

Data Processing Agreement

Kanda ApS

Åbogade 13, 3., 8200 Aarhus N, Denmark

Version 2

Version History

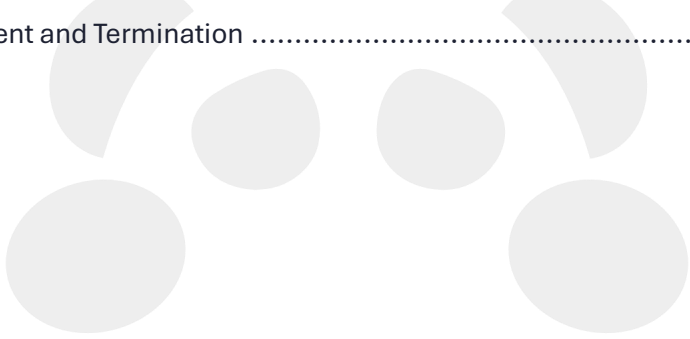
This document is reviewed to ensure its continuing relevance to the systems and process that it describes, and a record of contextual additions or omissions is given below:

Version	Date	Context
1	24/May/2018	<ul style="list-style-type: none">• Document creation
2	18/Mar/2026	<ul style="list-style-type: none">• Updated Appendix B: Specification of Processing<ul style="list-style-type: none">○ Scaleway SAS○ Sinch Mailgun & Mailjet



Table of Content

1. Preamble	4
2. The Rights and Obligations of the Data Controller	4
3. The Data Processor Acts According to Instructions	5
4. Confidentiality.....	5
5. Security of Processing.....	5
6. Use of Sub-Processors	6
7. Transfer of Data to Third Countries or International Organisations	7
8. Assistance to the Data Controller	7
9. Notification of Personal Data Breach	7
10. Erasure and Return of Data	8
11. Audit and Inspection	8
12. Commencement and Termination	8



1. Preamble

- 1.1 As part of the commencement of an agreement on providing the following services: Development and hosting of both Kanda-developed training courses as well as custom courses developed for the Customer. (hereinafter referred to as the ‘Main Agreement’), the Parties hereby enter into this data processing agreement (hereinafter referred to as the ‘Data Processing Agreement’). 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.
- 1.2 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).
- 1.3 The Data Processor’s delivery of the services under the Main Agreement means that the Data Processor will process the Personal Data pertaining to the registrants on behalf of the Data Controller.
- 1.4 The Clauses shall take priority over any similar provisions contained in other agreements between the parties.
- 1.5 The Clauses includes these Appendices, which apply in the following order:
- a. Information about the processing
 - b. Processing Specification Form
 - c. Instruction pertaining to the use of personal data

2. The Rights and Obligations of the Data Controller

- 2.1 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 State¹ data protection provisions and the Clauses.
- 2.2 The data controller has the right and obligation to make decisions about the purposes and means of processing personal data.
- 2.3 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.

¹ References to “Member States” made throughout the Clauses shall be understood as references to “EEA Member States”.

3. The Data Processor Acts According to Instructions

- 3.1 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 the Clauses and specifically Appendix B. 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.
- 3.2 The Data Processor shall not be under obligation to comply with a request from the Data Controller according to this clause if the request contravenes personal data legislation. The Data Processor shall inform the Data Controller if this sub-clause should become relevant.

4. Confidentiality

- 4.1 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.
- 4.2 The data processor shall at the reasonable request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

5. Security of Processing

- 5.1 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.
- 5.2 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.
- 5.3 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.

- a. 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.

6. Use of Sub-Processors

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

6.2 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.

- a. 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 15 calendar 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).

6.3 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.

- a. 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.

6.4 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.

6.5 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.

6.6 If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

7. Transfer of Data to Third Countries or International Organisations

- 7.1 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.
- 7.2 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.
- 7.3 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
- 7.4 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.
- 7.5 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.

8. Assistance to the Data Controller

- 8.1 The data processor shall, against reasonable remuneration, as required and to a reasonable extent assist in the data controller's fulfilment of its obligations in the processing of the Personal Data under the Clauses, including by:
- a. responding to registrants in their exercise of their rights
 - b. impact analyses
 - c. preliminary regulatory authority hearings

9. Notification of Personal Data Breach

- 9.1 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.
- 9.2 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.

