SaaS-Servicevertrag „PST“

nachfolgend „**Vertrag**“ genannt

zwischen

Praxis: _____

Str./Nr.: _____

PLZ/Ort. _____

Tel.: _____

E-Mail: _____

Ansprechpartner:

_____

nachfolgend „**ZENTRUM**“ genannt

und **LY.SEARCH gGmbH**

Schanzenstraße 1 D- 40549 Düsseldorf
Tel.: +49 221 699 93 811
E-Mail: post@lysearch.de

Ansprechpartner:
Katharina Legros (Geschäftsführer)

nachfolgend „**LY.SEARCH**“ genannt

nachfolgend gemeinsam „**Parteien**“ genannt

LY.SEARCH-Auftragsnummer: _____

Inhaltsverzeichnis

CLOUD-SERVICEVERTRAG PST

1 Präambel

LY.SEARCH bietet mit „PST“ einen **cloudbasierten Service für ärztliche Praxen** zur Lipohyperplasia dolorosa (LiDo) „Lipödem“ an, um teilnehmende Praxen bei der komplexen und sachgerechten Erfassung des Krankheitsbildes, relevanter Behandlungsmaßnahmen und Verlaufskontrolle zu unterstützen. Die Nutzung dieses Systems bietet LY.SEARCH als webbasierte Software-as-a-Service-Lösung (nachfolgend als „**Service**“ und „**PST**“ bezeichnet) an.

Im Rahmen ihrer wissenschaftlichen Ausrichtung verfolgt LY.SEARCH zudem das Ziel zum Aufbau einer eigenen **Lipohyperplasia dolorosa (LiDo) „Lipödem“-Datenbasis**, in welche die Daten der von ärztlichen Praxen erfassten Patienten in anonymisierter und strukturierter Form überführt und für eigene Forschungszwecke von LY.SEARCH verwendet bzw. für Forschungszwecke Dritter zur Verfügung gestellt werden sollen.

Das ZENTRUM möchte den Service für sich und seiner Praxis nutzen und drüber hinaus die Forschungstätigkeiten von LY.SEARCH unterstützten.

Vor diesem Hintergrund schließen die Parteien diesen Vertrag.

2 Vertragsgegenstand

2.1 Gegenstand dieses Vertrages ist die Nutzung des Service durch das ZENTRUM für sich und seine Praxis. Die Funktionalitäten und Leistungsmerkmale des Service sind abschließend beschrieben in **ANLAGE 1 – SERVICEBESCHREIBUNG**.

2.2 Voraussetzung für die Nutzung des Service durch das ZENTRUM sind ein auf dem neuesten Update-Stand befindlicher Internet-Browser und eine aktive Internetverbindung. Für beides ist das ZENTRUM verantwortlich; sonstige Mitwirkungspflichten des ZENTRUMS unter diesem Vertrag bleiben unberührt.

2.3 Das ZENTRUM wird darauf hingewiesen, dass der Service naturgemäß nur als Hilfestellung dienen kann und nicht von den ärztlichen Sorgfaltspflichten befreit. Das ZENTRUM ist und bleibt für die ihm obliegenden gesetzlichen Pflichten und die Ermittlung dieser Pflichten und relevanter Vorgaben verantwortlich.

3 Leistungsumfang

3.1 Die vertragsgegenständlichen Serviceleistungen beschränken sich auf die vom ZENTRUM gebuchten Services. Das ZENTRUM darf den von LY.SEARCH bereitgestellten Service nur zu internen, eigenen Zwecken über für das ZENTRUM von LY.SEARCH eingerichtete Benutzerzugänge nutzen (Zugang via Webinterface; vgl. Ziff. 3.2). Es ist dem ZENTRUM nur nach vorheriger und dokumentierter Freigabe durch LY.SEARCH gestattet, den Service für Dritte zu nutzen.

3.2 **Webinterface**: LY.SEARCH stellt dem ZENTRUM während der Laufzeit dieses Servicevertrages die Nutzung eines Webinterface über die Web-Benutzerschnittstelle (User Interface) in der jeweils aktuell von LY.SEARCH freigegebenen Softwareversion am Routerausgang des Rechenzentrums (Gateway), in dem die Software für den vertragsgegenständlichen Service gehostet wird zur Verfügung. Die für die Nutzung des Webinterface auf den Servern erforderliche Rechenleistung und der für die Datenverarbeitung erforderliche Speicherplatz werden von LY.SEARCH bereitgestellt.

3.3 **Professional Service (optional)**: Benötigt das ZENTRUM Unterstützung bei der Inbetriebnahme oder Nutzung des Service, bietet LY.SEARCH Unterstützungsleistungen durch den technischen Kundendienst von LY.SEARCH bzw. dessen technischen Dienstleister an.

4 Mitwirkungspflichten des ZENTRUMS

4.1 Das ZENTRUM benennt LY.SEARCH einen Ansprechpartner, der die zur Durchführung dieses Vertrages erforderlichen Auskünfte erteilen kann und als zentraler Ansprechpartner fungiert. Der vom ZENTRUM benannte Ansprechpartner ist zur Entgegennahme den Vertrag betreffender Erklärungen ermächtigt.

4.2 Das ZENTRUM hat seine internen IT-Systeme nach dem Stand der Technik eigenverantwortlich einzurichten, gegen Schadsoftware bzw. unbefugte Eingriffe Dritter abzusichern, instand zu halten, zu patchen und bei Bedarf zu erneuern. Insbesondere hat er sicherzustellen, dass seine IT-Systeme den jeweiligen Systemvoraussetzungen von LY.SEARCH zur Nutzung des Service entsprechen. Dies gilt im Falle der Nutzung des Webinterface Service u. a. für den verwendeten Internetbrowser (Mozilla Firefox oder Google Chrome).

4.3 Das ZENTRUM ist sich bewusst, dass die dem Service zugrundeliegende Software bzw. der Service selbst von LY.SEARCH fortlaufend weiterentwickelt wird. LY.SEARCH behält sich eine Änderung und/oder Ergänzung des Service vor, insbesondere für den Fall einer Anpassung an technische und/oder rechtliche Erfordernisse. Eine Änderungs- und/oder Anpassungsbefugnis besteht zudem in Fällen gebotener Behebung von etwaigen Sicherheitslücken sowie für den Fall, dass die Änderung für das ZENTRUM lediglich rechtlich vorteilhaft ist. Änderungen mit nur unwesentlichen Auswirkungen auf die Funktionen des Service stellen keine Leistungsänderungen im Sinne dieses Vertrages dar. Berechtigte Interessen des ZENTRUMS werden selbstverständlich angemessen berücksichtigt und über entsprechende Änderungen und/oder Ergänzungen wird angemessen informiert. Rechte des ZENTRUMS im Übrigen werden durch diesen Leistungsänderungsvorbehalt weder ausgeschlossen noch eingeschränkt.

