Terms and Conditions of Services

Life & Soft a SeqOne company, a simplified joint stock company with capital of €400.000, registered with the Montpellier Trade and Companies Register under number 790 422 331, having its registered office at 22 rue Durand - 34000 Montpellier (hereinafter the "**Provider**" or the "**Publisher**"), is a bioinformatics company whose purpose, in France and abroad, is the creation, development, marketing and operation of genetic data analysis and management systems and solutions. In particular, the Provider is the publisher of a platform called "Micro LifePipe", which is a software solution accessible in remote "SaaS" (Software as a Service) mode (hereinafter the "**Platform**") enabling professionals to analyze and interpret genomic data files for the purpose of identifying relevant information (hereinafter the "**Services**").

The Micro LifePipe offer includes access to three specialized analysis modules: Viro LifePipe (viral genomics analysis), Microbiome LifePipe (microbiome analysis), and Meta LifePipe (metagenomic analysis).

The "**Customer**", as defined in the Quotation or Offer.

Hereinafter referred to individually as the "**Party**" or collectively as the "**Parties**".

TITLE I - GENERAL PROVISIONS

ARTICLE 1 - DEFINITIONS

The terms defined in this article and used in these General Terms of Services have the following meanings:

- **Customer**: the legal entity identified in the Quotation or the Offer, having subscribed to the Services provided by the Service Provider under the Contract.
- **General Conditions of Services** or **GCS**: the present general conditions for the provision of services, including the general conditions of use of the Platform and the technical and organizational conditions of the Health Data Hosting Service.
- **Content**: all data, information or documents uploaded by a User or directly imported, on the Platform, relating to a File, in particular raw data from the sequencer, it being specified that data sequencing is carried out by the Customer under its sole responsibility.
- **Quotation**: document issued by the Service Provider and accepted by the Customer, describing in detail the Services subscribed to by the Customer.
- **Customer Data**: all data, including Personal Data and Health Data, that the Customer provides to SeqOne, it being understood that Customer Data may be Customer Data or Personal Data collected by or on behalf of the Customer, which are processed via the Platform.
- **Health Data**: any Personal Data relating to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about that person's state of health.
- **Personal Data**: any information relating to an identified or identifiable natural person (hereinafter referred to as the **Data Subject**); an "identifiable natural person" is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a

name, an identification number, location data, an online identifier, or to one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity.

- **Folder**: digital space accessible to Users, containing all documents and information, and allowing, depending on the options subscribed to by the Customer, access to the various Modules.
- **Data Protection Laws**: means all applicable worldwide data protection and privacy legislation applicable to the Customer under the Contract, including, without limitation, the Applicable Regulations, the CCPA and UK data protection and privacy laws, in each case as amended, consolidated or replaced from time to time.
- **Module** or **Workset**: ergonomic system enabling the User to designate the Content to be analyzed and to configure the analysis, software components enabling data analysis according to a precise algorithmic approach, as well as visualization and analysis assistance tools. The Micro LifePipe offer includes:
    - **Viro LifePipe**: Module dedicated to viral genomics analysis
    - **Microbiome LifePipe**: Module dedicated to microbiome composition and diversity analysis
    - **Meta LifePipe**: Module dedicated to metagenomic analysis

  Access to these Modules depends on the Services subscribed in the Quotation or Offer.
- **Offer**: an offer issued by a third party, such as a reseller, to which the Customer has directly subscribed, and which integrates the Services provided by SeqOne.
- **Platform**: software platform accessible remotely via a browser, enabling the storage and provision of analysis tools and computer interfaces integrating information from third parties. The Platform enables Users to access Modules or Worksets with a view to identifying, under the sole responsibility of the User, information relevant to the establishment of a medical diagnosis, which is grouped together in the form of a report.
- **Applicable regulations**: data protection laws applicable in Europe, including: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (iii) the applicable national implementations of (i) and (ii); or (iii) in relation to the United Kingdom, any applicable national legislation which replaces or transposes into domestic law the GDPR or any other data and privacy law following the United Kingdom's exit from the European Union; and (iv) the Swiss Federal Data Protection Act of June 19, 1992 and its ordinance; in each case, as amended, consolidated or replaced.
- **Data Controller**: means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. For the purposes of this Contract, the Customer is the Data Controller.
- **Services**: all the services provided by SeqOne to which the Customer has subscribed and defined in the Quotation or in the Offer, and including access to and use of the Platform and the Hosting Service.
- **Hosting Service**: the Health Data hosting services provided by SeqOne. The Hosting Service constitutes one of the "Services" as defined herein.

- **Processing**: any operation or set of operations, whether or not performed using automated processes and applied to Personal Data or sets of Personal Data, such as collection, recording, organization, structuring, storage, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other form of making available, reconciliation or interconnection, limitation, erasure or destruction.
- **User**: any natural person of legal age and capacity, designated by the Customer, who browses and uses the Platform, under the sole and exclusive responsibility of the Customer, the number of authorized Users being defined in the Quotation or in the Offer.
- **Personal Data Breach**: means a breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or unauthorized access to Personal Data transmitted, stored or otherwise Processed by SeqOne and/or its Subsequent Subcontractors in connection with the Supply. Breach of Personal Data shall not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful login attempts, pings, port scans, denial of service attacks and other network attacks on firewalls or networked systems.

ARTICLE 2 - PURPOSE

The purpose of these General Conditions of Services is to define the conditions and commitments of the Parties relating to the provision of Services by SeqOne, including in particular access to the Platform and the implementation of the Hosting Service.

The GCS include the general conditions of use of the Platform, the technical and organizational conditions under which SeqOne provides the Hosting Service, and a common section applicable to all the Services covered by the Contract.

ARTICLE 3 - CONTRACTUAL DOCUMENTS

The contractual relations between the Parties are governed by all the following documents, hereinafter referred to together as the "**Contract**", listed in descending hierarchical order as follows:

1. Where applicable, the special conditions of service agreed between the Parties (hereinafter referred to as the "**Special Conditions**");
2. The Quotation or Offer;
3. These General Conditions of Service and its Appendix:
    - Appendix I: Data Processing Agreement;

The Contract is the sole basis of the commercial relationship between SeqOne and the Customer and defines the contractual conditions under which the Service Provider provides the Customer with the Services described in the Quotation.

Any order for Services, any acceptance of a Quotation and, more generally, any use of the Platform implies definitive and irrevocable acceptance by the Customer and its Users of these GCS, which the Customer expressly acknowledges to have agreed to and accepted, and to have agreed to and accepted by all Users. The GCS apply without restriction or reservation to

all contractual relations between SeqOne and the Customer, subject to any stipulations to the contrary contained in Special Terms and Conditions expressly agreed between the Parties, and regardless of any clauses that may appear in the Customer's documents, in particular its general terms and conditions of purchase. The Customer hereby waives the right to rely on any clauses included in its own documents, and any reservation by the Customer on this point shall be deemed unwritten, even if its own documents provide otherwise. In all cases, any clause not expressly stipulated in the Quotation or in these GCS must be subject to SeqOne's prior written agreement.

Finally, and for greater clarity, it is specified that the CE-IVD (then IVDR) marking applies only to the Platform and not to reagents sold in bundles or to functionalities specifically identified as RUO on the Platform. Similarly, these GCS do not govern SeqOne partner kits and/or bundles, even if these partners are presented directly to the Customer by SeqOne.

The Contract constitutes the entire agreement between the Parties concerning its subject matter: it cancels and replaces all other agreements, letters of intent, representations and warranties, as well as all commercial practices, whether written or oral, previously entered into between the Parties. Notwithstanding the foregoing, in the event that this Contract forms part of a public procurement contract, the stipulations of the public procurement contract, as defined in the contractual documents issued by the public purchaser, shall prevail in the event of any contradiction with the provisions of this Contract.

The Contract may only be amended by a written document signed by all the Parties: it is therefore formally agreed that any tolerance or waiver by one of the Parties in the application of all or part of the commitments provided for, whatever the frequency and duration thereof, shall not constitute a modification of the Contract or generate any right whatsoever. The possible cancellation of one or more clauses of the Contract by a court decision or by mutual agreement between the Parties shall not affect its other stipulations, which shall continue to be in full force and effect. In the event that the performance of one or more of the clauses of the Contract is rendered impossible as a result of its cancellation, the Parties will attempt to reach agreement in order to establish a new clause, the spirit and letter of which will be as close as possible to the old clause, with the other stipulations of the Contract remaining in force.

ARTICLE 4 - DURATION

The Contract comes into force on the date of signature between the Parties and for the duration specified in the Quotation or the Offer. In the specific event that the Customer continues to use the Platform after the Contract has expired and/or the subscribed Services have been consumed, the Contract will be automatically renewed for an unlimited period until a new Quotation or Offer is signed, it being specified that either Party may terminate the renewed Contract in writing at any time with three (3) months' written notice.

ARTICLE 5 - DESCRIPTION OF SEQONE SERVICES

The Customer benefits from the Services described in the Quotation or Offer, under the conditions and within the limits set out in these T&C.

The **Micro LifePipe** subscription includes access to:

1. Viro LifePipe Module - Viral genomics analysis enabling:

- Upload of viral genomic data (FASTQ)
- Launch of bioinformatics pipelines for viral variant identification
- Visualization and annotation of viral mutations
- Generation of reports for viral surveillance and characterization

2. Microbiome LifePipe Module - Microbiome analysis enabling:

- Processing of 16S/ITS sequencing data and shotgun metagenomics
- Taxonomic profiling and diversity analysis
- Comparative analysis of microbial communities
- Functional annotation and pathway analysis

3. MEta LifePipe Module - Metagenomic analysis enabling:

- Assembly and binning of metagenomic data
- Gene prediction and functional annotation
- Metabolic pathway reconstruction
- Integration of multi-omic data

All modules include:

- Data upload and management capabilities
- Bioinformatics analysis pipelines
- Interactive visualization tools
- Collaboration features
- Report generation for research purposes
- Data download and export

Any Service that has not been used by the end of the Contract will be lost, with no right for the Customer to request reimbursement. In any event, the Customer acknowledges that the Platform is subject to change, and that the Services may be adapted accordingly at any time. The Customer will be notified of any withdrawal of the Services offered on the Platform by registered letter with acknowledgement of receipt, or by any other durable written medium providing proof of dispatch, or by extrajudicial act. The Customer may then terminate the Contract by registered letter with acknowledgement of receipt within one (1) month of notification. If the Customer does not make use of this termination option within the given period, he/she will be deemed to have accepted the modification of services as from its entry into force. It is specified that use of the Platform by the Customer may be subject to checks by SeqOne.

TITLE II - GENERAL CONDITIONS OF USE OF THE PLATFORM

ARTICLE 6 - CONDITIONS OF ACCESS TO THE PLATFORM

In consideration of payment of the price, SeqOne grants the Customer a personal, non-exclusive and non-transferable right (by any means whatsoever), for one or more User(s), to access the Platform in accordance with the conditions, including duration, defined in the Quotation or in the Offer. The Customer is hereby informed that the Platform is accessible in SaaS mode and/or locally (directly on the Customer's infrastructure, an option to be agreed under specific conditions and with SeqOne's prior agreement), and that access to the Platform will be made on the Customer's own hardware, on the Customer's own Internet access network compatible with the Platform, and under the Customer's own responsibility. The Customer is solely responsible for the hardware and software resources and Internet connection used. Telecommunication costs incurred in accessing the Platform are the sole responsibility of the Customer.

