Data Processing Agreement

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

between

The Customer identified during the account creation process on the Sheltr Whistleblower platform, acting as the Data Controller

(the Data Controller)

and

Cookie Information A/S (second name Sheltr A/S)
CVR 38758292
Købmagergade 19
1105 København K
Denmark

(the Data Processor)

each a ‘party’; together ‘the parties’

HAVE AGREED on the following Contractual Clauses (the Clauses) to meet the GDPR requirements and to ensure the protection of the rights of the data subject.

Table of Contents

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 regarding the processing of personal data and 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 main contract agreed upon between the parties, 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 in other agreements between the parties.

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

6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

7. Appendix B contains the Data Controller’s conditions for the Data Processor’s use of sub-processors and a list of sub-processors authorised by the Data Controller.

8. Appendix C contains the Data Controller’s instructions regarding the processing of personal data, the minimum security measures to be implemented by the Data Processor, and how audits of the Data Processor and any sub-processors are to be performed.

9. Appendix D contains provisions for other activities not covered by the Clauses.

10. The Clauses and appendices shall be retained in writing, including electronically, by both parties.

11. The Clauses do not exempt the Data Processor from obligations to which it is 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 State[1] data protection provisions and the Clauses.

2. The Data Controller has the right and obligation to decide about the purposes and means of processing personal data.

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

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

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 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 processing of personal data. Still, 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. The parties shall agree in the specific situation whether the Data Processor shall continue to comply with the instructions given by the Data Controller on the processing of personal data or whether the processing shall be suspended until the Data Controller has investigated the matter further. Notwithstanding the foregoing, the Data Processor will not have liability to the Data Controller or third-party Data Controllers for actions taken by the Data Processor in reliance upon the Data Controller’s instructions.

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. Based on 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. At the request of the Data Controller, the Data Processor shall demonstrate that the concerned persons under the Data Processor’s authority are subject to the abovementioned confidentiality.

5. Security of processing

1. Article 32 GDPR stipulates that, considering the state of the art, the costs of implementation, the nature, scope, context, and purposes of processing, and 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 to ensure 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 end, 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 under Article 32 GDPR by, among other things, providing the Data Controller with information concerning the technical and organisational measures already implemented by the Data Processor under 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 Data Controller's assessment—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

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

2. Therefore, the Data Processor shall not engage another processor (sub-processor) to fulfil the Clauses without the prior general written authorisation of the Data Controller.

3. The Data Processor has the Data Controller’s general authorisation for the engagement of sub-processors. The Data Processor shall inform the Data Controller in writing of any intended changes concerning the addition or replacement of sub-processors at least 1 month in advance, thereby allowing the Data Controller to object to such changes before the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the Data Controller can be found in Appendix B.

4. Where the Data Processor engages a sub-processor for carrying out specific processing activities on behalf of the Data Controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational

measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

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

5. A copy of such a sub-processor agreement and subsequent amendments shall – at the Data Controller’s request – be submitted to the Data Controller, thereby allowing the Data Controller to ensure that the same data protection obligations set out in the Clauses are imposed on the sub-processor. Clauses on business-related issues that do not affect the legal data protection content of the sub-processor agreement shall not require submission to the Data Controller.

6. If the sub-processor does not fulfil his data protection obligations, the Data Processor shall remain fully liable to the Data Controller as regards the fulfilment of the sub-processor's obligations. This does not affect the rights of the data subjects under the GDPR—particularly 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

1. Any transfer of personal data to third countries or international organisations by the Data Processor shall only occur based on 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, 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 before 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 an international organisation

    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 transferring personal data to a third country, including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

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

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
   j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the Data Processor's obligation to assist the Data Controller under Clause 6.3., the Data Processor shall furthermore, considering 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 communicate the personal data breach to the data subject without undue delay when the breach is likely to result in a high risk to the rights and freedoms of natural persons.

   c. the Data Controller's obligation is to assess the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment).

   d. The Data Controller is obliged 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 extent of the assistance required. This applies to the obligations foreseen in Clauses 9.1 and 9.2.

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 48 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 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, according 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.

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

10. Erasure and return of data

1. On termination of the provision of personal data processing services, the Data Processor shall be obliged to delete all personal data processed on behalf of the Data Controller without undue delay and certify to the Data Controller that it has done so unless Union or Member State law requires storage of the personal data.

11. Audit and inspection

1. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.

2. Procedures applicable to the Data Controller’s audits, including inspections, of the Data Processor and sub-processors are specified in appendices C.7. and C.8.

3. The Data Processor shall be required to provide the supervisory authorities, which, according 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. The parties' agreement on other terms

1. The parties may agree to 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 data subject's fundamental rights or freedoms and the protection afforded by the GDPR.

13. Commencement and termination

1. The Clauses shall become effective when the Data Controller accepts the Terms and Conditions, including this Agreement.

2. Both parties shall be entitled to require the Clauses to be renegotiated if changes to the law or the 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. They cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed upon between the parties.

4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the Data Controller pursuant to Clause 11.1 and Appendix C.4., either party may terminate the Clauses by written notice.