4.4 Das ZENTRUM wird Störungen unverzüglich gemäß Ziff. 6.2 melden. Das ZENTRUM wird LY.SEARCH bei der Fehlersuche aktiv unterstützen.

4.5 Das ZENTRUM hat jede missbräuchliche Nutzung des Service sowie der dem Service zugrunde liegenden Hard- und Software auf Seiten LY.SEARCH zu unterlassen. Eine Nutzung des Service zu rechtswidrigen Zwecken und/oder die Übermittlung rechtswidriger Inhalte über den Service sind untersagt.

4.6 Das ZENTRUM ist dazu verpflichtet, die ihm von LY.SEARCH übermittelten Benutzerpasswörter nach der Erstanmeldung unverzüglich in nur ihm bekannte Passwörter zu ändern. Die Zugangsdaten sind geheim zu halten. Eine Weitergabe an unberechtigte Dritte ist untersagt. Das ZENTRUM hat Sorge dafür zu tragen, dass sämtliche Personen, denen Zugangsdaten von LY.SEARCH und/oder dem Administrator des ZENTRUMS zur Verfügung gestellt werden, diese ebenfalls geheim halten.

4.7 Das ZENTRUM hat seine Benutzer-Daten, insbesondere Anschriften- und Kontaktdaten, während der Vertragslaufzeit aktuell zu halten und LY.SEARCH etwaige Änderungen mitzuteilen. Eine Aktualisierung bzw. Mitteilung hat das ZENTRUM über die Eingabe im Profil auf www.lysearch.de vorzunehmen; über etwaige Anpassungen wird das ZENTRUM LY.SEARCH zudem per E-Mail informieren.

4.8 **Das ZENTRUM ist für die Wahrung handelsrechtlicher und steuerrechtlicher Buchführungs- und Aufzeichnungspflichten (z.B. nach den GoBS, GDPdU), für die Archivierung und Einhaltung entsprechender Aufbewahrungsfristen und für die den berufsrechtlichen Regelungen entsprechenden Führung von Patientenakten und Behandlungsdokumentationen verantwortlich.** Das ZENTRUM verpflichtet sich zum Zwecke der Wahrung seiner Dokumentations- und Archivierungspflichten, die vom ZENTRUM zur Nutzung des Service übermittelten bzw. im Service hinterlegten Daten, namentlich Daten über Patientinnen und Patienten, in geeigneter Weise auf eigenen Systemen abzuspeichern, auszudrucken oder in sonstiger Weise aufzubewahren. **LY.SEARCH ist zu einer dauerhaften Aufbewahrung entsprechender Informationen für das ZENTRUM nicht verpflichtet und übernimmt insbesondere nicht die originär dem ZENTRUM obliegenden berufsrechtlichen Dokumentations- und Aufbewahrungspflichten.** Das ZENTRUM wird darauf hingewiesen, dass bei mangelnder Einhaltung der vorstehenden Vorschriften über die Sicherung und Aufbewahrung der genannten Daten durch das ZENTRUM im Falle einer systemseitigen Löschung, insbesondere bei Vertragsbeendigung, eine Wiederherstellung und/oder Rekonstruktion nicht möglich ist.

5 Verfügbarkeit

5.1 LY.SEARCH wird sich um eine möglichst hohe Verfügbarkeit des Services bzw. dessen Erreichbarkeit über das Webinterface bemühen.

5.2 LY.SEARCH übernimmt keine Garantie für die jederzeitige und unterbrechungsfreie Verfügbarkeit des Services bzw. dessen Erreichbarkeit über das Webinterface.

6 Service und Support

6.1 LY.SEARCH wird die dem Service zugrundeliegende Software während der Laufzeit dieses Vertrages pflegen und jeweils den aktuell freigegebenen Programmstand bzw. der jeweils aktuelle Service zur Nutzung durch das ZENTRUM bereitstellen. Die Pflege umfasst die Erhaltung und Wiederherstellung der Betriebsbereitschaft, die Diagnose und Beseitigung von Mängeln sowie ggf. – auf freiwilliger Grundlage und ohne Verpflichtung hierzu – funktionserweiternde Maßnahmen.

6.2 Das ZENTRUM ist verpflichtet, Funktionsausfälle und sonstige Störungen des Service LY.SEARCH unverzüglich und so präzise wie möglich anzuzeigen. Die Störungsmeldung durch das ZENTRUM erfolgt über ein von LY.SEARCH eingerichtete Störungsmeldungssystem; dieses ist erreichbar unter: support@lysearch.de. In der Störungsmeldung ist die Störung detailliert zu beschreiben:

- Beschreibung der Störung (nach Möglichkeit Screenshots beizufügen)
- Wann ist die Störung aufgetreten?
- Wie wirkt sich die Störung aus?

6.3 LY.SEARCH wird Störungen innerhalb angemessener Frist bearbeiten. Verbindliche Reaktions- oder Beseitigungszeiten werden nicht vereinbart.

6.4 Soweit nicht explizit abweichend vereinbart, schuldet LY.SEARCH unter diesem Vertrag keine weitergehenden Schulungs-, Beratungs-, Entwicklungs- und Einrichtungsleistungen.

7 Vergütung

7.1 Teilnehmende Praxen sind als ZENTREN nicht zur Zahlung von Entgelten für die Nutzung des Service verpflichtet. Der Service wird insoweit kostenfrei angeboten.

7.2 Es wird vorsorglich klargestellt, dass den teilnehmenden Praxen als ZENTREN kein Anspruch auf kostenlose Leistungen von LY.SEARCH über die reine Service-Nutzung hinaus zusteht; dies gilt insbesondere für etwaige Einzelbeauftragungen für besondere Auswertungen von Daten des ZENTRUMS oder die Erbringung wissenschaftlicher Leistungen bzw. Forschungstätigkeiten.

