SaaS Service Contract "PST

hereinafter referred to as "**Contract**

between

Practice: _____

Str. /No: _____

Postcode/Place. _____

Tel: _____

Email: _____

Contact person:

_____

hereinafter referred to as "**CENTER**

and **LY.SEARCH Ltd.**

Bockumer Straße 347
40489 Düsseldorf
Phone: +49 221 177 343 11
E-Mail: post@lysearch.de

Contact person:
Prof. hon. (Univ. Puebla) Dr. med. Manuel E. Cornely (Managing Director)

hereinafter referred to as " **LY.SEARCH** ".

hereinafter jointly referred to as the "**Parties**

LY.SEARCH-Auftragsnummer: _____

Table of contents

CLOUD SERVICE CONTRACT PST

Preamble

LY.SEARCH offers "PST", a **cloud-based service for medical practices** on lipohyperplasia dolorosa (LiDo) "lipedema", to support participating practices in the complex and appropriate recording of the clinical picture, relevant treatment measures and follow-up. The use of this system is offered by LY.SEARCH as a web-based Software-as-a-Service solution (hereinafter referred to as "**Service**" and "**PST**").

In the context of its scientific orientation, LY.SEARCH is also pursuing the goal of establishing its own **lipohyperplasia dolorosa (LiDo) "lipedema" database,** into which the data of patients registered by medical practices are to be transferred in anonymized, pseudonymized and structured form and used for LY.SEARCH's own research purposes or made available for third-party research purposes.

The CENTER would like to use the service for itself and its practice and furthermore support the research activities of LY.SEARCH.

It is against this background that the Parties enter into this Agreement.

Subject of the contract

The subject of this contract is the use of the Service by the CENTER for itself and its practice. The functionalities and features of the Service are conclusively described in **ANNEX 1 - SERVICE DESCRIPTION.**

A prerequisite for the use of the service by the CENTER is an Internet browser that is up to date with the latest updates and an active Internet connection . The CENTER is responsible for both; other obligations of the CENTER to cooperate under this contract remain unaffected.

The CENTER is advised that the service, by its nature, can only serve as an aid and does not relieve it of the medical duties of care. The CENTER is and remains responsible for the legal duties incumbent upon it and for determining these duties and relevant specifications.

Scope of services

The contractual services are limited to the services booked by the CENTER. The CENTER may use the Service provided by LY.SEARCH only for internal, own purposes via user accesses set up for the CENTER by LY.SEARCH (access via web interface; cf. sec. 0). The CENTER is permitted to use the Service for third parties only after prior and documented release by LY.SEARCH.

Web Interface: During the term of this Service Agreement, LY.SEARCH shall provide to CENTER the use of a web interface via the web user interface in the software version currently released by LY.SEARCH at the router output of the data center (gateway) in which the software for the Service under this Agreement is hosted. The computing power required for the use of the web interface on the servers and the storage space required for the data processing shall be provided by LY.SEARCH.

Professional Service (optional): If the CENTER requires assistance with commissioning or use of the Service, LY.SEARCH will provide support services through LY.SEARCH's technical support staff or its technical service provider.

Cooperation obligations of the CENTER

The CENTER shall designate a contact person to LY.SEARCH who can provide the information required to execute this Agreement and who shall act as the central contact person. The contact person designated by the CENTER is authorized to receive declarations concerning the contract.

The CENTER shall set up its internal IT systems on its own responsibility in accordance with the state of the art, secure them against malware or unauthorized third-party intervention, maintain them, patch them and renew them as required. In particular, it shall ensure that its IT systems meet the respective system requirements of LY.SEARCH for the use of the Service. In the case of use of the Web Interface Service, this applies, among other things, to the Internet browser used (Mozilla Firefox or Google Chrome).

The CENTER is aware that the software underlying the Service or the Service itself is subject to continuous further development by LY.SEARCH. LY.SEARCH reserves the right to modify and/or supplement the Service, in particular in the event of adaptation to technical and/or legal requirements. LY.SEARCH also reserves the right to modify and/or amend the Service in cases where it is necessary to remedy any security vulnerabilities and in cases where the modification is only legally advantageous for the CENTER. Changes with only insignificant effects on the functions of the service do not constitute changes in performance within the meaning of this contract. Legitimate interests of the CENTER will, of course, be adequately taken into account and appropriate information will be provided about corresponding changes and/or additions. Rights of the CENTER in other respects are neither excluded nor restricted by this reservation of the right to change services.

The CENTER will immediately report malfunctions in accordance with sec. 0 report. The CENTER will actively support LY.SEARCH in troubleshooting.

The CENTER shall refrain from any improper use of the Service and the hardware and software on which the Service is based on the part of LY.SEARCH. The use of the Service for illegal purposes and/or the transmission of illegal content via the Service are prohibited.

The CENTER is obligated to immediately change the user passwords provided to it by LY.SEARCH to passwords known only to it after the initial registration. The access data must be kept secret. Disclosure to unauthorized third parties is prohibited. The CENTER shall ensure that all persons who are provided with access data by LY.SEARCH and/or the administrator of the CENTER also keep such data secret.

The CENTER shall keep its user data, in particular address and contact data, up to date during the term of the contract and notify LY.SEARCH of any changes. The CENTER shall update or notify LY.SEARCH via the entry in the profile at www. lysearch.de; the CENTER shall also inform LY.SEARCH by e-mail of any adjustments.

