Datenschutzerklärung / Vereinbarung zur Auftragsverarbeitung

1. Einleitung

Mit Inkrafttreten der EU Datenschutzrichtlinie wurde der Schutz der persönlichen Daten von Nutzern und Anwendern hinsichtlich der Erhebung und Speicherung von Daten präzisiert und vereinheitlicht.

Der LCL biokey GmbH war der Schutz von persönlichen Daten schon immer Aufgabe und Verpflichtung. Patientendaten, die uns im Rahmen einer dienstleistungsbezogenen Auftragsverarbeitung im Zusammenhang mit der Diagnostik zugehen, werden sensibel und sicher verarbeitet und aufbewahrt.

Diese Praxis ist daher nichts Neues, sondern wird, bedingt durch die Regelungen der EU Datenschutzrichtlinie präzisiert und hiermit noch einmal gesondert bestätigt.

Sollten Ihnen diese nachstehenden Erklärungen nicht individuell genug und zu allgemein sein, so sind wir jederzeit bereit, diese noch einmal im Rahmen eines gesonderten Auftragsverarbeitungsvertrages zu formulieren und zu regeln. Wenden Sie sich hierzu bei Bedarf gerne an uns.

2. Gegenstand und Dauer eines Auftrages

(1) Der Auftragnehmer (LCL biokey GmbH) wird vom Auftraggeber (Zahnarztpraxis) damit beauftragt, Laboranalysen durchzuführen. Hierzu findet jeweils eine gesonderte Beauftragung mittels eines Auftragsformulares statt. Gegenstand und Umfang des Auftrags ergeben sich dabei aus der jeweiligen Analysevereinbarung bzw. dem jeweiligen Auftragsformular.

(2) Da der Auftragnehmer in Erfüllung dieser Aufgaben, personenbezogene Daten im Rahmen des Auftrages entgegennimmt und nach Weisung und im Interesse des Auftraggebers verarbeitet erfolgt die Dienstleistung als Auftragsverarbeitung nach den für den Auftraggeber einschlägigen deutschen und europäischen Datenschutzgesetzen.

(3) Die Vereinbarung beginnt mit Unterzeichnung und Entgegennahme der Beauftragung und endet mit der Löschung der personenbezogenen Daten nach Ende der gesetzlich notwendigen Verwahrdauer.

3. Umfang, Art und Zweck der Datenverarbeitung, Datenarten und Betroffenenkreis

(1) Der Umfang, die Art und der Zweck der vorgesehenen Verarbeitung personenbezogener Daten durch den Auftragnehmer werden konkret in der Leistungsvereinbarung beschrieben.

(2) Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien

- Personenstammdaten
- Analysedaten und Analyseergebnisse
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse), Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten

(3) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden/Auftraggeber (Zahnärzte)
- Patienten
- Beschäftigte und Ansprechpartner des Auftragnehmers

4. Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer verpflichtet sich, für die zu verarbeitenden Daten angemessene und dem Stand der Technik entsprechende technische und organisatorische Sicherheitsmaßnahmen nach den für den Auftraggeber einschlägigen deutschen und europäischen Datenschutzgesetzen zu treffen. Der Auftragnehmer berücksichtigt dabei insbesondere die Vorgaben des Art. 32 EU-Datenschutz-Grundverordnung (EU-DSGVO).

(2) Die Datensicherheitsmaßnahmen beim Auftragnehmer können im Laufe eines Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklungen unterliegen. Wesentliche Änderungen werden dabei vom Auftragnehmer mit dem Auftraggeber abgestimmt.

(3) Der Auftragnehmer ist verpflichtet, ein Verzeichnis der Verarbeitungstätigkeiten (Art. 30 EU-DSGVO) über die durch ihn im Auftrag verarbeiteten Daten zu erstellen und dieses auf Aufforderung dem Auftraggeber zur Verfügung zu stellen.

(4) Der Auftragnehmer stellt dem Auftraggeber auf Anforderung ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsdatenverarbeitung zur Verfügung. Sämtliche Zugriffsberechtigte Personen werden auf Aufforderung benannt.