8 Haftung

8.1 Eine Haftung von LY.SEARCH für einfach fahrlässige Pflichtverletzungen ist ausgeschlossen, sofern nicht Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit oder Garantien betroffen oder Ansprüche nach dem Produkthaftungsgesetz berührt sind.

8.2 Unberührt bleibt ferner die Haftung für die Verletzung von Pflichten, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht und auf deren Einhaltung das ZENTRUM regelmäßig vertrauen darf; insoweit ist die Haftung jedoch auf den typischerweise vorhersehbaren Schaden begrenzt. Eine Haftung für mittelbare Schäden sowie entgangenen Gewinn in Fällen einfach fahrlässiger Pflichtverletzungen ist im Verhältnis zu LY.SEARCH zudem ausgeschlossen; dieser Ausschluss dient der angemessenen Abbildung des Umstandes, dass für die Leistungen von LY.SEARCH unter diesem Vertrag keine Vergütung vorgesehen ist; für etwaig kostenpflichtige Zusatzleistungen gilt dieser Ausschluss nicht.

9 Vertragslaufzeit, Kündigung

9.1 Der Vertrag wird auf unbestimmte Zeit geschlossen; die Vertragslaufzeit beginnt mit Zusendung der Zugangsdaten durch LY.SEARCH an das ZENTRUM.

9.2 Der Vertrag ist jederzeit ordentlich mit einer Frist von vier Wochen zum Ende eines jeden Quartals kündbar.

9.3 Das Recht zur Kündigung aus wichtigem Grund bleibt unberührt. LY.SEARCH ist zur Kündigung aus wichtigem Grund insbesondere befugt, wenn das ZENTRUM einen bestehenden Zahlungsrückstand trotz Mahnung und angemessener Fristsetzung nicht ausgleicht und/oder das ZENTRUM den Service vertragswidrig für Dritte nutzt oder Dritten zur Nutzung überlässt.

9.4 Kündigungen unter diesem Vertrag bedürfen der Textform. Sofern das ZENTRUM per E-Mail kündigen möchte, hat dies an die E-Mail-Adresse kuendigung@lysearch.de zu erfolgen.

9.5 Das ZENTRUM wird darauf hingewiesen, dass mit Wirksamwerden einer Kündigung ein Zugriff auf den Service und die für vom ZENTRUM hinterlegten Daten durch das ZENTRUM nicht mehr möglich ist. Dem ZENTRUM obliegt die fortlaufende Sicherung bzw. der Export etwaig über die Vertragsbeendigung hinaus benötigter Daten; vgl. hierzu auch Ziff. 4.8.

10 Datenschutz und Vertraulichkeit

10.1 Das ZENTRUM wird im Rahmen des Vertrages und der Nutzung des Service die dem ZENTRUM obliegenden datenschutzrechtlichen Verpflichtungen, insbesondere gemäß DS-GVO und BDSG sowie berufsrechtliche Vorgaben strikt beachten. Soweit das ZENTRUM im Rahmen der Vertragsdurchführung bzw. Servicenutzung personenbezogene Daten an LY.SEARCH übermitteln sollte, **ist das ZENTRUM für eine entsprechende Übermittlungsbefugnis verantwortlich**.

10.2 Das ZENTRUM hat insbesondere dafür Sorge zu tragen, dass eine Übermittlung personenbezogener Patienten- bzw. Gesundheitsdaten ausschließlich mit Einwilligung der betroffenen Patienten erfolgt. Die Einwilligung hat die Übermittlung und Nutzung der Daten durch LY.SEARCH sowohl für Zwecke der Verlaufs- und Behandlungskontrolle durch bzw. für das ZENTRUM als auch die Verwendung anonymisierter Patientendaten für wissenschaftliche Forschungszwecke von LY.SEARCH abzubilden, wobei die unterschrieben Einwilligungserklärung vom ZENTRUM aufzubewahren ist. Einen FORMULIERUNGSVORSCHLAG für eine solche Einwilligungserklärung stellt LY.SEARCH dem ZENTRUM zur Verfügung. Die datenschutzrechtliche Verantwortlichkeit für die Ordnungsgemäßheit und Rechtsmäßigkeit der vom ZENTRUM verwendeten Erklärung verbleibt beim ZENTRUM; LY.SEARCH darf weder Rechtsberatungsleistungen erbringen noch kann LY.SEARCH die Verantwortung für das ZENTRUM übernehmen.

Das ZENTRUM wird LY.SEARCH zudem keine unmittelbaren Identifikationsmerkmale von Patienten wie Name, Anschrift und Krankenversicherungsnummer mitteilen bzw. über den Service verarbeiten lassen (auch nicht in Freifeldern wie Kommentarfeldern, etc.), sondern für eine Pseudonymisierung Sorge tragen (Verwendung ZENTRUMS-interner Kennungen bzw. Patienten-Nummern). LY.SEARCH prüft die vom ZENTRUM übermittelten bzw. über den Service zur Verarbeitung bereitgestellten Daten nicht dahingehend, ob diese ggf. doch unzulässig übermittelte unmittelbare Identifikationsmerkmale enthalten; das ZENTRUM ist für die Dateneingabe und Datenübermittlung an LY.SEARCH auch insoweit allein verantwortlich und wird die Datensätze vor Übermittlung bzw. Absendung sorgfältig und insbesondere auf Einhaltung der datenschutzrechtlichen Vorgaben prüfen.

10.3 Soweit LY.SEARCH unter diesem Vertrag personenbezogene Daten im Auftrag des ZENTRUMS verarbeitet, vereinbaren die Parteien eine Vereinbarung über Auftragsverarbeitung gemäß **ANLAGE 2 – AUFTRAGSVERARBEITUNG**. Diese Vereinbarung bildet einen integralen Bestandteil dieses Vertrages und sieht besondere Vorgaben zur Abbildung von Anforderungen an Berufsgeheimnisträger vor (ärztliche Schweigepflicht).

Es wird vorsorglich klargestellt, dass die unter diesem Vertrag vorgesehene Verwendung anonymisierter Patientendaten durch LY.SEARCH für wissenschaftliche Forschungszwecke

durch die Vereinbarung über Auftragsverarbeitung nicht beschränkt wird, die entsprechende Verwendung vielmehr von der Zweckbestimmung der Auftragsverarbeitung gedeckt ist; LY.SEARCH bleibt insbesondere auch nach Beendigung dieses Vertrages und/oder der Vereinbarung über Auftragsverarbeitung befugt, die bis zum Wirksamwerden der Vertragsbeendigung für die benannten Zwecke anonymisierten Daten weiterhin und dauerhaft zu verwenden.

