

# Terms of service

Terms of Service for Access and Use of SESAM Software as a Service (SaaS)

## 1. Introduction

### 1.1. Purpose

This document contains terms of service for Customers' access to and use of SESAM Software as a Service ("Services") provided by SESAM.IO AS 922 409 676 ("SESAM"). The services consist of both free- and paid subscriptions and the term "Customer" is used regardless of whether a Subscription Fee applies to a particular Customer's account. Some sections of this document will only apply to Customers with an account with a defined Subscription Fee. Upon ordering access to the Services, and confirming acceptance of the terms of service in this document, a legally binding agreement ("Agreement") is entered into between SESAM and the Customer. All Services, as they are available at any time, through the portal <https://portal.sesam.io>, are subject to the terms of this Agreement.

Upon entering into this Agreement and the registration of the Customer in SESAM's systems, the Customer is given a right to use the Services on the terms in this Agreement. Once access to the Services has been granted, the Customer will receive an e-mail to its registered e-mail address with the necessary access and login details.

The Services consist of various sub-services, and the right to use the Services only comprise the individual sub-services which the Customer has ordered, and received access to. Some of the Services are payable. The Customer's account overview sets out active sub-services which the Customer has ordered, including which Services are payable.

Some sub-services may be subject to additional terms and/or restrictions. Such additional terms and/or restrictions are set out in the terms of use for the sub-service together with the description of the sub-service in question.

### 1.2. Description of the Services

The Services are standardized services, and the Customer acknowledges that the functionality in the Services will change. The Customer is given the right to use the Services, with the functionality as provided from time to time. The right to use the Services is not connected to any specific version of the underlying software or any set functionality as provided at any time, but is rather connected to access to and use of the Services as they are at any given time. Details of the functionality of each of the Services can be found at <https://docs.sesam.io>.

## 2. The Right to use the Services

### 2.1. General

The Customer may set up Users and give these Users access to the Services with different roles (each individual referred to herein as a "User" and collectively as the "Users"). Users consist of natural persons in the employment or service of the Customer.

The Customer and the Customer's Users receive a worldwide, limited, terminable, non-exclusive and non-transferable right to use the Services in accordance with the terms of this Agreement, exclusively for the Customer's internal business purposes. This right is conditional on the payment of the applicable subscription fee and other fees ("Subscription Fee"). Any applicable Subscription Fee is provided on the Customer's account overview.

The Payment of the Subscription Fee and the compliance with the terms of this Agreement is a precondition for the right to use the Services.

SESAM may adjust the agreed Subscription Fee yearly, upon 3 months' written notice. In case of changes in public taxes, charges or other duties or other changes in public administrative practice affects the vendor's costs connected to the Service, the Subscription Fee may be adjusted correspondingly without prior notice.

The Customer may not allow a third party to use the Services in a service bureau or similar, or offer services dependent on the Services to a third party. However, the Customer may allow in- hire consultants or temporary employees to use the Services for Customers internal business purposes. The Customer may also use the Services to collect/deliver data from the applications and databases of the Customer's suppliers and/or customers.

The Services depend on standard software. When purchasing access to the Services, the Customer does not purchase a copy of, or license to, the software used to deliver the Services, but consecutively pay for a subscription to access the Services. To the extent that separate license- or other terms apply for use of third party software and/or services included in the Services, these are set out together with the description of the Services in question. Any terms for third party software and/or services take precedence over the terms of this Agreement.

## **2.2. The relationship between the Customer's Users and SESAM**

The Customer commits to adhere to the terms of this Agreement, and to ensure that any of its Users do the same. The Customer accepts the full responsibility for all activities connected to its Users, and its User's compliance with the terms of the Agreement. When the individual User accepts any terms upon logging into a Service, or on a later change of such terms, no Agreement is made between such individual User and SESAM. It is at all times the Customer who is party to any agreement with SESAM, and who has all rights and obligations set out in such agreement.

The Customer accepts that SESAM may contact the Customer, and any Customer administrators, through registered e-mail addresses and through telephone, and provide general marketing information or other information about the Services. Such information will not be sent to the Customer's other Users.

## **2.3. User administration**

If the Customer is a physical person, the Customer will be assigned a single User.

If the Customer is a legal person, Users are created and administrated by the Customer. Customer's administrators for this Agreement should be communicated to SESAM.

The logon information of an individual User shall not be shared or used by more than one physical person, but may freely be reassigned by the Customer's administrator. The Customer's administrator may also name further administrators and delete Users. The Customer shall ensure that all information about Users and administrators are up to date at all times.

Each User is responsible for keeping his/her username and password confidential. The Customer shall inform SESAM immediately in case of unauthorized use of a User's logon information. Users are authorized to provide SESAM's support personnel with access to their accounts where such access is necessary to provide support or else asked for by the User.

## **2.4. Requirements for use of the Services**

The Customer and any of its Users shall not transfer viruses, malware or any other harmful code to the Services or use the Services in a manner which gives a risk for such transfer. The Services shall not be used for any illegal or otherwise unauthorized purpose. When the Services are used outside of Norway, in cases

where the Customer's Users temporarily are staying abroad, the Customer is responsible for complying with the Norwegian, EU and United States of America export restrictions and -regulations, including assuring that the Services are not used in jurisdictions where such use would be contrary to such export restrictions and -regulations.

### **3. Technical information**

The Services will be delivered through the operating environment selected by SESAM at any time, unless it is agreed with the Customer that the Customer will use another operating environment. The Customer will be given minimum three months' notice in case of significant changes to the operating environment. SESAM reserves the right to change the operating environment, but will in such event notify the Customer of the change and of technical and legal effects of such change.

At the present time the operating environment selected by SESAM is Microsoft Azure. For Azure, separate terms of service apply from Microsoft: [Online Subscription Agreement](#) and [Online Services Terms](#). These terms apply as amended and updated by Microsoft at any time. SESAM has no responsibility for error and defects in such services.

SESAM and the Customer may agree on special requirements for the operating environment in a separate agreement.

To the extent technical requirements apply to the Customer's IT systems for the use of the various Services, e.g. requirements for bandwidth and/or hardware, this shall be set out together with the description of the Services in question.

## **4. Sesam's Responsibility for Quality of Service, Availability and Support**

### **4.1. Quality of Service**

SESAM warrants that the Services will perform substantially as described in applicable Documentation of Services. The Services will be subject to continual improvement.

If the Services do not function as described in applicable Documentation of Services, SESAM will correct verified errors in the Services at SESAM's own expense. SESAM may choose to replace the Services or functionality therein instead of performing a correction. If SESAM does not solve the verified errors according to the time-limits set out together with the description of the Services in question or does not replace the Service within a reasonable time, the Customer may cancel their subscription to that particular service in accordance with the terms in section 11. The Customer may not set forth any other claims due to defects or errors in the Services.

Links to websites not owned or controlled by SESAM that are available in the Services, related web pages or the documentation are provided without any responsibility or liability for SESAM. SESAM is not responsible for the content and/or information on such websites. In the same manner, SESAM is not responsible for defects and errors arising from the Customer's own applications, databases or other systems.