9.3 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.

10. Erasure and Return of Data

10.1 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 so unless Union or Member State law requires storage of the personal data.

10.2 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.

11. Audit and Inspection

11.1 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.

11.2 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.

11.3 The Data Processor shall be entitled to reasonable time and material payment for assistance under sub-clause 12.

12. Commencement and Termination

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

- 12.2 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.
- 12.3 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.
- 12.4 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.3., the Clauses may be terminated by written notice by either party.



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 of the processing is disclosing of personal data to the data processor in connection with data controllers users or employees use of the services in order for the data processor to execute necessary tasks connected to the services.

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):

The data Processor makes available IT-services to the data controller and hereby processes personal data about the data controller’s employees or users on the Data Processors servers.

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

“Name, e-mail address, employer, IP Address, test scores and other relevant statistics related to training and use of the services, attendance at online training and registration for specific training modules.”

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

Data Controllers employees and users using the services.

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:

Processing shall not be time-limited and shall be performed until this Data Processing Agreement is terminated or cancelled by one of the Parties.

Appendix B: Specification of Processing

The Parties have entered into the following agreement:

Data processor	Microsoft Corporation		
Services	We run our backend services on Microsoft Azure. Access to customer data by Microsoft operations and support personnel is denied by default.		
Approved subcontracted data processors	The Services include the following subcontracted data processors: <ul style="list-style-type: none"> • None 		
Geographical location(s) for the processing	Personal data will be processed in the following countries/locations:		
	<input checked="" type="checkbox"/> EU or EEA territories	<input type="checkbox"/> Other [Specify]	
Categories of registrants	Registrant categories include the following:		
	<input checked="" type="checkbox"/> Employees	<input type="checkbox"/> Customers and/or clients	
	<input type="checkbox"/> Suppliers	<input type="checkbox"/> Others	
Categories of personal data	Personal data to be processed include:		
	<input checked="" type="checkbox"/> Customer data e.g. name, title, address, telephone number, e-mail address, date of birth, sex, customer number, order number, service history and details.		
	<input type="checkbox"/> Commercial customers, partners and supplier details e.g. name, title, address, telephone number, e-mail address, date of birth, sex, service history and details.		
	<input type="checkbox"/> Financial data e.g. income, salary, assets, payments, purchases, loans, bank account, card number, credit ratings, insurance and pension details.		
	<input type="checkbox"/> Employment details e.g. name, address, telephone number, e-mail address, date of birth, sex, CPR number, job market history, appointment and dismissal details, employee history and courses.		
	<input type="checkbox"/> Other [Specify]		
	Special categories of personal data		
	<input type="checkbox"/> Race or ethnicity	<input type="checkbox"/> Political beliefs	<input type="checkbox"/> Religious or philosophical orientation
	<input type="checkbox"/> Trade union	<input type="checkbox"/> Genetic or biometric data	<input type="checkbox"/> Health information
	<input type="checkbox"/> Sexual orientation	<input type="checkbox"/> Criminal convictions	

Data processor	Exit Games GmbH		
Services	During multiplayer sessions, a user's name is shared with other participants using Exit Games' Photon Cloud services. The names of players are anonymized using encryption before being shared to the Photon Cloud servers. The IP address of the end user device is shared with Photon Cloud in order to enable IP routing.		
Approved subcontracted data processors	The Services include the following subcontracted data processors: <ul style="list-style-type: none"> • https://dashboard.photonengine.com/account/dpa 		
Geographical location(s) for the processing	Personal data will be processed in the following countries/locations:		
	<input checked="" type="checkbox"/> EU or EEA territories	<input type="checkbox"/> Other [Specify]	
Categories of registrants	Registrant categories include the following:		
	<input checked="" type="checkbox"/> Employees	<input type="checkbox"/> Customers and/or clients	
	<input type="checkbox"/> Suppliers	<input type="checkbox"/> Others	
Categories of personal data	Personal data to be processed include:		
	<input checked="" type="checkbox"/> Customer data e.g. name, title, address, telephone number, e-mail address, date of birth, sex, customer number, order number, service history and details.		
	<input type="checkbox"/> Commercial customers, partners and supplier details e.g. name, title, address, telephone number, e-mail address, date of birth, sex, service history and details.		
	<input type="checkbox"/> Financial data e.g. income, salary, assets, payments, purchases, loans, bank account, card number, credit ratings, insurance and pension details.		
	<input type="checkbox"/> Employment details e.g. name, address, telephone number, e-mail address, date of birth, sex, CPR number, job market history, appointment and dismissal details, employee history and courses.		
	<input checked="" type="checkbox"/> Other IP Address		
	Special categories of personal data		
	<input type="checkbox"/> Race or ethnicity	<input type="checkbox"/> Political beliefs	<input type="checkbox"/> Religious or philosophical orientation
	<input type="checkbox"/> Trade union	<input type="checkbox"/> Genetic or biometric data	<input type="checkbox"/> Health information
	<input type="checkbox"/> Sexual orientation	<input type="checkbox"/> Criminal convictions	