The CENTER is responsible for compliance with commercial and tax accounting and recording obligations (e.g. in accordance with GoBS, GDPdU), for archiving and complying with corresponding retention periods, and for maintaining patient files and treatment documentation in accordance with professional regulations. For the purpose of complying with its documentation and archiving obligations, the CENTER undertakes to store, print or otherwise retain in an appropriate manner on its own systems the data transmitted by the CENTER for the use of the Service or stored in the Service, namely data on patients. LY.SEARCH is not obligated to permanently store corresponding information for the CENTER and, in particular, does not assume the professional documentation and storage obligations originally incumbent upon the CENTER. It is pointed out to the CENTER that in the event of lack of compliance by the CENTER with the aforementioned regulations regarding the backup and storage of the aforementioned data, a recovery and/or reconstruction is not possible in the event of a system-side deletion, in particular upon termination of the contract.

Availability

LY.SEARCH will make every effort to ensure the highest possible availability of the Service or its accessibility via the web interface.

LY.SEARCH does not guarantee the uninterrupted availability of the service or its accessibility via the web interface at any time.

Service and support

LY.SEARCH shall maintain the software on which the Service is based during the term of this Agreement and provide the currently released program version or the current Service for use by the CENTER. The maintenance includes the maintenance and restoration of the operational readiness, the diagnosis and elimination of defects and, if necessary - on a voluntary basis and without obligation to do so - function-enhancing measures.

The CENTER is obligated to notify LY.SEARCH immediately and as precisely as possible of functional failures and other malfunctions of the Service. The fault report by the CENTER shall be made via a fault reporting system set up by LY.SEARCH; this can be reached at: support@lysearch.de. The fault report shall describe the fault in detail:

- Description of the fault (attach screenshots if possible)

- When did the malfunction occur?
- What is the effect of the disorder?

LY.SEARCH will process malfunctions within a reasonable period of time. Binding response or elimination times are not agreed.

Unless explicitly agreed otherwise, LY.SEARCH shall not owe any further training, consulting, development and setup services under this Agreement.

Remuneration

Participating practices, as CENTERS, are not obligated to pay fees for the use of the service. To this extent, the service is offered free of charge.

As a precautionary measure, it is clarified that the participating practices as CENTERS are not entitled to free services from LY.SEARCH beyond the pure service use; this applies in particular to any individual orders for special evaluations of data from the CENTER or the provision of scientific services or research activities.

Liability

Liability of LY.SEARCH for simple negligent breaches of duty is excluded, unless damages resulting from injury to life, body or health or guarantees are concerned or claims under the Product Liability Act are affected.

Furthermore, liability for the breach of obligations, the fulfillment of which enables the proper execution of the contract in the first place and compliance with which the CENTER may regularly rely on, shall remain unaffected; in this respect, however, liability shall be limited to the typically foreseeable damage. Liability for indirect damages as well as lost profits in cases of simple negligent breaches of duty is furthermore excluded in relation to LY.SEARCH; this exclusion serves to adequately reflect the fact that no remuneration is provided for the services of LY.SEARCH under this contract; this exclusion does not apply to any additional services for which a charge may be made.

Contract term, termination

The contract is concluded for an indefinite period of time ; the contract period begins with the sending of the access data by LY.SEARCH to the CENTER.

The contract can be terminated at any time with four weeks' notice to the end of each quarter.

The right to terminate for cause remains unaffected. LY.SEARCH is authorized to terminate for cause in particular if the CENTER does not settle an existing payment arrears despite a reminder and the setting of a reasonable deadline and/or if the CENTER uses the service for third parties in breach of contract or makes it available for use by third parties.

Cancellations under this contract must be made in text form. If the CENTER wishes to give notice by e-mail, this must be sent to the e-mail address exit@lysearch.de.

It is pointed out to the CENTER that once a termination becomes effective, access to the Service and the data deposited by the CENTER by the CENTER is no longer possible. The CENTER is responsible for the ongoing backup or export of any data required beyond the termination of the contract; cf. also Section 4.2. 0.

Data protection and confidentiality

Within the scope of the contract and the use of the service, the CENTER will strictly observe the data protection obligations incumbent upon the CENTER, in particular in accordance with the German Data Protection Regulation (DS-GVO) and the German Federal Data Protection Act (BDSG), as well as professional regulations. Insofar as the CENTER should transmit personal data to LY.SEARCH within the scope of the execution of the contract or use of the service, **the CENTER is responsible for a corresponding transmission authorization**.

In particular, the CENTER must ensure that personal patient or health data is transferred with the effective consent of the patients concerned. The consent shall reflect the transmission and use of the data by LY.SEARCH both for purposes of monitoring the course of and treatment by or for the CENTER and the use of anonymized and pseudonymized patient data for scientific research purposes by LY.SEARCH, and the signed consent form shall be retained by the

CENTER. LY.SEARCH will provide the CENTER with a FORM for such a consent form. The responsibility under data protection law for the correctness and legality of the declaration used by the CENTER remains with the CENTER; LY.SEARCH may not provide legal advice, nor may LY.SEARCH assume responsibility for the CENTER.

Furthermore, the CENTER will not provide LY.SEARCH with any direct identification features of patients such as name, address and health insurance number or allow them to be processed via the service (not even in free fields such as comment fields, etc.), but will ensure pseudonymization (use of CENTER-internal identifiers or patient numbers). LY.SEARCH does not check the data transmitted by the CENTER or made available for processing via the Service to determine whether they contain any direct identification features that may have been transmitted inadmissibly; the CENTER is also solely responsible for data entry and data transmission to LY.SEARCH in this respect and will check the data records carefully and, in particular, for compliance with data protection requirements before transmission or dispatch.

To the extent that LY.SEARCH processes personal data on behalf of the CENTER under this Agreement, the Parties agree to enter into an Agreement on Commissioned Processing pursuant to **ANNEX 2 - COMMISSIONED PROCESSING**. This agreement forms an integral part of this contract and provides for special requirements to map requirements for professional secrecy holders (medical secrecy).

