Compliance Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

DATA PROCESSING AGREEMENT – EFFORTLESS COMPLIANCE SOLUTION & SERVICE

Version 2.0, 23-04-2024

In accordance with Article 28(3) in the General Data Protection Regulation (GDPR)[1], this Data Processing Agreement is entered into between the Parties:

The Customer (Data Controller)

and

Compliance Partners ApS (Data Processor)
Reg. No. 43615661
Kultorvet 11, 4th.,
1175 Copenhagen C,
Denmark

The Parties HAVE AGREED on the following Standard Contractual Clauses ('the Clauses') to meet the requirements of the GDPR and to ensure the protection of the rights of the data subjects.

[1] Regulation (EU) 2016/679 of the European Parliament and the Council of 27-04-2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

Compliance Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

1. SECTION I

Clause 1

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 GDPR Article 28(3).

(3) In the context of the provision of the Effortless Compliance Solution ('the Solution') and Service ('the Service'), 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, categories of data subjects and categories of personal data and the duration of the processing.

(7) Appendix B contains a list of sub-processors authorized by the Data Controller.

(8) Appendix C contains the Data Controller's instructions with regard to the processing of personal data, the minimum security measures to be implemented by the Data Processor, and how audits of the Data Processor are to be performed.

(9) The Clauses along with appendices shall be retained in writing, including electronically, by both Parties.

(10) The Clauses shall not exempt the Data Processor from obligations to which the Data Processor is subject pursuant to the GDPR or other legislation.

Compliance Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

2. SECTION II

Clause 2
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 GDPR Article 24), the applicable EU or Member State[2] data protection provisions, and the Clauses.

(2) The Data Controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

(3) The Data Controller shall be responsible, i.e., for ensuring that the processing of personal data, which the Data Processor is instructed to perform, has a legal basis.

Clause 3
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 EU 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.

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

Compliance Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

Clause 4
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.

Clause 5
Security of Processing

(1) GDPR Article 32 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 organizational 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;

Compliance Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

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

(2) According to GDPR Article 32, 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 GDPR Article 32, i.e., providing the Data Controller with information concerning the technical and organizational measures already implemented by the Data Processor pursuant to GDPR Article 32 along with all other information necessary for the Data Controller to comply with the Data Controller's obligation under GDPR Article 32.
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 GDPR Article 32, the Data Controller shall specify these additional measures to be implemented in Appendix C.

Clause 6
The Use of Sub-Processors

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

(2) The Data Processor shall therefore not engage another processor (sub-processor) for the fulfillment of the Clauses without the prior general written authorization of the Data Controller.

(3) The Data Processor has the Data Controller's general authorization 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 14 (fourteen) 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). The list of sub-processors already authorized 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 organizational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

(5) 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) 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.

(7) The Data Processor shall agree to a third-party beneficiary clause with the sub-processor whereby – in the event the processor has factually disappeared, ceased to exist in law, or has become insolvent – the Data Controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

(8) If the sub-processor does not fulfill his data protection obligations, the Data Processor shall remain fully liable to the Data Controller as regards the fulfillment 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 GDPR Articles 79 and 82 – against the Data Controller and the Data Processor, including the sub-processor.

Compliance Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

Clause 8

Transfer of Data to Third Countries or International Organizations

(1) Any transfer of personal data to third countries or international organizations 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 GDPR Chapter V.

(2) In case transfers to third countries or international organizations, which the Data Processor has not been instructed to perform by the Data Controller, are 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 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 GDPR Chapter V on which they are based, shall be set out in Appendix C.

(5) The Clauses shall not be confused with standard data protection clauses within the meaning of GDPR Article 46(2)(c) and (d), and the Clauses cannot be relied upon by the Parties as a transfer tool under GDPR Chapter V.

Clause 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 organizational 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 GDPR Chapter III.

(2) 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.

(3) In addition to the Data Processor's obligation to assist the Data Controller, 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 Supervisory Authority, 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);

Compliance Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

(d) the Data Controller's obligation to consult the competent supervisory authority, The Danish Data 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 Data Controller to mitigate the risk.

(4) The Parties shall define in Appendix C the appropriate technical and organizational 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 Section II, Clause 9.1 and 9.2.

Clause 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 48 (forty-eight) hours after the Data Processor has become aware of the personal data breach to enable the Data Controller to comply with the Data Controller's obligation to notify the personal data breach to the competent supervisory authority, cf. the GDPR Article 33.

(3) In accordance with Section II, 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 the GDPR Article 33(3), shall be stated in the Data Controller's notification to the competent supervisory authority:

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

(b) the likely consequences of the personal data breach;

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

(4) The Parties shall define in Appendix C all the elements to be provided by the Data Processor when assisting the Data Controller in the notification of a personal data breach to the competent supervisory authority.

