Cloudmore Data Processing Terms

Version 2024-10

These Data Processing terms supplement the Cloudmore Master Agreement and sets out in which manner Cloudmore shall process Personal Data on behalf of You.

1 Introduction

These Data Processing Terms reflect the parties' agreement on the terms governing the processing and security of Your Personal Data in connection with the Data Protection Legislation.

2 Definitions

Capitalized terms used in these Data Processing terms, but not defined below, will have the meaning assigned to them in the Cloudmore Master Agreement.

"**Your Personal Data**" means Personal Data that is processed by Cloudmore on behalf of You in Cloudmore's provision of the Services.

"**Data Incident**" means a breach of Cloudmore's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Your Personal Data on systems managed by or otherwise controlled by Cloudmore. "Data Incidents" will not include unsuccessful attempts or activities that do not compromise the security of Your Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

"**Data Protection Legislation**" means, as applicable: (a) the GDPR including UK GDPR; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland).

"**Data Subject Tool**" means a tool (if any) made available by a Cloudmore Entity to Data Subjects that enables Cloudmore to respond directly and in a standardized manner to certain requests from Data Subjects in relation to Your Personal Data (for example, online advertising settings or an opt-out browser plugin).

"**EEA**" means the European Economic Area.

"**GDPR**" means Regulation (EU) 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.

"**Cloudmore Entity**" means Cloudmore AB or any other Affiliate of Cloudmore AB.

"Security Documentation" means any documentation that Cloudmore may make available in respect of the Services.

"Security Measures" has the meaning given in Section 7.1.1 (Cloudmore's Security Measures).

"Standard Contractual Clauses" means Standard Contractual clauses for the transfer of Personal Data to controllers or processors (as appropriate) established in third countries approved by the European and incorporated as Schedule 1 and 2 to these Data Processing Terms.

"Sub-Processors" means third parties authorized under these Data Processing terms to have logical access to and process Your Personal Data in order to provide parts of the Services and any related technical support.

"Third-party Sub-Processors" has the meaning given in Section 10.1 (Consent to Sub-Processor Engagement).

The terms "**Controller**", "**Data Subject**", "**Personal data**", "**Processing**", "**Processor**" and **"Supervisory Authority"** as used in these Data Processing Terms have the meanings given in the GDPR.

Any reference to a legal framework, statute or other legislative enactment is a reference to it as amended or re-enacted from time to time.

3 Duration of these Data Processing Terms

These Data Processing Terms will take effect on the Agreement Effective Date and, notwithstanding expiry of the Term, remain in effect until, and automatically expire upon, deletion of all Your Personal Data by Cloudmore as described in these Data Processing Terms.

4 Application of Data Protection Legislation

These Data Processing terms will only apply to the extent that the Data Protection Legislation applies to the processing of Your Personal Data.

5 Processing of Data

5.1 Nature and Purpose of the Processing

Cloudmore will be processing (including, as applicable to the Services and the instructions described in Your Instructions), collecting, recording, organizing, structuring, storing, altering, retrieving, using, disclosing, combining, erasing, and destroying) Your Personal Data for the purpose of providing the Services and any related technical support to You in accordance with these Data Processing Terms.

5.2 Roles and Regulatory Compliance; Authorization

The parties acknowledge and agree that:

a. Cloudmore is a processor of Your Personal Data under the Data Protection Legislation;
b. You are a controller or processor, as applicable, of Your Personal Data under the Data Protection Legislation; and
c. each party will comply with the obligations applicable to it under the Data Protection Legislation with respect to the processing of Your Personal Data.

Your Personal Data may include the types of personal data described at http://web.cloudmore.com/privacy/Services.

If You are a processor, You warrant to Cloudmore that Your instructions and actions with respect to Your Personal Data, including its appointment of Cloudmore as a processor, have been authorized by the relevant controller.

5.3 Categories of Data Subjects

Your Personal Data will concern the following categories of Data Subjects:

a. Data Subjects about whom Cloudmore collects personal data in its provision of the Services; and/or
b. Data Subjects about whom personal data is transferred to Cloudmore in connection with the Services by, at the direction of, or on behalf of You.

