 København SV

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

The personal data may not be transferred to a country outside the EU/EEA, unless the data controller has expressly and beforehand approved the transfer in writing. If required by law or at the request of the data controller, the data processor must accept the European Commission's Standard Contract Regulations (Commission's Implementing Decision (EU) 2021/914 of 4 June 2021) when transferring personal data to third countries. If, according to the data protection regulation, or at

the request of the data controller, new versions of the standard contract provisions must be adopted, the data processor must enter such new provisions, either as new agreements or as a replacement for already existing agreements. In addition, it is the responsibility of the data processor to ensure that there is a legal basis for transfer.

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 must annually, at its own expense, obtain an ISO 27001 certificate and an ISAE 3000 type II audit statement from an independent third party and, at the request of the data controller, draw up a management statement confirming that the data processor fulfills its obligations in accordance with the data protection regulation, data protection provisions in other EU law or the national law of the Member States and these Regulations.

The latest audit statement can be requested at any time from: https://tdc.dk/vilkaar subsection 15 Certifikater og revisionserklæringer.

If the data controller requests further information in connection with an audit of the data processor, the data processor must give the data controller access to these against payment of the data processor's reasonable costs in connection therewith.

In addition, the data controller or a representative of the data controller has, against payment of the data processor's reasonable costs in connection therewith, access to carry out inspections, including physical inspections, with the premises from which the data processor processes personal data, including physical locations and systems used to or in connection with the treatment. Such inspections may 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 must continuously supervise the sub-processor's compliance with the data protection regulation, data protection regulations in other EU law or the national law of the member states and these Regulations.

The data processor shall annually at the data processor's expense obtain an auditor report from an independent third party concerning the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The parties have agreed that the following types of auditor reports may be used in compliance with the Clauses: ISAE 3000, ISAE 3402, ISO 27001, SOC 2.

The auditor report shall upon request and without undue delay be submitted to the data controller for information.

Appendix D The parties' terms of agreement on other subjects

1. Confidentiality

1.1 Notwithstanding the contents of the Clauses, the Main Contract is confidential between the Parties to the effect that any sub-processors may only be informed of the contents of the Clauses and only to the extent necessary.

2. Information

2.1 To the extent relevant, the data controller must inform the data processor of any legislation other than the general personal data legislation in the EEA, as for example any special, local requirements for the storage of personal data in the country of the data controller. If such special legislation flows down and imposes more obligations on the data processor than the general personal data legislation, the data controller shall indemnify the data processor for increased, documented additional costs for any such adaption. In that respect, no consideration shall be taken to the circumstances of other customers, including any payments made by such customers.

3. Liability and indemnity

3.1 The parties' responsibilities under the Agreement follow the regulation of the Main Agreement. In relation to liability towards third parties, Article 82 of the Data Protection Regulation applies.

4. Severability

4.1 Should any provision of the Clauses be held to be unenforceable, illegal or invalid, such provision may by good faith negotiations or interpretation be replaced by provisions that to the widest extent possible gives effect to the intent and enforcement of the original provisions. If that is not possible, such term or provision shall to that extent be deemed not to form part of the Clauses. All other terms and conditions of the Clauses shall remain in full force and effect.