As a precautionary measure, it is clarified that the use of anonymized and pseudonymized patient data by LY.SEARCH for scientific research purposes as provided for under this Agreement is not limited by the Commissioning Agreement, but rather the corresponding use is covered by the purpose of the Commissioning Agreement; LY.SEARCH shall in particular remain authorized, even after termination of this Agreement and/or the Commissioning Agreement, to continue and permanently use the anonymized and pseudonymized data for the designated purposes until the termination of the Agreement becomes effective.

Subcontractor

LY.SEARCH is entitled to have the services owed under this contract performed by subcontractors. This applies in particular to the technical operation of data centers used for the realization of the Service. In this respect, LY.SEARCH shall ensure that appropriate agreements are made to protect confidentiality and data protection requirements.

Reference

LY.SEARCH is entitled to designate the CENTER as a reference center. If the CENTER does not wish to be designated as a reference center, the CENTER may at any time informally object to the designation of a reference center by LY.SEARCH.

Final provisions

General terms and conditions of the CENTER do not apply.

German law shall apply to the exclusion of the UN Convention on Contracts for the International Sale of Goods (CISG) and German private international law.

Verbal collateral agreements do not exist. Amendments or supplements to this contract must be made in text form to be effective. This formal requirement can only be waived by a declaration signed by both parties.

The CENTER may only assert rights of retention and rights to refuse performance in the case of undisputed or legally established counterclaims. Offsetting is also only permitted with undisputed or legally established counterclaims.

Should individual provisions of this contract be or become invalid in whole or in part, this shall not affect the validity of the remaining provisions. In place of the invalid provision, the parties undertake to agree on the provision that comes closest to the economic purpose of the invalid provision.

The place of jurisdiction is Cologne.

Attachments

APPENDIX 1 - SERVICE DESCRIPTION

ANNEX 2 - ORDER PROCESSING

Practice: _____

LY.SEARCH Ltd.

Place, the

Cologne, the _____

_____
Unterschrift

_____
Unterschrift

_____
Names in plain text

_____
Names in plain text

APPENDIX 1 - SERVICE DESCRIPTION

Lipohyperplasia dolorosa (LiDo) "lipedema" is a progressive disease of the fatty tissue with increasing painfulness. It is characterized by a symmetrical proliferation of fatty tissue on the thighs, lower legs, upper arms and forearms and leads to a dysproportion of the affected body parts to the often still slender trunk. The adipose tissue proliferation in the subcutaneous adipose tissue includes hyperplastic and hypertrophic adipocytes. The blood vessels are probably permeable and fragile, which may explain the tendency to hematoma. Presumably, fluid enters the interstitial tissues (edematization of adipose tissue, formation of high-volume lymphatic insufficiency) . Lipohyperplasia dolorosa (LiDo) "lipedema" fat contains fibrosis, enlarged and increased macrophages and often increased interleukin levels, indicating inflammation. Whether this increase in inflammatory parameters in LiDo is the result of tissue expansion and not a pathological condition of the expanding tissue per se is "work in progress" of one of the research groups collaborating with LY.SERACH.

LY.SEARCH GmbH was founded on the idea of giving those affected by lymphological diseases a chance to live their lives as unimpaired as possible, or even to obtain a cure, through basic research and patient-oriented improvements in diagnosis and treatment. In the field of lymphology, there are still many unexplored topics despite the high number of affected patients worldwide. Many things in this terra incognita have been insufficiently investigated so far. However, the prospects for a better future for patients are promising.

The intrinsic motivation of LY.SEARCH is to utilize many years of clinical and research experience. Through cooperation with scientists at universities and hospitals, LY.SEARCH initiates and facilitates targeted research for a better understanding of the causes, course and therapy of lymphological diseases. To simplify the reliable diagnosis and to achieve an improvement of treatment and disease management in applied lymphology is just as much a goal of LY.SEARCH as the increase of awareness in the public, in order to create awareness in the future that those affected are not alone with their disease, but can receive targeted help of various kinds.

Service and research purposes

With the PST service (Patients history, Signs and symptoms, Treatment and outcome), LY.SEARCH GmbH provides medical practices as centers with an **online service for the complex recording of lipohyperplasia dolorosa (LiDo) "lipedema".** This concerns both conservative and surgical measures or treatments. The PST service supports participating practices in the complex and appropriate recording of the clinical picture, relevant treatment measures and follow-up; the data is partly recorded by patients themselves and finally by the participating centers. In addition to the evaluation and care of individual patients, the service offers medical practices the possibility of having a structured evaluation carried out once a year of all or certain parts of the center's own patient base recorded via PST, in order to gain generalizing or statistical knowledge specific to the center. This annual analysis of the center's own patient data is part of the free service. Additional analyses by LY.SEARCH GmbH are subject to a fee.

Within the framework of its scientific orientation, LY.SEARCH GmbH, in addition to providing the described service for medical practices and their patients, is also pursuing the goal of **establishing its own lipohyperplasia dolorosa (LiDo) "lipedema" database**, into which the data of patients registered by medical practices is to be transferred in anonymized, pseudonymized and structured form and used or made available for **research purposes.** Personal patient data will not be passed on to third parties. LY.SEARCH GmbH hopes to gain considerable knowledge about lipohyperplasia dolorosa (LiDo) "lipedema", in particular its predisposition, prevalence and treatability, by providing as comprehensive and structured a database as possible.

ANNEX 2 - ORDER PROCESSING

[Standard contractual clauses (basis: DS-GVO)]

SECTION I

Clause 1 - Purpose and scope

a) These standard contractual clauses ("Clauses") are intended to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data, on the free movement of such data and repealing Directive 95/46/EC (the General Data Protection Regulation).
b) The controllers and processors listed in Annex I have agreed to these clauses to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679.
c) These clauses apply to the processing of personal data as specified in Annex II.
d) Annexes I to IV form an integral part of the clauses.
e) These clauses are without prejudice to the obligations to which the controller is subject under Regulation (EU) 2016/679.
f) These clauses do not in themselves ensure compliance with the obligations related to international data transfers under Chapter V of Regulation (EU) 2016/679.