Depending on the nature of the Services, these Data Subjects may include individuals: (a) who have visited specific websites or applications in respect of which Cloudmore provides the Services; and/or (b) who are customers or users of Your products or Services.

5.4 Your Instructions

By entering into these Data Processing Terms, You instruct Cloudmore to process Your Personal Data only in accordance with applicable law:

a. to provide the Services and any related technical support;
b. as further specified via Your use of the Services (including in the settings and other functionality of the Services) and any related technical support;
c. as documented in the form of the Agreement, including these Data Processing terms; and
d. as further documented in any other written instructions given by You and acknowledged by Cloudmore as constituting instructions for purposes of these Data Processing Terms.

5.4.1 Cloudmore's Compliance with Instructions

Cloudmore will comply with the instructions described in Section 5.4 (Your Instructions) (including with regard to data transfers) unless EU or EU Member State law to which Cloudmore is subject requires other processing of Your Personal Data by Cloudmore, in which case Cloudmore will inform You (unless that law prohibits Cloudmore from doing so on important grounds of public interest).

5.4.2 Third-party Product

If You use any Third-party Product, the Services may allow that Third-party Product to access Your Personal Data as required for the interoperation of the Third-party Product with the Services. For clarity, these Data Processing Terms do not apply to the processing of Personal Data in connection with the provision of any Third-party Product used by You, including personal data transmitted to or from that Third-party Product.

6 Data Deletion

6.1 Deletion During Term

During the Term Cloudmore will comply with any reasonable request from You to delete or anonymize Your Personal Data, insofar as this is possible taking into account the nature and functionality of the Services and unless EU or EU Member State

law requires storage and will carry out this instruction as soon as reasonably practicable and within a maximum period of 180 days.

Cloudmore may charge a fee (based on Cloudmore's reasonable costs) for any data deletion under Section 6.1. Cloudmore will provide You with further details of any applicable fee, and the basis of its calculation, in advance of any such data deletion.

6.2 Deletion on Term Expiry

On expiry of the Term, You instruct Cloudmore to delete or anonymize all Your Personal Data (including existing copies) from Cloudmore's systems in accordance with applicable law. Cloudmore will comply with this instruction as soon as reasonably practicable and within a maximum period of 180 days, unless EU or EU Member State law requires storage.

7 Data Security

7.1 Cloudmore's Security Measures and Assistance

7.1.1 Cloudmore's Security Measures

Cloudmore will implement and maintain technical and organizational measures to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described at https://web.cloudmore.com/privacy (the "**Security Measures**"). Cloudmore may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Processor Services.

7.1.2 Security Compliance by Cloudmore Staff

Cloudmore will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Sub-Processors to the extent applicable to their scope of performance, including ensuring that all persons authorized to process Your Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.1.3 Cloudmore's Security Assistance

You agree that Cloudmore will (taking into account the nature of the processing of Your Personal Data and the information available to Cloudmore) assist You in ensuring compliance with any obligations of You in respect of security of personal data and personal data breaches, including (if applicable) Your obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR, by:

a. implementing and maintaining the Security Measures in accordance with Section 7.1.1 (Cloudmore's Security Measures);
b. complying with the terms of Section 7.2 (Data Incidents); and
c. providing You with the Security Documentation in accordance with Section 7.4.1 (Reviews of Security Documentation) and the information contained in these Data Processing Terms.

7.2 Data Incidents

7.2.1 Incident Notification

If Cloudmore becomes aware of a Data Incident, We will (i) notify You of the Data Incident without undue delay and in any event within 72 hours, unless ordered otherwise by law enforcement or government agency; and (ii) promptly take reasonable steps to minimize harm and secure Your Personal Data.

7.2.2 Details of Data Incident

Notifications made under Section 7.2.1 (Incident Notification) will describe, to the extent possible, details of the Data Incident, including steps taken to mitigate the potential risks and steps Cloudmore recommends You take to address the Data Incident.

