## Changelog

| CHANGE | VERSION |
| --- | --- |
| 1.1. | Clauses 9.2. and 10.4., *(Corrected cross-references).* |
| 1.2 | Clause 7.6 (*now made optional and amended wording*) |
| | |

## Standard Contractual Clauses

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

between

The customer using EthNote
(With details as entered into the account page on EthNote)

(the data controller)

and

EthNote
Copenhagen Center for Social Data Science (SODAS)
Københavns Universitet
CVR 29979812
Øster Farimagsgade 5A
København K
Denmark

(the data processor)

each a ‘party’; together ‘the parties’

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

# 1. Table of Contents

## 2. Preamble



1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

3. In the context of the provision of EthNote, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

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

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

7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

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

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

11. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

## 3. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

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

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

## 4. The data processor acts according to instructions

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

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

## 5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

## 6. Security of processing

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

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

   a. Pseudonymisation and encryption of personal data;

   b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

   c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

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

2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

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

## 7. Use of sub-processors

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

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

3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

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

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

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

5. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

## 8. Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

    a. transfer personal data to a data controller or a data processor in a third country or in an international organization

    b. transfer the processing of personal data to a sub-processor in a third country

    c. have the personal data processed in by the data processor in a third country

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

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

## 9. Assistance to the data controller

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

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

a. the right to be informed when collecting personal data from the data subject
b. the right to be informed when personal data have not been obtained from the data subject
c. the right of access by the data subject
d. the right to rectification
e. the right to erasure (‘the right to be forgotten’)
f. the right to restriction of processing
g. notification obligation regarding rectification or erasure of personal data or restriction of processing
h. the right to data portability
i. the right to object
j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor’s obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

   a. The data controller’s obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, the Danish Data Protection Agency (Datatilsynet) unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

   b. the data controller’s obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

   c. the data controller’s obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

   d. the data controller’s obligation to consult the competent supervisory authority, the Danish Data Protection Agency (Datatilsynet) prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

## 10. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

2. The data processor’s notification to the data controller shall, if possible, take place within 72 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller’s obligation to

notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

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

   b. the likely consequences of the personal data breach;

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

4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

## 11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done unless Union or Member State law requires storage of the personal data.

   The data processor commits to exclusively process the personal data for the purposes and duration provided for by this law and under the strict applicable conditions.

## 12. Audit and inspection

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

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

## 13. The parties' agreement on other terms

1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly

or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

## 14. Commencement and termination

1. The Clauses shall become effective on the date of both parties' signature.

2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

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

5. Upon agreeing to the EthNote Terms of Service this data processing agreement shall be considered enforceable and binding for both the data controller and the data processor as an integrated part of the Terms of Service.

## 15. Data controller and data processor contacts/contact points

1. The parties may contact each other using the following contacts/contact points:

2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

   The contact details of the data controller shall be kept up to date on the EthNote account page.

   The contact details of the data processor:

   Name: EthNote, Copenhagen Center for Social Data Science (SODAS) at the University of Copenhagen
   Point of contact: Emilie Munch Gregersen
   E-mail: emg@sodas.ku.dk

# Appendix A Information about the processing



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

The purpose of the data processor's processing of personal data on behalf of the data controller is to support the operation, maintenance, and enhancement of EthNote, a Software as a Service (SaaS) application designed for the collection, processing, and analysis of ethnographic as well as other unstructured qualitative and quantitative social data.

EthNote is currently in the pilot project stage, hosted within the Center for Social Data Science (SODAS) at the University of Copenhagen, and funded by the Innovation Fund Denmark. EthNote is accessible to researchers, students, and data analysts in public and private organizations for relevant projects, with access granted through tester agreements.

### A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

The nature of the processing activities carried out by the data processor on behalf of the data controller include:

- **Data Storage and Management**: Securely storing and organizing ethnographic and other personal data collected through EthNote, ensuring data integrity and accessibility for authorized researchers, students and data analysts in public and private organizations.
- **Data Analysis, Modelling, and Visualization:** Securely analyzing, modelling, and visualizing ethnographic and other personal data collected through EthNote via EthNote's self-developed analytical modules based on open-source software...

- **Performance Optimization**: Ensuring that EthNote operates efficiently, handling the demands of ethnographic as well as other social science research and other analytics projects by optimizing system performance and scalability.

- **Security Measures**: Implementing robust security protocols to protect sensitive ethnographic as well as other unstructured qualitative and quantitative social data from unauthorized access and potential breaches, ensuring a secure environment for research and analytics activities.

- **Error-Handling and Bug-Fixing**: Proactively identifying, tracking, and resolving any software errors or bugs to maintain EthNote's reliability, ensuring that researchers, students, and data analysts in public and private organizations can carry out their projects without disruption.