Data processor	Scaleway SAS		
Services	During multiplayer sessions, a user's name is shared with other participants using Scaleway services. The names of players are anonymized using encryption before being shared. The IP address of the end user device is shared with Scaleway in order to enable IP routing.		
Approved subcontracted data processors	The Services include the following subcontracted data processors: <ul style="list-style-type: none"> • https://www.scaleway.com/en/subprocessorlist/ 		
Geographical location(s) for the processing	Personal data will be processed in the following countries/locations:		
	<input checked="" type="checkbox"/> EU or EEA territories	<input type="checkbox"/> Other [Specify]	
Categories of registrants	Registrant categories include the following:		
	<input checked="" type="checkbox"/> Employees	<input type="checkbox"/> Customers and/or clients	
	<input type="checkbox"/> Suppliers	<input type="checkbox"/> Others	
Categories of personal data	Personal data to be processed include:		
	<input checked="" type="checkbox"/> Customer data e.g. name, title, address, telephone number, e-mail address, date of birth, sex, customer number, order number, service history and details.		
	<input type="checkbox"/> Commercial customers, partners and supplier details e.g. name, title, address, telephone number, e-mail address, date of birth, sex, service history and details.		
	<input type="checkbox"/> Financial data e.g. income, salary, assets, payments, purchases, loans, bank account, card number, credit ratings, insurance and pension details.		
	<input type="checkbox"/> Employment details e.g. name, address, telephone number, e-mail address, date of birth, sex, CPR number, job market history, appointment and dismissal details, employee history and courses.		
	<input checked="" type="checkbox"/> Other IP Address		
	Special categories of personal data		
	<input type="checkbox"/> Race or ethnicity	<input type="checkbox"/> Political beliefs	<input type="checkbox"/> Religious or philosophical orientation
	<input type="checkbox"/> Trade union	<input type="checkbox"/> Genetic or biometric data	<input type="checkbox"/> Health information
	<input type="checkbox"/> Sexual orientation	<input type="checkbox"/> Criminal convictions	

Data processor	Auth0 Inc.		
Services	Auth0 facilitates single sign-on for the application and stores basic profile data for users logging in such as name, email address and IP address.		
Approved subcontracted data processors	The Services include the following subcontracted data processors: <ul style="list-style-type: none"> • https://www.okta.com/legal/trustandcompliance/subprocessors/ 		
Geographical location(s) for the processing	Personal data will be processed in the following countries/locations:		
	<input checked="" type="checkbox"/> EU or EEA territories	<input type="checkbox"/> Other [Specify]	
Categories of registrants	Registrant categories include the following:		
	<input checked="" type="checkbox"/> Employees	<input type="checkbox"/> Customers and/or clients	
	<input type="checkbox"/> Suppliers	<input type="checkbox"/> Others	
Categories of personal data	Personal data to be processed include:		
	<input checked="" type="checkbox"/> Customer data e.g. name, title, address, telephone number, e-mail address, date of birth, sex, customer number, order number, service history and details.		
	<input type="checkbox"/> Commercial customers, partners and supplier details e.g. name, title, address, telephone number, e-mail address, date of birth, sex, service history and details.		
	<input type="checkbox"/> Financial data e.g. income, salary, assets, payments, purchases, loans, bank account, card number, credit ratings, insurance and pension details.		
	<input type="checkbox"/> Employment details e.g. name, address, telephone number, e-mail address, date of birth, sex, CPR number, job market history, appointment and dismissal details, employee history and courses.		
	<input type="checkbox"/> Other [Specify]		
	Special categories of personal data		
	<input type="checkbox"/> Race or ethnicity	<input type="checkbox"/> Political beliefs	<input type="checkbox"/> Religious or philosophical orientation
	<input type="checkbox"/> Trade union	<input type="checkbox"/> Genetic or biometric data	<input type="checkbox"/> Health information
	<input type="checkbox"/> Sexual orientation	<input type="checkbox"/> Criminal convictions	