7.2.3 Delivery of Notification

Cloudmore will deliver notification of any Data Incident to Your notification email address or, at Cloudmore's discretion (including if You have not provided a notification email address), by other direct communication (for example, by phone call or an in-person meeting). You are solely responsible for providing the notification email address and ensuring that the notification email address is current and valid.

7.2.4 Third-party Notifications

You are solely responsible for complying with incident notification laws applicable to You and fulfilling any third-party notification obligations related to any Data Incident.

7.2.5 No Acknowledgement of Fault by Cloudmore.

Cloudmore's notification of or response to a Data Incident under this Section 7.2 (Data Incidents) will not be construed as an acknowledgement by Us of any fault or liability with respect to the Data Incident.

7.3 You Security Responsibilities and Assessment

7.3.1 Your Security Responsibilities.

You agree that without prejudice to Cloudmore's obligations under Sections 7.1 (Cloudmore's Security Measures and Assistance) and 7.2 (Data Incidents):

a. You are solely responsible for Your use of the Services, including:
    i. making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of Your Personal Data; and
    ii. securing the account authentication credentials, systems and devices You use to access the Services.
b. Cloudmore has no obligation to protect Personal Data that You elect to store or transfer outside of Cloudmore's and our Sub-Processors' systems.

7.3.2 Your Security Assessment

You acknowledge and agree that (taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of the processing of Your Personal Data as well as the risks to individuals) the Security Measures implemented and maintained by Cloudmore as set out in Section 7.1.1 (Cloudmore's Security Measures) provide a level of security appropriate to the risk in respect of Your Personal Data.

7.4 Reviews and Audits of Compliance

7.4.1 Reviews of Security Documentation

To demonstrate compliance by Cloudmore with its obligations under these Data Processing Terms, Cloudmore will make the Security Documentation available for review by You.

7.4.2 Your Audit Rights

Cloudmore will allow You or a third-party auditor appointed by You to conduct audits (including inspections) to verify Cloudmore's compliance with its obligations under these Data Processing Terms in accordance with Section 7.4.3 (Additional Business Terms for Audits). Cloudmore will contribute to such audits as described in this Section 7.4 (Reviews and Audits of Compliance).

7.4.3 Additional Business Terms for Audits

a. You will send any request for an audit to Cloudmore as described in Section 13.1 (Contacting Cloudmore).
b. Following receipt by Cloudmore of an audit request under this Section, Cloudmore and You will discuss and agree in advance on the reasonable start date, scope and duration of, and security and confidentiality controls applicable to such audit.
c. Cloudmore may charge a fee (based on Cloudmore's reasonable costs) for any audit under Section 7.4.2. Cloudmore will provide You with further details of any applicable fee, and the basis of its calculation, in advance of any such audit. You will be responsible for any fees charged by any third-party auditor appointed by You to execute any such audit.
d. Cloudmore may object to any third-party auditor appointed by You to conduct any audit under Section 7.4.2 if the auditor is, in Cloudmore's reasonable opinion, not suitably qualified or independent, a competitor of Cloudmore or otherwise manifestly unsuitable. Any such objection by Cloudmore will require You to appoint another auditor or conduct the audit yourself.
e. Nothing in these Data Processing Terms will require Cloudmore either to disclose to You or Your third-party auditor, or to allow You or Your third-party auditor to access:
    i. any data of any other customer of a Cloudmore Entity;
    ii. any Cloudmore Entity's internal accounting or financial information;
    iii. any trade secret of a Cloudmore Entity;
    iv. any information that, in Cloudmore's reasonable opinion, could: (i) compromise the security of any Cloudmore Entity's systems or premises; or (ii) cause any Cloudmore Entity to breach its obligations under the Data Protection Legislation or its security and/or privacy obligations to You or any third-party; or
    v. any information that You or Your third-party auditor seeks to access for any reason other than the good faith fulfilment of Your obligations under the Data Protection Legislation.