- **Data Backup and Disaster Recovery**: Regularly backing up data and implementing disaster recovery procedures to guarantee the continuity of research and other social science analysis activities and data availability, even in the event of system failures.

- **User Access and Authentication**: Managing user access to EtnNote through secure authentication processes, ensuring that only authorized researchers, students and data analysts in public and private organizations can access and work with the collected data.

- **Compliance with relevant Standards**: Adhering to relevant industry standards and best practices in data protection and information security, ensuring that the processing activities are compliant with legal and regulatory requirements.

- **Data Retention and Deletion**: Managing data retention policies to ensure that other and personal data are stored only as long as necessary for research and other analytics purposes, with clear procedures for data deletion when no longer needed or upon request.

- **Service Monitoring and Continuous Improvement**: Continuously monitoring EthNote's performance and gathering user feedback to implement ongoing improvements, ensuring that EthNote remains a valuable and effective tool for ethnographic and other qualitative and/or quantitative social science research and analysis.

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

Given the adaptable nature of EthNote, which allows data controllers to tailor EthNote to the specific needs of their research and other social scientific analysis projects, the types of personal data processed can vary widely depending on the data controller's choices.
The data controller retains full discretion over the selection of data categories.
As such, the processing may include all categories and types of personal data

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

Given the adaptable nature of EthNote, which allows data controllers to tailor EthNote to the specific needs of their research and other social scientific analysis projects, the categories of data subjects whose personal data may be processed can vary widely depending on the data controller's choices.
The data controller retains full discretion over the selection of data subjects.
As such, the processing may include all categories of data subjects.

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

The processing will continue for the duration of the agreement between the data controller and the data processor, or until all personal data has been deleted or returned in accordance with the data controller's instructions and the terms outlined in the Clauses.

## Appendix B Authorised sub-processors



### B.1. Approved sub-processors

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

| NAME | CVR | ADDRESS | PROCESSING LOCATION | DESCRIPTION OF PROCESSING |
|---|---|---|---|---|
| Supabase | 202005760H | 970 Toa Payoh North #07-04, Singapore 318992 | aws \| eu-central-1 | We use Supabase services to store user data comprising of notes, notifications, comments and account data such as email and username on a PostgreSQL Database located on encrypted AWS servers in eu-central-1. Supabase is SOC2 Type 2 certified. |
| AWS S3 (Amazon Inc) | 14326919 | 410 Terry Ave N, Seattle, Washington, 98109-5210, United States | Europe (Frankfurt) eu-central-1 | We use the file storage service AWS S3 to store user data comprising of all types of attachments (images, audio, video and documents) uploaded to notes on an object storage service that stores the data in NoSQL databases on encrypted AWS servers in eu-central-1. AWS S3 is SOC2 Type 2 certified and provide SOC 1, SOC 2 and SOC 3 reports twice a year. |
| AWS SES (Amazon Inc) | 14326919 | 410 Terry Ave N, Seattle, Washington, 98109-5210, United States | Europe (Frankfurt) eu-central-1 | We use the email service AWS SES for sending emails with one-time-passwords, invitations to projects and notifications about comments. |
| Google Maps API (Alphabet Inc) | 07525279 | 1600 Amphitheatre Parkway Mountain View, CA 94043 United State | europe-west1 (Belgium) | We use Google Maps API for finding locations based on user-submitted geolocation data. We also use their map service to show the location on a map. |

| NAME | CVR | ADDRESS | PROCESSING LOCATION | DESCRIPTION OF PROCESSING |
|---|---|---|---|---|
| Google Cloud Run (Alphabet Inc.) | 07525279 | 1600 Amphitheatre Parkway Mountain View, CA 94043 United State | europe-west1 (Belgium) | We use the hosting service Google Cloud Run to host our application |
| Pubnub | 11964015 | 1045 17th Street Suite 204 San Francisco, CA 94107 United States | EU Central | We use the real-time service Pubnub to notify users real time about any comments on notes or invitations to projects. |
| Prozense ApS | 39161877 | C/O N. B. Andersen Spinderigade 14, 2. th, Denmark | Denmark | Prozense handles the software development, testing and troubleshooting for EthNote. |

The data controller shall on the commencement of the Clauses authorise the use of the above-mentioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

## Appendix C Instruction pertaining to the use of personal data

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

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

The data processor shall carry out the processing activities as outlined in Section A.2 to ensure the operation, maintenance, and enhancement of EthNote.