The Customer is solely and exclusively responsible for the use of the Platform by its Users, and must take all necessary measures to protect and ensure that its Users protect their login details and passwords in terms of confidentiality and security. Each User has his/her own personal, reserved, non-disclosable and secure access to the Platform via his/her login and password. The Customer is hereby informed and accepts that the User's entry of his/her login and password constitutes proof of his/her identity, which will be confirmed by a double authentication process. The User is also responsible for maintaining the confidentiality of his/her login and password. He/she must immediately contact SeqOne at support@seqone.com if he/she notices that his/her account has been used without his/her knowledge. The Customer acknowledges the Publisher's right to take all appropriate measures in such a case. SeqOne may not under any circumstances be held responsible for the consequences of fraudulent use of the password by a third party, or its loss.

ARTICLE 7 - GENERAL OBLIGATIONS OF THE CUSTOMER AND USERS

The Customer acknowledges having taken cognizance of the characteristics and constraints, particularly technical, of the Platform as a whole, and declares that it meets his needs. The Customer undertakes to use the Platform in a fair manner, in accordance with the GCS and all applicable regulations. The Customer undertakes not to infringe the rights of third parties or public order. The Customer is solely and exclusively responsible for the Content he uploads or downloads on the Platform. The Customer warrants to SeqOne that he/she has all necessary rights and authorizations, in particular the consent of the persons whose Personal Data, including Health Data, is analyzed, and shall indemnify SeqOne at first request against any third-party claims, including those of individuals whose genomic characteristics have been uploaded to the Platform or for the use of any Service. The User shall refrain from uploading, in particular and without this list being exhaustive, infringing Content or Content linked to an illicit activity and more generally Content likely to infringe, in any way and in any form whatsoever, the rights of third parties or SeqOne, or personality rights, such as the right to privacy, image or honor or dignity. Any use of the Platform that violates, or suggests a violation of, any of these obligations may entitle SeqOne to terminate the Contract immediately and automatically. The Customer alone assumes the risks associated with its activity, and with obtaining the authorizations required to use and operate the Platform. The right to use the Platform is

exclusive of all other rights and does not in any way imply the right to perform any act not expressly authorized. In particular, the Customer undertakes not to undermine or attempt to undermine the integrity or security of the Platform. In this respect, the Customer undertakes in particular (i) not to disseminate computer data intended to disrupt the normal operation of the Platform, (ii) not to upload, post or transmit in any way whatsoever any Content containing computer viruses, worms, Trojan horses, codes or scripts likely to harm the integrity or confidentiality of the systems and data of SeqOne, other Users or any third party, (iii) not to extract data from the Platform for unauthorized reuse, and (iv) not to copy, modify, in particular by decompiling, disassembling, merging into other software or determining or in any other way, the source code, algorithms, structure or organization underlying the Platform, alter, adapt, create derivative works in particular by translating, arranging and more generally modifying all or part of the Platform. In the event of breach by the Customer or its Users of one or more of their obligations, access to the Platform may be temporarily suspended or withdrawn, and the Contract terminated immediately and automatically by SeqOne.

In addition, the contentious Content may be deleted and the account of the User having introduced the contentious Content may be temporarily or permanently blocked. Depending on the nature of the breach, the Customer may also be subject to infringement proceedings. The Customer must take the necessary steps to safeguard his/her own account and/or File information. Finally, the Customer undertakes to provide SeqOne with remote access to the Platform should technical support be required, if the Platform is accessible locally from the Customer's equipment. SeqOne undertakes to use this access only at the Customer's request.

ARTICLE 8 - GUARANTEES AND LIABILITY OF SEQONE

SeqOne undertakes to provide the Platform diligently and in accordance with IT best practice, in compliance with the principles set out in the ISO 27001 standard, it being specified that the Customer accepts SeqOne as a trusted third party and that SeqOne has only an obligation of means to the exclusion of any obligation of result, which the Customer expressly accepts.

The Platform is accessible 99% of the time, this rate of service corresponding to an unavailability of the Platform of twenty-two (22) hours per quarter, excluding planned maintenance (eight (8) hours of planned maintenance per year, per period of four (4) hours maximum, with five (5) working days' notice), with the exception of cases of force majeure and difficulties linked to the structure of the telecommunications network or technical difficulties.

SeqOne does not guarantee access to or permanent operation of the Platform, and reserves the right to interrupt, temporarily suspend or modify access to all or part of the Platform without prior notice in the event of an IT threat or suspicion of improper use by the Customer, without this interruption giving rise to any right to compensation for the Customer. Similarly, SeqOne does not guarantee the quality of communication links with the User, and may not be held liable for any failures or malfunctions observed on the communication networks used by the Customer. SeqOne cannot be held responsible for any interruption of the Services due to technical problems, congestion of the Internet network or failure of any other teletransmission system, which could prevent the normal operation of the Platform.

FURTHERMORE, SEQONE DOES NOT GUARANTEE ANY ECONOMIC

BENEFITS IN CONNECTION WITH THE USE OF THE PLATFORM, NOR DOES IT UNDERTAKE TO ACHIEVE ANY SPECIFIC RESULT, PARTICULARLY IN MEDICAL TERMS. SEQONE DOES NOT ENGAGE IN ANY MEDICAL ACTIVITY, AND MERELY MAKES COMPUTER TOOLS AVAILABLE TO PROFESSIONALS, WHO MUST USE THEIR KNOWLEDGE AND JUDGEMENT TO INTERPRET THE RESULTS PROPOSED BY THE PLATFORM. THUS, THE CUSTOMER ACKNOWLEDGES THAT USE OF THE PLATFORM IS AT HIS OR HER OWN RISK, PARTICULARLY AS REGARDS THE RESULTS OBTAINED, THE PREPARATION OF SUMMARY REPORTS, THEIR INTERPRETATION, AND THE OPERATION AND SECURITY OF HIS OR HER EQUIPMENT. AS SUCH, THE CUSTOMER IS ENTIRELY RESPONSIBLE FOR THE USE MADE BY ITS USERS OF THE RESULTS AND REPORTS OFFERED BY THE PLATFORM, AND FOR PRESERVING THE SECURITY AND INTEGRITY OF ITS DATA AND CONTENT, HARDWARE AND SOFTWARE WHEN USING THE PLATFORM. CONSEQUENTLY, SEQONE DOES NOT GUARANTEE THAT THE USE OF DOCUMENTS PUBLISHED VIA THE PLATFORM WILL MEET THE NEEDS AND/OR SITUATION OF THE CUSTOMER OR ITS USERS, AS THE MODULES AND INFORMATION (INCLUDING THOSE FROM THIRD-PARTY SITES) OFFERED BY SEQONE ARE GENERIC AND MUST BE COMPLETED AND CUSTOMIZED IN THEIR ENTIRETY BY THE USER. UNDER NORMAL CONDITIONS, SEQONE PERFORMS NO MODERATION, SELECTION, VERIFICATION OR CONTROL OF ANY KIND, WITH THE EXCEPTION OF VERIFICATION AND CONTROL OF THE INTEGRITY OF FILES UPLOADED BY USERS: SEQONE ACTS ONLY AS A CONTENT HOST AND CANNOT BE HELD RESPONSIBLE FOR CONTENT UPLOADED TO THE PLATFORM. THE EDITOR MAY PROVIDE HYPERTEXT LINKS TO WEBSITES PUBLISHED AND MANAGED BY THIRD PARTIES. HOWEVER, SEQONE EXERCISES NO CONTROL OVER OR SUPERVISION OF THESE THIRD-PARTY SITES AND CANNOT THEREFORE BE HELD RESPONSIBLE FOR THE CONTENT AND SERVICES MADE AVAILABLE BY THESE THIRD-PARTY SITES, FOR PROBLEMS OF SECURITY OR INTEGRITY OF THE USER'S DATA, HARDWARE AND SOFTWARE, OR FOR ANY CONSEQUENCES OR DAMAGE THAT MAY RESULT FROM THE USE OF THESE APPLICATIONS AND/OR THIRD-PARTY SITES. IN NO EVENT SHALL SEQONE BE LIABLE FOR ANY CONSEQUENTIAL AND/OR INDIRECT DAMAGES, INCLUDING BUT NOT LIMITED TO LOSS OF BUSINESS, LOSS OF CUSTOMERS, LOSS OF SALES, LOSS OF DATA, MORAL OR COMMERCIAL PREJUDICE, OR DAMAGE TO BRAND IMAGE, SUFFERED BY THE CUSTOMER AND/OR USER. SEQONE'S TOTAL LIABILITY FOR ALL PROVEN DIRECT DAMAGE CAUSED BY A BREACH OF SEQONE'S OBLIGATIONS, TO THE EXCLUSION OF ANY ELEMENT OR ACTION BY THE CUSTOMER OR A THIRD PARTY, SHALL IN NO CASE EXCEED THE AMOUNT (EXCLUDING TAXES) ACTUALLY PAID BY THE CUSTOMER TO SEQONE FOR ACCESS TO THE PLATFORM DURING THE LAST TWELVE MONTHS PRIOR TO THE OCCURRENCE OF THE DAMAGE.

Any dispute by the Customer concerning the performance or non-performance by SeqOne of

its obligations must be substantiated and sent by registered letter with acknowledgement of receipt sent at the latest within six (6) months of the alleged non-performance. Failing this, the Customer waives the right to invoke the alleged non-performance.

ARTICLE 9 - CUSTOMER LIABILITY

The use of the Platform for Research purposes requires the performance of a method validation under the Customer's routine conditions, which is the sole responsibility of the Customer. The Customer is solely responsible for the use of the Platform by the Customer and its Users, and in particular for obtaining all necessary authorizations for the use and exploitation of the Platform and the data generated, including the patient's consent, and for the Content uploaded to the Platform, and will consequently be personally liable for any damage caused to SeqOne, to any User or to any third party, in particular to any patient, as a result of the use of the Platform. In particular, the Customer is solely responsible for the use of the information received by using the Platform, its selection for the purpose of drawing up a report and its interpretation.

The Customer undertakes to inform the Publisher without delay of any breach of these GCS by one of its Users, and to indemnify SeqOne for any direct or indirect damage arising from the use of the Platform, including but not limited to all losses, costs, expenses, legal fees and sums paid in damages. Each of the Parties declares that it is covered by a professional insurance policy guaranteeing the consequences of any civil liability it may incur, and undertakes to provide the other Party with a valid insurance certificate on first request. By mutual agreement, the Parties exclude the application of article 1222 of the French Civil Code.

ARTICLE 10 - DELETION OF AN ACCOUNT

The Customer and the User may delete their account at any time, at their own discretion, by contacting SeqOne's customer service department at the following address: support@seqone.com. Deletion of an account does not entail termination of the Contract or suspension of the associated payment obligations.

TITLE III - TECHNICAL AND ORGANIZATIONAL CONDITIONS FOR THE PROVISION OF THE HOSTING SERVICE

ARTICLE 11 - HOSTING FACILITIES

SeqOne undertakes to host, or have hosted by a subcontractor, Customer Data on infrastructures located in countries detailed in Appendix I - Data Protection Agreement and Sub-Annex III, with encrypted backups stored in Ireland for disaster recovery purposes.