8 Impact Assessments and Consultations

You agree that Cloudmore will (taking into account the nature of the processing and the information available to Cloudmore) assist You in ensuring compliance with any obligations in respect of data protection impact assessments and prior consultation, including (if applicable) Your obligations pursuant to Articles 35 and 36 of the GDPR, by:

a. providing the Security Documentation in accordance with Section 7.4.1 (Reviews of Security Documentation);
b. providing the information contained in these Data Processing Terms; and

c. providing or otherwise making available, in accordance with Cloudmore's standard practices, other materials concerning the nature of the Services and the processing of Your Personal Data.

9 Data Subject Rights

9.1 Responses to Data Subject Requests

If Cloudmore receives a request from a data subject in relation to Your Personal Data, Cloudmore will:

a. if the request is made via a Data Subject Tool, respond directly to the data subject's request in accordance with the standard functionality of that Data Subject Tool; or
b. if the request is not made via a Data Subject Tool, advise the data subject to submit the request to You, and You will be responsible for responding to such request.

9.2 Cloudmore's Data Subject Request Assistance

You agree that Cloudmore will (taking into account the nature of the processing of Your Personal Data and, if applicable, Article 11 of the GDPR) assist You in fulfilling any obligation to respond to requests by Data Subjects, including (if applicable) Your obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, by:

a. providing the functionality of the Services;
b. complying with the commitments set out in Section 9.1 (Responses to Data Subject Requests); and
c. if applicable to the Services, making available Data Subject Tools.

Cloudmore is entitled to remuneration for any potential costs and expenses if You request that Cloudmore shall assist You with responding to a Data Subject's request to exercise his or her rights according to Applicable Data Protection Laws.

10 Sub-Processors

10.1 Consent to Sub-Processor Engagement

You specifically authorize the engagement of Cloudmore's Affiliates as Sub-Processors. In addition, You generally authorize the engagement of any other third parties as Sub-Processors ("Third-party Sub-Processor").

10.2 Information about Sub-Processors.

Information about Sub-Processors is available per Service at https://web.cloudmore.com/privacy/sub-processsors.

10.3 Requirements for Sub-Processor Engagement

When engaging any Sub-Processor, Cloudmore will:

a. ensure via a written contract that:
    i. the Sub-Processor only accesses and uses Your Personal Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Agreement (including these Data Processing Terms); and
    ii. if the GDPR applies to the processing of Your Personal Data, the data protection obligations set out in Article 28(3) of the GDPR are imposed on the Sub-Processor; and
b. remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Sub-Processor

10.4 Opportunity to Object to Sub-Processor Changes

When any new Third-party Sub-Processor is engaged during the Term, Cloudmore will, at least 30 days before the new Third-party Sub-Processor processes any of Your Personal Data, inform You of the engagement (including the name and location of the relevant Sub-Processor and the activities it will perform) by updating the Sub-Processor list at https://web.cloudmore.com/privacy/sub-processsors and by providing a notification to Your notification email address.

You may object to Cloudmore's assignment of a Third-Party Sub-Processor that shall Process Personal Data on behalf of You within 30 days of being informed of the engagement of the new Third-party Sub-Processor, whereby the Parties shall seek to agree on a solution which is acceptable to both Parties. If a mutual acceptable solution cannot be reached, You may terminate the corresponding Service Subscription Agreement immediately upon written notice to Cloudmore. This termination right is Your sole and exclusive remedy if You objects to any new Third-party Sub-Processor.

11 Transfer to and processing of personal data in a third country

Cloudmore is entitled to transfer Personal Data belonging to You, to a Third Country, provided that:

a. the Third Country according to a decision issued by the EU Commission provides an adequate level of protection for Personal Data which comprises the Processing of Personal Data;

b. Cloudmore ensures that there are appropriate safeguards in place in accordance with Applicable Data Protection Laws, e.g. Standard Contractual Clauses adopted by the EU Commission under Applicable Data Protection Laws, that comprises the transfer and the Processing of Personal Data; epending on whether your role is that of a data controller or a data processor, Module Two (Schedule 1) or Module Three (Schedule 2) will apply accordingly or
c. if there are any other exemptions under Applicable Data Protection Laws that comprise the Processing of Personal Data.

