Appendix [1] to Searis Terms of Service

Data Processing Agreement

BETWEEN:

Searis AS
Org.nr: 998 870 135
Krambugata 2
7011 Trondheim
Norway

("Searis" or the “Processor”)

AND

Customer for which Searis processes personal data

("Customer" or “Controller”)

hereinafter referred to individually as a “Party” or together as the “Parties”.

1. Background and purpose

Clarify is a software as a service tool developed by Searis, and made available to its customers as a subscription service. Searis delivers the Clarify application and associated services in accordance with the terms and conditions set out in Searis “Terms of Service” and the Searis "End User Terms" (collectively "Main Agreement").

This Data Processing Agreement (“DPA”) applies to Customers who uses the Clarify application and services in a way that involve processing of personal data. Clarify enables the Customer’s employees to upload any kind of information or data and Searis is not involved in uploading or facilitating such data entry.

The DPA sets out the regulates the responsibilities and obligations of the Parties where the Customer holds the role as Controller and Searis process personal data on their behalf, as Processor.

Where this DPA applies, the Processor will only process personal data for the purpose of fulfilling its obligations under the Main Agreement, on behalf of the Controller.

This DPA shall supplement any other agreements that the Parties have signed, such as purchase agreements, Terms of Service, End User Terms and Privacy Policy.

In the event of any conflicts between this DPA and other agreements between the Parties, this DPA shall take precedence with respect to the processing of personal data.

2. Obligations of the Controller

When the Customer uses Clarify in a way that entails uploading personal data, Customer will be responsible as Controller for personal data processed in the tool. When operating as a Controller, Customer must comply with its obligations pursuant to applicable national data protection legislation (for Norway, the Personal Data Act 2018) and the EU General Data Protection Regulation ("GDPR"), as well as the Main Agreement and this DPA.

3. Obligations of the Processor

When the Customer uses Clarify in a way that entails uploading personal data, Searis will take on the role and responsibility as Processor on behalf of the Customer.

3.1. General obligations

The Processor shall not:

a. process personal data for any other purposes or to a greater extent than provided for by this DPA.
b. process personal data beyond what is needed to comply with the obligations pursuant to the Main Agreement.
c. in any way disclose, pass on or transfer personal data on its own initiative unless this has been agreed in advance with the Controller or the Controller has given its prior written approval.
d. process personal data that it gains access to or becomes a party to through its work for the Controller in any other way than described in this DPA.

The Processor shall:

a. maintain up-to-date records of all of the categories of processing activities performed on behalf of the Controller, and maintain a list of all types of data processing.
b. provide the Controller with access to personal data processed by the Processor on behalf of the Controller, through providing access to the Clarify tool.
c. ensure that anyone given access to personal data processed on behalf of the Controller is familiar with this DPA and is subject to confidentiality obligations.
d. ensure that the Processor's systems comply with applicable requirements relating to data protection by design and by default. This includes implementing functionality to comply with data protection principles and functionality to protect the rights of data subjects.
e. give the Controller the support needed to fulfil its obligations to the data subjects in connection with Clarify.
f. facilitate data access mechanisms in cooperation with the Controller in order to enable the data subjects to exercise their rights with respect to accessing their personal data in Clarify, including responding to enquiries from data subjects who wish to exercise their rights.
g. immediately inform the Controller if the Processor believes that it has been given an instruction that contravenes the GDPR or other applicable data protection regulation.

3.2. Technical and organisational security measures

The Processor will adopt and implement adequate technical and organisational security measures that are needed to ensure compliance with applicable data protection regulation.