### C.2. Security of processing

The level of security shall take into account the nature, scope, context, and purposes of the processing activities, as well as the risks posed to the rights and freedoms of natural persons. Given that EthNote is designed for the collection, processing, and analysis of potentially sensitive ethnographic as well as other unstructured qualitative and quantitative social data, a **high level of security must be established** to protect personal data, particularly when it involves special categories of personal data as defined under Article 9 GDPR.

For the avoidance of doubt, the security of personal data related to endpoints from where the data controller accesses the systems of the data processor (for example web clients and apps) is the sole responsibility of the data controller, e.g. disk encryption and anti-malware on smartphones and other devices of the users of the data controller.

The data processor shall be both entitled and obligated to make decisions about the technical and organizational security measures that are necessary to achieve the required and agreed-upon level of data security. However, the data processor must implement the following minimum measures, which have been agreed upon with the data controller:

**Encryption of Personal Data**

- Encryption: All personal data must be encrypted both in transit and at rest using strong encryption methods. This ensures that data is protected during transmission between the data controller and the data processor.

**Ensuring Ongoing Confidentiality, Integrity, Availability, and Resilience**

- System and Service Testing: All developments and updates to EthNote must be rigorously tested in a staging environment before being deployed to production. Regular testing in the production environment ensures the smooth operation and security of EthNote.

- Confidentiality: Access to personal data should be restricted to authorized personnel only, using secure authentication and access control mechanisms. Additionally, admin / privileged access shall be restricted, requiring additional authentication security and only granted under justified circumstances.

- Integrity: Measures must be in place to ensure that personal data cannot be altered or tampered with during processing.

- Availability: EthNote must be designed to remain operational and accessible to authorized users, even in the face of potential disruptions or high demand.

- Resilience: EthNote should be capable of withstanding and recovering from potential threats, such as cyberattacks or hardware failures.

**Restoring Availability and Access to Personal Data**

- Data Backup: Personal data shall be backed up regularly to ensure that it can be restored in the event of a data loss incident. Backup procedures must include redundancy and off-site storage to protect against physical or technical incidents.

- Disaster Recovery: A comprehensive disaster recovery plan must be in place to ensure that, in the event of a system failure, personal data can be restored quickly, and services can be resumed with minimal downtime.

**Regular Testing, Assessment, and Evaluation of Security Measures**

- Continuous Monitoring: EthNote’s security shall be continuously monitored to detect and respond to any threats or anomalies in a timely manner.

**Access to Data Online**

- Controlled Access: Access to personal data stored online must be controlled through secure authentication methods, with single factor sign-on via email available for all users with broad access to personal data.

- Session Management: Sessions shall be automatically terminated after a period of inactivity to prevent unauthorized access.

- Protection against brute-force attacks: User accounts shall be temporarily deactivated if attempts at brute-force logins are detected, for example after 10 failed login attempts within a one hour period.

**Protection of Data During Transmission**

- Encryption in Transit: Data transmitted between the data controller and the data processor must be encrypted using secure protocols to ensure confidentiality and integrity.

- Secure Communication Channels: All communication channels must be secured against interception and unauthorized access.

**Protection of Data During Storage**

- Encryption at Rest: Personal data stored on physical devices must be encrypted to protect against unauthorized access, particularly in the event of a breach.

- Key Management: Encryption keys must be securely managed and protected against unauthorized access.

**Physical Security of Locations**

- Secure Facilities: The physical locations where personal data is processed or stored must have strong security measures in place, including access controls, surveillance, and environmental protections.

**Use of Home/Remote Working**

- Secure Remote Access: Employees working remotely must use secure connections, such as VPNs, and follow strict security protocols to protect personal data.

- Device Security: Personal data accessed remotely must be stored and processed on secure devices that are protected by encryption, strong passwords, and up-to-date security software.

**Logging Requirements**

- Audit Logs: Comprehensive logging must be implemented to record access to and actions performed on personal data. These logs should be regularly reviewed to detect and respond to unauthorized access or anomalies.

- Log Retention: Logs should be retained for a period of minimum 13 months as recommended by CFCS (the national Danish IT security authority: The Centre for Cyber Security) to ensure traceability and accountability while complying with relevant legal and regulatory requirements.

**C.3. Assistance to the data controller**

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

Taking into account the nature of the processing activities carried out through EthNote, the data processor shall assist the data controller by providing appropriate technical and organizational measures to fulfil the data controller's obligations under Chapter III of the GDPR. This assistance is facilitated primarily through the self-service functions available within EthNote, allowing the data controller to efficiently manage and respond to data subject rights requests. Specifically, these measures include:

- Right to be Informed: EthNote is not designed to interact directly with data subjects and as such does not include any functions related to the right to be informed, such as privacy notices.

- Right of Access: EthNote includes functionalities for the data controller to update or correct any inaccurate or incomplete personal data upon the data subject's request.