### **4.2. Service Level Agreements (SLA) targets, penalties**

The provisions in this section apply only to the Customers who pay a Subscription Fee.

SESAM's Service availability targets, SLA penalties, and fixed maintenance periods are set out together with the description of the Services in question.

SESAM may, from time to time, require additional maintenance periods beyond what is set out above, for example for major upgrades. Such maintenance periods will be notified to the Customer at least 48 hours in advance, and any unavailability does not count towards the calculation of Service availability targets.

### 4.3. Notification of errors

If the Customer experiences that the Services in whole or in part are unavailable, or have reduced performance, the Customer shall report the error via <https://support.sesam.io>. In order to ensure that SESAM gets necessary information to identify and correct the error, the Customer shall, together with the notification of error, provide accurate information about the error, including a description of how the error occurred, how many Users are affected, and which dataflows and/or systems are affected, or assist SESAM with gathering such information.

### 4.4. Support

The provisions in this section apply only to the Customers who pay a Subscription Fee.

SESAM will provide basic technical support to the Customer. This entails technical assistance, but SESAM does not warrant that any solution will be found for any problems or requests. The administration and configuration of the Services for the Customer is not included in the support, and may be provided according to separate agreements. This may include assistance connected to integrated applications/databases.

The Customer may contact SESAM support on business days (Monday to Friday except Christmas Eve, New Year's Eve and other Norwegian public holidays) between 08:00 and 16: hours Central European Time, or on specified times determined by SESAM. Any contact with SESAM support shall take place via <https://support.sesam.io>.

Support is provided in accordance with the following guidelines:

- A Customer with more than three Users shall designate a contact person for support, which will act as the Customer's point of contact with SESAM. Accordingly, the contact person shall provide first line support, and forward detailed information to SESAM's personnel.
- Support requests shall regard the Services, when used in a manner recommended by SESAM. Support shall not cover repair of information, data-correction in a database or problems caused by the Customer. Neither shall the support cover any matter outside of the Services as covered by the Customer's subscription.
- SESAM will recommend training or consulting services if the support request takes the form of being general training or education.
- Support does not include any form of consulting services.

## 5. Security

### 5.1. Rights to data

The Customer retains all rights to all data that is entrusted to SESAM for processing and which is stored or processed with help of the Services under this Agreement.

Upon termination of all Services or individual Services, SESAM may assist in transferring the data to a designated and usable format. Such a service should be ordered at least 30 days before the end of the subscription in question in order to ensure that the Customer can receive the data before deletion. Such assistance is invoiced by SESAM according to the at any time applicable fee schedule and terms for consultancy services. On termination of the subscription of the Service subscription, or subscription for an individual service, all Customer data will be deleted by SESAM.

### 5.2. Security

Customer's privacy is important to SESAM and SESAM will abide by SESAM's privacy policy. SESAM reserves the right to modify their privacy policy from time to time.

SESAM provides secure and reliable services, and will at any time have in place administrative, physical and technical security measures including backup solutions according to corresponding standards:

- SESAM has established an information security governance system where systems, routines and processes which was set up in accordance with ISO 27001 and 27018.
- A yearly third party audit shall be carried out in accordance with ISO 27001.
- A confidential summary report of the audit shall be produced, and made available to the Customer upon request.
- The summary report shall enable the Customer to assess whether the security level in SESAM's services are according to the Agreement and the Customer's requirements.

### **5.3 Processing of personal data**

The Services may entail processing of the Customer's personal data, e.g. storage in SESAM's operating environments, cf. section 3 above, unless otherwise is agreed with the Customer.

If the Services entail processing of the Customer's personal data, the Data Processing Addendum comes into force. The Data Processing Addendum forms part of the Terms Of Service. The Data Processing Addendum are hereby incorporated by reference and shall apply to the extent Customer Data includes Personal Data, as defined in the DPA. The DPA further states the Parties' obligations and rights as Controller and Processor, regarding the Processor's processing of Personal Data on behalf of the Controller. SESAM as the Processor, shall only process data in accordance with the Data Processing Addendum.

In the circumstance that the Services entail processing of the Customer's personal data the following will enter into force in addition to the Data Processing Addendum:

The Customer is the Controller in accordance with EU's General Data Protection Regulation ("GDPR") article 4 paragraph 7. SESAM is the Processor in accordance with GDPR article 4 paragraph 8.

The Customer as the Controller agrees and warrants that: - The Customer owns or otherwise has the right to transfer the personal data to the Service for processing, and that the Customer is responsible for the accuracy, integrity, contents, and legality of the personal data, including transfer and instructions; - Where applicable, that the processing of personal data is covered by an applicable permit, and/or has been notified to the applicable regulatory authorities and/or Data Subjects, and that the processing of personal data is not in violation of applicable law, hereunder GDPR. - It is the Customer's obligation as the Controller to notify the applicable regulatory authorities and/or Data Subjects in case of breach or unauthorized processing of personal data, incl. special categories. - The Customer, by way of its risk assessment, has verified that SESAM's security measures are effective and appropriate for the processing in question; - SESAM has provided sufficient guarantees in terms of logical, technical, physical and organizational security measures. - SESAM generally recommends that the Customer uses standard-level SLA or higher when processing personal data. - If it is set forth in the agreement that the processing of personal data includes processing of special categories of personal data or data processing that entails high risk, SESAM requires that the Customer uses standard-level SLA or higher.

## **6. Fees and Payment Terms**

For Services included in this Agreement, the Customer may have paid a Subscription Fee to SESAM as set out together with the description of the Services in question.

Dynamic price model:

The price model is a dynamic (running) price model that is renewed automatically until terminated by one of the parties as set out in section 11.

Fixed price model:

A fixed price model entails that Sesam gives a 50% discount of a set amount of data (GB), based on the dynamic price and provided that the Customer in the Agreement agrees to the fixed price model for a renewable term of 12 months.

If the Parties agrees upon fixed price, the Agreement will be for a term of 12 months calculated from the date it is agreed between the parties that the model is fixed price (most often the Date the Agreement is signed by both parties). If the Customer uses more data than the agreed upon fixed price model allows for that term, the fee for the data amount (GB) surpassing the agreed upon fixed price, will be double of what follows from the dynamic price model.

The Agreement will automatically be renewed with the same data amount (GB) for the following 12 months as that of the running term, unless the Customer gives at least one (1) month written notice prior to the expiration of the running term that they do not want to continue with the fixed price model at all, or if they want to make adjust to a higher or lower fixed price model for the following 12 months term. Renewals each 12 months will continue as long as the Agreement is running.

The Parties can additionally agree upon a support level of 24/7 provided that the Customer has agreed to a fixed price model of 50 GB/month or higher.

## **7. Right to Audit and Control**

The provisions in this section apply only to the Customers who pay a Subscription Fee.