Clause 2 - Unchangeability of the clauses

a) The parties undertake not to amend the clauses except to supplement or update the information specified in the annexes.
b) This does not prevent the parties from incorporating the standard contractual clauses set forth in these clauses into a more comprehensive contract and from adding other clauses or additional guarantees, provided that they do not directly or indirectly conflict with the clauses or interfere with the fundamental rights or freedoms of the data subjects.

Clause 3 - Interpretation

a) Where terms defined in Regulation (EU) 2016/679 are used in such clauses, such terms shall have the same meaning as in the relevant Regulation.
b) These clauses are to be interpreted in light of the provisions of Regulation (EU) 2016/679.
c) These clauses may not be interpreted in a way that is contrary to the rights and obligations provided for in Regulation (EU) 2016/679 or that restricts the fundamental rights or freedoms of the data subjects.

Clause 4 - Priority

In the event of any conflict between these clauses and the provisions of any related agreements existing between the parties or subsequently entered into or concluded, these clauses shall prevail.

Clause 5 - Tying clause (not occupied)

SECTION II

OBLIGATIONS OF THE PARTIES

Clause 6 - Description of the processing

The details of the processing operations, in particular the categories of personal data and the purposes for which the personal data are processed on behalf of the controller, are set out in Annex II.

Clause 7 - Obligations of the parties

7.1. instructions

a) The processor shall process personal data only on the documented instructions of the controller, unless it is required to process under Union law or the law of a Member State to which it is subject. In such a case, the Processor shall notify the Controller of such legal requirements prior to the processing, unless the law in question prohibits it on the grounds of an important public interest. The controller may issue further

instructions throughout the duration of the processing of personal data. These instructions shall always be documented.

b) The Processor shall inform the Controller without undue delay if it considers that instructions given by the Controller violate Regulation (EU) 2016/679 or applicable Union or Member State data protection provisions.

7.2. earmarking

The Processor shall process the Personal Data only for the specific purpose(s) set forth in Annex II, unless it receives further instructions from the Controller.

LY.SEARCH uses a software application to identify report crash details. This allows problems with crashes to be diagnosed and targeted for resolution. No personally identifiable information is collected during crash reporting. The data collected through logging, even when additional data is requested, does not contain information that allows developers to identify individuals.

7.3. Duration of the processing of personal data

The data shall be processed by the processor only for the duration specified in Annex II.

7.4. Security of processing

a) The Processor shall take at least the technical and organizational measures listed in Annex III to ensure the security of the Personal Data. This includes the protection of the data against a breach of security that results, whether accidental or unlawful, in the destruction, loss, alteration or unauthorized disclosure of, or access to, the data (hereinafter "personal data breach"). In assessing the appropriate level of protection, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, circumstances and purposes of the processing, as well as the risks involved for the data subjects.

b) The Processor shall grant its Personnel access to the Personal Data which are the subject of the Processing only to the extent strictly necessary for the performance, management and monitoring of the Contract. The Processor shall ensure that the persons authorized to process the Personal Data received have committed themselves to confidentiality or are subject to an appropriate legal duty of confidentiality.

7.5. Sensitive data

If the processing concerns personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, or containing genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning a person's health, sex life or sexual orientation, or data concerning criminal convictions and offences (hereinafter "sensitive data"), the Processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance with the clauses

a) The parties must be able to demonstrate compliance with these clauses.

b) The Processor shall promptly and appropriately handle requests from the Controller regarding the processing of Data pursuant to these Clauses.

c) The Processor shall provide the Controller with all information necessary to demonstrate compliance with the obligations set out in these Clauses and arising directly from Regulation (EU) 2016/679. At the request of the Controller, the Processor shall also allow and contribute to the audit of the processing activities covered by these Clauses at reasonable intervals or when there are indications of non-compliance. When deciding on a review or audit, the Controller may take into account relevant certifications of the Processor.

d) The Controller may conduct the audit itself or engage an independent auditor. Audits may include inspections of the Processor's premises or physical facilities and shall be conducted with reasonable advance notice, as appropriate.

e) The parties shall provide the relevant supervisory authority(ies) with the information referred to in this clause, including the results of audits, upon request.

7.7. Use of subcontracted processors

a) The Processor may subcontract its processing operations carried out on behalf of the Controller in accordance with these Clauses to a Subprocessor until revoked by the Controller. The Processor shall inform the Controller at least four weeks before subcontracting the relevant Subprocessor and shall provide the Controller with the information necessary for the Controller to decide on revocation. The list of sub-processors can be found in Annex IV, and LY.SEARCH shall keep Annex IV up to date at all times.

b) Where the Processor engages a sub-processor to carry out certain processing activities (on behalf of the Controller), such engagement shall be by way of a contract that imposes on the sub-processor substantially

the same data protection obligations as those applicable to the Processor under these Clauses. The Processor shall ensure that the Sub-processor complies with the obligations to which the Processor is subject in accordance with these Clauses and in accordance with Regulation (EU) 2016/679.

c) The Processor shall provide the Controller with a copy of such subcontracting agreement and any subsequent amendments upon the Controller's request. To the extent necessary to protect trade secrets or other confidential information, including personal data, the Processor may obscure the wording of the agreement before providing a copy.

d) The Processor shall be fully liable to the Controller for the Sub-processor's compliance with its obligations under the contract concluded with the Processor. The Processor shall notify the Controller if the Subprocessor fails to fulfill its contractual obligations.

e) The Processor shall agree with the Sub-processor on a third party beneficiary clause, according to which the Controller - in the event that the Processor ceases to exist factually or legally or is insolvent - shall have the right to terminate the subcontract and instruct the Sub-processor to delete or return the Personal Data.