5. Berichtigung, Löschung und Sperrung von Daten

Der Auftragnehmer darf die Daten, die er im Auftrag des Auftraggebers verarbeitet, nur berichtigen, löschen und sperren, wenn der Auftraggeber dies anweist. Der Auftragnehmer fertigt ohne Wissen des Auftraggebers keine Kopien oder Duplikate der Daten.

6. Pflichten des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind und er die innerbetriebliche Organisation so gestaltet, dass sie den besonderen Anforderungen des Datenschutzes unter Berücksichtigung des Berufsgeheimnisschutzes des Auftraggebers gerecht wird.

(2) Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und diese auf das Datengeheimnis und die Vertraulichkeit verpflichtet wurden. Dabei berücksichtigt der Auftragnehmer auch, dass ihm vom Auftraggeber Daten zur Verfügung gestellt werden, die dem besonderen Berufsgeheimnisschutz unterliegen. Die Verpflichtung ist so zu fassen, dass sie auch nach Beendigung eines Auftragsverhältnisses bestehen bleibt.

(3) Der Auftragnehmer sichert zu, dass die verarbeiteten Daten von den sonstigen Datenbeständen seines Unternehmens strikt getrennt werden.

(4) Soweit gesetzlich vorgeschrieben, bestellt der Auftragnehmer schriftlich einen Beauftragten für den Datenschutz. Die Kontaktdaten des Beauftragten für den Datenschutz werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Über einen Wechsel der Person des Beauftragten für Datenschutz beim Auftragnehmer ist der Auftraggeber unverzüglich zu unterrichten. Aktuell unterliegt der Auftragnehmer nicht der Größenvorgabe, ab derer ein Datenschutzbeauftragter zwingend zu installieren ist. Bis zur Erreichung der Mindestgröße überwacht die Geschäftsleitung die Einhaltung des Datenschutzes bzw. bestimmt einen Mitarbeiter, diese Aufgabe wahrzunehmen.

(5) Der Auftragnehmer darf die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich im Geltungsbereich der EU-DSGVO erheben, verarbeiten oder nutzen. Die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten in einem Drittland bedarf der vorherigen schriftlichen Einwilligung des Auftraggebers und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen der für den Auftraggeber notwendigen Datenschutzgesetze erfüllt sind.

(6) Der Auftragnehmer unterstützt den Auftraggeber bei allen gesetzlichen Informations- und Auskunftspflichten, die im Zusammenhang mit der Auftragsdatenverarbeitung stehen. Auskünfte an Betroffene oder Dritte darf der Auftragnehmer nur nach vorheriger Weisung des Auftraggebers erteilen. Soweit ein Be-

troffener seine Rechte nach den einschlägigen Datenschutzgesetzen unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(7) Der Auftragnehmer unterstützt den Auftraggeber, soweit notwendig, bei erforderlichen Datenschutz-Folgeabschätzungen.

(8) Dem Auftragnehmer ist bekannt, dass der Auftraggeber Berufsgeheimnisträger ist und Verstöße hiergegen nach § 203 StGB strafbewährt sind.

7. Berechtigung zur Begründung von Unterauftragsverhältnissen

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer im Rahmen seines Geschäftsbetriebes z.B. als Telekommunikationsleistungen, Post-//Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet zur Gewährleistung des Datenschutzes und der Datensicherheit, bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer nur nach Prüfung datenschutzrechtlicher Bestimmungen beauftragen. Eine Auslagerung auf Unterauftragnehmer ist zulässig, soweit diesem weiteren Auftragsverarbeiter im Wege eines Vertrages oder einer Vereinbarung dieselben Datenschutzauflagen und Pflichten nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO auferlegt werden.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

8. Kontrollrechte des Auftraggebers

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber oder eine von ihm beauftragte Person, berechtigt sind, die Einhaltung der Vorschriften über den Datenschutz durch geeignete Maßnahmen zu kontrollieren.

9. Mitzuteilende Verstöße des Auftragnehmers

(1) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten des Auftraggebers mit sich bringen sowie bei Verdacht auf eine Datenschutzverletzung. Gleiches gilt, wenn der Auftragnehmer feststellt, dass die bei ihm getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen.