SESAM shall, to the extent required by applicable audit standards or applicable governmental requirements/legislation, allow the Customer's internal or external auditors to observe SESAM's delivery of the Services with related Customer data and any documentation for the Services for the Customer. The Customer shall give reasonable notice before such audits, at least 20 calendar days, and the audit shall be carried out during normal business hours. The Customer acknowledges that scope of audit shall be limited to SESAM's own delivery of Service, as well as applicable documentation.

The Customers may not utilize auditors who are in direct competition with SESAM. The auditor(s) shall sign a confidentiality statement. The Customer shall adhere to SESAM's applicable regulations when access is given to SESAM's facilities.

Any costs which SESAM may have in relation to the audit, control and any possible further quality assurance that the Customer may require, will be invoiced to the Customer in accordance with SESAM's applicable rates.

## **8. Changes to the Agreement**

SESAM reserves the right to change the terms of this Agreement upon at least 30 days' notice.

Reference is made to SESAM's limited opportunity to change the terms in sections 5.2 and 5. regarding the processing of data. SESAM may not change section 5.1. to the detriment of the Customer.

## **9. Infringement of Third Party Rights**

The provisions in this section apply only to the Customers who pay a Subscription Fee.

SESAM shall defend the Customer against claims or law suits set forth by third parties claiming that the Customer's use of the Services infringes that third party's registered Norwegian or EU intellectual property rights, including, without limitations, patents, copyright, trade secrets, trademark or any other intellectual property rights. In the event of such claims the Customer shall immediately inform SESAM in writing.

SESAM shall, to the extent SESAM is responsible for the infringement, hold the Customer harmless against all costs, damages, expenses or losses that the Customer is ordered to pay by a court or agrees to pay in a

settlement, including attorney fees. This is subject to the full co- operation of the Customer with SESAM and that SESAM is in full control of the legal process and negotiations for a settlement. SESAM may at its own discretion (i) modify the Services so that there is no longer any infringement of third party rights, (ii) replace the Services with functionally equivalent services, (iii) provide a right for the Customer's continued use of the Services. If these options are not available, SESAM may terminate the Customer's access to the Products and Services with a refund of any fees paid for the subscription after the date of termination. The Customer may not set forth any other claims as a result of infringement of third party rights.

The previous right to be held harmless does not apply if the Services have been used in violation of these terms and conditions or if the claim arises out of any modification, integration or customization of the Services not performed by SESAM.

The Customer shall defend SESAM against any claims or lawsuits in which a third-party claim that the Customer's data or use of the Services in combination with the Customer's own applications, databases or other systems, is inconsistent with or infringes a third party's intellectual property rights, including without limitations, patents, copyright, trade secrets, trademark or any other intellectual property rights. SESAM shall immediately notify the Customer in writing in the event of such claims.

The Customer shall hold SESAM harmless against all costs, damages, expenses or losses that SESAM is sentenced to pay by a court or agrees to in a settlement, including attorney fees, provided that SESAM cooperates with the Customer at the Customer's own expense and that SESAM provides the Customer with full control over the legal process and settlement, and that the settlement releases SESAM from all liability.

## **10. Liability, Limitation of Liability etc.**

### **10.1. Limitation of liability**

If SESAM is held responsible for paying damages to the Customer as a consequence of breaches of any of the obligations under this Agreement, such damages will under no condition include compensation for indirect loss or damages of any kind that may arise as a result of, or in connection with, such breach. Indirect loss includes, but is not limited to, loss of profit of any kind, losses as a consequence of disrupted operations, loss of data, lost savings, losses due to deprivation and claims from third parties (except as set out in section 9 above). SESAM'S liability under this Agreement is therefore limited to direct loss, unless otherwise set out in mandatory applicable law, for example damages due to gross negligence or intent. Any refunds or compensation for direct loss and costs during any 12-month period shall not exceed an amount equivalent to 6 month's Subscription Fee's ex. VAT for the Services during the same period.

If standardized sanctions are agreed, these standardized sanctions shall be the sole remedy and no other claims may be made based on the same situation.

### **10.2. Force majeure**

If the use and execution of the Services is wholly or partly prevented or materially impeded by circumstances beyond the parties' control, both parties' obligations are suspended for as long as the circumstances are relevant and as long as these circumstances lasts. Such circumstances include, but are not limited to, strikes, lockouts, and any relationship which under Norwegian law will be regarded as force majeure. Each party may, however, in accordance with section 11 of this Agreement, terminate the Agreement if the force majeure makes it particularly burdensome for that party to continue the Agreement.

In the event that law, rules or regulations applicable to the use or delivery of the Services is changed or new rules or regulations are adopted after the Services have been made available on the market and this prevents SESAM from fulfilling the Customer's instructions pursuant to the Data Processing Addendum or other obligations in this Agreement and/or this requires full or partial termination of access to the Services for a limited or indefinite period of time, this shall be considered as a force majeure circumstance. SESAM is not in any way responsible for any such or other force majeure circumstance.

### **10.3. Circumstances for which SESAM not in any event is responsible**

Even though SESAM will use appropriate care to ensure secure transmission of information between the Customer and the Services, the Customer recognizes that the Internet is an open system, and that SESAM cannot warrant that a third party cannot or will not intercept or alter data during the transmission. SESAM takes no responsibility for such unauthorized access to, use or publication or loss of data.

Neither is SESAM responsible for lack of availability of the Services when this is directly or indirectly caused by the Customer or by circumstances for which the Customer is responsible or the reconstruction of data regardless of cause.

## **11. Cancellation and Suspension**

The Customer may cancel the Services or individual sub-services and thereby cancel the entire subscription for SESAM's Service using the Customer's account tool with applicable notice period. The cancellation takes effect from the start of the first month after the end of the notice period.

For non-paying Customers SESAM has the right to suspend or terminate access to all or any part of the Service at any time, with or without cause, with 14 days' prior notice. In case of abuse, access to Services may be suspended or terminated without notice, effective immediately.

The provisions for the reminding of this section apply only to the Customers who pay a Subscription Fee.

If a minimum term applies for some of the Services, the termination by the Customer takes effect after the expiration of such minimum term.

If payment is not made within 30 days after the due date, SESAM may, provided that the amount outstanding is not insignificant, suspend the Customer's access to the Services until payment is made. Suspension shall be notified in writing by SESAM, with a final and reasonable deadline for the Customer to settle the amount outstanding before suspension is made effective. SESAM may terminate the Customer's accounts for the Services if payment is not made to SESAM within 14 days after such suspension is made effective. The Customer shall pay delayed interest in accordance with applicable law for all Subscription Fees that are not settled before their due date. SESAM may make renewal of the Customer's subscription conditional on a shorter payment due date or increased invoice frequency after one case of delayed payment.

SESAM may terminate the Customer's subscription with 7 days' written notice if the Customer is in breach of any of his obligations under this Agreement, or if it becomes apparent that the Customer will materially breach this Agreement in the future. SESAM may with 6 days' written notice to the Customer also suspend the Customer's subscription to the Services if the Agreement is breached by the Customer. Such suspension may be in effect until the matter has been resolved.

