Standard Contractual Clauses (Data Processor Agreement)

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

Proceedy A/S
CVR 33646755
Fuglebakken 15
DK-8800, Viborg
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 3
3. The rights and obligations of the data controller 3
4. The data processor acts according to instructions 4
5. Confidentiality 4
6. Security of processing 4
7. Use of sub-processors 5
8. Transfer of data to third countries or international organisations 6
9. Assistance to the data controller 6
10. Notification of personal data breach 8
11. Erasure and return of data 8
12. Audit and inspection 8
13. The parties' agreement on other terms 9
14. Commencement and termination 9
15. Data controller and data processor contacts/contact points 9
Appendix A Information about the processing 11
Appendix B Authorised sub-processors 13
Appendix C Instruction pertaining to the use of personal data 14
Appendix D The parties' terms of agreement on other subjects 19

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 online services from Proceedy, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

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

6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

9. Appendix D contains provisions for other activities which are not covered by the Clauses.

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

11. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

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

2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions. If the data processor recognises illegal or unlawful actions are taken place, access to the service will be suspended and the data controller will be contacted immediately.

5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

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

6. Security of processing

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

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

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

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

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

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

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

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

7. Use of sub-processors

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

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

3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided 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 data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete 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 (Datatilsynet), 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 (Datatilsynet), prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

2. The data processor's notification to the data controller shall, if possible, take place within 24 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3) GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

    a. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

    b. the likely consequences of the personal data breach;

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

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

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done unless Union or Member State law requires storage of the personal data.

   The data processor commits to exclusively process the personal data for the purposes and duration provided for by this law and under the strict applicable conditions.

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	[NAME]
Position	[POSITION]
Date	[DATE]
Signature	[SIGNATURE]

   On behalf of the data processor

Name	Anders Juul
Position	CEO
Date	[DATE]
Signature	[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.

Data controller:
The registered administrator in Proceedy – e.g., verify in management.proceedy.dk

Data processor:

Name	Aage Nielsen
Position	CTO
Telephone	+45 41 22 10 13
E-mail	gdpr@proceedy.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:

The purpose is to organize, structure and present data to the users in a non-complex way. Service solutions offered by Proceedy are Software-as-a-Service cloud solutions.

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):

Proceedy services are software applications that collects, stores and present all kind of data entirely provided by the controller due to the concluded service agreement.

Proceedy processes data on behalf of the data controller by usual operation, hosting, data receival and forwarding, search, storage, restoration, deletion, restriction, maintenance, development, logging, support troubleshooting and other IT services associated with the data processor's delivery of the digital solution to the data controller in accordance with the agreement concluded between the parties.

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

Proceedy does **not** distinguish between the types of data that being processed – but keeps everything encrypted when data is being transferred and at rest.

However we treat all data as equal important. The processing includes the following types of personal data about data subjects:
☐ Non-sensitive categories of personal data

Name, address, e-mail, phone number, title, national and international social security numbers or similar, information in personal resumes, any information regarding legal cases, including case history/sequence of events, timeline the parties involved in the case etc.
Special categories of personal data (tick the boxes):
☒ Racial or ethnic origin
☒ Political opinions
☒ Religious beliefs
☒ Philosophical beliefs
☒ Trade union membership
☒ Health data
☒ Sex life or sexual orientation
☐ Genetic or biometric data for the purpose of identification
☒ Criminal convictions and offenses

In case other data than the above listed provided by the customer is processed in Proceedy – the responsibility relies entirely on the data controller.

See also C.2

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

Proceedy allows any form of categories and do not distinguee between them. It is **entirely** up to the data controller to specify the categories in article 30.

The categories below are examples:

- Employees
- Clients
- The counterparties lawyer
- Witnesses
- Business partners
- Counterparties
- Other third parties involved in or relevant to cases or in the proceedings

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

The processing is taking place as long as the main agreement is in force or until data controller has deleted all personal data.

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 Danmark ApS	13612870	Kanalvej 7 2800 Kgs. Lyngby	Providing hosting for the referred services (Zone: **North Europe**)
SendInBlue	FR80498019298	7 rue de Madrid Paris 75008	Sending mails from the platform

The data controller shall on the commencement of the Clauses authorise the use of the above-mentioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

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

The data processor will inform about any changes to the sub-processor list no later than 30 days before engagement with any new sub-processor.

