Outlay ApS - DPA

Standard Contractual Clauses

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

between

Company name OUTLAY ApS Company address Strevelinsvej 38 7000 Fredericia Denmark Company ID no. 25705564 Hereinafter referred to as data processor	Hereinafter referred to as data controller

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 subject.

1. **Table of contents**
2. Preamble
3. The rights and obligations of the data controller
4. The data processor acts according to instructions
5. Confidentiality
6. Security of processing
7. Use of sub-processors
8. Transfer of data to third countries or international organisations
9. Assistance to the data controller
10. Notification of personal data breach
11. Erasure and return of data
12. Audit and inspection
13. The parties' agreement on other terms
14. Commencement and termination
15. Data controller and data processor contacts/contact points
    Appendix A Information about the processing
    Appendix B Authorised sub-processers
    Appendix C Instruction pertaining to the use of personal data
    Appendix D The parties' terms of agreement on other subjects

2. 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 services related to outsourcing of the fi-nance function, as described in the agreement between the parties (the "Main 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. 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 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.

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

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 from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3. 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 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, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. 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 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.

5. 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.

6. Security of processing

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.

2. 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.

3. 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.

4. 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.

7. Use of sub-processors

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

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

3. 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.

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 giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

6. The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g., enabling the data controller to instruct the sub-processor to delete or return the personal data.

7. 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.

8. 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

4.   The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

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.

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 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 subjec

   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 pursuant to Clause 6.3., 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:

3.   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, at the place of the data controller's venue, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

4.   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;

5.   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);

6.   the data controller's obligation to consult the competent supervisory authority, at the place of the data controller's venue, 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.

7.   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 9.1. and 9.2.

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 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, 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.

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.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to, at the choice of the data controller, either (i) return all personal data processed on behalf of the controller and delete existing copies thereof; and/or (ii) 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.

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 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.

13. The parties' agreement on other terms

1. The parties may agree 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.

14. 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 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

5. Signature

Signee 1	Signee 2
Representative title	On behalf of
Adm. Direktør	
	IP Address
Company representative	-
Andreas Østergaard Borris	
On behalf of	
OUTLAY ApS	
Email	
aborris@keepers.dk	
IP Address	
-	
Signature will appear here	Signature will appear here

15. 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.

Name	Andreas Østergaard Borris
Position	CEO
Telephone	+4526365013

E-mail	aborris@keepers.nu

Appendix A Information about the processing

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

The purpose of the data processor's processing of personal data is to assist the data controller with outsourcing of the finance function, as described in Main Agreement. The purposes of the processing are, for example:

- Operation of the controller's finance function, including bookkeeping, cash management, reporting and controlling
- Advice and assistance related to the finance function

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):

Services provided according to the Main Agreement, including the provision of services in relation to finance function, including collection, recording, storage, systematisation and use.

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

The data processor shall process the types of personal data that the data controller directly or indirectly gives the data processor access to, which typically includes:

Ordinary categories of personal data, cf. Article 4(1) and Article 6 of the General Data Protection Regulation, including the following types of personal data:

- Name
- Telephone number
- E-mail
- Bank information

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

The data processor shall process personal data about the categories of data subjects that the data controller directly or indirectly gives the data processor access to, which typically includes:

- Employees
- Contact persons at business partners
- Customers

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:

These Clauses shall be effective for the duration of the provision of the services in accordance with the Main Agreement.

Appendix B Authorised sub-processers

B.1. Approved sub-processors

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

NAME	VAT	ADRESS	Name of Service /Tool	Description of processing	Purpose	Transfer to third country and legal basis for transfer
Visma e-conomic A/S	29403473	Visma e-conomic A/S Gærtorvet 1-5, 1799 København V Danmark	E-conomic	Accounting program	Accounting software. Used for project managment, invoicing and bookkeeping.	Denmark
Fenerum ApS	40430989	Hermodsvej 22, 2.	Fenerum	Subscription software	Handling all subscriptions to Outlay	Denmark
Teamwork Crew Ltd. trading as Teamwork.com	313652	Teamwork Campus One, Blackpool Retail Park, Blackpool, Cork, T23 F902, Ireland	teamwork	Project and team management software	Help desk service	Ireland
Keepers ApS	36079886	Strevelinsvej 38, 7000 Fredericia	Keepers	CFO services	Sales administration, onboarding, hosting master data	Denmark
Wecode	37496510	Thorsgade 59, 2, 2200 København N.	Wecode	Software developer	Software	Denmark

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

The data processor's notice of any planned changes in terms of addition or replacement of sub-processors must be received by the data controller no later than thirty (30) days before the addition or replacement is to take effect, in so far this is possible.