SESAM reserves the right to terminate any service in its entirety, or its availability in any market, with 6 months' notice before such termination takes effect or in case of force majeure with such notice which is reasonable under the circumstances.

When the Services, hereunder Users, are terminated, all data and copies of such data will be deleted from SESAMs servers upon the termination taking effect. The Customer will get access to his data as set out in section 5.1.

The limitation period for any claims arising in connection with this Agreement or breach of this Agreement is one year after the termination of the agreement. Claims forwarded after the limitation period is out of date and hence have no validity.

## **12. Confidentiality**

Information that comes into the possession of the parties in connection with implementation of the Agreement shall be kept confidential and shall not be disclosed to any third party without the consent of the other party.



If the Customer is a public body, the scope of the confidentiality obligation under this provision shall not go beyond that laid down by the Act of 10 February 1967 relating to Procedure in Cases concerning the Public Administration (Public Administration Act) or corresponding sector-specific regulations.

The confidentiality obligation pursuant to this provision shall not prevent the disclosure of information if such disclosure is demanded pursuant to laws or regulations, including any disclosure or right of access pursuant to the Act of 19 May 2006 relating to the Right of Access to Documents in the Public Administration (Freedom of Information Act). The other party shall, if possible, be notified prior to the disclosure of such information.

The confidentiality obligation shall not prevent the information from being used when there is no legitimate interest in keeping it confidential, for example when it is in the public domain or is accessible to the public elsewhere.

The parties shall take all necessary precautions to prevent unauthorized persons from gaining access to, or knowledge of, confidential information.

The confidentiality obligation shall apply to the parties' employees, subcontractors and other third parties who act on behalf of the parties in connection with the implementation of the Agreement. The parties may only transmit confidential information to such subcontractors and third parties to the extent necessary for the implementation of the Agreement, and provided that they are subjected to a confidentiality obligation corresponding to that stipulated in this clause.

The confidentiality obligation shall not prevent the parties from utilizing experience and expertise developed in connection with the implementation of the Agreement.

The confidentiality obligation shall continue to apply after the expiry of the Agreement. Employees or others who resign from their positions with one of the parties shall be subjected to a confidentiality obligation following their resignation as well, as far as factors mentioned above are concerned. The confidentiality obligation shall lapse five (5) years after the Agreement comes to an end, unless otherwise is stipulated by law or regulations.

### **13. Transfer**

Without obtaining SESAM's prior written permission, the Customer is not entitled to transfer all or part of the right to use the Services to another entity (either through mergers, de-mergers, bankruptcy, change of ownership or control or to affiliates or otherwise). SESAM may fully or partially transfer its rights and obligations under the Agreement to subsidiaries or other companies within the same group, hereunder use these as sub-contractors, provided that this is done in a manner assuring compliance with the obligations under the GDPR from the Customer's perspective.

### **14. Choice of Law**

This Agreement will be construed, regulated and interpreted in accordance with and governed by Norwegian laws, without giving effect to its conflicts of law principles. Further, Customer and SESAM agree to submit to the jurisdiction of Oslo, Norway for any legal disputes regarding this Agreement or its subject matter herein.

### **15. Disputes**

Any dispute or disagreement arising between the parties will be resolved by negotiations.

If such negotiations fail, either party may request that the case is brought before a Norwegian court. If the parties so agree, the case shall be decided by arbitration after Norwegian Act of 14. May 2004 no. 25 on arbitration. If the parties require confidential treatment of the arbitration proceedings, hereunder the arbitration court's verdict, this shall be agreed between the parties in writing together with the arbitration agreement.

The agreed legal venue shall be the location where SESAM has its registered address when the case is made before the court or arbitration court.

The following dispute resolution shall apply to the Customers who pay a Subscription Fee:

The parties will strive to resolve all disputes at the project management level. If any such dispute cannot be mutually resolved by the project managers within 7 days, then such dispute will immediately be referred to the parties' respective division vice presidents (or equivalents) for discussion and resolution. If such parties fail to resolve the dispute within 14 days, then such dispute will be referred to the party's respective Chief Operating Officer (or equivalent) for discussion and attempted resolution. If such dispute cannot be mutually resolved by such parties within 14 days, then either party may request that the case is brought before a Norwegian court. If the parties so agree, the case shall be decided by arbitration after Norwegian Act of 14. May 2004 no. 25 on arbitration. If the parties require confidential treatment of the arbitration proceedings, hereunder the arbitration court's verdict, this shall be agreed between the parties in writing together with the arbitration agreement.

The agreed legal venue shall be the location SESAM has its registered address when the case is made before the court or arbitration court.

# Appendix 1

## Description of the Services

### 1. Specification of the Services

SESAM shall deliver the Services and complete the tasks related to the Services as set out in section 1 and that is set out in the service catalogue in the table below.

Table 1: Service specification

SaaS-Service	Specification of tasks and contents of Sesam SaaS-Service
1. Description of the SaaS-Service	<p>SESAM is a data-oriented integration platform delivered as a Service. Sesam consists of service instances that exposes an API (see <a href="http://docs.sesam.io">http://docs.sesam.io</a> for documentation). The Service instance can be configured through this API. The Service may be configured to fetch data from various systems and databases, and the data that is so collected and stored in SESAM. Such configuration may be performed by the Customer or by a separate consulting agreement between SESAM and Customer. API's are also used to transform and expose the stored data. The SaaS-Service consists of two applications:</p> <ol style="list-style-type: none"><li>1. SESAM Integration Service that collects, connects and transforms data before it is routed to a receiving system or search engine.</li><li>2. SESAM Data Browser, which is a search interface against structured data that links with data in a search index populated from the SESAM Integration Service.</li></ol> <p>The SaaS-Service is secured with SSL-certificates that are unique for each Customer and through access controls that may be set for the stored data. Access to the SaaS-Service is through the currently supported interface published at <a href="http://sesam.io">sesam.io</a>.</p> <p>The Service Instance reports operations-oriented metadata back to SESAM. These metadata are used to monitor the system's conditions and provides the Customer with the opportunity to receive notifications on the data flow in the service.</p>
2. Requirements for scaleability	<p>The SaaS-Service can be scaled both in terms of the number of Users, amounts of data and requirements for computing capacity. Storage scales automatically, while increased computing power, monitoring or SLA-changes can be selected via the My Page in the SESAM-portal.</p>
3. Backup and securing data	<p>SESAM shall keep the Customer's data logically separated from any third parties' data to limit the risk of data loss or unauthorized disclosure. By «logically separated» is meant that necessary technical measures securing the data against unwanted alteration and access are implemented.</p> <p>Backup of data may be selected as an optional service on My Page in the SESAM-portal. The cloud service, as a basis, only contains copies of data from other sources that the Customer has chosen to integrate with, and transformations of such data. Therefore, all data may be re-imported and recreated when needed for such sources. Re-creating from back-up may, however, be faster for large quantities of data.</p>