7.8. International data transfers

a) Any transfer of data by the Processor to a third country or an international organization shall be made solely on the basis of documented instructions from the Controller or to comply with a specific provision under Union law or the law of a Member State to which the Processor is subject and shall comply with Chapter V of Regulation (EU) 2016/679.

b) The Controller agrees that in cases where the Processor uses a sub-processor pursuant to clause 7.7 for the performance of certain processing activities (on behalf of the controller) and such processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor may ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission pursuant to Article 46(2) of Regulation (EU) 2016/679, provided that the conditions for the application of such standard contractual clauses are met.

Clause 8 - Support of the person in charge

a) The processor shall immediately inform the controller of any request received from the data subject. He shall not respond to the request himself unless he has been authorized to do so by the controller.

b) Taking into account the nature of the processing, the processor shall assist the controller in fulfilling the controller's obligation to respond to requests from data subjects to exercise their rights. In fulfilling its obligations under points (a) and (b), the Processor shall follow the instructions of the Controller.

c) In addition to the Processor's obligation to assist the Controller under Clause 8(b), the Processor shall, taking into account the nature of the Data Processing and the information available to it, also assist the Controller in complying with the following obligations:

   1) Obligation to carry out an assessment of the impact of the intended processing operations on the protection of personal data (hereinafter "data protection impact assessment") where a form of processing is likely to result in a high risk to the rights and freedoms of natural persons;
   2) Obligation to consult the competent supervisory authority(ies) prior to processing where a data protection impact assessment indicates that the processing would result in a high risk, unless the controller takes measures to mitigate the risk;
   3) Obligation to ensure that personal data is factually accurate and up to date, in that the processor shall inform the controller without delay if it discovers that the personal data it processes is inaccurate or out of date;
   4) obligations under Article 32 of Regulation (EU) 2016/679.

d) The Parties shall specify in Annex III the appropriate technical and organizational measures for the Processor's assistance to the Controller in the application of this Clause and the scope and extent of the assistance required.

Clause 9 - Notification of personal data breaches

In the event of a personal data breach, the Processor shall cooperate with and provide appropriate assistance to the Controller to enable the Controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679, taking into account the nature of the processing and the information available to the Processor.

9.1 Violation of the protection of the data processed by the data controller.

In the event of a personal data breach in connection with the data processed by the Controller, the Processor shall assist the Controller as follows:

a) in notifying the personal data breach to the competent supervisory authority or authorities without undue delay after the breach has become known to the controller, if relevant (unless the personal data breach is unlikely to result in a risk to the personal rights and freedoms of natural persons);
b) in obtaining the following information to be included in the notification of the controller pursuant to Article 33(3) of Regulation (EU) 2016/679, which information shall include at least the following:
   1) the nature of the personal data, where possible, indicating the categories and approximate number of data subjects, and the categories and approximate number of personal data records concerned;
   2) the probable consequences of the personal data breach;
   3) the measures taken or proposed by the data controller to address the personal data breach and, where appropriate, measures to mitigate its possible adverse effects.

   If and to the extent that all such information cannot be provided at the same time, the initial notification shall include the information available at that time, and additional information, when available, shall be provided thereafter without unreasonable delay;
c) in complying with the obligation under Article 34 of Regulation (EU) 2016/679] or to notify the data subject without undue delay of the personal data breach where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2. violation of the protection of the data processed by the processor

In the event of a personal data breach in connection with the data processed by the Processor, the Processor shall notify the Controller thereof without undue delay after becoming aware of the breach. This notification shall contain at least the following information:

a) A description of the nature of the breach (specifying, if possible, the categories and approximate number of individuals affected and the approximate number of records affected);
b) Contact details of a contact point where further information about the personal data breach can be obtained;
c) the likely consequences and the measures taken or proposed to be taken to remedy the personal data breach, including measures to mitigate its possible adverse effects.

If and to the extent that all such information cannot be provided at the same time, the initial notification shall contain the information available at that time, and additional information shall be provided thereafter without unreasonable delay as it becomes available.

The Parties shall set out in Annex III any other information to be provided by the Processor to assist the Controller in fulfilling its obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III

FINAL PROVISIONS

Clause 10 - Violations of the clauses and termination of the contract

a) If the Processor fails to comply with its obligations under these clauses, the Controller may, without prejudice to the provisions of Regulation (EU) 2016/679, instruct the Processor to suspend the processing of personal data until it complies with these clauses or the contract is terminated. The Processor shall inform the Controller without undue delay if, for whatever reason, it is unable to comply with these clauses.
b) The Controller shall be entitled to terminate the contract insofar as it concerns the processing of personal data pursuant to these clauses if
   1) the controller has suspended the processing of personal data by the processor pursuant to letter a and compliance with these clauses has not been restored within a reasonable period of time and in any case within one month after the suspension;
   2) the Processor materially or persistently breaches these Clauses or fails to comply with its obligations under Regulation (EU) 2016/679;
   3) the Processor fails to comply with a binding decision of a competent court or the competent supervisory authority(ies) which has as its object its obligations under these clauses, Regulation (EU) 2016/679.
c) The Processor shall be entitled to terminate the Contract insofar as it concerns the processing of Personal Data pursuant to these Clauses if the Controller insists on the performance of its instructions after having been notified by the Processor that its instructions violate applicable legal requirements pursuant to Clause 7.1(b).
d) Upon termination of the contract, the Processor shall, at the choice of the Controller, erase all personal data processed on behalf of the Controller and certify to the Controller that this has been done, or return

all personal data to the Controller and erase existing copies, unless there is an obligation under Union or Member State law to retain the personal data. Until the deletion or return of the data, the Processor shall continue to ensure compliance with these clauses.