Appendix C Instruction pertaining to the use of personal data

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

Proceedy processes data on behalf of the data controller by usual operation, hosting, data receival and forwarding, implementation, search, storage, restoration, deletion, restriction, maintenance, development, logging, support, troubleshooting and other IT services associated with the data processor's delivery of the digital solution to the data controller in accordance with the agreement concluded between the parties.

C.2. Security of processing

The level of security shall take into account:

That the processing involves a large volume of personal data which are subject to Article 6 GDPR which is why a 'Medium' level of security should be established.

That the processing involves a medium to large volume of sensitive personal data which are subject to Article 9 GDPR which is why a 'High' level of security should be established.

The data processor has implemented a risk-based approach to IT security and the protection of personal data processed on behalf of the data controller.

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 high (and agreed) level of data security.

The data processor shall however – in any event and at a minimum – implement the following measures that applies[2] and have been agreed with the data controller:

Logging

The following security measures applies:

☒ All relevant network traffic	☒ Server logs (event, security, access, audit etc.)	☒ Database logs (event, security, access, audit etc.)
☒ All access attempts (successful and unsuccessful)	☒ Activities carried out by system admins and others with elevated rights	☒ Security incidents including deactivation of logging, changes to system rights and failed login-attempts

Antivirus, malware and firewalls

The following security measures applies:

☒ All external access to systems and databases where processing of personal data takes place is filtered through a secure firewall with a restrictive protocol.	☒ Use of port and IP-address filtration	☒ Protection against XSS and SQL injections is implemented in all services.

[2] Penetration tests, encrypted web-access etc. only applies for web-based services. Physical data center measures does not apply for public cloud services based on e.g. Azure, Amazon or similar.

☒ All file transfers are scanned using antivirus software	☒ Antivirus continuously updated	☒ The data processors internal networks are only accessible for authorized persons

Encryption
The following security measures applies:

☒ Effective and strong encryption based on a recognized algorithm is used for transmission of personal data though the internet and/or email	☒ A minimum of TLS 1.2 is being used for secure e-mail communication	☒ A minimum of TLS 1.2 is being used, and forced, for secure access to web services (http, API, S-FTP etc.)
☒ Stored sensitive and/or confidential personal data in files are encrypted using a strong algorithm	☒ Stored sensitive and/or confidential personal data in databases and filesystem is encrypted using a strong algorithm	☒ Stored data is encrypted using an automated generated key
☒ Stored data is encrypted using a AES-256 standard, similar or better		

Vulnerabilities and penetration test
The following security measures applies:

☒ Vulnerability scan is being done on each deploy	☒ Penetration-test is being done on a regular basis	☒ The results from scans are being used actively to ensure a sufficient level of security and to minimize the impact of hacker-attack, Denial-of-Service attacks etc.

Back up and availability
The following security measures applies:

☒ Critical patching is done within 4 weeks from evaluating the patch	☒ Security patching is prioritized and done on an asap basis	
☒ System monitoring is taking place on all systems where personal data is processed	☒ A guaranteed availability (SLA) exists	☒ A guaranteed availability of more than 98,5%

☒ Back-up is established to ensure that all systems and data, including personal data, can be restored if they are lost or altered.	☒ Back-up resides on alternate location	☒ Back-up is within the EU region
☒ It is logged who initiated the restore	☒ Restore can be done within 24 hours	☒ It is logged who requested the restore

Authorization, access control and security

The following security measures applies:

☒ Only employees with a work-related demand for personal data are granted access to personal data	☒ The assessment of an employee's work-related demands is carried out from a "need-to have" perspective, to ensure compliance with the principle of data minimization	☒ When employed, the new employee signs a confidentiality agreement
☒ All employees are informed about the management approved information security policy	☒ All potential new employees are subject to screening	☒ Specific procedures are in place to ensure that the access user rights of terminated employees are removed
☒ All new employees are introduced to the information security policy and the procedures for processing of personal data pertaining to the work-related responsibilities of the employee.	☒ The data processor does not operate with shared logins so the data processor will always be able to identify which employee performed a specific activity	☒ Laptop computers and other computers processing personal data include protection with commonly recognized encryption
☒ The data processor has implemented a complex password policy	☒ The data processor has implemented protection of moveable assets (encrypted USB keys etc.)	☒ If data is in cloud – MFA is required for admins
☒ Accessing company data from remote requires VPN or other secure (encrypted) connection	☒ If data is in cloud – MFA is required for all users	☒ External consultants are informed of the data processors security guidelines and obliged to comply them