Regardless of the above, the data controller accepts that there may be situations with a specific need for such change in terms of addition or replacement of sub-processors with a shorter notice or immediately. In such situations, the data processor will notify the data controller of such change as soon as possible.

If the data controller has any objections to such changes, the data controller shall notify the data processor thereof within ten (10) days after receipt of the data processor's notification of the change. The absence of objection by the controller will be considered as an acceptance of the sub-proccesor concerned.

In case of the data controller's objection, the data controller furthermore accepts that the data processor may be prevented from providing all or parts of the agreed services. Such non-performance cannot be ascribed to the data processor's breach. The data processor will maintain its claim for payment for such services, regardless of if they cannot be provided to the data controller.

If the data controller has reasonable and specific grounds to object to the use of a sub-processor, the data controller may terminate the Main Agreement with respect to those aspects of the service that cannot be provided without the use of the sub-processor as described in Appendix D.6.

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 according to the Main Agreement.

C.2. Security of processing

The level of security shall take into account:

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

The data processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

Organizational security

- The data processor has a documented information security policy that addresses how information security is embedded and implemented in the data processor's organisation.
- The processor maintains and enforces policies for the secure handling of information and for ensuring that personal data is processed in accordance with applicable law. The processor shall take appropriate steps to ensure that such policies are known to all employees by conducting regular training.
- The data processor shall ensure that third party service providers comply with a minimum set of controls prescribed by the data processor and are subject to confidentiality obligations prior to their use.
- The data processor regularly checks third party services and sub-processors based on the risk of their processing of personal data.
- Taking into account the current technical level, implementation costs and the nature, scope, context and purposes of the processing, the processor will implement and observe principles regarding data protection by design at all stages of the data and system life cycle.

Physical security

- Locations from which the data controller's data potentially can be accessed have appropriate physical security controls to protect against unauthorised access.
- The processor shall ensure the safe disposal of information, media, equipment and paper in accordance with industry standards.

System and network security

- Networks and devices on which personal data is processed are protected against unauthorised access or infiltration, both internally and externally.
- Network security is maintained through the use of commercially available equipment and industry standard techniques, including the performance of periodic external vulnerability scanning and the maintenance of perimeter defences, such as firewalls and intrusion prevention and detection systems.

- Anti-virus and anti-malware programs are used on operating systems along with security configurations. Provider's recommended security patches are deployed in a timely manner on both applications and operating systems.
- Encryption is used on portable hard drives, other devices and portable media, to the extent required to protect personal data. All personal data transmitted by the data processor must be encrypted while in transit.

Access control

- The processor shall ensure that the controller's personal data are accessed only by authorised persons by means of access control procedures that ensure access on a "least privilege" basis and that access is terminated where and when appropriate.
- Access via the Internet shall at a minimum be via multi-factor login, encrypted, and passwords shall be of sufficient length and complexity.
- The processor shall have user administration procedures in place that define user roles and their privileges, and how access is granted, modified and terminated.
- The processor shall perform regular checks on the rights granted.

Logging

- All login attempts must be logged to detect unauthorized access to personal information.
- Security logging must be enabled on all network equipment, servers and on all applications to the extent possible in the systems.
- Logs of access to personal data and use of personal data shall be monitored and periodically reviewed by the data processor to detect unauthorized access to personal data.

Backup

- The processor shall perform backups of the personal data processed on behalf of the data controller and shall have procedures in place for the purpose of ensuring recovery of backed-up data in a timely manner to ensure the availability and accessibility of personal data.
- The processor shall have a documented procedure for performing back-up. Such procedure shall identify the requirements for storage and deletion of data.
- Backups shall be protected against unauthorised access, including destruction, and shall be encrypted if the backup contains personal data where encryption based on a risk assessment is required.

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 in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

The Processor shall assist the Controller in the fulfilment of the Controller's obligations set forth in Clauses 9.1 and 9.2 to the extent required and requested by the Controller.

As regards the controller's obligations set forth in Clause 9.2, the specific obligation is that the processor shall assist in providing the information set forth in Clause 10.3 and further described in Article 33(3) of the General Data Protection Regulation.