For the avoidance of doubt, Personal Data may not be transferred to, or Processed in, a Third Country if none of the conditions outlined in Section 11 above exists.

12 Third Country Sub-Processor

Where a Sub-Processor is established in a Third Country which has not received an adequacy decision by the EU, the following will apply to the Processing:

a. You grant Cloudmore mandate to conclude relevant Standard Contractual Clauses, with such Sub-Processor in Your name and on Your behalf;
b. Module Three: Processor-to-Processor terms in the Standard Contractual Clauses apply (Cloudmore exporter);
c. You grant Cloudmore, on behalf of Third-Party Controller, mandate to conclude relevant Standard Contractual Clauses with such Sub-Processor, in Third-Party Controller's name and on Third-Party Controller's behalf; in this regard Module Three Clause 9 (a) option 2 applies and list of Sub-Processors is available at https://web.cloudmore.com/privacy/sub-processsors;
d. Clause 11 (a) second paragraph (optional language) shall not apply to the Standard Contractual Clauses
e. The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer is the Swedish Authority for Privacy Protection;
f. the provisions of the details of processing set out in Section 5 will be deemed to be incorporated into Appendix 1 of the Standard Contractual Clauses;
g. the security measures referred to in Clause 7.1.1 will be deemed to be set out in Appendix 2 to the Standard Contractual Clauses (where relevant); and
h. In the event of any conflict or contradiction between the terms of the Standard Contractual Clauses and any other agreement concluded between the Parties (if applicable), the provisions of the Standard Contractual Clauses shall prevail;
i. the Standard Contractual Clauses shall be subject to Swedish law and disputes arising from the Standard Contractual Clauses shall be subject the jurisdiction of Swedish courts unless the statutory jurisdiction of some other court applies.

You or Third-Party Controller remains the data exporter and Sub-Processors are the data importers under the Standard Contractual Clauses.

13 Contacting Cloudmore; Processing Records

13.1 Contacting Cloudmore

You may contact Cloudmore in relation to the exercise of Your rights under these Data Processing Terms via the methods described at http://web.cloudmore.com/privacy/contact/ or via such other means as may be provided by Us from time to time.

13.2 Cloudmore's Processing Records

You acknowledge that Cloudmore is required under the GDPR to:

a. collect and maintain records of certain information, including the name and contact details of each processor and/or controller on behalf of which Cloudmore is acting and (if applicable) of such processor's or controller's local representative and data protection officer; and
b. make such information available to the supervisory authorities.

Accordingly, You will, where requested and as applicable to You, provide such information to Cloudmore via the user interface of the Services or via such other means as may be provided by Cloudmore, and will use such user interface or other means to ensure that all information provided is kept accurate and up-to-date.

14 Liability

The provisions regarding liability under the Cloudmore Master Agreement shall apply correspondingly to these Data Processing terms.

15 Effect of these Data Processing Terms

If there is any conflict or inconsistency between the terms of these Data Processing terms and the Agreement, the Data Processing terms will govern unless specifically agreed otherwise in the respective Service Subscription Agreement. Subject to the amendment of these Data Processing Terms, the Service Agreement remains in full force and effect.

16 Changes to these Data Processing Terms

16.1 Changes to URLs

From time to time, Cloudmore may change any URL referenced in these Data Processing Terms and the content at any such URL. Cloudmore may only change the list of potential Services at https://web.cloudmore.com/privacy/services:

a. to reflect a change to the name of a Service;
b. to add a new Service; or
c. to remove a Service where either: (i) all contracts for the provision of that Service are terminated; or (ii) Cloudmore has Your consent.

16.2 Changes to Data Processing Terms

The Parties agree that these Data Processing Terms may be changed:

a. is expressly permitted by these Data Processing Terms, including as described in Section 16.1 (Changes to URLs);
b. reflects a change in the name or form of a legal entity;
c. is required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency; or
d. does not: (i) result in a degradation of the overall security of the Services; (ii) expand the scope of, or remove any restrictions on, Cloudmore's processing of Your Personal Data, as described in Section 5.4.1 (Cloudmore's Compliance with Instructions); and (iii) otherwise have a material adverse impact on Your rights under these Data Processing Terms.

