Senbee Data Processing Agreement

Standard Contractual Clauses

pursuant to Article 28(3) of Regulation 2016/679 (the General Data Protection Regulation) for the purpose of the processor's processing of personal data

Between

Name: ____

CVR no.: ____

Address:_______________________________________

hereinafter referred to as "the controller"

and

Name: Senbee A/S
CVR no.: 45638154
Address: Åbogade 15, 8200 Aarhus N

hereinafter referred to as "the processor"

each individually a "party" and together the "parties"

HAVE AGREED on the following standard contractual clauses (the "Clauses") for the purpose of complying with the General Data Protection Regulation and ensuring the protection of privacy and the fundamental rights and freedoms of natural persons.

1.Contents

2.Preamble

1. These Clauses set out the processor's rights and obligations when the processor carries out processing of personal data on behalf of the controller.

2. These Clauses have been drafted for the purpose of the parties' compliance with Article 28(3) of Regulation (EU) 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 (the General Data Protection Regulation).

3. In connection with the provision of Senbee Connect, the processor processes personal data on behalf of the controller in accordance with these Clauses.

4. The Clauses shall take precedence over any corresponding provisions in other agreements between the parties.

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

6. Appendix A contains further information about the processing of personal data, including the purpose and nature of the processing, the type of personal data, the categories of data subjects and the duration of the processing.

7. Appendix B contains the controller's conditions for the processor's use of sub-processors and a list of sub-processors whose use has been approved by the controller.

8. Appendix C contains the controller's instructions regarding the processor's processing of personal data, a description of the security measures that the processor must, as a minimum, implement, and how supervision of the processor and any sub-processors is carried out.

9. The Clauses with the attached appendices shall be retained in writing, including electronically, by both parties.

10. These Clauses do not release the processor from obligations imposed on the processor under the General Data Protection Regulation or any other legislation.

3.The controller's rights and obligations

1. The controller is responsible for ensuring that the processing of personal data is carried out in accordance with the General Data Protection Regulation (see Article 24 of the

Regulation), data protection provisions in other EU law or the national law of the Member States, and these Clauses.

2. The controller has the right and the obligation to make decisions as to the purpose(s) for which, and the means by which, personal data may be processed.

3. The controller is responsible, inter alia, for ensuring that there is a legal basis for the processing of personal data which the processor is instructed to carry out.

4.The processor acts on instructions

1. The processor may only process personal data on documented instructions from the controller, unless required to do so under EU law or the national law of the Member States to which the processor is subject. Such instructions shall be specified in Appendices A and C. Subsequent instructions may also be given by the controller while the processing of personal data is taking place, however, the instructions shall always be documented and retained in writing, including electronically, together with these Clauses.

2. The processor shall immediately notify the controller if, in the processor’s opinion, an instruction is in conflict with this Regulation or data protection provisions in other EU law or the national law of the Member States.

5.Confidentiality

1. The processor may only grant access to personal data processed on behalf of the controller to persons who are subject to the processor’s authority to issue instructions, who have undertaken to observe confidentiality, or who are subject to an appropriate statutory duty of confidentiality, and only to the extent necessary. The list of persons who have been granted access shall be reviewed on an ongoing basis. On the basis of this review, access to personal data may be revoked if access is no longer necessary, and the personal data shall thereafter no longer be available to those persons.

2. Upon request from the controller, the processor must be able to demonstrate that the relevant persons who are subject to the processor’s authority to issue instructions are subject to the above-mentioned duty of confidentiality.

6.Security of processing

1. Article 32 of the General Data Protection Regulation provides that the controller and the processor, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, shall implement

appropriate technical and organisational measures to ensure a level of security appropriate to those risks.

The controller shall assess the risks to the rights and freedoms of natural persons posed by the processing and implement measures to address those risks. Depending on their relevance, this may include:

a. pseudonymisation and encryption of personal data

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

c. the ability to restore the availability of 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 processing.

2. Pursuant to Article 32 of the Regulation, the processor, independently of the controller, shall also assess the risks to the rights of natural persons posed by the processing and implement measures to address those risks. For the purposes of this assessment, the controller shall make the necessary information available to the processor enabling the processor to identify and assess such risks.

