Standard Contractual Clauses

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

between

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

(the data controller)

and

Inscrive ApS
CVR 44650975
Rosenkrantzgade 12 D st,
8000 Aarhus
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....7
11. Erasure and return of data....8
12. Audit and inspection....8
13. The parties' agreement on other terms....8
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....15
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 the data processors services, 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.

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

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

4. The data processor acts according to instructions

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

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

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 On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

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

6. Security of processing

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

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

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

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

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

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

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

   If subsequently – in the assessment of the data controller – mitigation of the identified risks 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. 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 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. 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.

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	Viktor Lundsgaard Andersen
Position	CEO
E-Mail	viktor@inscrive.io
Date	
Signature	

15. Data controller and data processor contacts/contact points

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

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

Name	[NAME]
Position	[POSITION]
Telephone	[TELEPHONE]
E-mail	[E-MAIL]

Name	Søren Skou Jessen
Position	Compliance Officer

Telephone	+45 29 36 51 64
E-mail	support@inscrive.io[E-MAIL]

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 processing of the data controller's personal data takes place for the purpose of fulfilling the agreement entered into between the data processor and the data controller regarding the data processor's provision of the data processor's solutions and services. The purpose of the data processor's solution(s) and/or service(s) is to provide the solution Inscrive. The solution is a collaborative real-time online editor for LaTeX documents.

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):

As owner and provider of the solution, the data processor processes, through general operations, including hosting, display, organization, receipt, forwarding, structuring, adaptation, implementation, search, processing, storage, restoration, deletion, restriction, maintenance, development, logging, support, troubleshooting, and other IT services associated with the data processor's solution(s) and/or service(s) for the data controller in accordance with the agreement entered into between the parties.

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

The data processor generally processes the categories of personal data listed below. However, when using the solution, it is possible that the data controller may entrust the data processor with the processing of all types of data and personal data, whereby the data processor may potentially process all categories of personal data.

Ordinary personal data (cf. GDPR Article 4(1) and Article 6):
☒ Ordinary personal data.

Categories of personal data:
a) Contact details, such as name, email address
b) User information, such as username, user location, and behavior
c) Any other personal data necessary for the data controller's use of the data processor's provision of tools and services.

Sensitive personal data (cf. GDPR Article 9):
☐ N/A

☐ Racial or ethnic origin.
☐ Political opinions.
☐ Religious beliefs.
☐ Philosophical beliefs.
☐ Trade union membership.
☐ Genetic data.
☐ Biometric data.
☐ Health data.
☐ Sexual life or sexual orientation.

Information on individuals' strictly private matters (cf. GDPR Articles 6 and 9):
☐ N/A

☐ Criminal matters.
☐ Significant social problems.

Other strictly private matters not mentioned above:
☐ N/A

☐ Other private matters.

Information on CPR number (cf. GDPR Article 87):
☐ N/A

☐ CPR numbers.

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

The data processor generally processes the categories of data subjects listed below. However, when using the solution, it is possible that the data controller may entrust the data processor with the processing of all types of data and personal data, whereby the data processor may potentially process personal data about more categories of data subjects.

Categories of data subjects:
a) Employees
b) Students
c) Other data subjects who may use the solution.

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 not time-limited and continues until the subscription agreement between the parties concerning the provision of the data processor's tools to the data controller is terminated or cancelled by one of the parties.

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	LOKATION	DESCRIPTION OF PROCESSING
Hetzner	Germany	Hetzner is used for hosting and remote backup of the solution, including storage and processing of data. Hetzner is also used as the mail server service provider for sending emails. Thus, all data in the solution may be processed by Hetzner. Backup data is deleted after a rolling 7-day period. Data is encrypted via SSL and TLS 1.2 in transit.

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's notification of any planned changes regarding the addition or replacement of sub-processors must reach the data controller at least 30 days before the use or change takes effect, insofar as this is reasonably possible cf. contract provision 7, 7.3.

Notwithstanding the above, the data controller accepts that there may be special cases where there is a specific need for the change regarding the addition or replacement of sub-processors to take place on shorter notice or immediately. In such cases, the data processor will notify the data controller of the change as soon as possible.

If the data controller objects to the changes, the data controller must notify the data processor thereof before the notified effective date of the change. The data controller may only object if the data controller has reasonable, specific grounds for doing so.