16.2.1 Notification of Changes

If Cloudmore proposes a change to Data Processing Terms under Section 16.2(c) or (d), Cloudmore will notify You at least 30 days (or such shorter period as may be required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency) before the change will take effect by sending an email to Your notification email address. The Parties will then engage in good-faith negotiations to reach mutual agreement on the proposed changes.

16.2.2 Objection to Change

If You object to a proposed change under Section 16.2(d), You must notify Cloudmore within 30 days of receiving the notice of the proposed change. The Parties will seek to agree on a mutually acceptable solution. You understand that if You do not accept the proposed changes, Cloudmore may not be able to continue providing the Services under the current terms.. If a mutual acceptable solution cannot be reached, either Party may terminate the corresponding Service Subscription Agreement by providing 30 days' written notice to the other Party.

END

SCHEDULE 1 - Cloudmore EU Standard Contractual Clauses (Module 2: Controller-to-Processor)

Capitalized terms used but not defined in these Clauses have the meanings given to them in the Cloudmore Data Processing Terms.

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

1. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 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 (General Data Protection Regulation) ([1]) for the transfer of personal data to a third country.
2. The Parties:
    1. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
    2. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

3. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
4. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

1. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
2. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

1. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
    1. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
    2. Clause 8 – Clause 8.1(b), 8.9(a), (c), (d) and (e);

3. Clause 9 - Clause 9 (a), (c), (d) and (e);
4. Clause 12 – Clause 12(a), (d) and (f);
5. Clause 13;
6. Clause 15.1(c), (d) and (e);
7. Clause 16(e);
8. Clause 18 – Clause 18(a) and (b).

2. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

1. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
2. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
3. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Not used

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

1. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
2. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

1. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

2. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its

possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

4. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([4]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

1. (i) the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

2. (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

3. (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

4. (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

1. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

2. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

3. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

4. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

5. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

1. The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

2. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([8]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

3. The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

4. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

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

Clause 10

Data subject rights

1. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

2. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

3. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

1. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

2. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

3. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

    1. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

    2. refer the dispute to the competent courts within the meaning of Clause 18.

4. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

5. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

6. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

1. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

2. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

3. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

4. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

5. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

6. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

7. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

1. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.
   Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the

Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

2. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

1. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

2. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

    1. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

    2. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([12]);

    3. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

3. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

4. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

5. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

6. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by

the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

1. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

    1. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

    2. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

2. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

3. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

4. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

5. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

1. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

2. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

3. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

1. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

2. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

3. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

    1. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

    2. the data importer is in substantial or persistent breach of these Clauses; or

    3. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

4. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

5. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the Swedish law (*specify Member State*).

Clause 18

Choice of forum and jurisdiction

1. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

2. The Parties agree that those shall be the courts of the Sweden (*specify Member State*).

3. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

4. The Parties agree to submit themselves to the jurisdiction of such courts.

([1])Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.
([2]) Not applicable
([3]) Not applicable
([4]) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.
([5]) Not applicable
([6]) Not applicable
([7]) Not applicable
([8]) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.
([9]) Not applicable
([10]) Not applicable
([11]) Not applicable
([12]) As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: Cloudmore's Customer as specified in the Master Agreement and/or Subscription Agreement
Address: As specified in the Master Agreement and/or Subscription Agreement.

Contact person's name, position and contact details: Contact details for the data exporter are specified in the Master Agreement and/or Subscription Agreement. Details.

Activities relevant to the data transferred under these Clauses: The data importer provides the Services to the data exporter in accordance with the Master Agreement and/or Subscription Agreement.

Signature and date: The parties agree that execution of the this agreement and certification by the data exporter pursuant to Section 10.4 of the Data Processing Amendment shall constitute execution of these Clauses by both parties.