3. SECTION III – FINAL PROVISIONS

Clause 11
Deletion 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 so unless EU or Member State law requires the storage of the personal data.

Clause 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 GDPR 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.

(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

Compliance Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

Processor's physical facilities on presentation of appropriate identification.

Clause 13
The Parties' Agreements on Other Terms

(1) The Parties may agree on 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.

Clause 14
Commencement and Termination

(1) The Clauses shall become effective on the date of the Parties' signature of the Contract. The Contract may be signed electronically.

(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 Section III, Clause 11.1. and Appendix C, the Clauses may be terminated by written notice by either of the Parties.

Compliance Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

APPENDIX A – INFORMATION ABOUT THE PROCESSING

A.1 Purpose(s) for Which Personal Data is Processed

The Data Processor's processing of personal data on behalf of the Data Controller is processed with the purpose of providing the Solution and the Service. With the Solution and the Service, the Data Controller is, in general, helped with the tasks and documentation that are required under the GDPR.

A.2 Nature of the Processing

The Data Processor's processing of personal data on behalf of the Data Controller shall mainly pertain to reviewing and assessing the Data Controller's GDPR-related activities, for example, documentation required under the GDPR, as the record of processing activities (RoPA) and data processing agreements (DPAs), and performing data mapping, including the storage of documents related to above-mentioned activities. In addition, the Data Processor shall at the Data Controller's request perform a scan of relevant files, with the purpose of conducting a risk assessment.

A.3 Categories of Data Subjects

Processing concerns the following data subjects:

- the Data Controller's manager(s) and employees;
- the Data Controller's suppliers, including for example accountants, website hosters, and marketing providers;
- the Data Controller's data processors and sub-processors;
- persons who are subject to processing by the Data Controller itself ('data subjects'), such as for example, customers, applicants, and website visitors;
- the Data Processor's employees in the Effortless Compliance Team.

Compliance Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

A.4 Categories of Personal Data Processed

The categories of personal data collected depend on the content of the provided materials and files, in the event that the Data Controller has wished a scan. The following categories of personal data are assumptions as to what can be subject to processing:

General Personal Data

Profile Data
- First and Last name
- Address
- Tel. No.
- E-mail Address
- Birth Date.

Private Data
- Housing
- Cars
- Children
- Social Relationships
- Social Problems.

Technical Data
- Technical Preferences,
- Logins
- Identification No.
- Usernames
- Social Media Accounts
- Pictures
- Languages.

Employment Data
- Employment
- Absence
- Education
- Examinations.

Financial Data
- Economy
- Tax
- Wage
- Bank information.

Special Categories of Personal Data
- Racial Origin
- Ethnic Origin
- Political Opinions
- Religious Beliefs
- Philosophical Beliefs
- Trade Union Membership
- Genetics
- Biometrics
- Health
- Sex Life
- Sexual Orientation.

Other Categories of Personal Data
- Criminal Offences
- Civil Reg. No., including CPR. No.

A.5 Duration of the Processing

The Data Processor's processing of personal data on behalf of the Data Controller may be performed when the Clauses commence. Data processing under these

Compliance Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

Clauses can take place as long as the Data Processor processes and stores personal data received from or collected on behalf of the Data Controller, until the Data Controller or Processor terminates or cancels the Contract, and deletes the personal data in accordance with Section III, Clause 11(1).

APPENDIX B – LIST OF SUB-PROCESSORS

B.1 Approved Sub-Processors

On commencement of the Clauses, the Data Controller authorizes the engagement of the following sub-processors:

* Updated as of 22-04-2024

Name	Microsoft Ireland Operations Ltd.
Reg. No.	Reg. No. 256796
Address	Carmenhall and Leopardstown, D18 Dublin, Ireland
Description of the Processing	Microsoft Azure for Hosting Cloud Servers

The Data Controller shall on the commencement of the Clauses authorize the use of the abovementioned sub-processors for the processing described for that party. The Data Processor shall not be entitled – without the Data Controller's explicit written authorization – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or has another sub-processor perform the described processing.

Compliance Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

APPENDIX C – INSTRUCTION PERTAINING TO THE USE OF PERSONAL DATA

C.1 The Subject of/Instruction of 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 activities, depending on the Data Controller's wishes:

(1) During the initial onboarding sessions relevant information and material are provided to the Data Processor for review and assessment. On the basis of that information, and maybe the optional scanning session, the Data Processor shall conduct an assessment of the risk level. The Data Processor shall, in accordance with the Contract, provide access to the Solution and assist in data mapping and the setup of the RoPA, as well as other documentation that might be required.