The Processor shall:

a. establish and implement such measures in order to ensure confidentiality, integrity, availability and resilience of personal data processed in Clarify. This may include, amongst other things and depending on risk, adequate measures to prevent accidental or unlawful destruction or loss of data, unauthorised access to or dissemination of data, or any other use of personal data that is not in accordance with this DPA, as well as measures to make the data available and accessible again after any incidents.
b. have authorisation and management procedures in place to secure access to systems and data. Access to staff and partners shall be granted on a need to know basis.
c. establish the systems and procedures needed to ensure information security and deal with any personal data security breaches, including procedures for reporting breaches, restoring normal conditions, eliminating the cause of breaches and preventing their recurrence. If requested, the Processor shall give the Controller access to relevant security documentation and the systems used to process personal data.

d. find, record, report, document and close identified gaps related to personal data security breaches, including logging and documenting any attempt at unauthorised access and other personal data security breaches.
e. if a personal data security breach is suspected or confirmed, immediately notify the Controller. The notification shall describe the breach including its cause, duration and when it was discovered, the categories and approximate number of data subjects concerned, the categories and approximate number of personal data records concerned, the name and contact details of contact points where more information can be obtained, the likely consequences of the breach and which immediate measures have been implemented or are being considered to deal with the breach.
f. assist the Controller to comply with its obligations pursuant to GDPR Articles 32–34.
g. in conjunction with security audits performed by the Controller or a third party appointed by the Controller make available internal audit reports, internal procedures and routines, security architecture, risk and vulnerability assessments including mitigation measures and other documents of relevance to the audit.

notify the Controller of any circumstances that entail a change in the level of risk.

4. Use of subprocessors

By entering into the Main Agreement, the Controller has approved that the Processor use subprocessors to fulfil its obligations under the Main Agreement and DPA. The Processor will use the subprocessors specified in **Attachment 3** for the services indicated there and confirms that no other subprocessors will be used without prior notice.

Further, the Processor shall:

a. ensure that subprocessors are bound by obligations equivalent to the terms set out in this DPA, including confidentiality obligations.
b. ensure that subprocessors only process personal data in accordance with this DPA and only in so far as is necessary to perform the particular service supplied by the subprocessor.
c. keep an up-to-date list of the identity and location of the subprocessor specified in Attachment 3. The up-to-date list shall be available to the Controller on the www.clarify.us webpage.
d. In due course notify the Controller of any plans to use additional subprocessors or replace subprocessors. The Controller may object to the change only upon reasonable grounds due to data protection concerns.
e. upon the termination of the Main Agreement, ensure that subprocessors fulfil their obligation to erase or securely destroy all personal data, including any copies and backups of the data, unless further storage is required by law.

When operating as Processor, the Processor will at all times be fully responsible to the Controller for any work performed by subprocessors and for the subprocessors' compliance with the provisions of this DPA.

Third parties other than the Processor's subprocessors may only be given access to personal data if the Parties have signed a separate specific agreement to that effect, or if under legal obligation to disclose.

5. Transfers of personal data to third countries

Any transfer of personal data to third countries by the Processor shall only occur on the basis of documented instructions from the Controller.

If any Controller data originates from a third country (other than an EEA country) with one or more laws imposing data transfer restrictions or prohibitions and Controller has informed Processor of such data transfer restrictions or prohibitions, Controller and Processor shall ensure appropriate transfer mechanism (satisfying the country's data transfer requirement(s)) is in place, as reasonably requested by Controller and mutually agreed upon by both Parties, before transferring or accessing Controller's data outside of such country.

The Processor shall not be held responsible for actions of the Controller. The Controller is not entitled to use the Clarify tool in any country with data localization laws that would require Controller's environment to be hosted in said country.

6. Duration and termination of the DPA

This DPA becomes effective at the same time as the Main Agreement and will remain in effect for as long as the Main Agreement is in effect.

In the event of termination of the Main Agreement, this DPA will also terminate.

However, the Processor remains subject to the obligations stipulated in this DPA, as long as the Processor processes personal data on behalf of the Controller.

Upon termination of the Main Agreement, the Processor is obliged to, upon request of the Controller, delete all personal data to the Controller, as well as to delete existing copies, unless retention of personal data is prescribed by EU/EEA or national law.

7. Breach of contract, liability

Rights, obligations and liability in event of breach of contract is regulated in the Main Agreement.