Role (controller/processor): controller

Data importer(s):

Name: Cloudmore Entity as specified in the Master Agreement and/or Subscription Agreement
Address: As specified in the Master Agreement and/or Subscription Agreement.

Contact person's name, position and contact details: Contact details for the data importer are specified in the Master Agreement and/or Subscription Agreement.

Activities relevant to the data transferred under these Clauses: The data importer provides the Services to the data exporter in accordance with the Master Agreement and/or Subscription Agreement.

Signature and date: The parties agree that execution of this agreement and certification by the data exporter pursuant to Section 10.4 of the Data Processing Amendment shall constitute execution of these Clauses by both parties.

Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Specified in the Cloudmore Data Processing Terms.

Categories of personal data transferred

Specified in the Cloudmore Data Processing Terms.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

In general, Cloudmore does not process sensitive personal data unless specifically instructed by the data controller. However, in cases where sensitive data (such as health data, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, or data concerning a person's sex life or sexual orientation) is transferred, the following safeguards shall apply:

- Strict purpose limitation to ensure data is used solely for its intended purpose.
- Access restrictions ensuring that only authorized personnel who have completed specialized data protection training can access the sensitive data.
- Record-keeping of all access to the data, including a register of the persons accessing the data and the reasons for access.

- Restrictions on onward transfers to third parties, requiring prior authorization by the data controller.
- Additional security measures, such as encryption both in transit and at rest, pseudonymization where feasible, and multifactor authentication for system access.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Customer Personal Data may be transferred on a continuous basis until it is deleted in accordance with the terms of the Data Processing Amendment.

Nature of the processing

The data importer will process Customer Personal Data to provide Services in accordance with the Master Agreement and/or Subscription Agreement.

Purpose(s) of the data transfer and further processing

The data importer will transfer Customer Personal Data to provide Services in accordance with the Master Agreement and/or Subscription Agreement

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

For the duration of the Master Agreement and/or Subscription Agreement and after that until deletion as agreed.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
As above.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The Swedish Supervisory Authority.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The data importer will implement and maintain security standards at least as protective as those set out in Appendix 2 to the Data Processing Amendment.

The technical and organisational measures to be taken by Subprocessors are described in the “Subprocessor Security” section of that Appendix.

In addition, the data importer will comply with Clause 10(b) (Data subject rights) by complying with its obligations The technical and organisational measures taken by the data importer to assist the data exporter in fulfilling its obligations to respond to data subjects’ requests for the exercise of their rights under Regulation (EU) 2016/679 are set out in Sections 8 (Impact Assessments and Consultations) and 9 (Access etc.; Data Subject Rights; Data Export) of the Data Processing Amendment.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:
See: https://web.cloudmore.com/privacy/sub-processsors.

SCHEDULE 2 - Cloudmore EU Standard Contractual Clauses (Module 3: Processor-to-Processor)

SECTION I

Clause 1

Purpose and scope

1. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 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 (General Data Protection Regulation) ([1]) for the transfer of personal data to a third country.

2. The Parties:

    1. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

    2. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

3. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

4. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

1. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

2. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

1. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

    1. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

    2. Clause 8 – Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

    3. Clause 9 – Clause 9(a), (c), (d) and (e);

    4. Clause 12 – Clause 12(a), (d) and (f);

    5. Clause 13;

6. Clause 15.1(c), (d) and (e);
7. Clause 16(e);
8. Clause 18 – Clause 18(a) and (b);

2. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

1. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
2. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
3. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Not used

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

1. The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.
2. The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.
3. The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

4. The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter ([5]).

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

1. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

2. The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

4. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

1. The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([6]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

    1. (i) the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

    2. (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

    3. (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

    4. (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

2. Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

1. The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

2. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

3. The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

4. The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

5. Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

6. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

7. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

1. The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

2. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

3. The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

4. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

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

Clause 10

Data subject rights

1. The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

2. The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the

appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

3. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

1. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

2. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

3. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

    1. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

    2. refer the dispute to the competent courts within the meaning of Clause 18.

4. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

5. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

6. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

1. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

2. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

3. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

4. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

5. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

6. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

7. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

1. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

   Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

2. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

1. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

2. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

    1. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

    2. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

    3. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

3. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

4. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

5. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The data exporter shall forward the notification to the controller.

6. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

1. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

    1. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

    2. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
    The data exporter shall forward the notification to the controller.

2. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

3. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.

4. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

5. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

1. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

2. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. The data exporter shall make the assessment available to the controller.

3. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

1. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

2. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

3. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

    1. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

    2. the data importer is in substantial or persistent breach of these Clauses; or

    3. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.
    In these cases, it shall inform the competent supervisory authority and the controller of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

4. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

5. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the Swedish law (*specify Member State*).

Clause 18

Choice of forum and jurisdiction

1. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
2. The Parties agree that those shall be the courts of the Sweden (*specify Member State*).
3. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
4. The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: Cloudmore's Customer as specified in the Master Agreement and/or Subscription Agreement
Address: As specified in the Master Agreement and/or Subscription Agreement.

Contact person's name, position and contact details: Contact details for the data exporter are specified in the Master Agreement and/or Subscription Agreement. Details.

Activities relevant to the data transferred under these Clauses: The data importer provides the Services to the data exporter in accordance with the Master Agreement and/or Subscription Agreement.

Signature and date: The parties agree that execution of the this agreement and certification by the data exporter pursuant to Section 10.4 of the Data Processing Amendment shall constitute execution of these Clauses by both parties.

Role (controller/processor): controller

Data importer(s):

Name: Cloudmore Entity as specified in the Master Agreement and/or Subscription Agreement
Address: As specified in the Master Agreement and/or Subscription Agreement.

Contact person's name, position and contact details: Contact details for the data importer are specified in the Master Agreement and/or Subscription Agreement.

Activities relevant to the data transferred under these Clauses: The data importer provides the Services to the data exporter in accordance with the Master Agreement and/or Subscription Agreement.

Signature and date: The parties agree that execution of this agreement and certification by the data exporter pursuant to Section 10.4 of the Data Processing Amendment shall constitute execution of these Clauses by both parties.

Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Specified in the Cloudmore Data Processing Terms.

Categories of personal data transferred

Specified in the Cloudmore Data Processing Terms.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

In general, Cloudmore does not process sensitive personal data unless specifically instructed by the data controller. However, in cases where sensitive data (such as health data, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, or data concerning a person's sex life or sexual orientation) is transferred, the following safeguards shall apply:

- Strict purpose limitation to ensure data is used solely for its intended purpose.
- Access restrictions ensuring that only authorized personnel who have completed specialized data protection training can access the sensitive data.
- Record-keeping of all access to the data, including a register of the persons accessing the data and the reasons for access.
- Restrictions on onward transfers to third parties, requiring prior authorization by the data controller.
- Additional security measures, such as encryption both in transit and at rest, pseudonymization where feasible, and multifactor authentication for system access.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Customer Personal Data may be transferred on a continuous basis until it is deleted in accordance with the terms of the Data Processing Amendment.

Nature of the processing

The data importer will process Customer Personal Data to provide Services in accordance with the Master Agreement and/or Subscription Agreement.

Purpose(s) of the data transfer and further processing

The data importer will transfer Customer Personal Data to provide Services in accordance with the Master Agreement and/or Subscription Agreement

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

For the duration of the Master Agreement and/or Subscription Agreement and after that until deletion as agreed.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
As above.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The Swedish Supervisory Authority.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The data importer will implement and maintain security standards at least as protective as those set out in Appendix 2 to the Data Processing Amendment.

The technical and organisational measures to be taken by Subprocessors are described in the "Subprocessor Security" section of that Appendix.

In addition, the data importer will comply with Clause 10(b) (Data subject rights) by complying with its obligations The technical and organisational measures taken by the data importer to assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 are set out in Sections 8 (Impact Assessments and Consultations) and 9 (Access etc.; Data Subject Rights; Data Export) of the Data Processing Amendment.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:
See: https://web.cloudmore.com/privacy/sub-processsors.