SaaS-Service	Specification of tasks and contents of Sesam SaaS-Service
4. Reconstruction of data	If data is lost or corrupted due to causes which SESAM is responsible for, SESAM shall re-establish the data from the latest backup within reasonable time and at SESAM's own cost, if not otherwise agreed below. SESAM's responsibility for costs is limited to the costs for re-establishment of the data from the latest backup, and additional costs that may arise due to SESAM not having performed backups as set forth in the Agreement. Costs attributable to reconstruction of data after the latest backup may only be attributed to SESAM if the data loss is due to gross negligence by SESAM. If the cause of the data loss is such that the Customer shall carry the costs, the Customer shall approve the scope of the work before it commences.
5. Notification of updates of the Services	Major updates and planned maintenance / downtime is notified through the SESAM Service Desk.
6. System documentation for the Services	SESAM is documented here: <a href="https://docs.sesam.io/overview.html">https://docs.sesam.io/overview.html</a>
7. Third party cloud services included in the Services <i>or</i> Third party cloud services are included in the Services, but it is set forth in this agreement that the Customer will provide the operating environment	SESAM is delivered as a SaaS from virtual servers in Microsoft Azure Cloud. For Azure, separate terms of service apply from Microsoft: <a href="#">Online Subscription Agreement</a> and <a href="#">Online Services Terms</a> . These terms are binding on the Customer as they are amended and updated by Microsoft at any given time. <i>or</i> It is agreed between the parties that the Customer will acquire and use another operating environment with their own terms of service, when using SESAM's Services. The Customer is responsible for entering into contract with the supplier of the operating environment.
8. The Customer's responsibility in connection with the Services	Configuring routers and firewalls for expanding the Customer's network to include the Services, included securing the network communication. Configuring access to applications to be integrated with the Service. SESAM will assist with specifications for network configuration.

## 2. Service level agreement and standardized refunds

Since SESAM is delivered as SaaS, the Customer may consecutively select capacity and service levels as required. The applicable selected capacity and SLA-level will be defined at the Customer's My Page on the SESAM-portal.

The Customer shall report errors to SESAM according to the following procedure: Through SESAM Service Desk.

### 2.1. Availability for the Services

**Availability target** SESAM, as a SaaS, is provided with the target of 99.5% uptime per installation (cf. production environment, test or development, which corresponds to approximately 1 hour maximum unplanned downtime per month for the individual installation.

**Planned downtime** SESAM, as a SaaS, is maintained and updated almost continually. Planned maintenance is therefore nightly from 00:00 to 03:00 hours Central European Time.

Other planned maintenance shall be notified at least 48 hours in advance.

**Definition of downtime** If a service's API or User interface is not responding within a time period of ten minutes, this shall be considered downtime. This is monitored and logged by the SESAM-service. It is not

considered downtime if the error is in the Customer's applications, databases or other systems, or is due to downtime on the operating environment.

Points accumulated on unplanned downtime (to be calculated per installation):

On unplanned downtime, points are accumulated as set out below:

Table 2: Hours of downtime per month to points

Hours from	Hours to	Number of points
1	2	4
2	4	8
4	6	12
6	10	15
10		25

Upon non-conformity with these requirements, any standardized penalties set out under section 2.4 is to be calculated.

SESAM shall maintain a log of all events concerning downtime, with the date and time of when downtime was reported, cause/symptom, solution and duration of the downtime.

## 2.2. Capacity requirements

SESAM shall deliver on the following capacity requirements for the Services:

For SESAM Search the capacity levels Basic, Standard and Enterprise can be selected, which respectively guarantees 1, 5 and 10 RPS (Requests per second).

The selected level upon start of the Service period is set out in the price matrix in Appendix 2. If the Customer desires to change the level, this can be done on the Customer's My Page on the SESAM-portal.

For other SESAM SaaS-Services, no quantified capacity requirements apply.

## 2.3. Requirements for processing and reaction times

Upon errors in the Services, SESAM shall fulfil the following requirements for processing and reaction:

Table 3: Reaction time target and correction time

Level	Category	Enterprise	Standard	Basic	Correction target
A	Critical error that is so serious that the entirety or significant parts of the Services are not available or not functioning	1 hour	8 hour	n/a	A workaround of the error shall be delivered without undue delay, and at the latest within <ul style="list-style-type: none"><li>• Next business day for Enterprise</li><li>• 3 days for Standard</li><li>• n/a for Basic</li></ul> If this is not possible, a fix will be delivered within 10 days.

Level	Category	Enterprise	Standard	Basic	Correction target
B	Serious error that may be fixed with a work around, but which delay the usage of the Services	4 hours	2 days	n/a	A workaround of the error shall be delivered within 10 business days. If this is not possible, a fix will be delivered in the next release.
C	Less serious error, which does not entail delays in the usage of the Services	None	None	None	The error is evaluated with the goal of a fix in the next release in line with the normal release schedule.

All requirements in the table shall be calculated within SESAM's standard business hours, 0800 - 1600 hours Central European time, excluding public holidays and other holidays in Norway, and excluding Christmas Eve and New Year's Eve. The vendor assigns the priority for reported errors.

With "reaction time" is meant the time from the Customer has reported the error until SESAM has started the work on identifying the cause for an error. The "correction time" is the time from the error has been reported to SESAM until a temporary or permanent fix is implemented and a normal situation for the Service has been re-established. The correction time therefore includes the reaction time.

The above mentioned requirements do not apply for errors that are caused by errors in the Customer's applications, databases or other systems. Neither do the requirements apply for errors in the operating environment, but SESAM shall in such cases report relevant errors to supplier of the operating environment without undue delay.

The selected SLA-level upon start of the service period is set out in the price matrix in Appendix 2. If the Customer desires to change the level, this can be done on the Customer's My Page on the SESAM-portal.

To ensure the compliance with these requirements, SESAM shall be able to demonstrate that continuous monitoring of the Services is implemented, and that measures are taken to optimize the performance.

For each case of a non-adherence to the processing and reaction times set out above, points are accumulated within a month as set out below:

Table 4: Point accumulation

Description	Twice as long time	4 times as long time	8 times as long time	More than 8 times as long time
Reaction time, Critical error (A)	4 points	6 points	8 points	10 points
Reaction time, Serious error (B)	2 points	4 points	6 points	8 points
Correction time, Critical error (A)	4 points	6 points	8 points	10 points
Correction time, Serious error (B)	2 points	4 points	6 points	8 points

On this basis, standardized penalties are calculated as set out in section 2.4 below.

## 2.4. Standardized penalties

Standardized penalties are calculated per installation (cf. production environment, test or development) when actual measured availability (see section 2.1.) or processing and reaction times (see section 2.3) in a

SLA measurement period deviates from the agreed level, with the exception of errors due to the Customer or the Customer's other vendors. If the deviation within an installation impacts on several SLA-requirements, points are calculated only for the part of the service (see either section 2.1 or 2.3) that results in the highest number of points.

The invoicing period for services delivered and any standardized penalties is in arrears every month.