11 Nachunternehmer

LY.SEARCH ist dazu berechtigt, die unter diesem Vertrag geschuldeten Leistungen durch Nachunternehmer erbringen zu lassen. Dies gilt insbesondere für den technischen Betrieb von zur Realisierung des Service genutzten Rechenzentren. LY.SEARCH wird insoweit für angemessene Vereinbarungen zur Wahrung der Vertraulichkeit und datenschutzrechtlicher Anforderungen Sorge tragen.

12 Referenz

LY.SEARCH ist dazu berechtigt, das ZENTRUM als Referenzzentrum zu benennen. Sollte das ZENTRUM eine solche Benennung nicht wünschen, kann das ZENTRUM einer Referenzzentrumsbenennung jederzeit formlos gegenüber LY.SEARCH widersprechen.

13 Schlussbestimmungen

13.1 Allgemeine Geschäftsbedingungen des ZENTRUMS finden keine Anwendung.

13.2 Es gilt deutsches Recht unter Ausschluss des UN-Kaufrechts (CISG) und des Deutschen Internationalen Privatrechts.

13.3 Mündliche Nebenabreden bestehen nicht. Änderungen oder Ergänzungen dieses Vertrags bedürfen zu ihrer Wirksamkeit der Textform. Auf dieses Formerfordernis kann nur durch eine von beiden Parteien unterzeichnete Erklärung verzichtet werden.

13.4 Das ZENTRUM kann Zurückbehaltungs- und Leistungsverweigerungsrechte nur bei unbestrittenen oder rechtskräftig festgestellten Gegenansprüchen geltend machen. Eine Aufrechnung ist ebenfalls nur mit unbestrittenen oder rechtskräftig festgestellten Gegenansprüchen zulässig.

13.5 Sollten einzelne Bestimmungen dieses Vertrags ganz oder teilweise unwirksam sein oder werden, berührt dies die Wirksamkeit der übrigen Bestimmungen nicht. Anstelle der unwirksamen Bestimmung verpflichten sich die Parteien, die Regelung zu vereinbaren, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung am nächsten kommt.

13.6 Gerichtsstand ist Köln.

14 Anlagen

ANLAGE 1 – SERVICEBESCHREIBUNG

ANLAGE 2 – AUFTRAGSVERARBEITUNG

Praxis: _____	**LY.SEARCH gGmbH**
_____	Köln, den _____
Ort, den	
_____	_____
Unterschrift	Unterschrift
_____	_____
Namen in Klarschrift	Namen in Klarschrift

ANLAGE 1 – SERVICEBESCHREIBUNG

Die Lipohyperplasia dolorosa (LiDo) „Lipödem“ ist eine voranschreitende Erkrankung des Fettgewebes mit zunehmender Schmerzhaftigkeit. Sie ist gekennzeichnet durch eine symmetrische Vermehrung des Fettgewebes an Oberschenkeln, Unterschenkeln, Oberarmen und Unterarmen und führt zu einer Dysproportion der betroffenen Körperteile zum oftmals noch schlanken Körperstamm. Die Fettgewebsvermehrung im Unterhautfettgewebe beinhaltet hyperplastische und hypertrophe Adipozyten. Die Blutgefäße sind vermutlich durchlässig und brüchig, was die Neigung zu Hämatomen erklärt könnte. Vermutlich gelangt Flüssigkeit ins interstitielle Gewebe (Ödematisierung der Fettgewebes, Ausbildung eine lymphologischen Hochvolumentransportinsuffizienz). Lipohyperplasia dolorosa (LiDo) „Lipödem“ Fett enthält Fibrosen, vergrößerte und vermehrte Makrophagen und häufig erhöhte Interleukin-Werte, was auf Entzündungen hinweist. Ob diese Erhöhung der Entzündungsparameter bei LiDo die Folge der Gewebeausdehnung ist und nicht ein pathologischer Zustand des sich ausdehnen Gewebes an sich, ist „work in progress“ einer der Forschungsgruppen, die mit LY.SERACH kooperieren.

Die LY.SEARCH gGmbH entstand aus der Idee heraus, Betroffene mit lymphologischen Erkrankungen durch Grundlagenforschung sowie patientenorientierter Diagnose- und Behandlungsverbesserung eine Chance zu geben, ihr Leben so unbeeinträchtigt wie möglich zu gestalten oder gar eine Heilung zu erwirken. Auf dem Gebiet der Lymphologie gibt es trotz der weltweit hohen Anzahl betroffener Patient*innen noch viele unerforschte Themen. Manches ist bisher in dieser terra incognita nur unzureichend untersucht. Die Perspektiven für eine bessere Zukunft der Patient*innen sind jedoch vielversprechend.

Die intrinsische Motivation von LY.SEARCH ist es, langjährige Erfahrung in Klinik und Forschung zu nutzen. Durch Kooperation mit Wissenschaftler*innen an Universitäten und Kliniken initiiert und ermöglicht LY.SEARCH gezielte Forschung für ein besseres Verständnis von Ursachen, Verlauf und Therapie lymphologischer Erkrankungen. Die sichere Diagnosestellung zu vereinfachen und eine Verbesserung von Behandlung und Krankheitsbewältigung in der angewandten Lymphologie zu erreichen ist ebenso ein Ziel von LY.SEARCH wie die Steigerung der Awareness in der Öffentlichkeit, um zukünftig ein Bewusstsein dafür zu schaffen, dass Betroffene mit Ihrer Krankheit nicht alleine sind, sondern zielgerichtete Hilfe unterschiedlichster Art erhalten können.