14. Electronic Acceptance

1. This Data Processing Agreement is entered into between the Data Controller and Sheltr A/S upon acceptance of the Terms and Conditions and becomes effective on the date of such acceptance. The Data Processor makes this Agreement available for review during the sign-up for the Whistleblower solution. Upon the Customer's acceptance of the Terms and Conditions, this Agreement is deemed concluded and binding in accordance with Article 28(3) of the General Data Protection Regulation.

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:

To provide a software solution ('Whistleblower') that enables confidential or anonymous reporting of misconduct in accordance with the EU Whistleblower Directive.

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):

Collection, storage, and case management of whistleblower reports. This may include personal data written in messages exchanged between the whistleblower and assigned case manager, as well as other shared documentation as part of the investigation process until a case is ultimately closed.

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

The types of personal data processed about the data subject depend on the information shared voluntarily by the whistleblower. Hence, the processing includes, but is not necessarily limited to, the following types of personal data: full names, email addresses, details on the suspected misconduct, potentially sensitive data, including criminal allegations and health data.

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

Whistleblowers (employees, former employees, third parties), individuals named in whistleblower reports, investigators (internal or external), HR/legal staff.

A.5. The Data Processor’s processing of personal data on behalf of the Data Controller. Processing has the following duration:

The data processing duration depends on the Data Controller’s settings on the platform. Unless the Data Controller alters the retention settings, they accept the default values:

- Rejected cases: 30 days
- Concluded cases: 60 days
- Concluded cases handed to authorities: 180 days

The Data Controller accepts the Data Processor’s retention of system-generated data (e.g., case IDs, timestamps, activity logs) insofar as necessary for delivering the services provided by the Data Processor, and until the termination of the Agreement. However, the Data Controller can instruct the Data Processor to delete retained metadata at any time. At the termination of this Agreement, data will be deleted as set out in clause 11.1 unless otherwise instructed by the Data Controller.

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	CVR	ADDRESS	DESCRIPTION OF PROCESSING
Microsoft Danmark ApS	DK13612870	Kanalvej 7, 2800, Kongens Lyngby Denmark	Hosting in an EU/EEA region only cloud located in Norway

The Data Controller shall, on the commencement of the Clauses, authorise 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 authorisation – to engage a Sub-processor for different processing purposes than the ones which have been agreed upon in this Agreement.

B.2. Prior notice for the authorisation of sub-processors

The time period for authorisation of new Sub-processors is 1 month. This means that if the Processor wants to use a new Sub-processor to process personal data, the Data Processor needs to inform the Data Controller 1 month prior to using the new Sub-processor.

Appendix C - Instruction related 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:

- Operating a whistleblower portal accessible via the internet, where individuals can submit reports - anonymously or non-anonymously - regarding potential violations, misconduct, or other concerns relevant to applicable EU law.
- Receiving and storing reports submitted through the whistleblower portal, including any attached files, structured form data, and potential personal identifiers provided by the whistleblower.
- Providing a secure interface to authorised users selected by the Data Controller for reviewing, managing, and documenting actions taken in relation to each report, including case tracking, internal notes, and resolution steps.
- Where configured, the platform allows secure two-way communication between authorised case managers and anonymous reporters (whistleblowers) via the portal.
- Ensuring access to case details and related data is strictly limited to authorised personnel designated by the Data Controller, in accordance with role-based access controls and confidentiality requirements.
- Not processing or accessing report case content beyond what is necessary to ensure the operation of the platform, respond to technical support requests, or as explicitly instructed by the Data Controller.
- Deleting or retaining case contents and associated data in accordance with the Data Controller’s configuration settings or specific instructions, and as outlined in Clause 11.1.

C.2. Security of processing

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

Microsoft Azure

The Data Processor offers a SaaS solution and uses a Cloud supplier (Microsoft) to host the services, related components, and content provided online. Microsoft provides the infrastructure and associated security. All data is hosted on Microsoft's data centre in Norway. Azure Cloud has comprehensive compliance coverage: ISO 27001, ISO 27018, SOC 1, SOC 2, SOC 3, FedRAMP, HITRUST, MTCS, IRAP, and ENS.

Web servers, application servers, database servers, and physical storage in which data is kept are provided in a redundant multi-drive configuration, which provides mirrored storage and the required software to host the solution and associated services.

The service takes advantage of Azure's wide opportunities to ensure high availability, including full redundancy for all components and services, load balancing, automatic scaling of capacity, continuous backup and geo-replication of data, and a traffic manager to automatically geographic failover in case of an emergency at the data centre level.

The hosting service is provided in a safe ’limited access’ environment. There is a continuous supply of power and climate control, and the data centre is protected against natural disasters.

See more on Microsoft Azure security measures here: https://azure.microsoft.com/en-us/over-view/trusted-cloud/

The Data Processor reserves the right to change the location of the data centre without obtaining prior consent from the customer, provided that the new data centre provides the Customer with at least the same service level and security as the current one and that the new data centre is located within the EEA/EU.