Data processor	Sinch Mailgun + Mailjet
-----------------------	-------------------------

Services	We use Mailgun and Mailjet to send automated emails to VTP users. Recipient email addresses are temporary stored on Sinch infrastructure.
Approved subcontracted data processors	The Services include the following subcontracted data processors: <ul style="list-style-type: none"> • https://sinch.com/legal/data-protection-agreement-sub-processors/
Geographical location(s) for the processing	Personal data will be processed in the following countries/locations:
	<input checked="" type="checkbox"/> EU or EEA territories <input type="checkbox"/> Other [Specify]
Categories of registrants	Registrant categories include the following:
	<input checked="" type="checkbox"/> Employees <input type="checkbox"/> Customers and/or clients
	<input type="checkbox"/> Suppliers <input type="checkbox"/> Others
Categories of personal data	Personal data to be processed include:
	<input checked="" type="checkbox"/> Customer data e.g. name, title, address, telephone number, e-mail address, date of birth, sex, customer number, order number, service history and details.
	<input type="checkbox"/> Commercial customers, partners and supplier details e.g. name, title, address, telephone number, e-mail address, date of birth, sex, service history and details.
	<input type="checkbox"/> Financial data e.g. income, salary, assets, payments, purchases, loans, bank account, card number, credit ratings, insurance and pension details.
	<input type="checkbox"/> Employment details e.g. name, address, telephone number, e-mail address, date of birth, sex, CPR number, job market history, appointment and dismissal details, employee history and courses.
	<input type="checkbox"/> Other [Specify]
	Special categories of personal data
	<input type="checkbox"/> Race or ethnicity <input type="checkbox"/> Political beliefs <input type="checkbox"/> Religious or philosophical orientation
	<input type="checkbox"/> Trade union <input type="checkbox"/> Genetic or biometric data <input type="checkbox"/> Health information
	<input type="checkbox"/> Sexual orientation <input type="checkbox"/> Criminal convictions

Appendix C: Instructions pertaining to the use of Personal Data

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

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

The Data Processor shall use the disclosed personal data in order to deliver its services and making the services available for the employees or users of data controller.

C.2. Security of processing

The level of security shall take into account:

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

The Data Processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

The following technical and organizational security measures have been applied by the Data Processor:

- Access: All access to software, file systems and network is via log-in with username and password. Access to data is limited to relevant areas for each individual employee. In case of critical transactions authorization and authentication with certificates or similar can be applied.
- Data storage: Data is stored on central servers. Server rooms are physically protected with access control. Furthermore, security measures and precautions against incidents such as fire, smoke, water, power outages and theft have been installed and/or implemented in the server rooms. Networks are physically protected and separated from other data traffic.
- Back-up: Data back-up is completed daily, so that data can be recreated at any time so that no more than one day's of data can be lost. Back-up data is stored with copies on two internal and on one external location.
- Antivirus: Protection against viruses in files and e-mails is applied continuously.
- Education and IT awareness: For relevant employees IT awareness courses are conducted annually. Furthermore, the Data Processor has implemented guidelines when handling personal data.

C.3. Storage period/erasure procedures

Personal data is stored for 6 months after the termination of the Main Agreement after which the personal data is automatically erased by the data processor.

C.4. 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 once yearly, at the written request of data controller and at its expense obtain 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 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.

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 the data controller's representative shall in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the data processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the data controller deems it required."

C.5. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

The data processor shall once yearly, at the written request of data controller and at its expense obtain an inspection report from an independent third party concerning the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The 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.

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.