ANNEX I - LIST OF PARTIES

Person(s) responsible:

CENTER (see in detail cover sheet main contract)

Processor:

LY.SEARCH GmbH (see in detail cover sheet main contract)

Data protection officer: RA P. Weißmann, advokIT Rechtsanwälte und Datenschutzbeauftragte, Schirmerstr. 30, 50823 Cologne, T +49 (0) 221 9758 0850, datenschutz@advokit.de

ANNEX II - DESCRIPTION OF PROCESSING

Categories of data subjects whose personal data are processed

- Customers, patients

Categories of personal data that are processed

- Personal master data, contact data, health data

Sensitive data processed (if applicable) and restrictions or safeguards applied that take full account of the nature of the data and the associated risks, e.g., strict purpose limitation, access restrictions (including access only to individuals who have completed specific training), records of access to the data, restrictions on onward transfers, or additional security measures

- Health data, strict purpose limitation, supplementary use for science and research on an anonymized and pseudonymized data basis, technical operation by service providers experienced and proven in the healthcare sector

  Additional obligation of the order processor as follows (confidentiality obligation, § 203 StGB):

  LY.SEARCH undertakes to observe the same rules for the protection of secrets as are incumbent upon the person responsible. LY.SEARCH undertakes to obtain knowledge of third party secrets only to the extent that this is necessary for the fulfillment of the order. LY.SEARCH guarantees that all employees and vicarious agents who perform processing services for the person responsible are either subject to a legal obligation of secrecy or have contractually undertaken to observe data secrecy and have been sufficiently instructed about the obligations covered by data secrecy. The obligation to maintain secrecy shall continue to exist after the termination of this agreement or the main contract.

  § Section 203 of the Criminal Code - violation of private secrets

  (1) Any person who without authorization discloses another's secret, namely a secret belonging to the personal sphere of life or a trade or business secret, which he or she considers to be a

  1. physician, dentist, veterinarian, pharmacist or member of another medical profession that requires state-regulated training for the practice of the profession or the use of the professional title,

  2. professional psychologists with a state-approved scientific final examination,

  [...]

  7. members of a private health, accident or life insurance company or of a private medical, tax consulting or lawyer's clearing office

  or has otherwise become known, shall be punished by a term of imprisonment of up to one year or a fine.

  (2) [...]

  (2a) (omitted)

  (3) No disclosure within the meaning of this provision shall be deemed to have occurred if the persons referred to in paragraphs 1 and 2 disclose secrets to assistants working for them on a professional basis or to persons working for them in preparation for their profession. The persons referred to in paragraphs 1 and 2 may disclose third party secrets to other persons involved in their professional or service activities to the extent necessary for the use of the activities of the other involved persons; the same shall apply to other involved persons if they use other persons involved in the professional or service activities of the persons referred to in paragraphs 1 and 2.

  (4) A ***penalty of up to one year's imprisonment or a fine shall be imposed on anyone who, without authorization, discloses a secret belonging to another person which has become known to him or her in the course of or on the occasion of performing his or her duties as a***

contributor or as a data protection officer working for the persons referred to in paragraphs 1 and 2. *Likewise, a person shall be punished who*

1. as a person referred to in paragraphs 1 and 2, has not ensured that another cooperating person who unauthorizedly discloses a third party secret that has become known to him/her in the course of or on the occasion of his/her activity has been obliged to maintain confidentiality; this shall not apply to other cooperating persons who are themselves a person referred to in paragraphs 1 or 2,

2. as a contributory person referred to in paragraph 3, has made use of another contributory person who unauthorizedly discloses a third party secret that has become known to him/her in the course of or on the occasion of his/her activity, and has not ensured that the latter has been bound to secrecy; this shall not apply to other contributory persons who are themselves a person referred to in paragraphs 1 or 2, or

3. after the death of the person obligated under sentence 1 or under paragraphs 1 or 2, unauthorizedly discloses a third party secret which he or she learned from the deceased or obtained from the deceased's estate.

(5) Paragraphs (1) to (4) shall also apply if the perpetrator discloses the foreign secret without authorization after the death of the person concerned.

(6) If the offender acts for remuneration or with the intention to enrich himself or another or to harm another, the punishment shall be imprisonment for a term not exceeding two years or a fine.

LY.SEARCH has been advised that the aforementioned penalty provision applies to LY.SEARCH. By entering into this Agreement, LY.SEARCH declares to have been informed of the content of the aforementioned provisions.

LY.SEARCH undertakes to inform all employees and vicarious agents who perform processing services for LY.SEARCH equally about the contents of Section 203 of the German Penal Code and to oblige them to maintain confidentiality. If LY.SEARCH uses other processors for the performance of the contract in an authorized manner, LY.SEARCH shall be obliged to ensure by contract that the persons employed by the other processors are also bound to secrecy accordingly.

Type of processing

- Online service for complex data collection on lipedema; structured data collection and data management for medical practices, creation of anonymized, pseudonymized and structured database by order processors for research purposes according to SaaS service agreement

Purpose(s) for which the personal data are processed on behalf of the controller

- Data collection, data structuring and data evaluation for medical practices around lipedema; construction of anonymized, pseudonymized and structured data base by order processor for research purposes according to SaaS service contract

Processing duration

- According to SaaS service contract

In the case of processing by (sub)processors, the subject matter, nature and duration of the processing shall also be indicated.