Service-Leistungen und Forschungszwecke

Mit dem Service PST (**P**atients history, **S**igns and symptoms, **T**reatment and outcome) stellt die LY.SEARCH gGmbH als Anbieterin ärztlichen Praxen als Zentren einen **Online-Service für die komplexe Erfassung zur Lipohyperplasia dolorosa (LiDo) „Lipödem“** bereit. Dies betrifft sowohl konservative als auch operative Maßnahmen bzw. Behandlungen. Der Service PST unterstützt teilnehmende Praxen bei der komplexen und sachgerechten Erfassung des Krankheitsbildes, relevanter Behandlungsmaßnahmen und Verlaufskontrolle; die Erfassung der Daten erfolgt zu Teil durch Patient*innen selbst und abschließend durch die teilnehmenden Zentren. Das ZENTRUM erhält einmal jährlich eine standardisierte Basisauswertung, die von LY.SEARCH nach festgelegten Kriterien erstellt wird. Diese Basisauswertung umfasst ausschließlich die von LY.SEARCH definierten, zentralen Datenbestandteile und bildet nicht die Gesamtheit der eingegebenen Daten ab. Eine weitergehende, individualisierte Auswertung, die auf spezifische Fragestellungen oder erweiterte Datenbestandteile eingeht, wird vom LY.SEARCH gesondert in Rechnung gestellt.

Die LY.SEARCH gGmbH verfolgt im Rahmen ihrer wissenschaftlichen Ausrichtung neben der Bereitstellung des geschilderten Services für ärztliche Praxen und deren Patient*innen zudem das Ziel zum **Aufbau einer eigenen Lipohyperplasia dolorosa (LiDo) „Lipödem“-Datenbasis**, in welche die Daten der von ärztlichen Praxen erfassten Patienten in anonymisierter und strukturierter Form überführt und für **Forschungszwecke** verwendet bzw. zur Verfügung gestellt werden sollen. Eine Weitergabe personenbezogener Patientendaten an Dritte erfolgt nicht. Die LY.SEARCH gGmbH verspricht sich durch eine möglichst umfangreiche und strukturierte Datenbasis einen erheblichen Erkenntnisgewinn im Hinblick auf das Lipohyperplasia dolorosa (LiDo) „Lipödem“, insbesondere dessen Veranlagung, Verbreitung und Behandelbarkeit.

ANLAGE 2 – AUFTRAGSVERARBEITUNG

[Standardvertragsklauseln (Basis: DS-GVO)]

ABSCHNITT I

Klausel 1 – Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) sichergestellt werden.

b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 zu gewährleisten.

c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.

d) Die Anhänge I bis IV sind Bestandteil der Klauseln.

e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 unterliegt.

f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 erfüllt werden.

Klausel 2 – Unabänderbarkeit der Klauseln

a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3 – Auslegung

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4 - Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Klausel 5 – Kopplungsklausel (nicht besetzt)

ABSCHNITT II

PFLICHTEN DER PARTEIEN

Klausel 6 – Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 7 – Pflichten der Parteien

7.1. Weisungen

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2. Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3. Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

7.4. Sicherheit der Verarbeitung

a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5. Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

7.6. Dokumentation und Einhaltung der Klauseln

a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7. Einsatz von Unterauftragsverarbeitern

a) Der Auftragsverarbeiter darf keinen seiner Verarbeitungsvorgänge, die er im Auftrag des Verantwortlichen gemäß diesen Klauseln durchführt, ohne vorherige gesonderte schriftliche Genehmigung des Verantwortlichen an einen Unterauftragsverarbeiter untervergeben. Der Auftragsverarbeiter reicht den Antrag auf die gesonderte Genehmigung mindestens vier Wochen vor der Beauftragung des betreffenden Unterauftragsverarbeiters zusammen mit den Informationen ein, die der Verantwortliche benötigt, um über die Genehmigung zu entscheiden. Die Liste der vom Verantwortlichen genehmigten Unterauftragsverarbeiter findet sich in Anhang IV. Die Parteien halten Anhang IV jeweils auf dem neuesten Stand.

b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 unterliegt.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8. Internationale Datenübermittlungen

a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 im Einklang stehen.

b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8 – Unterstützung des Verantwortlichen

a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

   1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;
3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;
4) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.

d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9 – Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1. Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:
   1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
   2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
   3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

   Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679] oder, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2. Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);
b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;
c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

ABSCHNITT III

SCHLUSSBESTIMMUNGEN

Klausel 10 – Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn
   1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;
   2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 nicht erfüllt;
   3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 zum Gegenstand hat, nicht nachkommt.

c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.

d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

ANHANG I – LISTE DER PARTEIEN

Verantwortliche(r):

ZENTRUM (siehe im Einzelnen Deckblatt Hauptvertrag)

Auftragsverarbeiter:

LY.SEARCH gGmbH (siehe im Einzelnen Deckblatt Hauptvertrag)

Datenschutzbeauftragter:

ANHANG II – BESCHREIBUNG DER VERARBEITUNG

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

- Kunden, Patienten

Kategorien personenbezogener Daten, die verarbeitet werden

- Personenstammdaten, Kontaktdaten, Gesundheitsdaten

Verarbeitete sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Personen, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen

- Gesundheitsdaten, strenge Zweckbindung, ergänzende Nutzung für Wissenschaft und Forschung auf anonymisierter Datengrundlage, technischer Betrieb durch im Gesundheitswesen erfahrenen und bewährten Dienstleister

  Zusatzverpflichtung des Auftragsverarbeiters wie folgt (Schweigepflicht, § 203 StGB):

  LY.SEARCH verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Verantwortlichen obliegen. LY.SEARCH verpflichtet sich, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Auftragserfüllung erforderlich ist. LY.SEARCH gewährleistet, dass sämtliche Mitarbeiter und Mitarbeiterinnen sowie Erfüllungsgehilfinnen und Erfüllungsgehilfen die Verarbeitungsleistungen für den Verantwortlichen erbringen entweder einer gesetzlichen Geheimhaltungspflicht unterliegen oder sich entsprechend vertraglich zur Einhaltung des Datengeheimnisses verpflichtet haben und hinreichend über die vom Datengeheimnis umfassten Pflichten belehrt worden sind. Die Geheimhaltungspflicht besteht auch nach Beendigung dieser Vereinbarung bzw. des Hauptvertrages fort.

  § 203 Strafgesetzbuch – Verletzung von Privatgeheimnissen

  (1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

  1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,

  2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung,

  […]

  7. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen, steuerberatenden oder anwaltlichen Verrechnungsstelle

  anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

  (2) […]

  (2a) (weggefallen)

  (3) Kein Offenbaren im Sinne dieser Vorschrift liegt vor, wenn die in den Absätzen 1 und 2 genannten Personen Geheimnisse den bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglich machen. Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken.