3. In addition, the processor shall assist the controller in complying with the controller's obligation under Article 32 of the Regulation by, inter alia, making the necessary information available to the controller regarding the technical and organisational security measures which the processor has already implemented pursuant to Article 32 of the Regulation, and any other information necessary for the controller to comply with its obligation under Article 32 of the Regulation.

4. If addressing the identified risks, in the controller's assessment, requires the implementation of additional measures beyond the measures already implemented by the processor, the controller shall specify the additional measures to be implemented in Appendix C.

7.Use of sub-processors

1. The processor shall meet the conditions referred to in Article 28(2) and (4) of the General Data Protection Regulation in order to use another processor (a sub-processor).

2. The processor may therefore not use a sub-processor for the performance of these Clauses without the controller's prior general written authorisation.

3. The processor has the controller's general authorisation to use sub-processors. The processor shall notify the controller in writing of any planned changes concerning the addition or replacement of sub-processors with at least 30 days' notice, thereby giving the controller the opportunity to object to such changes before the use of the relevant sub-processor(s). A longer notice period in connection with specific processing activities may be stated in Appendix B. The list of sub-processors already approved by the controller appears in Appendix B.

4. Where the processor uses a sub-processor in connection with the performance of specific processing activities on behalf of the controller, the processor shall, by way of a contract or other legal act under EU law or the national law of the Member States, impose on the sub-processor the same data protection obligations as those set out in these Clauses, in particular providing sufficient guarantees that the sub-processor will implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of these Clauses and the General Data Protection Regulation.

   The processor is therefore responsible for ensuring that the sub-processor, at a minimum, complies with the processor's obligations under these Clauses and the General Data Protection Regulation.

5. Sub-processor agreement(s) and any subsequent amendments thereto shall, upon the controller's request, be provided in copy to the controller, thereby enabling the controller to ensure that corresponding data protection obligations as set out in these Clauses have been imposed on the sub-processor. Provisions on commercial terms that do not affect the data protection content of the sub-processor agreement shall not be provided to the controller.

6. If the sub-processor fails to fulfil its data protection obligations, the processor shall remain fully liable towards the controller for the fulfilment of the sub-processor's obligations. This does not affect the rights of data subjects under the General Data Protection Regulation, including in particular Articles 79 and 82 of the Regulation, vis-a-vis the controller and the processor, including the sub-processor.

8.Transfers to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations may only be carried out by the processor on the basis of documented instructions from the controller and shall always take place in accordance with Chapter V of the General Data Protection Regulation.

2. If a transfer of personal data to third countries or international organisations which the processor has not been instructed by the controller to carry out is required under EU law or the national law of the Member States to which the processor is subject, the processor shall notify the controller of that legal requirement before processing, unless the relevant law prohibits such notification on important grounds of public interest.

3. Without documented instructions from the controller, the processor may therefore not, within the framework of these Clauses:

   a. transfer personal data to a controller or processor in a third country or an international organisation

   b. entrust the processing of personal data to a sub-processor in a third country

   c. process the personal data in a third country.

4. The controller's instructions regarding the transfer of personal data to a third country, including any transfer basis under Chapter V of the General Data Protection Regulation on which the transfer is based, shall be set out in Appendix C.6.

5. These Clauses shall not be confused with standard contractual clauses as referred to in Article 46(2)(c) and (d) of the General Data Protection Regulation, and these Clauses cannot constitute a basis for transfers of personal data as referred to in Chapter V of the General Data Protection Regulation.

9.Assistance to the controller

1. Taking into account the nature of the processing, the processor shall, as far as possible, assist the controller by means of appropriate technical and organisational measures with the fulfilment of the controller's obligation to respond to requests for the exercise of the data subjects' rights laid down in Chapter III of the General Data Protection Regulation.