By way of derogation, in the event of transfer of Customer Data outside the EEA, the Service Provider guarantees:

- that the Customer's explicit consent is required for any transfer of Personal Data outside

the EEA, and
- compliance with the requirements of the GDPR and the provisions of the Agreement on the Protection of Personal Data set out in Appendix I of these GCS.

ARTICLE 13 - SEQONE'S COMMITMENTS - DESCRIPTION OF THE HOSTING SERVICE

(Note: Article 12 is not present in the source document)

13.1. Description of the Hosting Service and Expected Results

The Hosting Service comprises the hosting of Customer Data, including data resulting from genomic and/or molecular biology analyses, as well as clinical and administrative data associated with patients, which are processed via the Platform, the uses of which are described in Article 5.

The expected result for the Customer is access to a secure, high-performance and reliable environment for the entire life cycle of its genomic analyses, from raw data to the final report.

SeqOne is bound by a general obligation of means, and undertakes in this respect to provide the Hosting Service in accordance with the rules of the art and its profession, and in particular to contribute its know-how, experience and expertise, as well as any hardware and/or software required.

13.2 Quality and performance indicators (Service Level Agreement)

13.2.1. Service indicators

In accordance with article R.1111-11 6° of the French Public Health Code, SeqOne has set up quality and performance indicators to enable the Customer to verify the Platform's level of service.

Service indicators	**Definition and measurement method**	**Guaranteed Level (SLA)**	**Measurement frequency**
Platform availability rate	"Availability of critical web interfaces and APIs, enabling connection, consultation and analysis launch. Formula: ((Total Quarter Time - Unplanned Downtime) / Total	99%	Quarterly

	Quarter Time) x 100. Unavailability is measured by SeqOne's external monitoring tools."		

SeqOne thus guarantees an annual Platform availability rate of 99%, this service rate corresponding to Platform unavailability of 22h per quarter, excluding planned maintenance (8 hours of planned maintenance per quarter, per period of 4 hours maximum, with 5 working days' notice), with the exception of cases of force majeure and difficulties linked to the structure of the telecommunications network or technical difficulties.

13.2.2. Application of penalties

In the event of non-compliance with the "**Platform Availability Rate**" defined above, over a given calendar month, the Customer will be entitled to a service credit applicable to his next invoice. Service credits must be claimed by the Customer in writing within thirty (30) days of the end of the month in which the breach occurred.

The scale of penalties is as follows:

- **Platform availability rate between 95.0% and 99.0%**: penalty equivalent to 5% of the annual value corresponding to the number of analyses performed over the contractual year (price of Services), calculated *pro rata temporis* over the measurement period.
- **Platform availability rate below 95.0%**: penalty equivalent to 10% of the annual value corresponding to the number of analyses carried out over the contractual year (price of Services), calculated on a *pro rata temporis basis* over the measurement period.

For example: If the platform is unavailable for a cumulative period of 44 hours from April 1st to June 30th, the availability rate is (91 days * 24 hours - 44 hours) / (91 days * 24 hours) = 98%. If a customer carries out 1,000 analyses for €50,000 over the year, the customer is entitled to a discount of €50,000 / 4 * 5% = €625.

Furthermore, the total cumulative amount of penalties payable over a period of 12 consecutive months may not exceed 10% of the total amount of invoices for the Service affected over this same period.

13.2.3. Service reporting

SeqOne constantly monitors service indicators and keeps the associated performance data. At the Customer's written request, SeqOne undertakes to compile and supply a summary performance report for the past month(s) concerned. This report will be delivered electronically within a maximum of ten (10) working days after receipt of the request.

13.3 SeqOne guarantees

As part of the Hosting Service, SeqOne guarantees the availability, integrity, confidentiality, traceability and auditability of Customer Data.

13.3.1 Guarantee of Availability

SeqOne undertakes to implement all technical means necessary to ensure a high level of availability of the Platform. In this respect, SeqOne guarantees an annual availability rate for the Platform, as well as the calculation methods and applicable penalties, as defined in article 13.2 of these General Conditions of Services.

In addition, the Platform uses redundancy mechanisms over several Availability Zones to compensate for hardware failures.

It is specified that SeqOne implements a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP) in compliance with ISO 27001 requirements. These plans include: (i) risk scenarios and mitigation strategies to limit service interruptions, and (ii) regular tests and updates to ensure their effectiveness.

13.3.2. Integrity guarantee

SeqOne undertakes to protect the integrity of Customer Data against accidental or malicious alteration or corruption. To this end, the following measures have been implemented:

- **File Integrity Check**: checksum mechanisms (e.g. MD5, SHA-256) are used when uploading and transferring data files to verify that they have not been altered.
- **End-to-end data protection**: implementation of (i) AES-256 encryption for data at rest, (ii) TLS 1.3 for all data in transit, and (iii) regular key rotation managed by a secure key management system (KMS).
- **Transactional mechanisms and integrity constraints** are implemented at database level to guarantee the consistency of structured information (metadata, annotations, etc.) and database integrity.

13.3.3. Confidentiality guarantee

SeqOne implements state-of-the-art technical and organizational measures to guarantee the strict confidentiality of Customer Data.

- **Enhanced access control policies**: (i) role- and attribute-based access control mechanisms (ABAC); (ii) time-based restrictions for high-privilege accounts and (iii) automated alerts in the event of abnormal access patterns.
- **Segregation of Customer Data**: SeqOne guarantees strict logical segregation of each Customer's Customer Data within its shared infrastructure. Under no circumstances may a Customer access the Customer Data of another Customer.
- **Encryption**: Systematic encryption of Customer Data (at rest and in transit) is a fundamental measure to protect its confidentiality.
- **Staff obligations**: in accordance with article 27 of these GCS, SeqOne staff are subject to reinforced contractual confidentiality obligations. Access to Customer data by SeqOne personnel is strictly limited to maintenance or support operations, and is carried out (except in the event of a security emergency) after notification or with the agreement of the Customer.

13.3.4 Guarantee of Traceability & Auditability

SeqOne ensures complete logging and monitoring: (i) all access logs are encrypted,

tamper-proof and retained for twelve (12) months, (ii) real-time analysis is performed to detect and respond to unusual activity, and (iii) detailed log review reports are made available to the Customer on a quarterly basis.

SeqOne makes available on request reports detailing: (i) security indicators (e.g. number of threats detected, vulnerabilities resolved), (ii) ISO 27001 compliance status, and (iii) recommendations for improving security posture.

ARTICLE 14 - RIGHTS OF DATA SUBJECTS

14.1 Information and consent of Data Subjects

The Customer, as the party responsible for the processing carried out as part of the Hosting Service, is solely responsible for informing and obtaining the consent of the Data Subjects to the Personal Data, including Health Data, which is the subject of said processing.

In this context, the Customer undertakes to ensure that this information includes, in a clear, intelligible and appropriate manner, all mandatory information concerning the protection of Personal Data. The Customer also undertakes to inform the Persons concerned of any changes likely to occur to the Hosting Service whenever SeqOne informs it of such changes.

14.2. Exercise of the rights of Data Subjects

The Customer undertakes to ensure that the rights of Data Subjects whose Personal Data is hosted under this Agreement are respected. In this respect, the Customer undertakes in particular to:

- Inform Data Subjects that they have the right to object to such hosting, provided that they invoke a legitimate reason, as set out in the same article;
- Inform them of their rights under Regulation (EU) 2016/679 (GDPR), namely:
    - Right of access to their Personal Data;
    - Right of rectification;
    - Right to object;
    - Right to limit processing;
    - Right to erasure ("right to be forgotten");
    - Right to portability of their Personal Data;
    - Right to lodge a complaint with the competent supervisory authority (in France, the CNIL);
    - The right to define directives concerning the fate of their Personal Data after their death.

To the extent that the Customer is unable to respond independently to a request for the exercise of rights by a Data Subject, SeqOne will provide the Customer, upon the Customer's written request, with reasonable assistance in responding to said request for the exercise of rights by a Data Subject or to any request from personal data protection authorities regarding the Processing of Personal Data under the Agreement. The Customer shall reimburse SeqOne for reasonable costs arising from such assistance.

Where a Data Subject exercises its rights directly with SeqOne at dpo@seqone.com, SeqOne

will promptly inform the Customer and advise the Data Subject to submit its request directly to the Customer. The Customer shall be solely responsible for responding in a substantial manner to this request to exercise rights or to any communication involving Personal Data.

ARTICLE 15 - ACCESS TO HOSTED HEALTH DATA

SeqOne has an authorization policy for personnel involved in the Hosting Service. The authorization policy identifies the various persons authorized to intervene as part of the provision of the Hosting Service, and determines the procedures for granting access rights, such as validation, duration, revocation, suspension, modification and deletion.

In this respect, it is specified that access to Customer Data is strictly limited to authorized SeqOne personnel, in accordance with the principle of least privilege. Any request for access rights is systematically subject to prior validation and documentation.

ARTICLE 16 - PERSONAL DATA BREACHES

As soon as SeqOne becomes aware of any Personal Data Breach, SeqOne undertakes to notify the Customer without undue delay, and will provide the Customer with timely information relating to the Personal Data Breach as soon as SeqOne becomes aware of it or as reasonably requested by the Customer. Such notification shall be made in accordance with the provisions of Appendix I of these GCS.

At the Customer's request and expense, SeqOne will promptly provide the Customer with the reasonable assistance necessary to enable the Customer to notify the relevant Personal Data breaches to the competent authorities and/or the Data Subjects, if the Customer is required to do so under the applicable Regulations.

All the terms and conditions and the procedure applicable in the event of a Personal Data Breach are specified and detailed in Appendix I of these General Conditions of Services.

ARTICLE 17 - SUBCONTRACTING

The Customer authorizes SeqOne to use subcontractors subject to prior notification to the Customer and the conclusion of a written agreement with the subcontractors.

The list of subcontractors is regularly updated and made available to the Customer on request.

SeqOne ensures that all suppliers and subcontractors comply with strict security standards, including contractual agreements reflecting ISO 27001 requirements. SeqOne undertakes to immediately terminate any contract with a subcontractor that does not comply with these requirements.

The conditions applicable to the use of subsequent subcontractors are specified in Appendix I of these GCS.

ARTICLE 18 - TECHNICAL MODIFICATIONS AND UPGRADES TO THE

HOSTING SERVICE

SeqOne undertakes to inform the Customer of any modifications or technical developments introduced by SeqOne or imposed by the applicable legal framework which may impact the Customer's Health Data hosting services (article R. 1111-11(9) of the French Public Health Code). This information will be communicated to the Customer in writing within a reasonable timeframe, and will specify the nature of the modification or change, its potential impact on the Services, and the timetable for its implementation.

In the event that such modification or change does not comply with the service levels and guarantees as defined in article 13 of these GCS, the Customer's prior written agreement will be required before implementation of such modification or change. SeqOne provides the Customer with all the information necessary to enable him to make an informed decision. In the event of disagreement by the Customer, the Parties undertake to negotiate alternative solutions in good faith. If no acceptable solution is found, either Party may terminate the Contract by registered letter with acknowledgement of receipt. Changes or developments imposed by the applicable legal framework and requiring urgent implementation to ensure regulatory compliance may be applied by SeqOne after informing the Customer as soon as possible. In this case, SeqOne undertakes to minimize any negative impact on service levels and guarantees and to fully inform the Customer.