(2) The Data Processor shall assist in the management of requests about the data subjects' rights and data breaches.

(3) On an ongoing basis, as determined in the Service Level Agreement ('SLA'), the Data Processor shall review and maintain the Data Controller's documentation.

(4) The Data Processor and their sub-processors are authorized to process personal data for the purpose of operating and supporting the end-user's use of the product, as well as for development, subscription management, and ensuring security, which is necessary for the delivery of a stable and secure product that complies with applicable legal requirements set out in the Contract and the GDPR.

C.2 Security of the Processing

(1) The level of security shall take into account:
   (a) that a large amount of personal data POTENTIALLY can be subject to processing;
   (b) that, if the scanning session is chosen, a large amount of special and other categories of personal data POTENTIALLY can be subject to

processing, and such data can have a high impact on the rights and freedoms of natural persons;

(c) but it is EXPECTED that most processing activities will involve no personal data or mostly general personal data, which is why a 'medium' level of security must be established.

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

(3) The Data Processor shall however – in any event and at a minimum – implement the following measures. The Data Processor undertakes to ensure the following technical measures:

(a) that personal data stored in the Data Processor's files is stored and transferred in an encrypted state, with encryption-at-rest and encryption-at-transit;

(b) that personal data stored in the Solution is segregated, so that the personal data and information contained in the Solution cannot be accessed by unauthorized persons;

(c) that access to the Solution is controlled, and subject to access control;

(d) that necessary security measures are in place to prevent and limit the execution of malware or similar code, including through ongoing updating of software, hardware and communication systems, and code validation;

(e) that the Data Controller can see if the content of the Solution has been changed, and in that case, by whom;

(f) that the end-users who have used the Solution have the opportunity to correct or add information to the platform themselves;

(g) that the Data Controller can extract the necessary data from the solution if the Data Controller wishes to stop using the Solution. Data can be extracted in a machine-readable format by the Data Controller themselves so that the Data Controller's and Processor's access to special categories of personal data or confidential information is minimized.

Compliance Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

The Data Processor undertakes to ensure the following organizational measures:

(a) that encrypted personal data and the encryption keys are stored separately;

(b) that the personal data can be recovered following technical or physical incidents, and to have procedures in place in the form of disaster recovery and business continuity plans to ensure continued operations;

(c) that personal data in the Solution and regarding the Data Controller is limited to what is absolutely necessary, and that, to the extent possible, the Data Processor and sub-processors are limited to process pseudonymized personal data and do not possess, or are unable to access without the Data Controller's permission or knowledge, personal data;

(d) that third parties who gain legitimate access to the Solution can only get access to encrypted data, that activities that involve access to special and other categories of personal data are logged, and that third parties are subject to a non-disclosure clause;

(e) to have procedures in place to detect and handle data breaches, so that the Data Controller can inform the data subjects without undue delay;

(f) that, upon discovery of a data breach, the necessary information is registered for the purpose of case analysis and for possible follow-up investigations requested by the Data Controller;

(g) procedures for the correct and secure processing of physical material taken from the Solution for legal purposes, including storage, distribution, and data extracted from home offices, and ensure that the Data Processor's employees are instructed in the correct processing of personal data, have received security training, are subject to non-disclosure clauses and similar or equivalent organizational measures.

C.3 Storage Period/Erasure Procedures

Personal data is stored for the duration of the Contract with an addition of 3 (three) years after which the personal data is automatically erased by the Data Processor.

Compliance Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

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

C.4 Instruction on the Transfer of Personal Data to Third Countries

The Data Processor is not permitted to transfer personal data to locations in third countries without the express written consent of the Data Controller.

If the Data Controller does not in these Regulations, or subsequently, provide documented instructions regarding the transfer of personal data to a third country, the Data Processor is not entitled to make such transfers within the framework of these Regulations.

C.5 Procedures for the Data Controller's Audits and Inspections

The Data Controller's audits and inspections are carried out as an integral part of the ongoing meetings between the Parties. At meetings between the Parties, the Data Processor's compliance with the GDPR, the applicable EU or Member State data protection provisions, and the Clauses can be discussed based on the Parties' mutual assessment of the threat picture, updated assessments of critical vulnerabilities, identified breaches, and the overall security of the processing activities regulated by these Clauses. The Data Processor shall hereafter in writing provide the Data Controller with a report of the overall level of compliance with the GDPR, the applicable EU or Member State data protection provisions, and the Clauses, if wished.

The Data Controller may contest the scope and/or methodology of the report and may in such cases, at the Data Controller's expense, request a new audit/inspection under a revised scope and/or different methodology, from an independent third party.

Compliance Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

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.