   This entails that the processor shall, as far as possible, assist the controller in ensuring compliance with:

   a. the duty to provide information where personal data are collected from the data subject
   b. the duty to provide information where personal data have not been obtained from the data subject
   c. the right of access
   d. the right to rectification
   e. the right to erasure ("the right to be forgotten")
   f. the right to restriction of processing

g. the duty to notify in connection with 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 processor's obligation to assist the controller pursuant to Clause 6.3, the processor shall furthermore, taking into account the nature of the processing and the information available to the processor, assist the controller with:
    a. the controller's obligation, without undue delay and, where feasible, no later than 72 hours after having become aware of it, to notify a personal data breach to the competent supervisory authority, the supervisory authority competent for the controller (lead supervisory authority), unless it is unlikely that the personal data breach will result in a risk to the rights and freedoms of natural persons

    b. the controller's obligation, without undue delay, to communicate a personal data breach to the data subject when the breach is likely to result in a high risk to the rights and freedoms of natural persons

    c. the controller's obligation, prior to processing, 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 controller's obligation to consult the competent supervisory authority, the supervisory authority competent for the controller (lead supervisory authority), 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 controller to mitigate the risk.

3. The parties shall specify in Appendix C the necessary technical and organisational measures by which the processor shall assist the controller, as well as the scope and extent thereof. This applies to the obligations arising from Clauses 9.1 and 9.2.

10.Notification of a personal data breach

1. The processor shall notify the controller without undue delay after becoming aware that a personal data breach has occurred.

2. The processor's notification to the controller shall, where possible, take place no later than 24 hours after the processor has become aware of the breach, so that the controller can comply with its obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 of the General Data Protection Regulation.

3. In accordance with Clause 9.2(a), the processor shall assist the controller in notifying the breach to the competent supervisory authority. This means that the processor shall assist by providing the information set out below, which, pursuant to Article 33(3), must be included in the controller's notification of the breach to the competent supervisory authority:

    a. the nature of the personal data breach, including, where possible, the categories and approximate number of affected data subjects and the categories and approximate number of affected personal data records

    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 relevant, measures to mitigate its possible adverse effects.

4. The parties shall specify in Appendix C the information which the processor shall provide in connection with its assistance to the controller in the controller's obligation to notify personal data breaches to the competent supervisory authority.

11.Deletion and return of information

1. Upon termination of the services relating to the processing of personal data, the processor shall be obliged to return all personal data and delete existing copies, unless EU law or the national law of the Member States requires the storage of the personal data.

   The processor undertakes to process the personal data solely for the purpose(s), for the period and under the conditions prescribed by such rules.

12.Audit, including inspection

1. The processor shall make available to the controller all information necessary to demonstrate compliance with Article 28 of the General Data Protection Regulation and these Clauses, and shall allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

2. The procedures for the controller's audits, including inspections, of the processor and sub-processors are further specified in Appendices C.7 and C.8.

3. The processor shall be obliged to grant supervisory authorities which, pursuant to applicable legislation, have access to the controller's or the processor's premises, or

representatives acting on behalf of the supervisory authority, access to the processor’s physical premises upon presentation of appropriate identification.

13. The parties’ agreement on other matters

1. The parties may agree on other provisions regarding the service relating to the processing of personal data, e.g. liability, provided that such other provisions do not directly or indirectly conflict with the Clauses or impair the data subject’s fundamental rights and freedoms under the General Data Protection Regulation.

14. Entry into force and termination

1. The Clauses shall enter into force on the date of both parties’ signature hereto.

2. Either party may request that the Clauses be renegotiated if changes in law or impracticalities in the Clauses give rise thereto.

3. The Clauses shall remain in force for as long as the service relating to the processing of personal data continues. During this period, the Clauses cannot be terminated unless other provisions governing the provision of the service relating to the processing of personal data are agreed between the parties.

4. If the provision of the services relating to the processing of personal data ceases, and the personal data have been deleted or returned to the controller in accordance with Clause 11.1 and Appendix C.4, the Clauses may be terminated by either party by written notice.

5. Signatures

   On behalf of the controller

   Name: ____

   Title: ____

   Telephone number: ____

   E-mail: ____

   Signature: ____

On behalf of the processor

Name: Tristan White
Title: CEO
Telephone number: +45 26 81 83 48
E-mail: tw@senbee.com

Signature: ____

15. Contact persons at the controller and the processor

The parties may contact each other through the contact persons set out below.

The parties are obliged to keep each other continuously informed of changes regarding contact persons.

The controller

Name: ____

Title: ____

Telephone number: ____

E-mail: ____

The processor

Name: Tristan White
Title: CEO
Telephone number: +45 26 81 83 48
E-mail: tw@senbee.com

Appendix A, Information about the processing

A.1. The purpose of the processor’s processing of personal data on behalf of the controller

The processor processes personal data for the purpose of providing, operating and maintaining the Senbee platform in accordance with the controller’s instructions, including support for the platform’s functions, administration, user management, support, troubleshooting, security, and logging.