Additional safety measures at Cookie Information
The Whistleblower portal is accessible to whistleblowers through a secure, cookie-free, and tracking-free web interface available at whistleportal.co/[company-specific-identifier]. The admin web application and related case data are accessed via wb.sheltr.eu. Access requires a secure connection and validated login credentials. The web-based application employs secure HTTP (SSL/HTTPS) with TLS 1.2 to protect data transmissions over the internet. All data transmitted through the platform is encrypted in transit, ensuring confidentiality during communication.

Only selected employees, adhering to the principles of least privilege, have access to the production environment. To gain access, an authorised user must possess a unique username and password and be connected via a dedicated VPN. Furthermore, two-factor authentication is required for accessing all operational systems, and IP restrictions are implemented to protect all critical systems.

C.3. Assistance to the Data Controller

The Data Processor shall, insofar as this is possible, within the scope and the extent of the assistance specified below, assist the Data Controller following Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

The Data Controller may submit any request for assistance to a single point of contact support@sheltr.eu.
- At the request of the Data Controller, the Data Processor will assist the Data Controller in complying with data subject rights requests by identifying personal data held by the Data Processor. Depending on the platform configuration and the Data Controller's access settings, the Data Controller can access all data related to submitted reports via the user interface.
- If the Data Processor receives a request directly from a data subject, it shall forward the request to the Data Controller without undue delay.
- The Data Processor has implemented procedures to ensure the Data Processor's assistance to the Data Controller in case of events described in Clause 9.2.

The Data Processor assists only as necessary for the Data Controller to respond to lawful requests by identifiable data subjects and does not itself determine eligibility or the legal basis for such requests.

C.4. Storage period/erasure procedures

The Data Controller has generally instructed the Data Processor to retain data as specified in Appendix A. However, the Data Controller can instruct the Data Processor to delete data at any time. At the termination of this Agreement, data will be deleted as set out in clause 11.1.

C.5. Processing location

Processing of the personal data by the Data Processor under these Clauses cannot be performed at other locations than the following without the Data Controller's prior written authorisation:

The sub-processor provides the Data processor premises within the EU and the cloud, as specified in Appendix B.

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

The Data Processor has instructed the sub-processor set out in Appendix B.1 to only process data within the EU/EEA. However, the Data Processor cannot entirely exclude that, in some instances, the sub-processor may access data from the US for business continuity and support purposes and where required to do so by law enforcement authorities. To the extent such access is deemed instructed to transfer, the Data Controller acknowledges having instructed the Data Processor to allow for such transfer. Such access, if any, is strictly limited to technical support and does not include access to the content of submitted reports.

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 Controller or the Data Controller's representative shall have access to perform a physical inspection of 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 to ascertain the Data Processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The Data Controller must send any request for an audit under Clause 11 to the Data Processor as set out in Section 15. The Data Processor and the Data Controller will discuss and agree in advance on the reasonable start date, scope, and duration of security and confidentiality controls applicable to any audit or inspection. Any audit or inspection requested by the Data Controller will be at the Data Controller's cost.

The Data Processor may object to any third-party auditor appointed by the Data Controller to conduct any audit if the auditor is, in the Data Processor's reasonable opinion, not suitably qualified or independent, a competitor of the Data Processor or otherwise manifestly unsuitable.

Any such objection by the Data Processor will require the Data Controller to appoint another auditor or conduct the audit itself. The auditor in question must be subject to confidentiality, either contractually or by law.

Where a sub-processor makes available security audit reports, certifications, declarations, etc., the Data Controller may request access to such reports. The Data Controller accepts that the Data Processor's audit of processing performed by sub-processors is carried out by reviewing such available security audit reports, certifications, or declarations.

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. Any such further measures shall be for the Data Controller's costs. The Data Processor will provide
the Data Controller with further details of any applicable fee and costs for itself and any sub-

processor, and the basis of its calculation before any such audit. The Data Controller acknowledges and accepts that audits and inspections of sub-processors may be subject to restrictions and standard terms provided by such sub-processors.

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

The Data Processor shall annually, at the Data Processor's expense, obtain an AUDITOR'S REPORT or INSPECTION REPORT concerning the Sub-processor's compliance with the GDPR and forward said documentation to the Data Controller.

The Parties agree that the ISAE 3000 standard and SOC2 Type II are applicable for this purpose.

Appendix D - The parties’ terms of agreement on other subjects

The Data Processor’s liability towards the Data Controller is subject to the limitations set out in the Agreement. The Data Processor shall be liable towards data subjects for damages caused by processing only where the Data Processor has not complied with its obligations under the GDPR or where the Data Processor has acted outside or contrary to the lawful instructions of the Data Controller.

To the extent that the data subjects claim compensation from the Data Processor in accordance with the GDPR or other provisions on joint liability for Data Controllers and Data Processors, the Data Controller will indemnify and reimburse the Data Processor for any claim which is not due to the Data Processor’s violation of the Clauses or the GDPR.

Where the Data Controller requests the Data Processor’s assistance following Clause 9.1. and 9.2 and Appendix C.1.3, the Data Processor shall, to the extent the request for assistance is not caused by the Data Processor acts or omissions in violation of this Agreement or the Data Processor’s direct obligations under GDPR and the Danish Data Protection Act, be entitled to reasonable compensation for its services.