



DATA PROCESSING AGREEMENT

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

(the data controller)

and

GAIS A/S

CVR 44574780

P. O. Pedersens Vej 2

8200 Aarhus

Danmark

(the data processor)

each a 'party'; together 'the parties'

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subje



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 Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).
3. In the context of the provision of the GAIS-platform in accordance with a subscription (**the subscription agreement**), 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. This Data Processing Agreement and the subscription agreement are interdependent and cannot be terminated separately. However the data processing agreement can - without terminating the subscription agreement - be replaced by another valid data processing agreement.
6. Three appendices are attached to the Clauses and form an integral part of the Clauses.
7. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.
8. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.
9. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.
10. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.
11. The Clauses shall not exempt the data processor or controller from obligations to which they are subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

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 Article 24 GDPR), the applicable EU or Member State¹ data protection provisions and the Clauses.

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



2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.
3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

3. The rights and obligations of the data controller

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

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.

5. Behandlingssikkerhed

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

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

- a. Pseudonymisation and encryption of personal data;
- b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.



2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.
3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller’s obligations pursuant to Articles 32 GDPR, by inter alia providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller’s obligation under Article 32 GDPR.

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

6. Use of sub-processors

1. The data processor has the data controller’s general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.
2. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

3. 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.
4. 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.



5. In case of the data processors bankruptcy the data controller is entitled to enter into the rights of the data processor regarding any sub-processors processing of personal data allowing the data controller to instruct sub-processors in deletion and/or return of the processed personal data.

7. Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.
2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.
3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:
 - a. transfer personal data to a data controller or a data processor in a third country or in an international organization
 - b. transfer the processing of personal data to a sub-processor in a third country
 - c. have the personal data processed in by the data processor in a third country

8. Assistance to the data controller

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

- a. the right to be informed when collecting personal data from the data subject
 - b. the right to be informed when personal data have not been obtained from the data subject
 - c. the right of access by the data subject
 - d. the right to rectification
 - e. the right to erasure ('the right to be forgotten')
 - f. the right to restriction of processing
 - g. notification obligation regarding rectification or erasure of personal data or restriction of processing
 - h. the right to data portability
 - i. the right to object
2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 5.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:



- a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;
 - b. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;
 - c. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);
 - d. the data controller's obligation to consult the competent supervisory authority, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.
3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 8.1. and 8.2.

9. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.
2. The data processor's notification to the data controller shall, if possible, take place within 24 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.
3. In accordance with Clause 8(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

1. On termination of the provision of personal data processing services, the data processor shall be under obligation - after allowing the data controller no less than 30 days to transfer data - 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 or otherwise agreed upon in Appendix C.

11. Auditing and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.
2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.
3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

12. Commencement and termination

1. The Clauses shall become effective on the date of both parties' signature.
2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.
3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.
4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 10.1. and Appendix C.4., the Clauses may be terminated by written notice by either party. unless otherwise stated in Appendix A.5.

13. Data controller and data processor contacts/contact points

1. The parties may contact each other using the following contacts/contact points.
2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

The Data Processor

Name	Henrik Steuer Carlsen
Position	Head of Operations
Telephone	+45 4140 6371
E-mail	henrik@gais.dk



Appendix A Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

The data controller can use the GAIS-platform as owned and operated by the data processor, to collect and process information about employees, volunteers and administrators with the purpose of conducting employee-surveys.

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):

That the data processor provides the GAIS platform to the data controller and thereby stores, processes, and manages personal data of participants in GAIS surveys for the data controller.

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

The processing always includes, at a minimum, the registered person's name, email, age, position, country of employment, and gender.

The data controller can choose to use the GAIS platform for processing other information, and the registered individuals can submit free-text comments that may contain additional information including information categorized as confidential and/or sensitive. This information is subject to the processing.

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

Employees, volunteers and contacts of the data controller, whose information the data controller transfers for processing by the data processor.

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

The processing is not time-limited and continues for as long as there is a contractual basis between the parties that requires the data processor to perform data processing on behalf of the data controller.

The data controller can terminate the processing at any time and, in accordance with the conditions for terminating the data processing basis including appendix C, request the data processor to delete the processed personal data.



Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

NAME	ADDRESS	DESCRIPTION OF THE DATA PROCESSING
Microsoft Ireland Operations Limited	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18 D18 P521, Ireland	<p>The company provides IT systems to the data processor, used for the following data processing activities:</p> <ul style="list-style-type: none"> • Hosting and processing of personal data on the GAIS platform via Azure • Exchange of personal data via email through Outlook • Possible data processing in Office programs (Excel/Word) <p>All data processing takes place within the EU. However, the subprocessor is owned by a US corporation (Microsoft Corporation), which may lead to unintended data transfers to the USA in accordance with Schrems II. For this reason, the subprocessor has adhered to the EU-U.S. Data Privacy Framework, and additional measures have been implemented in the agreement.</p>
MongoDB Limited	Building Two, Number One Ballsbridge Shelbourne Road, Ballsbridge Dublin, D04 Y3x9, Ireland	<p>The company provides a database system and hosting for the GAIS platform's database via Azure servers.</p> <p>All data processing takes place within the EU. However, the subprocessor is owned by a US corporation (MongoDB Inc.), which may lead to unintended data transfers to the USA in accordance with Schrems II. For this reason, the subprocessor has adhered to the EU-U.S. Data Privacy Framework, and additional measures have been implemented in the agreement.</p>
Brevo / SendInBlue	106 boulevard Hausmann, 75008 Paris, France	<p>The company provides an email solution for sending all emails from the GAIS platform, including invitations to surveys, links to reports, etc.</p> <p>All data processing takes place within the EU.</p>
Pipedrive OÜ	Mustamäe tee 3a, 10615 Tallinn, Estonia	<p>The company provides a CRM system for GAIS, where customer data can be processed. This includes information solely on contacts at the customer's organization.</p> <p>All data processing takes place within the EU. However, the subprocessor is owned by a US corporation (Pipedrive Inc.), which may lead to unintended data transfers to the USA in accordance with Schrems II. For this reason, the subprocessor has adhered to the EU-U.S. Data Privacy Framework, and additional measures have been implemented in the agreement.</p>



Freshworks Inc.	San Mateo, 2950 S Delaware St Suite 201, USA	<p>The company provides a support system for GAIS, where personal data may be processed in connection with support cases. All data processing takes place in the EU and the USA.</p> <p>The subprocessor has adhered to the EU-U.S. Data Privacy Framework, and additional measures have been implemented in the agreement.</p>
SFDC Ireland Limited	Salesforce Tower, 60 R801, North Dock Ireland	<p>Supplies the Slack-platform used as a tool for internal communication. Personal data may be temporarily exchanged through Slack.</p> <p>All data processing takes place in Germany and However, the subprocessor is owned by a US corporation (Salesforce Inc.), which may lead to unintended data transfers to the USA in accordance with Schrems II. For this reason, the subprocessor has adhered to the EU-U.S. Data Privacy Framework, and additional measures have been implemented in the agreement.</p>

The data controller shall on the commencement of the Clauses authorise the use of the above mentioned sub-processors for the processing described for that party. The data processor shall not be entitled without notification in accordance with section 6 to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.



Appendix C Instruction pertaining to the use of personal data

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

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

The data processor supplies the GAIS-platform for the data controller allowing the data controller processing of the following data:

- Names
- E-mails
- Age
- Positions
- Country of work
- Gender
- Company information
- Other data as required by the data controller

The data processor upon the data controller's request will collect additional information from the registered individuals through digital surveys and give the data controller access to anonymized data.

As part of the processing, the data processor is required to create an anonymized copy of the GAIS responses upon completion of GAIS responses. Subsequently, the data processor can use the anonymized data for its own purposes without charge with the purpose of benchmarks and general statistics.

C.2. Security of processing

As the data processing through information and responses from the registered persons may contain personal information under the GDPR article 9 as 'special categories of personal data' the security level should reflect that the processing will include such confidential and sensitive information.

The data processor is entitled and obliged to make decisions about which technical and organizational security measures should be used to create the necessary (and agreed) security level around the information.

However, the data processor must, in all cases and at a minimum, implement the following measures, as agreed with the data controller.

Data confidentiality and integrity 'at rest'

Data should be stored and structured if possible and within reason as to reduce any derived consequences of a breach of data security. This is done through partial pseudonymisation where unique and randomly generated IDs are used as identifiers between different types of data so a security breach of one kind of data is less likely to result in breach of other types of data.

Additionally data should be encrypted as a minimum using AES256-CBC.

Availability, resilience and recovery

The GAIS-platform is actively monitored to ensure that incidents resulting in reduced availability immediately are acted upon. Additionally any incidents - including minor incidents - are reviewed monthly.

The platform and database is automatically backed up in real time with point-in-time restore within the last 24 hours and the following full backups kept for up to 3 months:

- Daily backups: Saved for 7 days



- Weekly backups: Saved for 4 weeks
- Monthly backups: Saved for 3 months

When restoring from backup it's ensured that any deleted data isn't by mistake restored through:

- Any deletion of personal data is logged with the user ID and a timestamp
- When restoring from backup the log is consulted to make sure that deleted data either isn't restored, or is deleted immediately after restoration without backup
- Entries in the log are deleted after 6 months

Database and application operates with fully automatised monitoring and redundancy within multiple 'availability zones' in Microsoft Azure Northern Europe. In the event of a failure of the underlying hardware, the platform will automatically switch over to healthy instances in other zones. Failed instances are automatically restored and reintroduced.

Both the database and the application automatically scale capacity according to the registered load.

Regular testing

Incidents and alarms from the GAIS-platformen are reviewed monthly where any errors or deficiencies of the measures will be handled.