A.2. The processor’s processing of personal data on behalf of the controller primarily concerns (the nature of the processing)

The processing includes recording, structuring, storage, adaptation, retrieval, consultation, disclosure (to authorised users and any sub-processors), alignment or combination, restriction and erasure of personal data in connection with the use of the Senbee platform.

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

Name, e-mail address, telephone number, organisational affiliation (company, department, role), user ID, access and activity log data (e.g. login, actions in the platform), as well as other information that the controller chooses to register or upload in the Senbee platform (e.g. free text fields, notes and attachments), and access- and visit-related information to the extent that the controller uses the platform’s functions for such purposes.

A.4. The processing includes the following categories of data subjects

Users created by the controller in the Senbee platform, including the controller’s employees, administrators and other internal users, as well as external users to whom the controller grants access, e.g. tenants, guests/visitors, supplier contacts and other business partners.

A.5. The processor’s processing of personal data on behalf of the controller may commence after the entry into force of these Clauses. The processing has the following duration

The processing continues for the term of the agreement, i.e. for as long as the processor provides services to the controller. Upon termination of the services, the processing ceases, and the personal data shall thereafter be handled in accordance with Clause 11 on deletion and return.

Appendix B, Sub-processors

B.1. Approved sub-processors

Upon the entry into force of the Clauses, the controller has approved the use of the following sub-processors:

Name	Country	Description of processing
Google Workspace	United States	Operation of office and collaboration tools (e-mail, documents, etc.) for Senbee's internal operations.
UpCloud	Finland	Hosting/operations as part of Senbee's operations.
SMTP2GO	New Zealand	Sending of e-mails (e.g. notifications).
GatewayAPI	Denmark	Sending of SMS (e.g. notifications).
Economic	Denmark	Financial system for internal operations.
Slack	United States	Internal communication as part of Senbee's operations.
Pipedrive	United States	CRM for internal operations.
Featurebase	Estonia	Live chat and feedback functionality in the platform.

Upon the entry into force of the Clauses, the controller has approved the use of the above-mentioned sub-processors for the described processing activity. The processor may not, without the controller's written approval, use a sub-processor for a processing activity other than the one described and agreed, or use another sub-processor for this processing activity.

Appendix C, Instructions regarding the processing of personal data

C.1. The subject matter of the processing / instructions

The processor's processing of personal data on behalf of the controller is carried out by the processor performing the following:

The processor is instructed to process personal data to the extent necessary to provide, operate, maintain and support the Senbee platform in accordance with the agreement, including:

- to host and store data (in the cloud or in the controller's environment in the case of an on-prem delivery)
- to make data available to the controller's authorised users via the platform's functions
- to administer user access and roles in accordance with the controller's instructions
- to carry out logging, monitoring and troubleshooting for operational and security purposes
- to perform backup, restoration and deletion/return upon termination
- to provide technical support and maintenance, including bug fixes and updates

C.2. Security of processing

The level of security shall reflect:

The processing includes ordinary personal data relating to users and contacts as well as user and activity data. The processing may include information which the controller enters or uploads into the platform. As a general rule, the platform is not intended for the processing of special categories of personal data or data relating to criminal convictions and offences. The level of security is determined on the basis of the nature, scope, context and purposes of the processing as well as risks of varying likelihood and severity to the rights and freedoms of data subjects, and is assessed as an appropriately high level of security for a professional B2B SaaS solution.

The processor is thereafter entitled and obliged to make decisions on which technical and organisational security measures shall be implemented in order to establish the necessary (and agreed) level of security.

However, in all circumstances and at a minimum, the processor shall implement the following measures agreed with the controller:

Requirements for pseudonymisation and encryption
Personal data are encrypted during transmission (TLS or equivalent). Personal data are encrypted at rest in relevant systems where this is technically feasible and appropriate based on

risk. Security information such as passwords is stored as a one-way hash. Pseudonymisation is used where relevant to reduce risk in connection with logging and troubleshooting.