ARTICLE 19 - AUDITS

SeqOne will regularly commission an independent audit to evaluate and document the adequacy of the technical and organizational measures implemented as part of the Services, and will share, at the Customer's written request, a summary of the results of such audit and/or other related information that the Customer may reasonably request. Customer may also designate, at Customer's expense, an authorized representative of Customer's choice reasonably acceptable to SeqOne to view, up to once per calendar year, the latest audit report, which may only be viewed at the certified site, upon thirty (30) calendar days' notice and during normal business hours, provided that such representative enters into a confidentiality agreement with SeqOne and Customer or is legally bound by an obligation of professional secrecy. Copying of the audit report is not authorized, and its viewing is subject to the signing of a confidentiality agreement with SeqOne and the Customer, and to compliance with the regulations and procedures in force at the certified site. If SeqOne does not perform such audits or share the results thereof with the Customer, the latter is authorized to verify the adequacy of SeqOne's technical and organizational measures by himself or through an authorized representative of his choice reasonably acceptable to SeqOne, provided that such representative enters into a confidentiality agreement with SeqOne and the Customer or is legally bound by an obligation of professional secrecy. If the Customer wishes to carry out such audits, the Customer must provide SeqOne with a written audit plan (including all technical details likely to have an impact on the hosting of Customer Data and, if applicable, the identity of the provider appointed by the Customer) for approval by SeqOne with three (3) months' notice. SeqOne reserves the right to refuse the service provider designated by the Customer on reasonable grounds, in particular if there is a risk of conflict of interest or competition. The Customer (and where applicable its representative) undertakes to treat all audit reports and all

information relating thereto as confidential information of SeqOne protected by article 8 of these GCU and by articles L.151-1 et seq. of the French Commercial Code protecting business secrecy.

ARTICLE 20 - GUARANTEES AND PROCEDURES

The Customer confirms that it has read the User version of the procedures and guarantees put in place by SeqOne in the event of failure of the Hosting Service and declares that it accepts them unreservedly.

SeqOne undertakes to answer any questions the Customer may have concerning these procedures and guarantees; the Customer is invited to send any questions to the following address: support@seqone.com

In addition, if SeqOne fails to comply with the service level guarantees defined in article 13.2 of these GCS, the Customer is entitled to request the application of the penalties provided for in the said article, under the conditions set out therein. In the event of serious, repeated and duly documented failures, demonstrating the Service Provider's inability to provide the service at the expected level of quality, the Customer shall have the right to terminate the contract for fault and to trigger the Reversibility procedure described in article 21 of the GCS.

ARTICLE 21 - REVERSIBILITY AND ASSISTANCE

21.1 Reversibility

SeqOne will provide the Customer, within thirty (30) days of the end of the Contract, or early termination of the service, with a basic export of the Customer Data in a commonly used, machine-readable format. This format will be VCF and TSV and will include at least the following basic Customer Data fields: sample identification. The standard return of Customer Data is included in our prices. However, any additional verification, such as manual validation of content by an operator, will be subject to an additional quote. However, this basic export is intended to facilitate the Customer's transition and may not include all Customer Data elements, specific Customer Data structures or functionalities present within the LifePipe Platform. Customer acknowledges that it is solely responsible for importing and using the exported Customer Data in a new system or environment. SeqOne will provide reasonable technical documentation relating to the structure and format of the exported Customer Data, but will not be obliged to provide any further assistance relating to the migration of Customer Data or integration into third party systems. The export of Customer Data will be carried out via a secure transfer method, for which SeqOne may charge a reasonable fee based on current tariffs. Following the provision of the simple export of Customer Data to the Customer and a reasonable period of ninety (90) days, SeqOne will, unless legally required to retain such Customer Data, securely delete or anonymize Customer Data in its possession or control in accordance with its standard data deletion policies and applicable laws and regulations, including the GDPR. Subject to any legal or regulatory obligations, SeqOne will provide Customer, upon Customer's written request at the end of the Customer Data retention period, with written confirmation of such deletion. Upon completion of the Customer Data deletion activities, SeqOne will provide the Customer, upon the Customer's written request, with a

written certificate of deletion. This certificate will include a detailed record of the Customer Data deletion activities undertaken, specifying the categories of Customer Data deleted, the deletion methods employed and the dates of such activities. SeqOne will ensure that the deletion methods used comply with industry best practices for the secure disposal of Customer Data and are adequate to prevent unauthorized access or retrieval of deleted Customer Data. SeqOne reserves the right to delete commercially sensitive information from the detailed log to the extent permitted by applicable law. The provision of the deletion certificate and log is subject to the Customer's performance of all its obligations under the Agreement.

21.2 Support

SeqOne provides support to the Customer during the transition period, including training of new service providers, documentation and technical assistance for the extraction and migration of Customer Data. These services are provided on the basis of a prior written quotation provided by SeqOne to the Customer.

ARTICLE 22 - CONTRACTUAL REFERENT

In the event of an incident having an impact on Customer Data, SeqOne undertakes to contact the contractual referent that the Customer undertakes to designate to SeqOne on the day of acceptance of these General Conditions of Services. In the event of a change, it is the Customer's responsibility to update this contact information and communicate it to SeqOne without delay. It is specified that the contractual referent must be able to designate a healthcare professional authorized to access Customer Data, when necessary.

TITLE III: COMMON PROVISIONS

(Note: This appears to be mislabeled as Title III in the source, likely intended as Title IV)

ARTICLE 23 - CONFIDENTIALITY

In addition to the strict observance of business secrecy stipulated in articles L.151-1 to L-154-1 of the French Commercial Code, each of the Parties undertakes, under penalty of damages, to (i) treat as strictly confidential all information which is not in the public domain and which has been communicated to it in connection with the negotiation, conclusion, performance, renewal, extension, expiry and termination of the Contract, (ii) not to disclose it to any person or in any form whatsoever without the express prior written consent of the other Party, and (iii) to use it solely for the performance of the Contract. Each Party may, however, communicate any confidential information received from the other Party to its advisors (lawyers, chartered accountants, auditors, bankers) legally bound by an obligation of professional secrecy when such communication is necessary. In the event of an administrative or judicial obligation to disclose confidential information, the Party having disclosed the confidential information will be informed and its comments solicited in order to be able, insofar as possible, to oppose or limit the extent of the disclosure. Any use by the Customer of SeqOne's names, corporate names and/or intellectual property rights, and more generally any communication by the Customer concerning the conclusion of the Contract and the use of the Platform, must first be validated in writing by SeqOne as to its content and medium. The Customer expressly acknowledges that

SeqOne is entitled to mention the use of the Platform by the Customer to third parties, on any promotional material, brochure or website for example. This obligation of confidentiality shall survive termination of the Contract for any reason whatsoever for a period of ten (10) years.

ARTICLE 24 - INTELLECTUAL PROPERTY

SeqOne remains the sole and exclusive owner of all its rights, in particular its intellectual property rights, including all rights to the Platform, its brands, trade names, logos, designs, texts, graphics, images, audio files, videos, and any other elements protected by intellectual property rights. The Customer expressly acknowledges that the Contract shall in no way be construed as granting or transferring to it any right of ownership over the tangible or intangible assets belonging to SeqOne. Any reproduction, representation, adaptation, modification, publication, transmission to a third party other than the patient, distortion, integration into another site, commercial exploitation and/or total or partial reuse of the Platform, by any process and on any medium, is strictly prohibited and may constitute an act of infringement punishable by the French Intellectual Property Code or an act of unfair competition. The Customer undertakes not to infringe, directly or indirectly, SeqOne's intellectual property rights. The Customer expressly acknowledges that SeqOne has a right of access to the elements uploaded to the Platform for the purpose of improving the Platform and Services for the benefit of all customers, for example the improvement of algorithms for alignments and annotations. For these purposes only, SeqOne may reuse, after having anonymized them, the elements put online by the User on the Platform, with the exception of FASTQ files, which will be deleted. Lastly, SeqOne guarantees that it holds all the rights required to operate the Platform. Thus, the Publisher will indemnify the Customer against any action or claim that may be brought by a third party on the grounds that any of the elements making up the Platform (excluding content provided by third-party sites) would constitute an infringement of a copyright or any other intellectual property right of a third party. Indemnification of the Customer by SeqOne is expressly subject to the following conditions: (i) that the Customer informs SeqOne of any claim as soon as it becomes aware of it, (ii) that the Customer provides SeqOne with all documents and information in its possession as well as all assistance required that may be necessary for its defense, and (iii) that the Customer entrusts SeqOne with the exclusive control of any litigation arising therefrom, unless otherwise agreed between the Parties and to the exclusion of any action brought before the criminal courts. SeqOne will then bear the reasonable costs and damages that the Customer would have to pay in execution of any judicial decision that has become final. SeqOne accepts no liability in the event of modification or irregular use of the Platform or the resulting elements (in particular the final reports) by the Customer or a third party, or the combination of the elements making up the Platform with third-party elements.

ARTICLE 25 - COMPLIANCE WITH APPLICABLE REGULATIONS

25.1 Customer undertakings

The Customer expressly declares, warrants and undertakes to comply with the following, under penalty of termination of the Contract and damages: (i) to comply in all respects with the international conventions, laws, regulations, rules and practices of the profession applicable to it, in particular with regard to health, research, taxation, social matters, the fight against money laundering and the financing of terrorism, the fight against fraud and corruption, the fight

against discrimination, the protection of the environment and the protection of personal data; (ii) that the funds to be used to pay for the Services do not and will not originate from a criminal offence, do not and will not participate in the financing of terrorism, are not and will not be linked to money laundering or the financing of terrorism; (iii) not to do anything, directly or indirectly, by any means whatsoever, that might harm the interests or image of SeqOne or the operation of the Platform, and in particular not to engage in acts of counterfeiting or unfair competition. The Customer is responsible for obtaining all necessary authorizations for the use and exploitation of the Platform and the data generated.

SeqOne points out that, within the meaning of the GDPR, the Customer has the qualification of controller of the Personal Health Data placed online on the Platform by the Customer. In this context, the Customer will be responsible for complying with all requirements that apply to it under the applicable Regulations with regard to the Customer's processing of Personal Data and the instructions it gives to SeqOne in this regard. In particular, but without prejudice to the generality of the foregoing, the Customer acknowledges and agrees that the Customer shall be solely responsible for:

- the accuracy, quality and legality of Customer Data and the means by which the Customer has acquired Personal Data, including Health Data;
- complying with all necessary transparency and legality requirements required by Data Protection Laws for the collection and use of Personal Data, including informing, obtaining necessary consents and authorizations (in particular for use by the Customer for research purposes) which are the sole responsibility of the Customer;
- ensure that the Customer has the right to transfer or grant access to the Personal Data to SeqOne for Processing in accordance with the terms of the Contract which includes this DPA;
- ensure that the Customer's Instructions to SeqOne regarding the Processing of Personal Data comply with applicable laws, including Data Protection Laws; and
- comply with all Data Protection Laws applicable to Personal Data or content created, sent or managed in the performance of the Agreement.