The calculation basis for standardized penalties is the last monthly subscription fee for the application installation in question. The penalty is calculated as the given percentage of the calculation basis. The maximum total standardized penalty is 40% of the subscription fee for the Service for the installation in question in the same billing period.

The deviation from the agreed service quality (SLA) is measured in the number of points incurred by SESAM during a one-month period. Points are calculated for reaction time, correction time and non-planned downtime within the installation in question.

Table 5: Accumulated points to reduction of fee

Points from	Points to	Reduction of monthly subscription fee for the relevant installation
1	10	0%
11	20	-5%
21	30	-10%
31	40	-15%
41	50	-20%
51	60	-25%
61		-40%

## Appendix 2

### Subscription Fee, payment terms

#### 1. Subscription fee

The Subscription Fee for the Services are set depending on the computing power, data volume, selected monitoring functionality and SLA-level.

Fees for standard services are set out in Euro, and are calculated into Norwegian Kroner based on the Central Bank of Norway's exchange rate on the invoicing day.

Compute is automatically upgraded if data use exceeds specified limits. You can upgrade without additional data storage in case you want higher performance.

If data storage is more than 1TB you will be billed with an additional Multi compute for every TB above 1TB. As an example, if you have 4,5TB of data you will be billed with 5 quantities of Multi computes.

The fees for the Services are set out below in Euro exclusive of VAT:

#### Developer environment

A developer environment has a fixed price and serves a single developer, or a CI test environment. These do not have support for backup, VPN, or SLA and can not host test, staging or production environments. The development environment is cloud-only and restricted. We strongly encourage following [test-driven development practices](#) by using the `Sesam Client` `<sesam-client>`.

Table 6: Developer environments

Compute	Pr environment
Fixed price developer - 1 Engine < 20 GB Data	€50.00

#### Production and test environment

Table 7: Runtime environments<sup>1</sup>

Compute	Pr environment
Single compute - 4 Engines < 350 GB Data	€900.00
Multi compute - 16 Engines < 1 TB Data	€3,300.00

Table 8: Data prices<sup>2</sup>

Data	Pr GB
Storage	€14.00
VPN	€2.00

<sup>1</sup>Geo-replicated backup is included in cloud environments.

<sup>2</sup>1-year fixed price option available. 50% data price reduction for the fixed data amount, with 100% price increase for data exceeding the fixed data amount. Number of computes is determined by the maximum of fixed data amount and actual data amount.



Table 9: Monitoring

Monitoring	Pr Pipe
Basic - Status	€0.00
Standard - Insight	€5.00
Enterprise - Notifications	€20.00

Table 10: SLA<sup>3</sup>

Support - Response time	Pr GB
Standard - 8h	€15.00
Enterprise - 1h	€30.00
Premium 0,5h x 24/7 <sup>4</sup>	€100.00

### 1. Invoicing

From the start of the Services, SESAM shall invoice the Customer monthly in arrears for the agreed fees for the Service minus any standardized penalties, with reference to appendix 1 section 2.4.

The invoice shall be specified in a manner that allows the Customer to control the individual price items, including any incurred standardized penalties. SESAM offers electronic invoicing where the standard format on signature of the Agreement is EHF.

### 3. Due date

Invoices are due after 30 calendar days.

### 4. Price adjustment

SESAM may adjust the agreed Subscription Fee once per year, upon 3 months' written notice.

If, after the signature of the Agreement, changes in public taxes, charges or other duties or other changes in public administrative practice affects the vendor's costs connected to the Service, the subscription fee shall be adjusted correspondingly without prior notice.

<sup>3</sup>Premium SLA requires 1 year fixed price commitment for minimum 50GB data.

<sup>4</sup>SLA is billed for minimum 50GB data and a maximum of 300GB.

# Appendix 3

## Data processing agreement

In accordance with EU's General Data Protection Regulation ("GDPR") article 28 paragraph 3 and the prevailing Norwegian Personal Data Act. This Data Processing Agreement ("DPA") enters into force if and when the Services entail processing of the Customer's Personal Data and will form part of the Terms of Service for Access and Use of SESAM Software as a Service (SaaS) ("Terms of Service"). The terms used in this DPA shall have the meanings set forth in this DPA. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Terms of Use. Except as modified below, the terms of the Terms of Use shall remain in full force and effect.

### 1. Definitions

1.1 In this Agreement, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "Applicable Laws" means (a) GDPR - EU General Data Protection Regulation 2016/679;

(b) EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

(c) European Union or Member State laws with respect to all the Personal Data in respect of which the Controller is subject to EU Data Protection Laws; and

(d) any other applicable law with respect to all the Personal Data in respect of which the Controller is subject to any other Data Protection Laws;

1.1.2 "Controller" means Customer, and the Customer determines the purpose and means of processing the Personal Data;

1.1.3 "Processor" means Vendor (or a Subprocessor), which processes Personal Data on behalf of the Controller;

1.1.4 "Personal Data" means any information relating to an identified or identifiable natural person which is Processed by the Processor on behalf of the Controller pursuant to or in connection with the Principal Agreement;

1.1.5 "Data Protection Laws" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any member state or other country;

1.1.6 "EEA" means the European Economic Area;

1.1.7 "Third Countries" means non-EU/EEA-countries that do not have a sufficient level of security for processing personal data;

1.1.1 "Services" means the SESAM SaaS-services that will be supplied pursuant to the specifications in the Principal Agreement;

1.1.2 "Subprocessor" means any person (including any third party, but excluding an employee of the Processor) appointed by or on behalf of the Processor to Process Personal Data on behalf of the Controller in connection with the Principal Agreement.

### 2. Processing of Personal Data on the Controller's behalf

2.1.1 This Agreement comes into force if and when the Customer chooses to enter and store Personal Data in the Services. The Agreement is an appendix to the Principal Agreement and does not imply any changes to the commercial terms between the parties.

2.1.2 The object of this Agreement is to set out the rights and obligations pursuant to the GDPR, the prevailing Norwegian Act on the Processing of Personal Data, with additional Regulation(s). This Agreement shall ensure that the Personal Data regarding the Data Subjects is not used in a non-compliant manner or compromised to un-authorized parties.

2.1.3 SESAM will process Personal Data necessary for the purpose to perform the Services in accordance to the Agreement, and as further instructed by Customer in its use of the Services.

2.1.4 This Agreement shall ensure that the Personal Data processed by the Processor on behalf of the Controller, is only processed in compliance with Applicable Laws and according to the Controller's documented instructions.

2.1.5 The subject matter of the Processing of the Personal Data is set out in the Principal Agreement and this Agreement, and the duration of the processing shall be for the duration of the Customer's right to use the Services pursuant to the Principal Agreement.

2.1.6 The Processor will typically not have access to the Personal Data. The Personal Data is only to be stored in the Processor's operating environment. Where Personal Data is stored in the operating environment that is part of the Processor's Services, the Processor shall only monitor and provide support on the Services and not process the Personal Data in any way other than what is stipulated in the Principal Agreement. If the Controller wants the Processor to carry out any other form of processing of the Personal Data, the Controller must make the request by a written change order to the Processor. Further/other processing of the Personal Data as a result of such a change order may lead to increased costs for the Processor and must thus be covered by the Controller, see section 2.5.