C.4. Storage period/erasure procedures

Upon termination of the provision of personal data processing services, the data processor shall either delete or return the personal data in accordance with 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.5 Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorisation:

Primarily from the data processor and the sub-processor's locations including locations under their and their employees' control.

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

The data processor is only allowed to transfer personal data to a country outside the European Union or EEA (a "Third Country") or an international organization located in a Third Country as further specified below.

C.6.1. General approval of transfer of personal data to secure Third Countries

With the Clauses, the data controller provides a general and prior approval (instruction) for the data processor to transfer personal data to Third Countries if the European Commission has determined that the Third Country/the relevant area/the relevant sector has a sufficient level of protection.

C.6.2 Approval of transfer to specific recipients of personal data in Third Countries subject to appropriate safeguards

The data controller instructs the data processor to transfer personal data to Third Countries, when necessary, in order for the data processor to deliver the service in accordance with the Main Agreement, including by using the listed sub-processors transferring personal data to Third Countries as described in regulations in Appendix B.1.

The controller has given consent to the use of the specified sub-processor(s) and instructions for the transfer of personal data to third countries in the provision of the Services

The legal basis for transferreing personal data to third countries is the European Commission's Standard Contractual Clauses ("SCC"), concluded between the data processor and the sub-processor(s) specified in Appendix B.1. This means that the data processor will be considered as the data exporter and the sub-processor as data importer. When personal data is transferred to the sub-processors specified in Appendix B.1, both parties agree to be obliged by the obligations in accordance with the SCC.

In case the European Commission completes new Standard Contractual Clauses subsequent to the formation of the original Standard Contractual Clauses, the data processor is authorized to renew, update and/or use the Standard Contractual Clauses in force from time to time.

The content of these Clauses shall not be deemed to change the content of such safeguards, incl. the Standard Contractual Clauses.

If the controller does not provide in these Provisions or subsequently a documented instruction regarding the transfer of personal data to a third country, the data processor is not entitled to make such transfers within the scope of these Provisions.

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

Pursuant to Articles 24 and 28 of the General Data Protection Regulation, the data controller is entitled and obliged to monitor the data processor's processing of personal data on behalf of the data controller. The data controller's monitoring of the data processor may consist in one of the following actions from the data controller:

- Self-checking based on documents provided to the data controller by the data processor,
- Written inspection, or
- Physical inspection.

<u>C.7.1 Self-checks</u>

The data controller may ask questions regarding supervision to the data processor and the data controller can, at his or her request, access a range of documents for the purpose of self-checking, including:

- A description of the physical and organisational security measures at the data processor.
- IT-security policy.

<u>C.7.2 Written inspection and physical inspection</u>

The data controller may choose to carry out an inspection either as a written inspection or as a physical inspection. The inspection may be carried out by the data controller and/or in cooperation with a third party who has entered into a non-disclosure agreement with the data processor. An inspection must be based on the security measures agreed between the parties.

Procedure and reporting of written inspection or physical inspection:

- The data controller shall contact the data processor by email to GDPR@keepers.nu with request for a written inspection and/or a physical inspection.
- At written inspections the data controller shall give notice to the data processor hereof without undue delay,
- At physical inspections the data controller shall arrange a date for the inspection in advance with the data processor.
- The data processor confirms receipt and confirms the date for such inspection.
- The inspection is made.
- The data controller drafts a report that is subsequently sent to the data processor.
- The data processor will review the draft report and provide potential comments to the data controller's observations (can be repeated several times).
- The final report is concluded by the data controller.
- The inspection is ended.

The data controller's costs, if applicable, relating to physical inspection shall be defrayed by the data controller. The data processor shall, however, be under obligation to set aside the resources (mainly time) required for the data controller to be able to perform the inspection.

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

The data processor regularly audits its sub-processors using a risk-based approach based on the best practices for such audits generally applied from time to time. Such may include review of audit reports, use of questionnaires and other appropriate means.

Appendix D The parties' terms of agreement on other subjects

D.1 - In general

In relation to the data processor's processing of personal data on behalf of the data controller, the parties have agreed on the specific terms outlined below.

In case of discrepancy between the Clauses and the terms laid down in this appendix D, appendix D shall take precedence.

D.2 - Consequences of the data controller's unlawful instructions

The data controller is aware that the data processor depends on the data controller's instructions to which extent the data processor is entitled to use and process personal data on behalf of the data controller.