The Customer shall inform SeqOne without undue delay if it is unable to comply with its obligations under the applicable Regulations or, as the case may be, Data Protection Laws.

In any event, the obligations relating to Personal Data are defined by the Parties in Appendix I of these General Conditions of Services.

25.2 SeqOne's commitments

SeqOne undertakes to comply with the applicable Regulations and to process the Customer's Personal Data in accordance with the Data Protection Agreement set out in Appendix I to these General Conditions of Services. It is specified that SeqOne cannot be held responsible for compliance with Data Protection Laws applicable to the Customer or to its sector of activity and which are not directly applicable to it.

SeqOne integrates privacy principles into system design by (i) conducting Data Protection Impact Assessments (DPIA) for all new projects and (ii) ensuring that anonymization and pseudonymization techniques are used, where appropriate.

SeqOne establishes (i) differentiated retention schedules according to data sensitivity and legal obligations, (ii) secure archiving systems incorporating automatic deletion mechanisms and (iii) annual reviews of retention policies with consideration of Customer feedback.

25.3. Allocation of responsibility for Personal Data security

SeqOne and the Customer acknowledge that the security of information on the Platform is a shared responsibility. The Parties undertake to implement and maintain the security measures falling within their respective perimeters.

ARTICLE 26 - ISO 27001 COMPLIANCE

SeqOne guarantees that its Information Security Management System (ISMS) complies with ISO 27001 standards. It undertakes to maintain this certification and to ensure that all processes are continuously aligned with these standards in order to effectively manage information security risks. In particular, SeqOne certifies that its ISMS: (i) aligns with the requirements of ISO 27001:2022, including risk assessment, treatment plans, (ii) covers all assets, processes and personnel involved in hosting and processing data, (iii) incorporates documented procedures for incident response, asset management and secure software development, and (iv) is reviewed annually by an external certification body to ensure compliance with evolving security standards.

SeqOne clearly defines roles and responsibilities for information security at all levels of the organization, ensuring that the leadership and support requirements of ISO 27001 are met. In this respect, SeqOne defines detailed roles for all personnel involved in health data processing with (i) an Information Security Officer (ISO) responsible for overseeing the ISMS, (ii) an Incident Response Team responsible for handling security events in accordance with ISO 27001 and (iii) an Internal Audit Team conducting quarterly compliance reviews against ISO 27001 requirements.

SeqOne undertakes to (i) regularly update its ISMS on the basis of audit results, technological advances and regulatory developments, and (ii) keep a record of all improvements to the ISMS and make it available to the Customer on request. Furthermore, as part of the continuous improvement of the ISMS, SeqOne undertakes (i) to update its ISMS policies every year in line with emerging threats and audit findings, and (ii) to set up a customer feedback mechanism to integrate security improvements.

In any event, the scope of certification is explicitly detailed in the contractual appendices, covering (i) the geographical locations of hosting facilities, (ii) the types of data hosted and associated processing activities, and (iii) third-party systems and services integrated as part of the ISMS.

ARTICLE 27 - STAFF TRAINING

SeqOne undertakes to implement an advanced training program for its employees, guaranteeing (i) annual training on ISO 27001 standards, adapted to the specific roles of employees, (ii) phishing simulations and security exercises to assess and improve team responsiveness and (iii) documentation of participation and an assessment of the effectiveness

of the training provided.

SeqOne guarantees that all of its personnel, as well as any person acting under its authority or on its behalf in the performance of the Services, are subject to reinforced contractual confidentiality obligations, covering in particular all confidential data and information, including Personal Data and Health Data processed under the Contract.

ARTICLE 28 - FINANCIAL CONDITIONS

Unless otherwise agreed in writing by the Service Provider, SeqOne's invoices are payable in the currency of the Offer or Quotation, it being specified that the reference price and the price in Euros are payable in cash, in full and in one instalment, within 30 (thirty) days of their date of issue. The due date will be stated on the invoice sent by SeqOne to the Customer. At SeqOne's discretion, a deposit may be required when ordering Services. All payments made by the Customer will only be considered effective after final receipt by SeqOne. In accordance with the provisions of article 1344 of the French Civil Code, it is expressly agreed between the Parties that the Customer will be validly placed in default by the mere due date of the obligation. In the event of late payment, penalties are payable on the day following the invoice due date and are calculated on the basis of a rate of 10% (ten percent), without the need for prior formal notice. The Customer shall also pay SeqOne a flat-rate indemnity of €40 (forty euros) for collection costs, without the need for prior formal notice. The Publisher reserves the right to request additional compensation from the Customer if the collection costs actually incurred exceed this amount. In addition, if the Customer does not fulfil its obligations due within fifteen (15) days of the due date, SeqOne may suspend the performance of its obligations until full payment of its invoices, without this in itself being considered as a termination of the Contract by SeqOne.

ARTICLE 29 - TERMINATION FOR NON-PERFORMANCE

In addition to suspension of the Contract by SeqOne in the event of non-performance by the Customer of any of its obligations, in particular payment, SeqOne may at any time temporarily suspend access by the Customer or a User if SeqOne observes or has reasonable grounds to believe that the Customer and/or a User is using the Platform in breach of the Contract or any applicable regulations.

In accordance with articles 1224 et seq. of the French Civil Code, in the event of non-performance by the Customer of any of its obligations, SeqOne may, in addition to compulsory performance of the Contract and the award of damages, notify the Customer by registered letter with acknowledgement of receipt or by any other durable written medium providing proof of dispatch, or by extrajudicial act, of the wrongful termination of the Contract, fifteen (15) days after sending a formal notice to perform which has remained unsuccessful. In the event of definitive non-performance, in particular where it is no longer possible to remedy the situation due to the nature of the obligation (for example, in the event of a breach of an obligation not to do something), the Contract may be immediately terminated by SeqOne, without prior notice, as from the date of notification of termination by operation of law to the Customer by registered letter with acknowledgement of receipt or by any other durable written medium providing proof of dispatch, or by extrajudicial act.

ARTICLE 30 - FORCE MAJEURE

The Parties shall not be held liable if the non-performance or delay in performance of any of their obligations is due to force majeure as defined in article 1218 of the French Civil Code. The Party observing the event must immediately inform the other Party of its inability to perform its obligation and justify this by registered letter with acknowledgement of receipt or by any other durable written medium providing proof of dispatch, or by extrajudicial act. The suspension of obligations shall in no case be a cause of liability for non-performance, nor lead to the payment of damages or late penalties. If the impediment is temporary and does not exceed a period of fifteen (15) days, performance of the obligation is suspended ipso jure for the duration of the force majeure event, and the term of the Contract is extended by the duration of the suspension. It is specified that during this suspension, the costs generated by the situation will be borne by the Party prevented from performing its obligations. As soon as the cause of the suspension of their mutual obligations has disappeared, the Parties will make every effort to resume normal performance of their contractual obligations as soon as possible. To this end, the Party prevented shall notify the other of the resumption of its obligation by registered letter with acknowledgement of receipt or by any other durable written medium providing proof of dispatch, or by extrajudicial act. If the impediment exceeds a period of fifteen (15) days, the other Party may give notice of termination of the Contract to the impeded Party. If the impediment is definitive, the Contract will be automatically terminated by operation of law. Termination of the Contract for reasons of force majeure may only take place fifteen (15) days after formal notice has been given of the intention to apply the present clause, by registered letter with acknowledgement of receipt or by any other durable written medium providing proof of dispatch, or by extrajudicial act.

ARTICLE 31 - TERMINATION OF THE CONTRACT

The services exchanged between the Parties since the conclusion of the Contract and until its termination, for any reason whatsoever (expiry of the term, termination for non-performance, termination for force majeure), having found their usefulness in the course of the reciprocal performance of the Contract, shall not give rise to restitution.

SeqOne reserves the right to retain Customer and User content, documents and information for as long as is necessary to respond to any subsequent request from legal or administrative authorities, to protect the rights of SeqOne, its customers, Users and/or third parties. However, SeqOne is under no obligation to Customers, Users and/or any third party to store content, documents and information, unless the Parties have agreed to a storage option in the Quotation or Offer.

ARTICLE 32 - INDEPENDENCE OF THE PARTIES

Each of the Parties expressly declares that it is, will remain and will appear to third parties as an independent commercial and professional partner assuming alone the risks of its own operation. The Contract shall in no way be construed as constituting a partnership agreement, a de facto or joint venture, a sales agent agreement or an employment contract.

ARTICLE 33 - NON-SOLICITATION

The Customer undertakes, for the entire duration of the Contract and for two (2) years following the end of the Contract, for whatever reason, not to solicit, offer to hire or hire any person who, regardless of status or duration, has been an employee of SeqOne, without the prior written consent of SeqOne. Should the Customer fail to comply with this obligation, it undertakes to compensate SeqOne with an indemnity equal to twelve (12) months' gross remuneration of the SeqOne employee.

ARTICLE 34 - TRANSFER OF CONTRACT

SeqOne's rights and obligations under the Contract may be freely transferred and/or subcontracted by SeqOne by any means to any individual or legal entity of its choice. However, as with any Customer account, the Contract and the rights associated with it are personal, non-transferable and non-transferable by the Customer, to any person/entity, by any means whatsoever, without the prior written consent of SeqOne. Consequently, the Customer shall notify SeqOne in writing prior to the completion of any project which would involve or result in any transfer of the Contract by the Customer. SeqOne shall have the discretionary right to object to the proposed project, it being specified that any failure by SeqOne to respond within thirty (30) days of receipt of the notification shall constitute acceptance of the transfer project.

In the event of an authorized transfer of the Contract, the Customer undertakes to ensure that any amendment to the Contract is signed by the third party beneficiary within thirty (30) days of the transfer, failing which the Contract may be terminated by SeqOne to the exclusive detriment of the Customer. In the absence of prior written agreement from SeqOne, the Customer shall remain jointly and severally liable with the third party beneficiary to the Publisher for the performance of the obligations arising from the Contract, and the guarantees granted by the Customer to guarantee such performance shall remain for the benefit of SeqOne. Any attempt by the Customer to transfer the Contract without the prior written consent of SeqOne shall be null and void and may result in the termination of the Contract by SeqOne to the exclusive detriment of the Customer.

ARTICLE 35 - APPLICABLE LAW AND JURISDICTION

The Contract and more generally any use of the Platform are governed exclusively by French law. All disputes relating to the conclusion, existence, validity, interpretation, performance, renewal, extension, expiry and termination of the Contract, and more generally to the use of the Platform, as well as their consequences and aftermath, shall be subject to the exclusive jurisdiction of the Commercial Court of Paris, even in the event of multiple defendants or the introduction of third parties, to the exclusion of those falling within the exclusive jurisdiction of a French judicial court, which shall be subject to the exclusive jurisdiction of the Judicial Court of Paris.