- Hosting and technical operation, duration according to SaaS service contract

ANNEX III -TECHNICAL AND ORGANIZATIONAL MEASURES, INCLUDING TO ENSURE THE SECURITY OF DATA

The technical-organizational measures of LY.SEARCH GmbH at the location of the administration, Gereonstr. 18-32, 50670 Cologne for the Service PST are described below under **A.**. Technical-organizational measures of the technical service provider and subcontractor for the technical realization of the Service PST are furthermore described under **B.**

A. Technical-organizational measures LY.SEARCH GmbH for Service PST

Basic measures

Fundamental measures that serve to safeguard the rights of data subjects, respond immediately in emergencies, meet the requirements of technology design, and protect data at the employee level:

- There is an internal data protection management system, compliance with which is constantly monitored and evaluated on an ad hoc basis and at least semi-annually.
- The software used is always kept up to date, as are virus scanners and firewalls.
- Regular reviews are carried out to determine whether the state of the art has changed and whether there is a need to adapt the IT systems accordingly.
- The hardware and software used is regularly checked for functionality.
- The protection needs classification for data processing operations is reviewed regularly.

1. Confidentiality

1.1 Access control / Access control

- All systems are secured with a firewall (hardware).
- An always up-to-date virus protection is set up.
- An always up-to-date software version is set up.
- Authorization/authentication concepts limited to the most necessary Access regulations.
- Organizational authorization (e.g., by the supervisor) and technical authorization (e.g., by the administrator) are granted by different persons.
- All systems are secured with a firewall (software).
- Attention is paid to the proper destruction of data carriers.
- An individual user ID is assigned per user.
- There is a password policy with definition of a minimum length and specifications for the Complexity of passwords (e.g. upper and lower case, numbers, special characters)
- Passwords are created exclusively by the user.
- Remote maintenance is performed exclusively via unique user IDs (no collective accounts).
- A change of the password is technically enforced at regular intervals.
- The disclosure of passwords is prohibited.
- Passwords are stored exclusively in encrypted form.

1.2 Access control

- The allocation of keys and transponders is regulated in writing.
- There is a security guard who carries out control rounds in the evening
- There is a reception
- Access for persons outside the company is regulated.
- Transponder locking system
- Window security: Doors, gates and windows are firmly locked outside operating hours.
- Supervision of auxiliary staff
- Visitors are not allowed to move unaccompanied in the building
- Employees of service providers who are free to move around the company premises (e.g. cleaning staff, messengers, suppliers) are separately bound to confidentiality.

1.3 Pseudonymization

- Especially for the PST service: Users of the service transmit pseudonymized patient data for processing, so that to this extent already only pseudonymized data are transmitted and processed; assignment of the pseudonyms is only possible by the respective users themselves, not by LY.SEARCH GmbH.

2. Integrity

2.1 Transport and transfer control

- There is a binding instruction for data collection.
- The use of private data carriers (e.g. USB sticks, external hard drives) is prohibited.
- All employees who handle personal data are separately (e.g. through
- contract, declaration of commitment) or legally obligated to maintain secrecy.
- Encryption of data carriers and connections

2.2 Input control

- Failed attempts to access the data processing systems are logged.
- Every administrator activity is technically logged.

3. Availability and resilience

- Constantly controlled backup and recovery concept.
- The IT systems are maintained by specialists who undergo regular training.
- Overvoltage protection
- Updates of software are performed centrally.
- Data backups are also regularly performed at locations geographically different from the servers. Places stored / kept.
- Regular systematic execution of data backups (BackUps)
- Data recovery from backups is tested regularly.
- Network and server infrastructure have effective virus and malware protection

4. Procedures for regular review, assessment and evaluation

4.1 Incident Response Management

Support for security breach response

- Recourse to technical service provider

4.2 Privacy friendly settings

Privacy by design / privacy by default

- Especially for the PST service: Users of the service transmit pseudonymized data for processing, so that to this extent only pseudonymized data are processed; assignment of the pseudonyms is thus only possible by the users themselves, not by LY.SEARCH GmbH.

4.3 Order control (outsourcing to third parties)

- Selection of the subcontractor under due diligence aspects (especially with regard to data security)
- prior examination of and documentation of the safety measures taken at the subcontractor's premises
- written instructions to the subcontractor (e.g. by order processing contract)
- Obligation of the subcontractor's employees to data secrecy

- Subcontractor has appointed data protection officer
- Ensuring the destruction of data from the subcontractor's systems after the completion of the order
- Effective control rights agreed with respect to the subcontractor
- continuous monitoring of the subcontractor and its activities

5. Special data protection measures

Especially for the service PST: Obligation of secrecy (§ 203 StGB)

B. Technical-organizational measures (technical operation, Bergnet GmbH)

1. Confidentiality

1.1 Access control

The offices and store of Bergnet GmbH are located in a building in Lindlar.

The entrances to the offices of Bergnet GmbH are locked day and night. Access of walk-in customers to the store is possible only during opening hours and when an employee is present. Only the landlord and the tenant of the premises have access to the building. A locking system is used, which is managed by the tenant (the management of Bergnet GmbH).

Key allocation and key management is carried out according to a defined process that regulates the granting or withdrawal of access authorizations for rooms both at the beginning of an employment relationship and at the end of an employment relationship.

Access authorizations are only granted to an employee if this has been requested by the respective supervisor and/or management. The principle of necessity is taken into account when issuing authorizations.

Visitors are admitted to the building only after the reception desk has opened the door, and then to the offices. The reception can see the entrance door and ensures that each visitor reports to the reception.

Each visitor will be escorted by the receptionist to their respective contact person. Visitors are not allowed to move freely in the office without an escort.

The entrances and windows of the office building and also the offices of Bergnet GmbH are secured with an alarm system. This can be activated and deactivated manually.