2.1.7 Where the Controller stores the Personal Data in their own operating environment, the Processor will not be able to access the Personal Data unless the Controller provides such access. The Processor shall monitor and provide support on the Services and not process the Personal Data in any way other than what is stipulated in the Principal Agreement. If the Controller wants the Processor to carry out any other form of processing of the Personal Data, the Controller must make the request by a written change order to the Processor and then provide access to the Personal Data. Further/other processing of the Personal Data as a result of such a change order may lead to increased costs for the Processor and must thus be covered by the Controller, see section 2.5.

## **2.2 Categories of Personal Data and Data Subjects**

2.2.1 The Customer may submit Personal Data to the Services, which may include, but is not limited to, categories of Personal Data such as first and last name, home address, mobile number, job title, date of birth, education/qualifications, personal identification number, salary, bank account number, passwords, pictures and so on.

2.2.2 The Customer may submit Personal Data to the Services, which may include, but is not limited to, categories of Data Subjects such as customers, end users, employees, agents, advisors, job applicants, partners, suppliers, clients and customers.

2.2.3 In the case that the Controller processes special categories of Personal Data, this must be specifically agreed upon with the Processor in advance of such Processing.

## **2.3 The Controller's Obligations**

2.3.1 The Controller shall provide the Processor with written instructions on the processing of the Personal Data on behalf of the Controller, hereunder transferring the Personal Data to any country or territory as reasonably necessary for the provision of the Services and consistent with the Principal Agreement and in accordance with Applicable Laws.

2.3.2 The Controller shall ensure that the processing of the Personal Data is lawful.

2.3.3 The Controller shall authorise the Processor to provide each Subprocessor with the same written instructions that the Processor has been provided with.

2.3.4 The Controller has provided the Data Subjects with the necessary information according to Applicable Laws; and it is the responsibility of the Controller to collect any consents from the Data Subjects for the processing of Personal Data taking place according to the Principal Agreement.

## **2.4 The Processor's obligations**

2.4.1 The Processor shall only process the Personal Data on behalf of the Controller and on written instructions from the Controller, unless Processing is required by Applicable Laws to which the Processor is subject, in which case the Processor shall to the extent permitted by Applicable Laws inform the Controller of that legal requirement before the relevant Processing. The Processor shall only process the Personal Data for the sole purpose and to the extent necessary to provide the Services, in accordance with the terms in this Agreement and Applicable Laws.

2.4.2 The Processor does not have the right of use of the Personal Data, and may therefore not process them for their own purposes under any circumstances.

2.4.3 The Processor has carried out the technical and organizational security measures as described in this Agreement's section 4, in order to protect the Personal Data from loss, misuse or un-authorized alternation or dissemination, or against other illegal processing. These measures represent a level of security appropriate to the risks represented by the processing, taking into account the costs of the implementation.

2.4.4 The Processor shall give the Controller access to its applicable security documentation, and in other respects assist, so that the Controller may comply with his own responsibilities according to Applicable Laws.

2.4.5 The Controller has, unless otherwise agreed or pursuant to Applicable Laws, the right to access the Personal Data being processed and the systems used for this purpose. The Processor shall provide necessary assistance for such access to be given.

2.4.6 The Processor is subject to confidentiality regarding the documentation and the Personal Data for which it gains access to under this Agreement. This provision also applies after the termination of this Agreement.

2.4.7 The Processor may freely choose where it geographically stores the Personal Data, although in such a manner that the Personal Data shall not be stored in countries outside of EU/EEA without a separate written agreement or the transfer/storage being included in a special arrangement (e.g. "SCC"). The Controller may at any time require information on where the Personal Data is stored.

2.4.8 The Processor shall, without undue delay, notify the Controller on any request from governmental authorities or the police regarding the disclosure of the Personal Data, unless this is prohibited (e.g. prohibited by the Penal Code to preserve the confidentiality of an investigation), on any unauthorized access to or unauthorized disclosure of the Personal Data (see section 7.1) and on any request received directly from a Data Subject, without answering the request unless otherwise authorized to do so. The Processor will only disclose the Personal Data to governmental authorities or the police when legally obliged to do so, e.g. court order, judgement, order with a basis in law or similar.

2.5 In the case that the Controller's instructions or the Processor's assistance to the Controller lead to increased costs for the Processor compared to what was initially agreed upon between the parties, the Controller shall compensate the Processor for the increased cost in accordance with the Processor's regular terms and hourly rates.

## **3. Processor's Personnel**

3.1 The Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of the Processor who is given access to the Personal Data.

3.2 The Processor shall ensure in each case that access is strictly limited to those individuals who need to know/have access to the relevant Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Processor.

3.3 The Processor shall ensure that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality. The obligations of confidentiality will survive the termination of the personnel engagement.

#### **4. Security**

4.1 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 Processor shall in relation to the Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in GDPR Article 32 (1). The safeguards are designed to prevent accidental or unlawful destructions, loss, alteration, unauthorized access, security oversight and enforcement.

4.2 In assessing the appropriate level of security, the Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

4.3 The Controller confirms that the Processor has provided sufficient guarantees that they will implement appropriate technical and organizational measures that ensure that the processing meets the requirements of Applicable Laws, hereunder the protection of the Data Subjects' rights.

4.4 The Controller confirms to have assessed any security measures specifically stated in the Principal Agreement and thus accepted by the Controller, and the Controller is responsible (as between the parties and to data subjects and supervisory authorities) if those measures in themselves do not meet the GDPR standard of appropriateness. In the assessment the Controller has taken into account that any pre-stated description may only deal with specific aspects of the required security arrangements rather than describing a comprehensive solution.

4.5 The Processor will maintain the measures for the protection of security, confidentiality and integrity of the Personal Data. Measures are described in our Privacy Policies and is set forth in the Principal Agreement clause 5. The SESAM Services are upon accepting this Agreement ISO/IEC 27001:2013 certified.

#### **5. Subprocessing**

5.1 The Controller authorises the Processor to appoint (and permit each Subprocessor appointed in accordance with this section 5 to appoint) Subprocessors in accordance with this section 5 and any restrictions in the Principal Agreement.

5.2 The Processor may continue to use those Subprocessors already engaged by the Processor as of the date this Agreement enters into force, subject to the Processor in each case as soon as practicable meeting the obligations set out in section 5.4.

5.3 The Processor shall give the Controller prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within 2 weeks of receipt of that notice, the Controller notifies the Processor in writing of any objections (on reasonable grounds) to the proposed appointment, the Processor shall not appoint (or disclose any Personal Data to) that proposed Subprocessor until reasonable steps have been taken to address the objections raised by the Controller, and the Controller has been provided with a reasonable written explanation of the steps taken.

5.4 The Processor is responsible for the Subprocessor's performance in regards of the processing of Personal Data in accordance with the requirements of the GDPR.