Ongoing confidentiality, integrity, availability and resilience
Access to personal data is restricted on a need-to-know basis and according to the principle of least privilege, including role-based access control. Administrative access is protected with strong authentication. Changes to systems and configurations are managed and documented. Security updates and vulnerabilities are handled according to established processes. Organisational measures are implemented, including security policies, training and vendor management.

Timely restoration in the event of a physical or technical incident
Backups are performed and procedures are established for restoring data and systems. Backup and restore are tested regularly. In the case of an on-prem delivery, backup and restoration responsibilities are set out in the contractual basis, and the processor provides assistance as needed.

Regular testing, assessment and evaluation
Ongoing risk assessments and security reviews of relevant controls are carried out. The effectiveness of technical and organisational measures is assessed regularly, including through internal controls, vendor assessments, and testing of backup/restore and relevant security measures.

Access via the internet
Access to the platform is provided via secure connections (HTTPS/TLS). Session management and protection against unauthorised access are implemented, including rate limiting where relevant. The controller is responsible for proper access management of its own users.

Protection during transmission
Data are transmitted encrypted using TLS or equivalent. Integration calls and API access are secured with appropriate authentication mechanisms (e.g. tokens or keys) and restricted as necessary.

Protection during storage
Data are stored in systems with access control, logging and appropriate protection against unauthorised access. Encryption at rest is used where relevant. Backups are stored securely and access is restricted.

Physical security of locations
For cloud delivery, physical security is ensured through the data centre provider’s controls. For on-prem delivery, the controller is responsible for the physical security of the infrastructure where the processing takes place, unless otherwise agreed.

Home and remote workplaces

The processor’s personnel may work remotely under controlled conditions, including requirements for screen lock, up-to-date devices, device encryption where relevant, secure network access and compliance with internal remote work policies.

Logging
Logging is performed of relevant security and operational events, including authentication, administrative actions and material changes. Access to logs is restricted, and logs are protected against unauthorised alteration. Log retention and access are assessed on a risk basis.

C.3 Assistance to the controller

The processor shall, as far as possible, within the scope and extent set out below, assist the controller in accordance with Clauses 9.1 and 9.2 by implementing the following technical and organisational measures:

The processor assists the controller in fulfilling its obligations under the data protection rules to the extent that it concerns the processor’s processing and taking into account the nature of the processing and the information available to the processor. Assistance is, as a general rule, provided through the platform’s standard functionality and standard documentation. Assistance requiring significant additional resources, development or separate investigations may be provided subject to a separate agreement and remuneration.

The processor implements the following measures to assist the controller:

- makes relevant information about the processing and the security measures available, including information on sub-processors used
- supports the handling of data subjects’ rights by enabling search, extraction/export, rectification and erasure to the extent supported by the platform’s functions
- assists in the event of security incidents by notifying and providing available information about the incident, affected data and implemented remedial measures
- assists with DPIAs and any prior consultation by making available relevant information about the processing and the technical and organisational measures, to the extent it concerns the processor’s delivery

C.4 Retention period / deletion procedure

Personal data are stored in the production environment for the term of the agreement and for as long as the controller has an active account and uses the services. Upon termination of the service relating to the processing of personal data, the processor shall, upon request, return the personal data in a commonly used, machine-readable format and shall thereafter delete the personal data in accordance with Clause 11.1.

Backups may contain personal data for a limited period after deletion/termination as part of the processor’s normal backup rotation for up to 30 days, after which they are deleted or overwritten. Personal data in backups are not actively made available unless necessary for restoration.

In the case of an on-prem delivery, personal data are stored and deleted in the controller's environment in accordance with the controller's instructions and configuration, and the processor provides assistance with export and deletion as needed.

C.5 Location of processing

Processing of the personal data covered by the Clauses may not, without the controller's prior written approval, take place at locations other than the following:

Processing may take place at the following locations:

1. Cloud delivery: In the processor's hosting environment in the EU (primarily Germany) used by the processor and/or the sub-processors listed in Appendix B (e.g. hosting and operations provider).
2. On-prem delivery: In the controller's own locations and/or hosting environment made available by the controller, where the processor's access may take place remotely in accordance with the controller's instructions.
3. Support and operations: At the processor (Senbee A/S) and relevant sub-processors listed in Appendix B, to the extent necessary for support, troubleshooting, security and maintenance.