(4) ***Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als mitwirkende Person oder als bei den in den Absätzen 1 und 2 genannten Personen tätiger Beauftragter für den Datenschutz bekannt geworden ist.*** *Ebenso wird bestraft, wer*

1. als in den Absätzen 1 und 2 genannte Person nicht dafür Sorge getragen hat, dass eine sonstige mitwirkende Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind,

2. als im Absatz 3 genannte mitwirkende Person sich einer weiteren mitwirkenden Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, bedient und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind, oder

3. nach dem Tod der nach Satz 1 oder nach den Absätzen 1 oder 2 verpflichteten Person ein fremdes Geheimnis unbefugt offenbart, das er von dem Verstorbenen erfahren oder aus dessen Nachlass erlangt hat.

(5) Die Absätze 1 bis 4 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart.

(6) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

LY.SEARCH wurde darauf hingewiesen, dass die vorgenannte Strafvorschrift für LY.SEARCH Anwendung findet. LY.SEARCH erklärt mit Abschluss dieser Vereinbarung, vom Inhalt der genannten Bestimmungen unterrichtet zu sein.

LY.SEARCH verpflichtet sich, sämtliche Mitarbeiterinnen und Mitarbeiter sowie Erfüllungsgehilfinnen oder Erfüllungsgehilfen, die Verarbeitungsleistungen für LY.SEARCH erbringen, gleichermaßen über den Inhalt des § 203 StGB zu unterrichten und zur Geheimhaltung zu verpflichten. Zieht LY.SEARCH in befugter Weise weitere Auftragsverarbeiter zur Vertragserfüllung heran, ist LY.SEARCH verpflichtet, vertraglich sicherzustellen, dass auch die beim weiteren Auftragsverarbeiter beschäftigten Personen entsprechend zur Verschwiegenheit verpflichtet werden.

Art der Verarbeitung

- Online-Service für die komplexe Erfassung zum Lipödem; strukturierte Datenerfassung und Datenhaltung für ärztliche Praxen, Aufbau anonymisierter und strukturierter Datenbasis durch Auftragsverarbeiter für Forschungszwecke gemäß SaaS-Servicevertrag

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden

- Datenerfassung, Datenstrukturierung und Datenauswertung für ärztliche Praxen rings um das Lipödem; Aufbau anonymisierter und strukturierter Datenbasis durch Auftragsverarbeiter für Forschungszwecke gemäß SaaS-Servicevertrag

Dauer der Verarbeitung

- Gemäß SaaS-Servicetrag

Bei der Verarbeitung durch (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben.

- Hosting und technischer Betrieb, Dauer gemäß SaaS-Servicevertrag

ANHANG III –TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN, EINSCHLIEßLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

Nachstehend sind unter **A.** die technisch-organisatorischen Maßnahmen der LY.SEARCH gGmbH für den Service PST beschrieben. Technisch-organisatorische Maßnahmen des technischen Dienstleiters und Unterauftragnehmers für die technische Realisierung des Services PST sind darüber hinaus unter **B.** beschrieben.

A. Technisch-organisatorischen Maßnahmen LY.SEARCH gGmbH für Service PST

1. Vertraulichkeit

1.1 Zutrittskontrolle

- Alarmanlage
- Absicherung von Gebäudeschächten
- Manuelles Schließsystem
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Personenkontrolle beim Empfang
- Sorgfältige Auswahl von Reinigungspersonal
- Sorgfältige Auswahl von Wachpersonal

1.2 Zugangskontrolle

- Erstellen von Benutzerprofilen
- Passwortvergabe
- Passwort-Richtlinien (regelmäßige Änderung, Mindestlänge, Komplexität etc.)
- Authentifikation mit Benutzername / Passwort
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Gehäuseverriegelungen
- Einsatz von VPN-Technologie bei der Übertragung von Daten
- Verschlüsselung mobiler IT-Systeme
- Verschlüsselung mobiler Datenträger
- Verschlüsselung der Datensicherungssysteme
- Sperren externer Schnittstellen (USB etc.)
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Personenkontrolle beim Empfang
- Sorgfältige Auswahl von Reinigungspersonal
- Sorgfältige Auswahl von Wachpersonal
- Einsatz von Intrusion-Detection-Systemen
- Einsatz von Anti-Viren-Software
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall

1.3 Zugriffskontrolle

- Berechtigungskonzept
- Verwaltung der Rechte durch Systemadministrator
- Regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte (insb. bei Ausscheiden von Mitarbeitern o.Ä.)
- Anzahl der Administratoren ist das „Notwendigste“ reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten

- Sichere Aufbewahrung von Datenträgern
- physische Löschung von Datenträgern vor Wiederverwendung
- ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- Einsatz von Aktenvernichtern bzw. Dienstleistern
- Protokollierung der Vernichtung
- Verschlüsselung von Datenträgern

1.4 Trennungskontrolle

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Logische Mandantentrennung (softwareseitig)
- Berechtigungskonzept
- Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- Versehen der Datensätze mit Zweckattributen / Datenfeldern / Signaturen
- Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten und abgesicherten IT-System • Trennung von Produktiv- und Testsystem

1.5 Pseudonymisierung

- Speziell für den Service PST: Nutzer des Service übermitteln pseudonymisierte Patientendaten zur Verarbeitung, so dass insoweit bereits nur pseudonymisierte Daten übermittelt und verarbeitet werden; Zuordnung der Pseudonyme ist nur durch die jeweiligen Nutzer selbst möglich, nicht durch die LY.SEARCH gGmbH

2. Integrität

2.1 Transport- und Weitergabekontrolle

- Einsatz von VPN-Tunneln
- Verschlüsselung der Kommunikationswege (z.B. Verschlüsselung des EMail-Verkehrs)
- Verschlüsselung physischer Datenträger bei Transport

2.2 Eingabekontrolle

- Automatische Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

3. Verfügbarkeit und Belastbarkeit

- Unterbrechungsfreie Stromversorgung (USV)
- Klimatisierung der Serverräume
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen in Serverräumen
- Feuerlöschgeräte in Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Erstellen eines Backup- & Recoverykonzepts
- Testen von Datenwiederherstellung
- Erstellen eines Notfallplans
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1 Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

- Rückgriff auf technischen Dienstleister

4.2 Datenschutzfreundliche Einstellungen

Privacy by Design / Privacy by default

- Speziell für den Service PST: Nutzer des Service übermitteln pseudonymisierte Daten zur Verarbeitung, so dass insoweit bereits nur pseudonymisierte Daten verarbeitet werden; Zuordnung der Pseudonyme ist damit nur durch die Nutzer selbst möglich, nicht durch die LY.SEARCH gGmbH