5.5 With respect to each Subprocessor, the Processor shall:

5.5.1 before the Subprocessor's first processing of the Personal Data (or, where relevant, in accordance with section 5.2), ensure that the Subprocessor does not process Personal Data covered by this Agreement in any way that is not necessary for the performance of the Services, and that the Personal Data is not given to anyone else without this being specified in this Agreement or is permitted by the Controller in a prior written notice;

5.5.2 ensure that the arrangement between the Processor and the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for the Personal Data as those set out in this Agreement and meet the requirements of GDPR article 28 (3); and

5.5.3 provide to the Controller for review such copies of the Processors' agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Agreement) as the Controller may request from time to time.

## 5.6 Processing of Personal Data outside of the EU/EEA

5.6.1 If the agreement between the Processor and the Subprocessor involves a transfer to a Third Country, the Standard Contractual Clauses must at all relevant times be incorporated into the agreement between the Processor and the Subprocessor. Or, prior to the Subprocessor's first processing of Personal Data, the Processor must ensure that the Subprocessor enters into an independent agreement with the Controller that incorporates the Standard Contractual Clauses;

5.6.2 If the Processor is to enter into an agreement with Subprocessors in countries outside the EU/EEA, this should only be done according to EU model agreements for the transfer of personal data to Third Countries, or other applicable legal grounds for transfers to Third Countries in accordance with GDPR Chapter 5. The same applies even if Personal Data is stored in the EU/EEA when personnel with access to the data are located outside the EU/EEA.

5.6.3 If the Controller approves such transfers, the Processor shall cooperate with the Controller to ensure the legality of the transfers.

## 6. Data Subject Rights

6.1 Taking into account the nature of the Processing, the Processor shall assist the Controller by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligations to respond to requests to exercise Data Subject rights under Applicable Laws.

6.2 Section 2.5 applies equivalently to this section 6.1.

## 7. Personal Data Breach

7.1 The Processor shall notify the Controller without undue delay upon the event that the Processor or any Subprocessor becoming aware of a Personal Data Breach affecting the Personal Data, providing the Controller with sufficient information to allow the Controller to meet any obligations to report or inform the applicable Supervisory Authorities and/or the Data Subjects of the Personal Data Breach under Applicable Laws.

7.2 The Processor shall cooperate with the Controller and take such reasonable commercial steps as are directed by the Controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

7.3 Section 2.5 applies equivalently to this section 7.2.

## 8. Data Protection Impact Assessment and Prior Consultation

8.1 The Processor shall provide reasonable assistance to the Controller with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities,

which the Controller reasonably considers to be required of the Controller by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of the Personal Data by, and taking into account the nature of the Processing and information available to, the Processor.

8.2 Section 2.5 applies equivalently to this section 8.1.

## **9. Deletion or return of the Personal Data**

9.1 Subject to sections 9.2 and 9.3 the Processor shall as soon as possible and within 4 weeks of the date of cessation of any Services involving the Processing of the Personal Data (the “Cessation Date”), delete and procure the deletion of all copies of those Personal Data.

9.2 Subject to section 9.3, the Controller may in its absolute discretion by written notice to the Processor within 1 week of the Cessation Date require the Processor to (a) return a complete copy of all of the Personal Data to the Controller; and (b) delete and procure the deletion of all other copies of the Personal Data Processed by the Processor. The Processor shall comply with any such written request within 5 weeks of the Cessation Date.

9.3 The Processor may retain and store the Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws. Such cases always entail the provision that the Processor ensures the confidentiality of all such Personal Data and ensures that such Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

9.4 The Processor shall provide written certification to the Controller that it has fully complied with this section 9 within 5 weeks of the Cessation Date.

9.5 All costs connected to extraordinary measures in connection with deletion and/or providing copies of the Personal Data are to be carried by the Controller.

## **10. Audit rights**

10.1 Subject to sections 10.2 and 10.3, the Processor shall make available to the Controller on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits by the Controller or an auditor mandated by the Controller in relation to the Processing of the Personal Data by the Processor.

10.2 Information and audit rights of the Controller only arise under section 10.1 to the extent that the Principal Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Applicable Laws (including, where applicable, GDPR article 28 (3) (h)).

10.3 The Controller undertaking an audit shall give the Processor reasonable notice of any audit to be conducted under section 10.1, and shall avoid causing any damage, injury or disruption to the Processor’s premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit. The Processor need not give access to its premises for the purposes of such an audit:

10.3.1 to any individual unless he or she produces reasonable evidence of identity and authority;

10.3.2 outside normal business hours, as they are set out in the Principal Agreement, at those premises, unless the audit needs to be conducted on an emergency basis and the Controller undertaking an audit has given notice to the Processor that this is the case before attendance outside those hours begins; or

10.3.3 for the purposes of more than one audit, in respect of the Processor, in any calendar year, except for any additional audits that the Controller will be required to perform in accordance with Applicable Laws by a Supervisory Authority when the Controller responsible for the audit has identified the relevant request in its notice to the Processor.

10.4 The Controller shall treat all information obtained from the Processor arising from an audit as the Processor's strictly confidential information and not disclose the information to any third party or use the information otherwise than in connection with the audit.

10.5 The Processor shall immediately inform the Controller if, in its opinion, an instruction pursuant to this section 10 infringes the GDPR or other EU or Member State data protection provisions.

10.6 Section 2.5 applies equivalently to this section 10.3.

## **11. Transfers to Third Countries**

11.1 If the Controller by form of written instruction to the Processor prior to any such processing, instructs the Processor to transfer Personal Data to a Third Country, the Controller (as "Data Exporter") and Processor/Subprocessor (as "Data Importer") must enter into an agreement that includes the Standard Contractual Clauses.

11.2 The Standard Contractual Clauses shall come into effect under section 11.1 on the later of:

11.2.1 the data exporter becoming a party to them;

11.2.2 the data importer becoming a party to them; and

11.2.3 commencement of the relevant Restricted Transfer.

## **12. General Terms**

### **Governing law and jurisdiction**

12.1 This Agreement shall be subject to and interpreted in accordance with Norwegian laws. The parties to this Agreement hereby submit to the jurisdiction of the Courts of Oslo.

### **Order of precedence**

12.2 Nothing in this Agreement reduces the Processor's obligations under the Principal Agreement in relation to the protection of Personal Data or permits the Processor to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Principal Agreement.

12.3 In the event of inconsistencies between the provisions of this Agreement and any other agreements between the parties, including the Principal Agreement (except where explicitly agreed otherwise in writing) the provisions of this Agreement shall prevail.

### **Changes in Data Protection Laws, etc.**

12.4 The parties shall revise this Data Processing Agreement in the event of relevant changes to the Applicable Laws.

### **Severance**

12.5 Should any provision of this Agreement be invalid or unenforceable, then the remainder of this Agreement shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.



**Liability and liability limitations**

12.6 Each party is responsible for that party's processing of Personal Data being in accordance with the GDPR.