In the event of the data controller's objection, the data controller simultaneously accepts that the data processor may be prevented from delivering all or part of the agreed services. Such non-performance cannot be attributed to the data processor as a breach. The data processor retains its right to payment for such services, regardless of whether they can be delivered to the data controller.

Where it has been specifically agreed that the data processor may not use sub-processors without the prior approval of the data controller, the data controller accepts that this may result in the data processor being prevented from fulfilling the services. If the data controller has refused changes regarding the addition or replacement of sub-processors, the failure to deliver services will therefore not be regarded as a breach of the parties' agreement regarding the delivery of services, attributable to the data processor, in cases where the non-performance can be attributed to circumstances of a sub-processor.

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:

general operations, including hosting, display, organization, receipt, forwarding, structuring, adaptation, implementation, search, processing, storage, restoration, deletion, restriction, maintenance, development, logging, support, troubleshooting, and other IT services connected with the data processor's solution and/or service to the data controller pursuant to the agreement entered into between the parties where the Provider offers the solution.

Inscrive is an online collaborative real-time editor for LaTeX documents aimed at researchers and students. The solution allows real-time collaboration on files with the purpose of creating documents such as reports, theses, PhDs, doctoral dissertations, and similar.

C.2. Security of processing

The level of security shall take into account:

The data processor's solutions and services generally involve the processing of personal data as defined in Appendix A of the data processing agreement. Regardless of the scope of Appendix A, the data processor has chosen to implement a generally high level of security reflecting the possibility of such processing. The data processor is thus entitled and obliged to decide which technical and organizational security measures must be implemented in order to establish the necessary (and agreed) level of security.

However, the data processor must – in all circumstances and as a minimum – implement the following measures agreed with the data controller:

Information security

The data processor has implemented policies, controls, and processes covering the following areas of information security:

- Confidentiality: Ensuring that unauthorized persons cannot access data that may be misused to the detriment of the data processor's customers, business partners, and employees.
- Integrity: Ensuring that systems contain accurate and complete information.
- Availability: Ensuring that relevant information and systems are available and stable.

Instruction

Written procedures exist requiring that personal data may only be processed when an instruction is present. Assessments are carried out on an ongoing basis – and at least once a year – as to whether procedures must be updated. The data processor only processes personal data in accordance with the instructions from the data controller.

Physical security

The data processor must maintain physical security measures to protect premises used for processing personal data, including the storage of personal data covered by the Data Processing Agreement against unauthorized access and manipulation.

The data processor must implement appropriate technical measures to limit the risk of unauthorized access to premises where personal data is processed. Where necessary, the data processor must evaluate and improve the effectiveness of such measures.

The level of physical security must always reflect the current threat landscape as well as the sensitivity and volume of personal data covered by the Data Processing Agreement.

Communication links and encryption
The data processor has appropriate technical measures to protect systems and networks, including protecting data during transmission and access via the internet, and to limit the risk of unauthorized access and/or installation of malicious code.

The data processor uses appropriate encryption technologies and other equivalent measures in accordance with legal requirements, approved standards for encryption of classified information, and good data processing practice.

Where required under applicable national and international legislation, standards regarding encryption of classified information, or good data processing practice, the data processor applies encryption technologies and other equivalent measures.

Transmission of sensitive and confidential information over the internet is protected by encryption. Technological solutions for encryption are available and activated. The firewall only permits encrypted data traffic. Formal procedures are in place to ensure that the transmission of sensitive and confidential information over the internet is protected by strong encryption based on a recognized algorithm.

Firewall or similar technical measures
External access to systems and databases used for processing personal data may only occur through a VPN. Administrative access must exist to maintain firewall configuration and rulesets.

Antivirus
Systems and databases used for processing personal data are equipped with antivirus software, which is continuously updated.

Backup
The data processor must have internal contingency procedures ensuring restoration of services without undue delay in the event of operational interruptions, in accordance with the main agreement. The data processor ensures daily backup.
Backup of configuration files and data must take place continuously so that relevant data can be restored. Backups must be stored in such a way that they are not accidentally or unlawfully (e.g., due to fire, flooding, accident, theft, etc.) destroyed, lost, corrupted, exposed to unauthorized access, misused, or otherwise processed in violation of the applicable rules and regulations for the processing of personal data.
Backups must be stored physically separate from primary data and in a security-approved data center.