(2) Meldungen über eine Verletzung des Schutzes personenbezogener Daten an den Auftraggeber erfolgen schriftlich und enthalten

- eine Beschreibung der Art der Verletzung und soweit möglich, Angaben über Kategorie und Zahl der betroffenen Datensätze
- eine Erläuterung der vom Auftragnehmer ergriffenen Maßnahmen zur Behebung der Verletzung und der Verringerung möglicher nachteiliger Auswirkungen.

10. Weisungen des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber im Anschluss unverzüglich in Schriftform.

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen geltende Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

11. Beendigung des Auftrags/ Dauer

(1) Die Auftragsdatenverarbeitung ist vom Bestehen eines Dienstleistungsvertrages abhängig. Endet dieser Dienstleistungsvertrag, so endet auch die darauf beruhende Auftragsdatenverarbeitung, ohne dass es einer gesonderten Kündigung bedarf.

(2) Der Auftraggeber kann den Dienstleistungsvertrag ohne Einhaltung einer Frist kündigen, wenn der Auftragnehmer einen schwerwiegenden Verstoß gegen die Datenschutzbestimmungen der einschlägigen deutschen und europäischen Datenschutzgesetze begeht und dem Auftraggeber aufgrund dessen die Fortsetzung der Auftragsverarbeitung bis zum Ablauf der ordentlichen Kündigungsfrist oder bis zu einer vereinbarten regulären Beendigung des Dienstleistungsvertrages nicht zugemutet werden kann.

(3) Nach Abschluss der Auftragsdatenverarbeitung hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Datenträger und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, an den Auftraggeber zurückzugeben. Nicht mehr benötigte Daten sind durch den Auftragnehmer unverzüglich zu löschen, sofern der Löschung keine gesetzlichen Speicherfristen entgegenstehen. Hierüber ist der Auftragnehmer durch den Auftraggeber schriftlich in Kenntnis zu setzen. Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

(4) Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse über Personen, Geschäftsgeheimnisse und Datensicherheitsmaßnahmen auch nach Beendigung des Vertrages vertraulich zu behandeln.

12. Haftung

Hierzu wird auf Art. 82 der EU-DSGVO hingewiesen.

13. Schlussbestimmungen

(1) Die Parteien sind verpflichtet, alle im Rahmen des Auftragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Vertragspartei vertraulich zu behandeln. Geschäftsgeheimnisse sind alle auf ein Unternehmen bezogene Tatsachen, Umstände und Vorgänge, die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich sind und an deren Nichtverbreitung der Geheimnisträger ein berechtigtes Interesse hat. Datensicherheitsmaßnahmen sind alle technischen und organisatorischen Sicherheitsmaßnahmen, die eine Partei nach den für den Auftraggeber einschlägigen Datenschutzgesetzen getroffen hat. Diese Geheimhaltungspflicht besteht nach Beendigung dieses Vertrags fort.

(2) Sofern eine Partei weitergehenden Geheimnisschutzregeln unterliegt und sie dies der anderen Partei zu Auftragsbeginn schriftlich mitteilt, ist auch diese Partei verpflichtet, die Geheimnisschutzregeln zu beachten.

(3) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf Datenträger und Datenbestände des Auftraggebers ausgeschlossen.

(4) Für Änderungen und sonstige Nebenabreden des Auftragsverhältnisses ist Schriftform erforderlich.

Herzogenrath, im Januar 2021

LCL biokey GmbH

Andrea Hoffmann
Geschäftsführerin

Anlage – Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrolle
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, Alarmanlagen
- Zugangskontrolle
  Keine unbefugte Systembenutzung, z.B.: Kennwörter, Verschlüsselung von Datenträgern
- Zugriffskontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
- Trennungskontrolle
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden
- Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung
- Eingabekontrolle
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Verfügbarkeitskontrolle
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), Virenschutz, Firewall, Meldewege und Notfallpläne;
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Datenschutz-Management; Incident-Response-Management
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO); Auftragskontrolle
- Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.