4.3 Auftragskontrolle (Outsourcing an Dritte)

- Auswahl des Subunternehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- vorherige Prüfung der und Dokumentation der beim Subunternehmer getroffenen Sicherheitsmaßnahmen
- schriftliche Weisungen an den Subunternehmer (z.B. durch Auftragsverarbeitungsvertrag)
- Verpflichtung der Mitarbeiter des Subunternehmers auf das Datengeheimnis
- Subunternehmer hat Datenschutzbeauftragten bestellt
- Sicherstellung der Vernichtung von Daten von den Systemen des Subunternehmers nach Beendigung des Auftrags
- Wirksame Kontrollrechte gegenüber dem Subunternehmer vereinbart
- laufende Überprüfung des Subunternehmers und seiner Tätigkeiten

5. Besondere Datenschutzmaßnahmen

- Speziell für den Service PST: Verpflichtung Schweigepflicht (§ 203 StGB)

B. Technisch-organisatorische Maßnahmen (technischer Betrieb, Bergnet GmbH)

1. Vertraulichkeit

1.1 Zutrittskontrolle

Die Büroräume und das Ladenlokal der Bergnet GmbH befinden sich in einem Gebäude in Lindlar.

Die Zugänge zu den Büroräumen der Bergnet GmbH sind Tag und Nacht verschlossen. Zugang von Laufkundschaft zum Ladenlokal ist nur während der Öffnungszeiten und bei Anwesenheit eines Mitarbeiters möglich. Zugang zum Gebäude haben nur der Vermieter und der Mieter der Räume. Eskommt ein Schließsystem zum Einsatz, das vom Mieter (der Geschäftsführung der Bergnet GmbH) verwaltet wird.

Die Schlüsselvergabe und das Schlüsselmanagement erfolgt nach einem definierten Prozess, der sowohl zu Beginn eines Arbeitsverhältnisses als auch zum Ende eines Arbeitsverhältnisses die Erteilung bzw. den Entzug von Zutrittsberechtigungen für Räume regelt.

Zutrittsberechtigungen werden einem Beschäftigten erst erteilt, wenn dies durch den jeweiligen Vorgesetzten und/oder die Geschäftsführung angefordert wurde. Bei der Vergabe von Berechtigungen wird dem Grundsatz der Erforderlichkeit Rechnung getragen.

Besucher erhalten erst nach Türöffnung durch den Empfang Zutritt zu dem Gebäude, und dann zu den Büroräumen. Der Empfang kann die Eingangstür einsehen und trägt Sorge dafür, dass jeder Besucher sich beim Empfang meldet.

Jeder Besucher wird in von der Empfangsperson zu seinem jeweiligen Ansprechpartner begleitet. Besucher dürfen sich nicht ohne Begleitung in den Büroräumen frei bewegen.

Die Eingänge und Fenster des Bürohauses und auch der Büroräume der Bergnet GmbH sind mit einer Alarmanlage gesichert. Diese kann manuell aktiviert und deaktiviert werden.

1.2 Zugangskontrolle

Um Zugang zu IT-Systemen zu erhalten, müssen Nutzer über eine entsprechende Zugangsberechtigung verfügen. Hierzu werden entsprechende Benutzerberechtigungen von Administratoren vergeben. Dies jedoch nur, wenn es von dem jeweiligen Vorgesetzten beantragt wurde. Der Antrag kann auch über die Geschäftsführung gestellt werden.

Der Benutzer erhält dann einen Benutzernamen und ein Initialpasswort, das bei erster Anmeldung geändert werden muss. Die Passwortvorgaben beinhalten eine Mindestpasswortlänge von 8 Zeichen, wobei das Passwort aus Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen bestehen muss.

Passwörter werden alle 90 Tage gewechselt. Ausgenommen hiervon sind Passwörter, die über eine Mindestlänge von 16 Zeichen verfügen. Hier ist ein automatischer Passwortwechsel nicht indiziert.

Remote-Zugriffe auf IT-Systeme der Bergnet GmbH erfolgen stets über verschlüsselte Verbindungen. Auf den Servern der Bergnet GmbH ist ein Intrusion-Prevention-System im Einsatz. Alle Server- und Client-Systeme verfügen über Virenschutzsoftware, bei der eine tagesaktuelle Versorgung mit Signaturupdates gewährleistet ist.

Alle Server sind durch Firewalls geschützt, die stets gewartet und mit Updates und Patches versorgt werden. Der Zugriff von Servern und Clients auf das Internet und der Zugriff auf diese Systeme über das Internet ist ebenfalls durch Firewalls gesichert. So ist auch gewährleistet, dass nur die für die jeweilige Kommunikation erforderlichen Ports nutzbar sind. Alle anderen Ports sind entsprechend gesperrt.

Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen. Passwörter werden grundsätzlich verschlüsselt gespeichert.

1.3 Zugriffskontrolle

Berechtigungen für IT-Systeme und Applikationen der Bergnet GmbH werden ausschließlich von Administratoren eingerichtet.

Berechtigungen werden grundsätzlich nach dem Need-to-Know-Prinzip vergeben. Es erhalten demnach nur die Personen Zugriffsrechte auf Daten, Datenbanken oder Applikationen, die diese Daten, Anwendungen oder Datenbanken warten und pflegen bzw. in der Entwicklung tätig sind.

Voraussetzung ist eine entsprechende Anforderung der Berechtigung für einen Mitarbeiter durch einen Vorgesetzten. Der Antrag kann auch bei der Personalabteilung gestellt werden.

Es gibt ein rollenbasiertes Berechtigungskonzept mit der Möglichkeit der differenzierten Vergabe von Zugriffsberechtigungen, das sicherstellt, dass Beschäftigte abhängig von ihrem jeweiligen Aufgabengebiet und ggf. projektbasiert Zugriffsrechte auf Applikationen und Daten erhalten.

Die Vernichtung von Datenträgern und Papier erfolgt durch einen Dienstleister, der eine Vernichtung nach DIN 66399 gewährleistet.

Alle Mitarbeiter bei Bergnet GmbH sind angewiesen, Informationen mit personenbezogenen Daten und/oder Informationen über Projekte in die hierfür ausgewiesenen Vernichtungsbehältnisse einzuwerfen.