Use of home/remote workplaces
If data processing takes place from ad hoc and/or home workplaces, the data processor must ensure that these comply with the security requirements of this Data Processing Agreement with appendices and applicable legislation.

The data processor must, among other things, ensure:

- That encrypted connections are used between the ad hoc workplace and the data processor's/data controller's network.

- That the data processor has an internal instruction to its employees regarding ad hoc and home workplaces.

In addition, the data processor must, where technically possible, use two-factor authentication.

Instruction of employees
The data processor ensures that employees are at all times familiar with and sufficiently trained and instructed regarding the purpose of data processing, policies, workflows, and their duty of confidentiality.

An information security policy exists, which has been reviewed and approved by management within the last year. The information security policy has been communicated to relevant stakeholders, including the data processor's employees.

The information security policy generally complies with the requirements for safeguards and processing security in data processing agreements entered into. Formal procedures are in place to verify employees at hiring. Employees have signed a confidentiality agreement. Employees have been introduced to:

- The information security policy.
- Procedures concerning data processing, as well as other relevant information.

Procedures exist to ensure that the rights of terminated employees are deactivated or cease upon termination, and that assets such as access cards, PCs, mobile phones, etc., are retrieved.

Formal procedures ensure that terminated employees are reminded of their continued duty of confidentiality and general secrecy obligation. The employment contract includes guidelines stipulating that employees remain subject to confidentiality after termination of employment. The data processor provides awareness training to employees covering general IT security and processing security in relation to personal data.

There is documentation that all employees with access to or who process personal data have completed the offered awareness training.

Disposal of equipment
The data processor must have formal processes to ensure the effective deletion of personal data before the disposal of electronic equipment.

Logging

1. Ensures logging in all environments where personal data is processed.
2. Logging of access to the solution.
3. Ensures that the scope of security logging is defined based on a risk assessment carried out by the data processor.
4. Ensures sufficient storage capacity to retain security logs for the required period.
5. Ensures that ongoing spot checks are performed to verify that security logs contain the expected information.
6. Balances log retention periods against the need to analyze cyberattacks, support investigations, and respect the rights and freedoms of natural persons.
7. Ensures that collected information on user activity in logs is protected against deletion and manipulation.

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:

Rights of data subjects, cf. section 9.1.

- The data processor must assist in observing the rights of data subjects by, for example, being able to provide access, deletion, restriction, and rectification of information, and ensuring this also occurs at sub-processors.
- The data processor must assist in fulfilling the rights of data subjects without undue delay.
- The data processor must have a procedure describing how requests from a data subject regarding their rights are handled.

Breaches and incidents, cf. section 9.2.

Information to be provided:

- Facts about the identified breach (time, place, cause)
- When the breach began, when it was discovered, and when it was stopped
- The nature of the personal data breach, including whether there has been a breach of confidentiality, integrity, and availability
- The categories and approximate number of affected data subjects, if possible
- The categories of personal data, if possible
- Name and contact details of a contact point where further information can be obtained
- Description of the likely consequences of the breach
- Description of the measures taken or proposed to be taken as part of handling the breach and its possible adverse effects

C.4. Storage period/erasure procedures

Personal data is stored for the duration of the parties' agreement regarding the data processor's provision of the data processor's solution(s) and/or service(s) to the data controller, or pursuant to a separate written agreement, after which it is deleted by the data processor.

Upon termination, the data processor must either delete or return the personal data in accordance with Provision 11.1, unless the data controller – after signing these Provisions – has changed the data controller's original choice. Such changes must be documented and stored in writing, including electronically, in connection with the Provisions.

C.5. Processing location

Processing of personal data covered by the Provisions may not, without the prior written approval of the data controller, take place at other locations than those stated in this Data Processing Agreement and the addresses appearing for the sub-processors used, as well as further sub-processors, as set out in the applicable Appendix B.

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

If the data controller has not in these Provisions or subsequently provided documented instructions regarding the transfer of personal data to a third country, the data processor is not entitled under these Provisions to make such transfers, unless such a transfer is to one of the authorized sub-processors listed in Appendix B. The transfer basis is applied in accordance with

Chapter V of the GDPR concerning transfers of personal data to third countries or international organizations. The specific transfer bases are set out in the applicable Appendix B.