C.6 Instructions regarding transfers of personal data to third countries

The processor may only transfer personal data to third countries or international organisations to the extent necessary for the provision of the services, and only where (i) the transfer takes place in accordance with the controller's documented instructions and (ii) a valid transfer mechanism pursuant to Chapter V of the General Data Protection Regulation exists.

Transfers may take place to the third countries where the processor's sub-processors or their processing locations are established, cf. Appendix B and the processor's at all times updated list of sub-processors.

The transfer mechanism is, depending on the specific sub-processor and processing location:

a) the European Commission's adequacy decision (GDPR Article 45), where relevant, or
b) the European Commission's Standard Contractual Clauses (SCC) (GDPR Article 46(2)(c)), supplemented by relevant technical and organisational measures based on a risk assessment, or
c) for transfers to the United States: the EU–US Data Privacy Framework (GDPR Article 45), where the recipient is certified thereunder, otherwise SCC pursuant to point (b).

In the case of an on-prem delivery, as a general rule no third-country transfers take place from the controller's environment, unless the controller itself configures or instructs integrations or sub-processors that result in such a transfer.

If the controller does not, in these Clauses or subsequently, provide documented instructions regarding transfers of personal data to a third country, the processor is not authorised to carry out such transfers within the framework of these Clauses.

C.7 Procedures for the controller's audits, including inspections, of the processing of personal data entrusted to the processor

The processor shall once annually, at its own expense, obtain an audit report or statement from an independent third party regarding the processor's compliance with the General Data Protection Regulation, data protection provisions in other EU law or the national law of the Member States, and these Clauses.

The parties agree that the following types of audit report or statement may be used in accordance with these Clauses: an ISO 27001 certificate, an ISAE 3000/3402 statement, a SOC 2 Type II report, or an equivalent independent third-party audit/inspection report covering relevant technical and organisational measures.

Audit reports or statements shall be forwarded to the controller without undue delay for information. The controller may challenge the scope and/or method of the audit report or statement and may, in such cases, request a new audit report or inspection report under different scope and/or using a different method.

Based on the results of the audit report or statement, the controller is entitled to request the implementation of additional measures in order to ensure compliance with the General Data Protection Regulation, data protection provisions in other EU law or the national law of the Member States, and these Clauses.

In addition, the controller or a representative of the controller has access to carry out inspections, including physical inspections, of the locations from which the processor carries out processing of personal data, including physical locations and systems used for or in connection with the processing. Such inspections may be carried out when the controller finds it necessary.

Any costs incurred by the controller in connection with a physical inspection shall be borne by the controller itself. However, the processor is obliged to allocate the resources (primarily time) necessary for the controller to carry out its inspection.

C.8 Procedures for audits, including inspections, of the processing of personal data entrusted to sub-processors

As a general rule, the processor obtains and reviews the sub-processors' independent third-party audit reports and/or certifications. Relevant documentation shall be made available to the controller upon request. Physical inspections at sub-processors shall be carried out only to the extent possible under the sub-processor's terms.

The processor shall once annually, at the sub-processor's expense, obtain an audit report or statement from an independent third party regarding the sub-processor's compliance with the General Data Protection Regulation, data protection provisions in other EU law or the national law of the Member States, and these Clauses.

The parties agree that the following types of audit reports or statements may be used in accordance with these Clauses: SOC 2 Type II, ISAE 3000/3402, ISO 27001 certification, or an equivalent independent third-party audit/inspection report.

The audit report or statement shall be forwarded to the controller without undue delay for information. The controller may challenge the scope and/or method of the audit report or statement and may, in such cases, request a new audit report or inspection report under different scope and/or using a different method.

Based on the results of the audit report or statement, the controller is entitled to request the implementation of additional measures in order to ensure compliance with the General Data Protection Regulation, data protection provisions in other EU law or the national law of the Member States, and these Clauses.

In addition, the processor or a representative of the processor has access to carry out inspections, including physical inspections, of the locations from which the sub-processor carries out processing of personal data, including physical locations and systems used for or in connection with the processing. Such inspections may be carried out when the processor (or the controller) finds it necessary.

Documentation for such inspections shall be forwarded to the controller without undue delay for information. The controller may challenge the scope and/or method of the inspection and may, in such cases, request that a new inspection be carried out under different scope and/or using a different method.