If the data controller's instruction is considered as unlawful according to the data processor's reasonable evaluation the data processor is able to end further processing than storage until the data controller gives supplementary instruction on whether the processed personal data once again can be processed legally or if the personal data shall be handed over or deleted. The data processor's end of processing in such situations cannot lead to breach of these Clauses or the parties Main Agreement.

The data processor is not liable for any claims arising from the data processor's acts or omissions, to the extent such acts or omissions are a direct data processing activity exercised in accordance with the data controller's instructions and if the data processor is held liable or sanctioned the data controller shall hold the data processor harmless.

D.3 – Implementation of other security measures

The data processor is entitled to implement and maintain other security measures than what has been specified in the Clauses and Appendix C.2, however, provided that such other security measures as a minimum provide the same level of security as the described security measures.

D.4 - Provisions regarding a beneficiary third party in connection to sub-processors

The parties have agreed that Clause 7.6 of the Clauses (as specified below) shall not apply between the parties.

Thus, the following text shall be deleted from the Clauses: "The data processor shall in his agreement with the sub-processor include the data controller as a third-party beneficiary in the event of the bankruptcy of the data processor to enable the data controller to assume the data processor's rights and invoke these as regards the sub-processor, e.g. so that the data controller is able to instruct the sub-processor to perform the erasure or return of data."

D.5 - Use of sub-processors supplying on standard terms

Regardless of Clause 7 it is emphasized that if the data processor uses a sub-processor, who provides services on its own terms, which the data processor cannot deviate from, the sub-processor's terms for such processing performed by such sub-processor will apply. With these Clauses, the data controller accepts and instructs that such specific processing activities are based on the sub-processor's terms.

D.6 – The data controller's objection to a sub-processor

If the data controller has any objections to the application of a sub-processor, the data controller shall notify the data processor thereof without undue delay before such change is to take effect as described in Appendix B.2. The data controller may only object to such changes if the data controller has reasonable and specific grounds for such objection.

However, the data controller may terminate the Main Agreement with 30 days' written notice to the end of the month with respect to those aspects of the service that cannot be provided without the use of the sub-processor. Any prepaid payments covering the remainder of the term of the Main Agreement following the expiry of the termination period will be refunded to the data controller.

The data controller may also terminate the entire Main Agreement with 30 days' written notice to the end of a month if the processor is prevented from providing all of the agreed services in accordance with the Main Agreement. Any prepaid payments covering the remainder of the term of the Main Agreement following the expiry of the termination period will be refunded to the data controller.

D.7 - Compensation

The data processor is entitled to receive reasonable payment for time spent as well as other direct costs incurred by the data processor relating to assistance and services provided by the data processor to the data controller. Such assistance and services may include but is not limited to assistance and service described in Clause 9, 10, 12, C.3 and C.7, changes to the instruction, cooperation with supervisory authorities etc.

The compensation is calculated on the basis of the time spent and the agreed hourly rates in the Main Agreement regarding the data processor's provision of services to the data controller, and if no hourly rates have been agreed on, the data processor's current hourly rates will be applied, with the addition of any cost paid, including also cost to be paid by the data processor for the assistance of sub-processors.

If the data processor's assistance and/or service leads to claims for increased security measures to be observed in relation to agreement regarding the data processor's provision of services to the data controller and Appendix C, the data processor will, as far as possible, implement such additional security measures pursuant to further agreement with the data controller, provided that the data processor receives payment for such work. The data processor shall furthermore be entitled to receive payment for the implementation of other security measures if the data processor's ongoing evaluations leads to increased requirements for such security measures compared to the Clauses regarding the data processor's provision of services to the data controller. The data processor will introduce and implement such additional security measures pursuant to further agreement with the data controller.

Regardless of the above a party does not have the right to claim compensation for assistance, service or implementation of changes to the extent where such assistance or changes are a direct consequence of the party's own breach of these Clauses.

D.8 - Limitation of liability

The limitation of liability in the Main Agreement applies to the data processor's processing of the personal data under these Clauses, including with regard to art. 82 of the General Data Protection Regulation.

Signee 1	Signee 2
Representative title **Adm. Direktør**	On behalf of
Company representative **Andreas Østergaard Borris**	IP Address -
On behalf of **OUTLAY ApS**	
Email **aborris@keepers.dk**	
IP Address -	
Signature will appear here	Signature will appear here