ARTICLE 36 - CAPACITY AND CONSENT

The Customer declares, acknowledges and guarantees:

- to have conducted the negotiations preceding the conclusion of the Contract in good faith;
- to have communicated to SeqOne all information likely to determine its consent and of which it could legitimately be unaware;

- to have had all the time, information and means necessary to study, negotiate and sign the Contract in full knowledge of the facts;
- that after this freely conducted negotiation of the Contract, her consent is given without constraint of any kind and in full knowledge of the obligations contained therein, the Contract expressing her free and informed will;
- that the identification details given in the Quotation or Offer are accurate;
- that he/she has the capacity, power and all necessary authorizations to enter into this Contract, which does not constitute a breach of any obligation to a third party;
- that it is a duly constituted entity in accordance with the rules applicable to it;
- that it is not in a state of suspension of payments and is not the subject of any insolvency proceedings, in particular any conciliation, ad hoc mandate, safeguard, receivership or compulsory liquidation proceedings.

The signatory of the Agreement declares, acknowledges and warrants that he/she has the capacity, power and all necessary authorizations to sign this Agreement in the name and on behalf of the Customer he/she represents.

Appendix I: Personal Data Processing Agreement

> **Explanatory note:** This Data Protection Agreement has been drafted in accordance with the Annex to European Commission Implementing Decision (EU) 2021/915 of June 4, 2021 on standard contractual clauses between controllers and processors under Article 28 (7) of the GDPR.

TITLE I. GENERAL PROVISIONS

ARTICLE 1. DEFINITIONS

The terms hereinafter defined shall have the meaning and scope given in their definition as specified below:

- **"Standard Contractual Clauses"** means the standard contractual clauses for the transfer of Personal Data outside Europe approved pursuant to Commission Implementing Decision (EU) 2021/914 of June 4, 2021 on standard contractual clauses for the transfer of personal data to third countries under Regulation (EU) 2016/679 of the European Parliament and of the Council.
- **"European Data"** means Personal Data subject to the protection of European Data Protection Laws.
- **"Personal Data"** means any information relating to an identified or identifiable person, including any personal health data, where such information is contained in Customer Data and is protected in the same way as personal data, personal information or personally identifiable information under Data Protection Laws. This also includes Health Data.
- **"Europe"** means the European Union, the European Economic Area and/or their member states and Switzerland.

- **"Instructions"** means written and documented instructions issued by a Processor to a Subcontractor, directing the Subcontractor to perform a specific or general action with respect to Personal Data (including, but not limited to, anonymization, blocking, deletion, provision).
- **"Extra-European Regulation"** means any regulation included in the definition of Data Protection Laws, but emanating from a country outside the European Economic Area (hereinafter "Third Country").
- **"Data Controller"** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. For the purposes of this Agreement, the Customer is considered to be the Data Controller.
- **"Subcontractor"** means a natural or legal person, public authority, agency or other body that Processes Personal Data on behalf of the Controller. For the purposes of this Agreement, SeqOne is considered to be a Sub-processor.
- **"Subsequent Subcontractor"** means any subcontractor engaged by SeqOne to assist SeqOne in fulfilling its obligations in providing the Services under the Agreement. Subsequent Subcontractors may include third parties or Affiliates of SeqOne but exclude any employee or consultant of SeqOne.
- **"Processing"** means any operation or set of operations performed on Personal Data encompassing the collection, recording, organization, structuring, storage, adaptation or modification, extraction, consultation, use, disclosure by transmission, dissemination or any other form of making available, alignment or combination, restriction or erasure of Personal Data. The terms "Processing", "Processes", "Processed" and the conjugations of the verb "Process" shall be interpreted accordingly.
- **"Personal Data Breach"** means a breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized access to Personal Data transmitted, stored or otherwise Processed by SeqOne and/or its Subsequent Subcontractors in connection with the Supply. Personal Data Breach shall not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful login attempts, pings, port scans, denial of service attacks and other network attacks on firewalls or networked systems.

Terms not otherwise defined in this Agreement shall have the meanings set forth in the Agreement.

ARTICLE 2. PURPOSE

The Parties hereby acknowledge that the Processing of Personal Data, as described in Sub-Annex II, will be implemented by **SeqOne in its capacity as Subcontractor** (hereinafter the "**Subcontractor**"), in the name and on behalf of the **Customer acting in its capacity as Data Controller** (hereinafter the "**Data Processor**").

The purpose of this Personal Data Processing Agreement (hereinafter the "**Agreement**") is to define the legal conditions under which the Subcontractor undertakes to process Personal Data on behalf of the Data Controller in connection with the provision of the Services covered by the Contract.

This Agreement includes the following appendices:

- Sub-Annex I - DESCRIPTION OF PROCESSING
- Sub-Schedule II - SECURITY MEASURES
- Sub-Schedule III - SUBCONTRACTING - LOCATION OF DATA
- Sub-Annex IV - LIST OF EXTRA-EUROPEAN REGULATIONS.

This Agreement reflects the agreement of the Parties with respect to the Processing of Personal Data by SeqOne on behalf of the Customer as part of the Services provided by SeqOne to the Customer pursuant to the Contract signed between SeqOne and the Customer.

This Agreement has thus been established in order by the Parties to ensure compliance with the applicable Regulations, and in particular with Article 28 of the GDPR.

This Agreement applies to the Processing of Personal Data as described in Sub-Annex I.

This Agreement is without prejudice to the obligations to which the Data Controller is subject by virtue of the Applicable Regulations.

It is specified that this Agreement alone is not sufficient to ensure compliance with the obligations relating to international transfers in accordance with Chapter V of the GDPR.

This Agreement is complementary to and forms an integral part of the Contract and comes into force upon signature of the Contract. In the event of any conflict or inconsistency with the terms of the Quotation/Offer or the GCS or the Special Conditions, this Agreement shall prevail with respect to such conflict or inconsistency.

ARTICLE 3. MODIFICATION AND DURATION OF AGREEMENT

Notwithstanding any other stipulation to the contrary in the Agreement and without prejudice to the stipulations of the Article "Instructions" or the stipulations of the Article "Security" of this Agreement, SeqOne reserves the right to make updates and modifications to this Agreement.

The duration of this Agreement is aligned with the duration of the Contract.

ARTICLE 4. INTERPRETATION

This Agreement shall be read and interpreted in light of the provisions of the applicable Regulations.

This Agreement shall not be interpreted in a manner contrary to the rights and obligations set forth in the Applicable Regulations or in a manner that infringes the fundamental rights or freedoms of the persons concerned.

ARTICLE 5. HIERARCHY

In the event of any inconsistency between this Agreement and the provisions of related agreements existing between the Parties at the time this Agreement is agreed or entered into subsequently, this Agreement shall prevail.

TITLE II. OBLIGATIONS OF THE PARTIES

ARTICLE 6. DESCRIPTION OF PROCESSING

Details of the Processing operations, and in particular the categories of Personal Data and the purposes of the Processing for which Personal Data is processed on behalf of the Data Controller, are specified in Sub-Annex I.

ARTICLE 7. OBLIGATIONS OF THE PARTIES

7.1 Instructions

The Subcontractor shall only process Data on the basis of a documented Instruction from the Data Controller, unless it is required to do so under the applicable Regulations or the law of a country to which it is subject. In this case, the Subcontractor shall inform the Data Controller of this legal obligation prior to Processing, unless prohibited by law for important reasons of public interest. Instructions may also be given subsequently by the Data Controller throughout the duration of the Processing of Personal Data. Such Instructions must always be documented.

The Parties agree that the Contract, which includes this Agreement, together with the Services subscribed to by the Customer in accordance with the Contract, constitute the Customer's complete and final Instructions concerning the Processing of Personal Data. Additional Instructions outside the scope of the Instructions will require prior written agreement between the Customer and SeqOne.

The Subcontractor shall immediately inform the Data Controller if, in its opinion, an Instruction given by the Data Controller constitutes a breach of the Applicable Regulations. Similarly, if the Subcontractor learns that it cannot Process Personal Data in accordance with the Data Processor's Instructions due to a legal requirement under applicable law, the Subcontractor will (i) promptly inform the Data Processor of such legal requirement to the extent permitted by applicable law; and (ii) if necessary, cease all Processing (other than simply storing and maintaining the security of the Personal Data concerned) until the Data Processor issues new Instructions with which the Subcontractor is able to comply. If this provision is invoked, the Subcontractor will not be liable to the Processor under the Contract for any breach of the Contract until the Processor issues new legal Instructions concerning the Processing.

7.2. Purpose limitation

The Processor processes Personal Data solely for the specific purpose(s) of the Processing, as defined in Sub-Annex I.

7.3. Security of Processing and Personal Data

The Subcontractor implements at least the technical and organizational measures specified in Sub-Annex II to ensure the security of Personal Data. These measures include the protection of data against any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data (Personal Data Breach).

In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing, as well as the risks to Data Subjects. SeqOne performs periodic risk assessments: (i) once a year and after any significant change in infrastructure or processes, (ii) using a detailed risk matrix classifying threats according to their impact and likelihood, (iii) providing a summary report to the Customer on request, including mitigation strategies for identified risks.

The Data Controller acknowledges that, notwithstanding any provision to the contrary, the Subcontractor may modify or update the technical and organizational measures specified in Sub-Annex II, at its discretion provided that such modification or update does not result in a material degradation of the protection offered by said Security measures.

In the event of a security incident involving Customer Data, SeqOne provides (i) an initial notification within 24 hours of detection of a high severity incident, (ii) a detailed incident report within 48 hours, including a root cause analysis and corrective measures, and (iii) direct communication channels for emergency collaboration with the Data Controller.

The Subcontractor only grants members of its staff access to Personal Data subject to Processing to the extent strictly necessary for the performance, management and monitoring of the Contract. The Subcontractor shall ensure that any member of its staff whom it authorizes to Process Personal Data (i) is subject to appropriate confidentiality obligations (whether contractual or legal) in respect of such Personal Data and (ii) undergoes training in data security best practice as specified in the Contract.

7.4. Health Data

Where Processing involves Health Data, the Subcontractor applies specific limitations and/or additional safeguards.

7.5. Documentation and compliance

The Parties must be able to demonstrate compliance with this Agreement.

The Subcontractor shall deal promptly and adequately with the Data Processor's requests concerning Data Processing in accordance with this Agreement. The Subcontractor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations set forth in this Agreement and arising directly from the Applicable Regulations.

At the request of the Data Controller, the Processor shall also permit and contribute to audits of the Processing activities covered by this Agreement, at reasonable intervals or in the presence of indications of non-compliance. When deciding on a review or audit, the Controller may take into account relevant certifications in the possession of the Processor. The Data Controller may decide to carry out the audit itself or to appoint an independent auditor. Audits may also include inspections at the Subcontractor's premises or physical facilities and are, where appropriate, carried out with reasonable notice.

The Parties shall make available to the competent supervisory authority(ies), upon request, the information set out in this Article, including the results of any audit.

7.6. Use of Subsequent Subcontractors

The Subcontractor has the general authorization of the Data Controller to engage Subcontractors on the basis of an agreed list set out in sub-Appendix III. The Subcontractor specifically informs the Controller in writing of any plans to modify this list by adding or replacing Subsequent Subcontractors at least thirty (30) days in advance, thus giving the Controller sufficient time to object to these changes before the recruitment of the Subsequent Subcontractor or Subcontractors concerned. This objection is valid only if it is based on a legitimate reason. The Subcontractor shall provide the Data Controller with the information necessary to enable him to exercise his right to object.