1.2 Access control

To gain access to IT systems, users must have the appropriate access authorization. To this end, corresponding user authorizations are issued by administrators. However, this is only done if it has been requested by the respective supervisor. The request can also be made via the management.

The user is then given a username and an initial password, which must be changed the first time the user logs in. The password defaults include a minimum password length of 8 characters, where the password must consist of upper/lower case letters, numbers and special characters.

Passwords are changed every 90 days. Exceptions to this are passwords with a minimum length of 16 characters. Here, an automatic password change is not indicated.

Remote access to IT systems of Bergnet GmbH always takes place via encrypted connections. An intrusion prevention system is in use on the servers of Bergnet GmbH. All server and client systems have virus protection software, with a daily supply of signature updates guaranteed.

All servers are protected by firewalls, which are always maintained and provided with updates and patches. Access by servers and clients to the Internet and access to these systems via the Internet is also secured by firewalls. This also ensures that only the ports required for the respective communication can be used. All other ports are blocked accordingly.

All employees are instructed to lock their IT systems when they leave them. Passwords are always stored in encrypted form.

1.3 Access control

Authorizations for IT systems and applications of Bergnet GmbH are set up exclusively by administrators.

Authorizations are always granted according to the need-to-know principle. Accordingly, only those persons are granted access rights to data, databases or applications who maintain and service these data, applications or databases or are involved in their development.

The prerequisite is a corresponding request for authorization for an employee by a supervisor. The request can also be submitted to the Human Resources Department.

There is a role-based authorization concept with the option of differentiated assignment of access rights, which ensures that employees receive access rights to applications and data depending on their respective area of responsibility and, if necessary, on a project basis.

The destruction of data carriers and paper is carried out by a service provider who guarantees destruction in accordance with DIN 66399.

All employees at Bergnet GmbH are instructed to place information containing personal data and/or information about projects in the destruction bins designated for this purpose.

Employees are generally prohibited from installing unauthorized software on IT systems.

All server and client systems are regularly updated with security updates.

1.4 Separation

All IT systems used by Bergnet GmbH for customers are multi-client capable. The separation of data from different customers is always guaranteed.

1.5 Pseudonymization & Encryption

Administrative access to server systems is always via encrypted connections. In addition, data on notebooks is stored on encrypted data carriers. Corresponding hard disk encryption systems are in use.

2. Integrity

2.1 Input control

The entry, modification and deletion of personal data processed by Bergnet GmbH on behalf is always logged.

Employees are required to work with their own accounts at all times. User accounts may not be shared or used jointly with other persons.

2.2 Transfer control

A transfer of personal data, which takes place on behalf of customers of Bergnet GmbH, may only take place to the extent that this is agreed with the customer or to the extent that this is necessary for the provision of the contractual services for the customer.

All employees working on a customer project are instructed with regard to the permissible use of data and the modalities of data disclosure.

As far as possible, data is transmitted to recipients in encrypted form.

The use of private data carriers is prohibited for employees at Bergnet GmbH in connection with customer projects.

Employees of Bergnet GmbH are regularly trained on data protection topics. All employees have also been obligated to handle personal data confidentially.

3. Availability and resilience

Data on Bergnet GmbH server systems is backed up incrementally at least daily and "fully" weekly. The backup media are encrypted and moved to a physically separate location. The import of backups is tested regularly.

The IT systems have an uninterruptible power supply. There is a fire detector and CO2 fire extinguishers in the server room. All server systems are subject to monitoring, which immediately triggers messages to an administrator in the event of malfunctions.

There is an emergency plan at Bergnet GmbH, which also includes a restart plan.

4. Procedures for regular review, assessment and evaluation

Data protection management is implemented at Bergnet GmbH. There is a guideline on data protection and data security and guidelines to ensure that the objectives of the guideline are implemented.

A Data Privacy and Information Security Team (DST) has been set up to plan, implement, evaluate and make adjustments to measures in the area of data privacy and data security.

The guidelines are regularly evaluated and adjusted with regard to their effectiveness.

In particular, it is ensured that data protection incidents are recognized by all employees and reported to the DST without delay. The DST will investigate the incident immediately. If data processed on behalf of customers is affected, care is taken to ensure that they are informed immediately about the nature and scope of the incident.

In the case of processing of data for own purposes, if the conditions of Art. 33 GDPR are met, a notification to the supervisory authority will be made within 72 hours after becoming aware of the incident.

4.1 Order control

The processing of the data storage takes place exclusively in the European Union unless this is explicitly agreed otherwise with the customer.

An external data protection officer has been appointed at Bergnet GmbH.

When external service providers or third parties are involved, an order processing contract is concluded by Bergnet GmbH in accordance with the requirements of the applicable data protection law after a prior audit by the data protection officer. Contractors are also regularly monitored during the contractual relationship.

4.2 Data protection through technology design and data protection-friendly default settings

At Bergnet GmbH, care is taken during the development of the software to ensure that the principle of necessity is already taken into account in connection with user interfaces. For example, form fields and screen masks can be designed flexibly. Thus, mandatory fields can be provided or fields can be deactivated.

Bergnet GmbH's software supports both input control through a flexible and customizable audit trail that enables unalterable storage of changes to data and user permissions.

Permissions on data or applications can be set flexibly and granularly.

ANNEX IV - LIST OF SUBPROCESSORS

This annex must be completed in the case of a separate authorization of sub-processors (clause 7.7(a), option 1).

The Controller has authorized the use of the following sub-processors:

Name: Bergnet Ltd.

Address: Feilenhauerstraße 6, 51789 Lindlar

Name, function and contact details of contact person: Andreas Böhm, Management, phone: 02266 903-0, e-mail: info@bergnet.de

Description of the processing (including a clear delineation of responsibilities if multiple sub-processors are approved): Technical operation and support of the SAAS software as well as hosting.