- Right to Rectification: EthNote includes functionalities for the data controller to update or correct any inaccurate or incomplete personal data upon the data subject's request.

- Right to Erasure ('Right to be Forgotten'): The data controller can utilize EthNote's self-service tools to delete personal data in compliance with data subject requests, ensuring that such data is removed from the system within the required timelines.

- Right to Restriction of Processing: Ethnote does not have any functionality regarding restriction of processing. The data controller must handle this manually for example by moving the personal data to an Excel spreadsheet or another place of their choosing.

- Notification Obligations: EthNote is not designed to interact directly with data subjects and as such does not include any functions related to the notification obligations of GDPR.

- Right to Data Portability: EthNote facilitates the export of personal data in a structured, commonly used, and machine-readable format, enabling the data controller to comply with data portability requests.

- Right to Object: EthNote does not have any functionality that supports the right to object. This must be handled manually by the data controller.

- Right Not to be Subject to Automated Decision-Making: EthNote does not contain any functionality related to automated decision-making, including profiling, that significantly affects data subjects.

In addition to the functions supporting data subject rights requests, the data processor shall also, at additional cost, assist the data controller in meeting compliance obligations related to Data Protection Impact Assessments (DPIA) including consultation with the Supervisory Authorities, data breach handling and related services.

**C.4. Storage period/erasure procedures**

*EthNote enables data controller to delete personal data manually whilst having an account. If data controller uses the Services to delete any data.*

*Personal data is stored for as long as the data controller remains a user.*

*Upon termination of the provision of personal data processing services, the data processor shall delete the data in EthNote, including any personal data, in accordance with Clause 11.1., unless the data controller – after the entering into the agreement – has modified the data controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.*

**C.5. Processing location**

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

As described in section B, the addresses of our data processors and at any subsequent processors as well as at any remote work locations.

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

While we do not carry out any third country transfers of personal data directly, we do use the global sub-processors as described in section B above. These have world-wide support staff and sub-contractors all over the world.
The controller accepts such transfers when entering into this agreement.

If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

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

*The data processor shall at any time upon the request of the data controller and at the data controller's expense prove the compliance with the obligations laid down in this Data Processing Agreement by suitable means, including self-audits and certificates. The data controller is obliged to provide information to the data controller to the extent that this is necessary to carry out the inspection as defined above.*
*If necessary in individual cases, the data controller may demand an inspection of the data processed by the data processor for the data controller and of the data processing systems and programs used.*

*After prior notification and with a reasonable period of notice, the data controller may carry out the inspection within the meaning of the above defined at the data controller's premises during normal business hours. In doing so, the data controller shall ensure that the inspections are only carried out to the extent necessary to avoid disproportionately disturbing the data processor's business operations. The parties assume that an inspection is required at most once a year. Further inspections shall be justified by the data controller, stating the reason. In the case of on-site inspections, the data controller shall reimburse the data processor for the expenses incurred, including personnel costs, for the supervision and accompaniment of the inspectors on site to a reasonable extent. The bases for the calculation of costs will be communicated to the client by the data processor before the inspection is carried out. The data processor may make the controls dependent on prior notification with an appropriate lead time and on the signing of a confidentiality agreement. If the inspector commissioned by the data controller is in a competitive relationship with the data processor, the data processor has a right of objection.*

*At data controller's option, proof of compliance with the technical and organizational measures may also be furnished, instead of an on-site inspection, by the submission of a suitable, up-to-date audit certificate, reports or report extracts from independent bodies (e.g. auditors, revision, data protection officer, IT security department, data protection auditors or quality auditors) or suitable certification, if the audit report enables the data controller to satisfy itself in a reasonable manner that the technical and organizational measures in with this Data Processing Agreement are being complied with.*

*Based on the results of such an audit/inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.*

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

*The data processor shall at any time upon the request of the data controller and at the expense of the data controller prove the compliance of the chosen sub-processors with the obligations laid down in this Data Processing Agreement by suitable means, including self-audits and certificates. A copy of data processing agreement(s) with sub-processors and any subsequent amendments to these must be sent to the data controller following the data controller's request for this to ensure that corresponding data protection obligations to those applicable under this agreement have been imposed on the sub-processor.*

*The data processor must document how the data processor continuously ensures that sub-processors comply with the same data protection obligations as those stipulated in the data processing agreement between the data controller and the data processor.*

*Once a year, the data processor must, for its own account, present a declaration or an inspection report from an independent third party regarding the sub-processor's compliance with the General Data Protection Regulation, data protection regulations in other Union law or Member State law and this agreement.*

**Appendix D The parties' terms of agreement on other subjects**