Beschäftigten ist es grundsätzlich untersagt, nicht genehmigte Software auf den IT-Systemen zu installieren.

Alle Server- und Client-Systeme werden regelmäßig mit Sicherheits-Updates aktualisiert.

1.4 Trennung

Alle der Bergnet GmbH für Kunden eingesetzten IT-Systeme sind mandantenfähig. Die Trennung von Daten von verschiedenen Kunden ist stets gewährleistet.

1.5 Pseudonymisierung & Verschlüsselung

Ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen. Darüber hinaus werden Daten auf Notebooks auf verschlüsselten Datenträgern gespeichert. Es befinden sich entsprechende Festplattenverschlüsselungssysteme im Einsatz.

2. Integrität

2.1 Eingabekontrolle

Die Eingabe, Änderung und Löschung von personenbezogenen Daten, die von Bergnet GmbH im Auftrag verarbeitet werden, wird grundsätzlich protokolliert.

Mitarbeiter sind verpflichtet, stets mit ihren eigenen Accounts zu arbeiten. Benutzeraccounts dürfen nicht mit anderen Personen geteilt bzw. gemeinsam genutzt werden.

2.2 Weitergabekontrolle

Eine Weitergabe von personenbezogenen Daten, die im Auftrag von Kunden von Bergnet GmbH erfolgt, darf jeweils nur in dem Umfang erfolgen, wie dies mit dem Kunden abgestimmt oder soweit dies zur Erbringung der vertraglichen Leistungen für den Kunden erforderlich ist.

Alle Mitarbeiter, die in einem Kundenprojekt arbeiten, werden im Hinblick auf die zulässige Nutzung von Daten und die Modalitäten einer Weitergabe von Daten instruiert.

Soweit möglich werden Daten verschlüsselt an Empfänger übertragen.

Die Nutzung von privaten Datenträgern ist den Beschäftigten bei Bergnet GmbH im Zusammenhang mit Kundenprojekten untersagt.

Mitarbeiter der Bergnet GmbH werden regelmäßig zu Datenschutzthemen geschult. Alle Mitarbeiter sind auch zu einem vertraulichen Umgang mit personenbezogenen Daten verpflichtet worden.

3. Verfügbarkeit und Belastbarkeit

Daten auf Serversystemen von Bergnet GmbH werden mindestens täglich inkrementell und wöchentlich „voll“ gesichert. Die Sicherungsmedien werden verschlüsselt an einen physisch getrennten Ort verbracht. Das Einspielen von Backups wird regelmäßig getestet.

Die IT-Systeme verfügen über eine unterbrechungsfreie Stromversorgung. Im Serverraum befindet sich ein Brandmelder sowie CO2-Feuerlöscher. Alle Serversysteme unterliegen einem Monitoring, das im Falle von Störungen unverzüglich Meldungen an einen Administrator auslöst.

Es gibt bei Bergnet GmbH einen Notfallplan, der auch einen Wiederanlaufplan beinhaltet.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Bei der Bergnet GmbH ist ein Datenschutzmanagement implementiert. Es gibt eine Leitlinie zu Datenschutz und Datensicherheit und Richtlinien, mit denen die Umsetzung der Ziele der Leitlinie gewährleistet wird.

Es ist ein Datenschutz- und Informationssicherheits-Team (DST) eingerichtet, das Maßnahmen im Bereich von Datenschutz und Datensicherheit plant, umsetzt, evaluiert und Anpassungen vornimmt.

Die Richtlinien werden regelmäßig im Hinblick auf ihre Wirksamkeit evaluiert und angepasst.

Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Mitarbeitern erkannt und unverzüglich dem DST gemeldet werden. Dieses wird den Vorfall sofort untersuchen. Soweit Daten betroffen sind, die im Auftrag von Kunden verarbeitet werden, wird Sorge dafür getragen, dass diese unverzüglich über Art und Umfang des Vorfalls informiert werden.

Bei der Verarbeitung von Daten für eigene Zwecke wird im Falle des Vorliegens der Voraussetzungen des Art. 33 DSGVO eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Kenntnis von dem Vorfall erfolgen.

4.1 Auftragskontrolle

Die Verarbeitung der Datenhaltung erfolgt ausschließlich in der Europäischen Union es sei denn dies ist expliziert mit dem Kunden anders vereinbart.

Bei der Bergnet GmbH ist ein externer Datenschutzbeauftragter benannt.

Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben jeweils anzuwendenden Datenschutzrechts ein Auftragsverarbeitungsvertrag nach zuvor durchgeführten Audit durch den Datenschutzbeauftragten von der Bergnet GmbH abgeschlossen. Auftragnehmer werden auch während des Vertragsverhältnisses regelmäßig kontrolliert.

4.2 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Bei der Bergnet GmbH wird schon bei der Entwicklung der Software Sorge dafür getragen, dass dem Grundsatz der Erforderlichkeit schon im Zusammenhang mit Benutzer-Interfaces Rechnung getragen wird. So sind z.B. Formularfelder, Bildschirmmasken flexibel gestaltbar. So können Pflichtfelder vorgesehen oder Felder deaktiviert werden.

Die Software der Bergnet GmbH unterstützt sowohl die Eingabekontrolle durch einen flexiblen und anpassbaren Audit-Trail, der eine unveränderliche Speicherung von Änderungen an Daten und Nutzerberechtigungen ermöglicht.

Berechtigungen auf Daten oder Applikationen können flexibel und granular gesetzt werden.

ANHANG IV – LISTE DER UNTERAUFTRAGSVERARBEITER

Dieser Anhang muss im Falle einer gesonderten Genehmigung von Unterauftragsverarbeitern ausgefüllt werden (Klausel 7.7 Buchstabe a, Option 1).

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

Name: Bergnet GmbH

Anschrift: Feilenhauerstraße 6, 51789 Lindlar

Name, Funktion und Kontaktdaten der Kontaktperson: Andreas Böhm, Geschäftsführung, Telefon: 02266 903-0, E-Mail: info@bergnet.de

Beschreibung der Verarbeitung (einschließlich einer klaren Abgrenzung der Verantwortlichkeiten, falls mehrere Unterauftragsverarbeiter genehmigt werden): Technischer Betrieb und Betreuung der SAAS-Software sowie Hosting