The Data Controller has a maximum of thirty (30) days from the date of receipt of this information to present any objections to the Subcontractor. If the Data Controller informs SeqOne of such an objection, the Parties will discuss the Data Controller's concerns in good faith with a view to reaching a commercially reasonable resolution. If no such resolution can be reached, Subcontractor, at its sole discretion, will not appoint the new Subsequent Subcontractor or will allow the Processor to suspend or terminate the Agreement in accordance with the terms of the Agreement without liability to either Party (but without prejudice to any costs incurred by the Processor prior to suspension or termination).

In the absence of any objection, within the time allowed or without any response from the Data Controller, the subsequent subcontracting in question will be implemented in accordance with the terms notified by the Subcontractor.

The Subcontractor selects its Subsequent Subcontractors on the basis of strict criteria, assessing their technical and organizational guarantees, their level of security, and their certifications (in particular ISO 27001) and compliance with applicable Regulations. The Subcontractor undertakes to carry out regular audits of Subsequent Subcontractors, which may include physical inspections and documentary reviews.

Where the Processor recruits a Subcontractor to carry out Processing activities on behalf of the Controller, it does so by means of a contract which imposes on the Subcontractor, in substance, the same data protection obligations as those imposed on the Subcontractor under this Agreement. The Subcontractor shall ensure that the Third-Party Subcontractor complies with the obligations to which it is itself subject under the Contract (in particular the obligations relating to the hosting of health data), including this Agreement and the applicable Regulations.

At the request of the Data Controller, the Subcontractor shall provide the Data Controller with a copy of this contract with the Subsequent Subcontractor and any subsequent amendments thereto. To the extent necessary to protect business secrets or other confidential information, including Personal Data, the Subcontractor may redact the text of the contract before distributing a copy.

The Subcontractor remains fully responsible to the Data Controller for the performance of the obligations of the Subsequent Subcontractor in accordance with the contract entered into with the Subsequent Subcontractor. The Subcontractor shall inform the Data Controller of any breach by the Subsequent Subcontractor of its contractual obligations.

The Processor agrees with the Subsequent Processor on a third-party beneficiary clause according to which - in the event that the Processor has materially disappeared, ceased to exist in law or become insolvent - the Data Controller has the right to terminate the contract entered into with the Subsequent Processor and to instruct the Subsequent Processor to erase or return the Personal Data.

7.7. International transfers

Any cross-border transfer shall be made in accordance with the Data Protection Laws applicable to such transfer.

The Parties agree that where the Subcontractor recruits a Subsequent Subcontractor in accordance with Article 7.6 to carry out specific processing activities (on behalf of the Data Controller) and such processing activities involve a transfer of Personal Data within the meaning of Chapter V of the GDPR, the Subcontractor assures the Data Controller of the implementation of appropriate safeguards in accordance with the applicable Regulations, and generally Data Protection Laws.

In particular, any transfer of European Data to a third country or international organization by the Subcontractor is carried out in accordance with Chapter V of the GDPR. The Subcontractor thus undertakes not to transfer European Data to a third country or recipient not recognized as offering an adequate level of protection of Personal Data (within the meaning of the applicable Regulations), unless the Subcontractor first takes all necessary measures to ensure that the transfer complies with the applicable Regulations. Such measures may include (without limitation) the transfer of such European Data to a recipient covered by an appropriate framework or other legally adequate transfer mechanism recognized by competent authorities or courts as offering an adequate level of protection of Personal Data, to a recipient that has obtained validation of its Binding Corporate Rules (BCR) in accordance with the Applicable Regulations, or to a recipient that has signed in each case appropriate Standard Contractual Clauses as adopted or approved in accordance with the Applicable Regulations.

In the event that the performance of the Hosting Service involves, on the part of the Subcontractor or one of its Subsequent Subcontractors, remote access to European Data from a third country, the Subcontractor shall inform the Data Controller in advance of the absence of an adequacy decision within the meaning of Article 45 of the GDPR, as well as of the appropriate safeguards put in place in accordance with Article 46 of the GDPR to frame this transfer. The Subcontractor notifies the Data Controller of said safeguards and, where applicable, any other additional measures to ensure a level of personal data protection equivalent to that guaranteed by European Union law. These elements are detailed in Sub-Appendix III "Subsequent Subcontracting - Data Location".

Where the Subcontractor or one of its Subsequent Subcontractors involved in the Hosting Service is subject to the legislation of a third country that does not ensure an adequate level of protection within the meaning of Article 45 of the GDPR, the Subcontractor undertakes to inform the Data Controller, of the extra-European Regulations likely to result in unauthorized access, within the meaning of Article 48 of the GDPR, to European Data. It specifies the measures implemented to mitigate the risks of such access as well as the residual risks that

would remain despite these measures. All of this information can be found at: https://trust.seqone.com/compliance and in Sub-Appendix IV "List of Extra-European Regulations".

ARTICLE 8. ASSISTANCE FROM THE DATA CONTROLLER

The Subcontractor shall promptly inform the Data Controller of any request it has received from a Data Subject and shall advise the Data Subject to submit its request directly to the Data Controller. The Subcontractor does not itself follow up such a request. The Subcontractor provides reasonable assistance to the Data Controller in fulfilling its obligation to respond to requests from Data Subjects to exercise their rights, taking into account the nature of the processing. In doing so, the Subcontractor shall comply with the Data Controller's Instructions. The Data Controller will reimburse the Subcontractor for reasonable costs arising from such assistance.

In addition, the Subcontractor shall further assist the Controller in ensuring compliance with the following obligations, taking into account the nature of the Processing and the information available to the Subcontractor:

- To the extent that the required information is reasonably available to SeqOne and the Data Processor does not have access to the required information, the Subcontractor will provide the Data Processor with reasonable assistance with any data protection impact assessment as well as prior consultations with supervisory or other competent data privacy authorities to the extent required by the Applicable Regulations, it being understood that such assistance will be financially borne by the Customer.
- The obligation to ensure that Personal Data is accurate and up to date, informing the Data Controller without delay if the Subcontractor learns that the Personal Data it processes is inaccurate or has become obsolete;
- The obligations set out in Article 32 of the GDPR.

The Parties define in Sub-Annex II the appropriate technical and organizational measures by which the Processor is required to assist the Data Controller in the application of this Article, as well as the scope and extent of the assistance required.

ARTICLE 9. NOTIFICATION OF PERSONAL DATA BREACH

In the event of a personal data breach, the Subcontractor shall cooperate with and assist the Controller for the purposes of compliance with its obligations under the applicable Regulations, including Articles 33 and 34 of the GDPR, whichever is applicable, taking into account the nature of the processing and the information available to the Subcontractor.

9.1. Personal Data Breach in relation to data processed by the Processor.

In the event of a Personal Data Breach relating to data processed by the Data Controller, the Subcontractor shall provide assistance to the Data Controller:

- For the purposes of notifying the Personal Data Breach to the competent supervisory authority(ies), as soon as possible after the Data Controller becomes aware of it, if applicable (unless the Personal Data Breach is unlikely to give rise to a risk to the rights

and freedoms of natural persons);

- For the purposes of obtaining the following information, which, in accordance with Article 33(3) of the GDPR, must be included in the Data Controller's notification, and include, at a minimum:
  - The nature of the Personal Data, including, if possible, the categories and approximate number of Persons affected by the Personal Data Breach and the categories and approximate number of Personal Data records affected;
  - The likely consequences of the Personal Data Breach;
  - The measures taken or proposed to be taken by the Data Controller to remedy the Personal Data Breach, including, where appropriate, measures to mitigate any negative consequences.
- Where, and to the extent that, it is not possible to provide all the information at the same time, the initial notification shall contain the information available at that time and, as it becomes available, additional information shall subsequently be communicated as soon as possible;
- For the purposes of satisfying, in accordance with Article 34 of the GDPR, the obligation to communicate the Personal Data Breach to the Data Subject as soon as possible, where the Personal Data Breach is likely to give rise to a high risk to the rights and freedoms of natural persons.

9.2. Personal Data Breach in relation to data processed by the Subcontractor

In the event of a Personal Data Breach in relation to data processed by the Subcontractor, the Subcontractor shall notify the Data Controller as soon as possible after becoming aware of it.

This notification shall contain at least:

- A description of the nature of the Personal Data Breach found (including, if possible, the categories and approximate number of Persons affected by the Personal Data Breach and Personal Data records affected);
- Details of a contact point from which further information can be obtained about the Personal Data Breach;
- Its likely consequences and the measures taken or proposed to be taken to remedy the Personal Data Breach, including to mitigate any negative consequences.

Where, and to the extent that, it is not possible to provide all the information at the same time, the initial notification will contain the information available at that time and, as it becomes available, additional information will subsequently be communicated as soon as possible.

At the Customer's request and expense, SeqOne will promptly provide the Customer with the reasonable assistance necessary to enable the Customer to notify the relevant Personal Data Breaches to the competent authorities and/or the Data Subjects, if the Customer is required to do so under the applicable Regulations.

The parties define in Sub-Appendix II all other elements that the Processor must communicate when providing assistance to the Controller for the purposes of fulfilling the latter's obligations under Articles 33 and 34 of the GDPR.

TITLE III. FINAL PROVISIONS

ARTICLE 10. NON-COMPLIANCE WITH CLAUSES AND TERMINATION

Without prejudice to the provisions of the applicable Regulations, in the event of a breach by the Processor of its obligations under this Agreement, the Controller may instruct the Processor to suspend the Processing of Personal Data until the Processor has complied with this Agreement or until the Contract is terminated. The Subcontractor shall promptly inform the Data Controller if it is unable to comply with this Agreement, for whatever reason.

The Data Controller shall be entitled to terminate the Contract insofar as it relates to the Processing of Personal Data in accordance with this Agreement if:

- The Processing of Personal Data by the Subcontractor has been suspended by the Data Controller in accordance with the first paragraph of this Article and compliance with the Agreement is not restored within a reasonable time and, in any event, within one (1) month of the suspension;
- The Subcontractor is in serious or persistent breach of this Agreement or its obligations under the applicable Regulations;
- The Subcontractor fails to comply with a binding decision of a competent court or the competent supervisory authority(ies) concerning its obligations under this Agreement or the Applicable Regulations.

The Processor shall be entitled to terminate the Contract insofar as it relates to the Processing of Personal Data under this Agreement where, after informing the Processor that its Instructions breach applicable legal requirements in accordance with Article 7.1, the Processor insists that its Instructions be followed.

ARTICLE 11. FATE OF PERSONAL DATA

Following termination of the Contract for any reason whatsoever, the Subcontractor shall, at the option of the Data Controller, delete all Personal Data processed on behalf of the Data Controller and certify to the Data Controller that it has carried out such deletion, or return all Personal Data to the Data Controller and destroy existing copies, within 90 days of the termination or end of the Contract in accordance with the procedures and deadlines set forth in the Contract, unless a law requires it to be kept longer. It is expressly agreed that the provisions of article "Reversibility" of the General Conditions of Services fully apply to such return or deletion of Personal Data.

The Subcontractor shall continue to ensure compliance with these clauses until the data is deleted or returned.