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

Within a period of 12 months, the data processor must at its own expense prepare a self-assessment statement from an independent third party regarding the data processor's compliance with the GDPR, data protection provisions in other EU law, or national law of the Member States, and these Provisions.

The self-assessment statement will be made available to the data controller on the data processor's website.

The data controller may, against payment, challenge the scope and/or method of the statement and may in such cases request a new statement under other scope and/or using another method.

Based on the results of the statement, the data controller is entitled to request the implementation of additional measures to ensure compliance with the GDPR, data protection provisions in other EU law, or national law of the Member States, and these Provisions.

The data controller or a representative of the data controller also has, against payment, access to carry out inspections, including physical inspections, of the premises from which the data processor processes personal data. Such inspections may be conducted whenever the data controller deems it necessary.

Any expenses incurred by the data controller in connection with a physical inspection are borne by the data controller itself.

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

The data processor must at its own expense obtain annually a control report regarding the sub-processor's compliance with the GDPR, data protection provisions in other EU law, or national law of the Member States.
Documentation of such inspections is provided to the data controller upon request for its information.

Appendix D The parties' terms of agreement on other subjects

D.1 Liability and breach
Any breach of the Provisions shall be governed and handled in accordance with the parties' agreement regarding the provision of the services.

In cases where the data processor has paid amounts to data subjects in accordance with Article 82 of the GDPR or Section 26 of the Danish Liability for Damages Act (*erstatningsansvarsloven*), the data processor has full recourse against the data controller for the amount paid which exceeds the agreed liability limitation in the parties' agreement regarding the provision of the services.
The parties have hereby contractually deviated from Article 82(5) of the GDPR and Section 26 of the Danish Liability for Damages Act.
Notwithstanding GDPR Article 82(5), a party who has paid compensation to a data subject that does not constitute full compensation may exercise recourse in accordance with the principle in Article 82(5).
With respect to other compensation for non-material damage to data subjects, the principle in Article 82 shall likewise apply regarding the internal final allocation of liability between the data processor and the data controller.
The parties may not claim recourse or damages against each other for fines or other penalties imposed under Section 41 of the Danish Data Protection Act (*databeskyttelsesloven*) or for penalty notices accepted under Section 42 of the Danish Data Protection Act.

D.2 Consequences of the data controller's unlawful instructions
The data controller acknowledges that the data processor is dependent on the data controller's instructions regarding the extent to which the data processor is entitled to use and process personal data on behalf of the data controller. The data processor is therefore not liable for claims arising from the data processor's actions or omissions, to the extent that such actions or omissions are a direct data processing activity carried out in accordance with the data controller's instructions, unless it can be established that the data processor was aware of the illegality of the processing.

D.3 Use of sub-processors providing on standard terms
Notwithstanding contract provision 7, it shall be emphasized that if the data processor uses a sub-processor that provides its services on its own terms, which the data processor is not able to deviate from, the sub-processor's terms shall apply to the processing activities entrusted to such sub-processor. Where processing takes place under a sub-processor's terms, this is specified for the relevant sub-processor in the list of sub-processors. By these Provisions, the data controller gives its acceptance of and instruction that such specific processing activities shall take place on the sub-processor's terms.

D.4 Deletion and return of data
It is agreed between the parties that the data controller shall instruct regarding the data processor's deletion and return of personal data in connection with the termination of the Provisions.
The data controller must, no later than 30 days after the processing of personal data has ceased, inform the data processor whether all personal data shall be deleted or returned to the data controller. In cases where personal data must be returned to the data controller, the data processor must also delete any copies. The data processor must ensure that any sub-processors likewise comply with the data controller's instruction.
If the data processor has not received notification from the data controller within 30 days after the processing of personal data has ceased, the data processor shall send a reminder to the data controller. If the data controller thereafter does not inform the data processor whether all personal data shall be deleted or returned to the data controller, the data processor shall, without further notice, be entitled to delete the personal data.
The data processor is entitled to remuneration for its processing activities up until the time the data controller notifies the data processor whether all personal data shall be deleted or returned to the data controller.