Risk assessments

The following security measures applies:

☒ In general - risk assessments were performed within the last 12 months	☒ Risk assessment of own data processing on behalf of the data controller	☒ Risk assessments of sub data processors
☒ Risk assessments are approved by the management	☒ If risk assessment shows medium or high-risk appropriate controls or actions of mitigation are applied	

Controls

The following security measures applies: https://www.datatilsynet.dk/media/7592/dataansvarlige-og-databehandlere.pdf

☒ Controls related to authorizations and access are in place	☒ A self-made control 'framework' is in place and actively used	☒ Control responsibilities is assigned appropriate employees
☒ Controls are paired to a risk management approach	☒ Yearly ISAE3000 or equivalent independent inspection report (available from 2023) available for data controller on request	

Data privacy by design and by default
This topic is mandatory for data processors developing own systems and/or applications.

The following security measures applies:

☒ Data processor is aware of the 'Data protection by design and by default' terminology and guidelines from the European Data Protection Board	☒ Data processor has its own manual, processes, and design guides for ensuring data protection by design and by default	☒ Relevant employees (e.g. architects, designers and developers) are updated on an on-going basis regarding latest practices for data protection by design and by default
☒ Relevant employees (e.g. architects, designers, and developers) was updated on latest best-practice within data protection by design and by default within the last 6 months	☒ Implemented default security measures for development is documented and can be shared with data controller	☒ No production data is being used either in development, test or other environments

C.3. Assistance to the data controller

The data processor shall insofar as this is possible assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the relevant technical and organisational measures.

Proceedy builds services, applications and documentation in a way that the data controller is self-reliant. In case of the need of assistance the controller can contact support at support@proceedy.dk or call us. The assistance regarding GDPR related matters is free of charge.

C.4. Storage period/erasure procedures

Personal data processed by the service is stored and erased in accordance with the policies of the data controller.

Upon termination of the provision of personal data processing services, the data processor shall delete 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:

- The place of the data processor's place of business or within the data regions mentioned in Annex B, section B.1.

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

The data controller does not give instructions regarding the transfer of personal data to a third country. Thus, the data processor is not entitled within the framework of these Regulations to carry out such transfers.
This also means that the processor is not allowed – within the scope of clause 7.3 – to chance any sub processor to at sub-processor that is placed or controlled by a company in a third country that has not been approved by the European Commission.

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 annually at the data processors expense obtain an auditor's report or an inspection report from an independent third party concerning the data 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's report or an inspection report may be used in compliance with the Clauses:

Reports based on the principles of ISAE 3000 standard or equivalent independent inspection report.

The auditor's report or an inspection report shall without undue delay be submitted to the data controller for information. The data controller may contest the scope and/or methodology of the report and may in such cases request a new audit/inspection under a revised scope and/or different methodology. A new audit/inspection under a revised scope will be at the data controller's cost. The data controller is entitled to ask questions regarding the report without being billed.

Based on the results of such an audit/inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data controller or a representative of the data controller also has – for a fee – access to carry out inspections, including physical inspections, of the locations from which the data processor processes personal data. Such inspections may be carried out when the data controller deems it necessary and after appropriate prior notice.

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

The auditor's report or inspection report shall cover the audits performed by the data processor of possible sub-processors. This means that the data processor performs an annual inspection of all sub-processors as a part of the data processors risk management system and by the guidelines provided by the Danish Data Protection Agency (Datatilsynet). The audits shall have the same scope as described under C.7.

Documentation for such inspections is forwarded upon request to the data controller for information.

Appendix D The parties' terms of agreement on other subjects

The parties' agreement on liability and limitation of liability appears from the agreement entered into between the data processor and the data controller on the data processor's delivery of a digital solution to the data controller, as long as this does not directly or indirectly contravene the Regulations or impair the fundamental rights and freedoms of the data subject, which follow from the data protection regulation.