Consequently, since SeqOne will not retain any copies of the Customer's Personal Data, the Customer acting as Data Controller will take all measures it deems appropriate to be able to respond to any request from judicial or administrative authorities including data protection authorities and/or any Data Subject and/or any third party relating to the Processing of Personal Data under the Contract.

ARTICLE 12. RE-USE OF PERSONAL DATA

In accordance with the GDPR, the Data Controller grants SeqOne a right to reuse Personal Data (pseudonymized data) and/or aggregated data derived from the use of the Platform for purposes of continuous improvement of the Platform and its performance.

This right is granted to SeqOne without prejudice to SeqOne's obligation to comply with the provisions of the applicable Regulations.

The rights thus granted are for the entire duration of the Contract and for the entire duration of current or future legal protection. Within the meaning of the GDPR, the Data Controller declares that it has assessed and validated the compatibility of the various uses for the re-use of Personal Data, as described above, with the initial purposes of the Processing of Personal Data carried out under its responsibility and described in Sub-Annex I.

Sub-Annex I. Description of Processing

a. Purpose of Processing. SeqOne will Process the Personal Data necessary to perform the Services under the Contract and as indicated by the Customer in its use of the Services in accordance with the Contract. The specific purpose of the Processing is the performance of next generation sequencing (NGS) analyses via the Platform, which has been designed for genetic analysis, which includes, but is not limited to, the Services subscribed to by the Customer.

b. Duration of Processing. Subject to the provisions of the "Fate of Personal Data" section of this Agreement, SeqOne will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

c. Categories of Data Subjects. Customer may submit Personal Data in connection with the use of the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to, Personal Data relating to the following categories of Data Subjects:

- Employees
- Patients

d. Categories of Personal Data. The Customer may submit Personal Data in connection with the use of the Services, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, but is not limited to, the following categories of Personal Data:

- **Employees**:
  - Identification data: name, address, telephone, e-mail, position
- **Patients**:
  - patient pseudonym (required to run an analysis)
  - surname, first name (if applicable)
  - gender
  - **special categories of Personal Data**:
    - Genomic data: genomic samples and genomic alterations, biological signature;

- Health data: diseases, phenotypes, tumor-related information (size, stage, etc.);
- Patient history data: effectiveness of previous treatment, follow-up, allergies.

e. Nature of Processing operations. Personal Data will be Processed in accordance with the Contract (including this Agreement) and may be subject to the following Processing activities:

- Storage and other Processing necessary to provide, maintain and improve the Services and/or the Platform;
- Disclosure in accordance with the Agreement (including this DPA) and/or in accordance with applicable laws.

Sub-Annex II. Security Measures

SeqOne currently observes and implements the technical and organizational security measures described in the Contract, the Agreement and this Sub-Annex III, and aimed at guaranteeing an appropriate level of security, taking into account the nature, scope, context and purpose of the Processing, as well as the risks to the rights and freedoms of natural persons.

a. Access control.

i) Preventing unauthorized access to the Platform

- **Outsourced processing**: SeqOne hosts its Platform with outsourced cloud infrastructure providers that are approved for the Hosting of Health-related Data. In addition, the Provider maintains contractual relationships with suppliers in order to perform the Services in accordance with the Agreement. The Provider relies on contractual agreements, privacy policies and supplier compliance programs to protect the data processed or stored by these suppliers.
- **Physical and environmental security**: SeqOne hosts its product infrastructure with multi-tenant outsourced infrastructure providers. Physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications.
- **Authentication**: SeqOne implements a uniform password policy on its Platform. Customers interacting with the Platform via the user interface must authenticate themselves before accessing non-public data.
- **Authorization**: Customer Data is stored in shared storage systems accessible to customers only via application user interfaces and application programming interfaces. Customers are not authorized to access the underlying application infrastructure directly. The authorization model for each of SeqOne's products is designed to ensure that only appropriately designated individuals can access the relevant functionality, views and customization options. Authorization to access datasets is achieved by validating user permissions against the attributes associated with each dataset.
- **Application Programming Interface (API) access**: public product APIs can be accessed using an API key or via Oauth authorization.

ii) Preventing unauthorized use of the Platform

- **Access controls**: network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ from one infrastructure provider to another, and include

Virtual Private Cloud (VPC) implementations, security group assignment and traditional firewall rules.

- **Static code analysis**: security reviews of code stored in SeqOne's source code repositories are carried out, checking for coding best practices and identifiable software flaws.
- **Penetration testing**: the Publisher maintains relationships with industry-recognized penetration testing service providers. At least 1 penetration test is carried out every 2 years by an independent third party (cyber security company). The purpose of penetration testing is to identify and resolve predictable attack vectors and potential abuse scenarios.

iii) Limits to privilege and authorization requirements

- **Product access**: A subset of SeqOne employees has access to products and Customer Data via controlled interfaces. The purpose of providing access to a subset of employees is to provide efficient Customer support, resolve potential problems, detect and respond to security incidents and implement data security. Each access is authorized by senior managers, and employee roles are reviewed at least once every six months by the Quality and Regulatory department and signed off by senior managers.

b. Transmission control.

- **In transit**: SeqOne makes HTTPS encryption (also known as SSL or TLS) available on each of its connection interfaces. The Provider's HTTPS implementation uses industry-standard algorithms and certificates.
- **At rest**: The Provider stores user passwords in accordance with policies that follow industry-standard security practices. SeqOne has implemented technologies to ensure that stored data is encrypted at rest.

c. Entry control.

- **Detection**: SeqOne has designed its infrastructure to record detailed information on system behavior, traffic received, system authentication and other application requests. Internal systems have aggregated log data and alert appropriate staff to malicious, unintended or abnormal activity. SeqOne staff, including security, operations and support personnel, are responsive to known incidents.
- **Response and follow-up**: the Publisher maintains a log of known security incidents that includes descriptions, dates and times of relevant activities and incident resolution. Suspected and confirmed security incidents are investigated by security, operations or support personnel; and appropriate resolution actions are identified and documented. For any confirmed incident, the Service Provider will take appropriate measures to minimize damage to the product and the Customer or unauthorized disclosure. Notification to the Customer will be in accordance with the terms of the Contract.

d. Availability control.

- **Infrastructure Availability**: Infrastructure providers use commercially reasonable efforts to ensure a minimum availability of 99%. Suppliers maintain a minimum of N+1 redundancy for power, network and HVAC services.
- **Fault tolerance**: backup and replication strategies are designed to guarantee redundancy and failover protection in the event of a major processing failure. Customer data is backed

up to multiple durable data stores and replicated to multiple availability zones.

- **Replicas and online backups**: wherever possible, production databases are designed to replicate data between at least 1 primary and 1 secondary database. All databases are backed up and maintained using at least industry-standard methods.
- SeqOne products are designed for redundancy and transparent failover. The server instances that support the products are also designed to avoid single points of failure. This design helps SeqOne operations to maintain and update product applications and the backend while limiting downtime.

Sub-Annex III. List of Subsequent Subcontractors - Data Localization

SeqOne has currently appointed the following subcontractors:

Company name and address of subcontractor	**Function**	**Data location**
Amazon Web Services, Inc. 410 Terry Ave. N., Seattle, WA 98109-5210, United States	Cloud infrastructure provider on which the Platform is operated for the provision of physical and virtual infrastructure hosting services (server, storage, databases, networks).	Location of data centers: - Prod-EU: AWS Europe (Paris) and - exclusively for backup - AWS Europe (Ireland), - Or Prod-CH: AWS Switzerland and - exclusively for backup - AWS Europe (Ireland), - Or Prod-AU: AWS Australia and - exclusively for backup - AWS Singapore, - Or Prod-US: AWS US (North Virginia) and - exclusively for backup - AWS US (Ohio).

Sub-Annex IV: List of extra-European regulations

The table below lists the main extra-European Regulations under which SeqOne or a Subcontractor involved in the Hosting Service, would be required to allow access not authorized by Union law within the meaning of Article 48 of the GDPR and likely to apply in the context of the Hosting Service.

Third countries	**List of non-European Regulations**	**Measures implemented to mitigate the risks of**

		unauthorized access to Personal Data induced by these extra-European Regulations & Description of residual risks
United States	- Clarifying Lawful Overseas Use of Data Act (CLOUD Act) - The USA Patriot Act - Foreign Intelligence Surveillance Act Section 702 (FISA) - Executive Order 12333	Although Customer Data is located in the European Union, transfers of technical or support Personal Data to the U.S. parent company of the Subcontractor may be necessary at the request of U.S. authorities under standard procedures including the ability to object. In such a case, SeqOne ensures that its Third-Party Processor is certified as compliant with the *EU-U.S. Data Privacy Framework (DPF)*, the European Commission's adequacy decision which provides a legal basis for such transfers while imposing strict data protection obligations. To protect Customer Data against any access request from non-European authorities that does not comply with EU law, SeqOne implements a set of technical, organizational and contractual mitigation measures, such as systematic encryption, control of encryption keys, contractual commitment to challenge, and Transparency.

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1. Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties: (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').

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

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

Clause 2. Effect and invariability of the Clauses

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

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

Clause 3. Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions: (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7; (ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b); (iii)

Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e); (iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f); (v) Clause 13; (vi) Clause 15.1(c), (d) and (e); (vii) Clause 16(e); (viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

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

Clause 4. Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5. Hierarchy

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

Clause 6. Description of the transfer(s)

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

Clause 7 – Optional. Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8. Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data

importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE FOUR: Transfer processor to controller

8.1. Instructions
(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.
(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.
(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.
(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.
8.2. Security of processing
(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.
(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
8.3. Documentation and compliance
(a) The Parties shall be able to demonstrate compliance with these Clauses.
(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9. Use of sub-processors

Reserved

Clause 10. Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11. Redress

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

Clause 12. Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.
(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13. Supervision

Reserved

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

Clause 14. Local laws and practices affecting compliance with the Clauses

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

including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred; (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards; (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]
(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15. Obligations of the data importer in case of access by public authorities

15.1. Notification
(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it: (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or (ii) becomes aware of

any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer. [For Module Three: The data exporter shall forward the notification to the controller.]
(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]
(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.
15.2. Review of legality and data minimisation
(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]
(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16. Non-compliance with the Clauses and termination

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

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where: (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension; (ii) the data importer is in substantial or persistent breach of these Clauses; or (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses. In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.
(d) The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17. Governing law

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of France.

Clause 18. Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of Paris, France.

APPENDIX

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

ANNEX I

A. LIST OF PARTIES

Data exporter(s): 1.

- **Name:** SEQONE
- **Address:** SeqOne a simplified joint-stock company with a share capital of €61.754, registered with the RCS of Montpellier under number 829 581 586, having its registered office at 22 rue Durand - 34000 Montpellier
- **Contact person's name, position and contact details:** Danaë GERAUD
- **Activities relevant to the data transferred under these Clauses:** As described in the DPA executed between the Parties
- **Role (controller/processor):** Processor

Data importer(s): 1.

- **Name/Address:** contact details of the data importer(s), including any contact person with responsibility for data protection must be shared by email to dpo@seqone.com. All related information will be stored in Seqone's CRM.
- **Role (controller/processor):** Controller

B. DESCRIPTION OF TRANSFER

As described in the DPA executed between the Parties

ANNEX III

(Note: Annex II is not present in the source document)

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

As described in the DPA executed between the Parties