Procedures should be - as a minimum - tested and reviewed once per year including:

- Restore from backup
- Reviewing and random samples in all relevant logs
- Testing of alarms and incident warnings on the platform
- Reviewing and random samples of data accessing and APIs
- Reviewing and random samples on compliance of internal processes

Upon significant changes - for example changing offices, replacing sub-processors or major architectural changes on the platform affected procedures and measures should be updated and tested.

Access to data through the internet

The GAUS-platform is an online web-app that is accessed through a web browser allowing access to data through the internet to the extent data is shown on the platform.

Access is handled through temporary tokens given upon login and/or through an email. Upon expiry of the token the user has to be reauthorized.

Access outside the customer facing user interface requires whitelisted IP and/or two-factor authorization.

Data confidentiality and integrity 'in transit'

When exchanging data between database, application server and browser-app data should as a minimum be encrypted with TLS 1.2. Any exchange of data should as limited as possible following:

- The exchange is limited to the smallest collection of data necessary
- Only summarized responses are sent to the browser-app
- As a rule personal data shouldn't be exchanged between the three systems as information is sent pseudonymized using IDs and only to a small extent is it necessary to send actual personal (fx to show a list over invitees and create the org. on the platform)

Physical security

Personal data is only stored on servers placed at our sub-processors location guaranteeing a high degree of physical security including:



- The physical access is limited to very few and specific individuals
- Perimeter protection through logs, monitoring and physical barriers
- Two-factor biometric authentication and camera surveillance

GAISs own offices will not contain any personal data as data only is accessed online from here. As Data is accessible from our location the following however applies:

- All computers are encrypted, require biometric authentication and are not left unlocked
- Offices are locked and the alarm is enabled when no one is in the offices
- 3rd party security company is actively monitoring the offices
- Employees are instructed in using common sense when allowing non GAIS-employees access to the office (fx suppliers, customers, etc.)

Additionally as data can be accessed from home offices the following applies:

- All computers are encrypted, require biometric authentication and are not left unlocked
- Access to certain areas of the platform requires VPN
- Employees are instructed in using common sense when handling data, including not copying or leaving personal information accessible

Logs

All access to the database is logged with login credentials, timestamp and IP.

C.3. Assistance to the data controller

The data processor should, to the extent possible within the scope and extent below, assist the data controller in accordance with Clause 8.1 and 8.2 by implementing the following technical and organizational measures:

- Deletion of personal data at the request of the data controller or the data subject.
- Providing the ability to extract the data subject's information at the request of the data controller or the data subject.
- Providing the necessary information to the data controller and the data subject to comply with the obligation to inform.

C.4. Storage period/erasure procedures

Personal data is stored with the data processor until the data controller requests their deletion or return, or until the main agreement terminates, as per Appendix A.5.

C.5. Processing location

Processing primarily occurs at multiple locations in Denmark and at subprocessor locations in the EU. Processing of the personal data covered by the agreement may occur at these locations, as well as other locations, provided that data access is SSL encrypted and only accessed via an IP address approved by the data processor.

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

Unless otherwise agreed between the parties in Appendix B, data processing may not take place in third countries.

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

The data processor will once a year draw up a report detailing the data processors audit and any findings in the audit. The report shall as a minimum describe the following as well as results hereof:

- Audit and inspections of sub-processors
- Test and audits of internal procedures and measures
- Data breaches
- Compliance with the data processing agreement



- Internal awareness and training
- Additional measures implemented since last report

The report is made available on the data processors website and the data controller is notified with a direct link to the report.

The data controller or a representative of the data controller can conduct additional auditing of the data processor when, in the data controller's assessment, there is a need for such an audit.

As a starting point, audits are conducted in writing, and the data processor participates in the audit at no charge, unless the extent or frequency is disproportionate to the data processing.

Any expenses related to a physical audit are covered by the data controller. However, the data processor is obligated to allocate the resources (primarily time) necessary for the data controller to conduct its audit.

C.8 Procedurer for databehandlerens revision, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til underdatabehandlere

The data processor or a representative of the data processor conducts yearly audits of sub-processors by obtaining available auditing reports. If the results of the auditing reports make it clear that the additional auditing is needed the data processor will do so.

In case of high risk data processing - understood as processing of larger amounts of data, special categories of data and/or other confidential or sensitive information - the auditing report should as a minimum be of the type ISAE 3000 SOC 2.

In case of lower risk data processing - understood as not containing special categories of data and/or other confidential or sensitive information - the auditing report should as a minimum be of the type ISO 27001 or SOC 3.

Upon the data controllers request the auditing report will be sent to the data controller. Based on the results of the report, the controller is entitled to request the implementation of additional measures to ensure compliance with the General Data Protection Regulation, data protection provisions in other Union or Member State law and these Regulations.

The processor or a representative of the processor shall also have access to carry out inspections, including physical inspections, of the premises from which the sub-processor processes personal data, including physical premises and systems used for or in connection with the processing. Such inspections may be carried out whenever the processor (or controller) deems it necessary.

Documentation of such inspections shall be provided to the controller upon such request. The data controller may challenge the framework and/or methodology of the inspection and may in such cases request the performance of a new inspection under a different framework and/or using a different methodology.