8. Choice of law and legal venue

Choice of law and legal venue is regulated in the Main Agreement.

ATTACHMENT 1

PURPOSE OF THE PROCESSING, DURATION, DATA AND PROCESSING ACTIVITIES

A. The purpose of and duration of the processing

The Processor is a software development company. The Clarify tool is a software as a service application, which enables users to upload any kind of data to the tool for data management purposes. The content of this DPA reflects the limited amount of personal data the Processor handles on behalf of the Controller, when the Controller uploads personal data and use the Clarify tool in a manner that entails processing of personal data.

Personal data is stored with the Processor for the duration of the Main Agreement or until the Controller requests that the data is erased. Exceptions are data where there is a legal requirement for the Processor on further storage.

B. Processing of personal data

The following types of processing are covered by the DPA:

Type of processing	Processing activities
Structuring	The Controller may upload personal data in the Clarify tool or apply functionality that entails processing of personal data in the tool.
Storage	The Controller may upload personal data in the Clarify tool or apply functionality that entails storage of personal data in the tool.
Erasure or destruction	The Processor may, upon instructions from the Controller, erase or destruct uploaded data.
Disclosure/Transfer	The Processor may, upon instructions from the Controller or pursuant to legal obligations or court orders, disclose or transfer personal data to third parties.

C. Types of data

Personal data
Name
Address (billing)
Contact information including e-mail
IP-addresses
Names
Usernames
Membership information
Analytics and usage data
Order-history and information-Contracts
Communication
Support
Pictures
Additional types of personal data may occur, subject to Controllers use of the Clarify tool

D. Categories of data subjects

The Processor will be processing contact information on Controller’s actual, potential, or former customers and/or members, employees, suppliers, business and collaboration partners and affiliates.

The Processor put its products for the disposal of the Controller as a service, and it is not possible for Processor to fully determine or describe categories of data subjects. If the Controller host data on further categories of data subjects with the Processor it is the Controller’s obligation to register this information.

ATTACHMENT 2

DETAILED REQUIREMENTS RELATING TO INFORMATION SECURITY

1. Technical and organizational measures baseline Physical Access Controls

Processor shall take reasonable measures to prevent physical access, such as secured buildings, to prevent unauthorized persons from gaining access to personal data.

2. System Access Controls

Processor shall take reasonable measures to prevent personal data from being used without authorization. These controls shall vary based on the nature of the processing undertaken and may include, among other controls, authentication via passwords and/or two-factor authentication, documented authorization processes, documented change management processes and/or logging of access on several levels.

3. Data Access Controls

Processor shall take reasonable measures to provide that personal data is accessible and manageable only by properly authorized staff, direct database query access is restricted and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the personal data to which they have privilege of access; and, that personal data cannot be read, copied, modified or removed without authorization in the course of processing. The Processor shall take reasonable measures to implement an access policy under which access to its system environment, to personal data and other data by authorized personnel only.

4. Transmission Controls

Processor shall take reasonable measures to ensure that it is possible to check and establish to which entities the transfer of personal data by means of data transmission facilities is envisaged so personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport.

5. Input Controls

Processor shall take reasonable measures to provide that it is possible to check and establish whether and by whom personal data has been entered into data processing systems, modified or removed. Processor shall take reasonable measures to ensure that (i) the personal data source is under the control of data exporter; and (ii) personal data integrated into Processor’s systems is managed by secured file transfer from the Processor and data subject.

ATTACHMENT 3

AUTHORIZED SUB-PROCESSORS

Name	Area of service	Location
Auth0	Authorization	Germany & Ireland
Segment	Analytics	United States
Amplitude	Analytics	United States
Google Cloud	Cloud Service Provider	Finland
Mailchimp	Email service provider	United States
Apple	Push notifications	United States
Google	Push notifications	United States
Stripe	Payment processing	EU / United States
Intercom	Support	United States
Webflow	Web hosting / contact forms	United States
Statuspage	Uptime notifications	United States