**VEREINBARUNG ÜBER DATENVERARBEITUNG**

1. *Definitionen:* Im Rahmen dieser Vereinbarung über Datenverarbeitung („DVV“) kommen den folgenden Begriffen die folgenden Bedeutungen zu:

* „Angemessenes Land“ bezeichnet ein Land, in Bezug auf welches die Europäische Kommission, der Datenschutzbeauftragte oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit festgestellt hat, dass es in seinem Zuständigkeitsbereich einen adäquaten Schutz gewährleistet.
* „Einschlägiges Datenschutzrecht“ bezeichnet die geltenden Datenschutz- und Datensicherheitsgesetze, zu denen je nach Fall das US-amerikanische Datenschutzrecht, das EU-Datenschutzrecht, das UK-Datenschutzrecht und das schweizerische Datenschutzrecht zählen.
* „Verantwortlicher“, „Auftragsverarbeiter“, „Betroffener“, „personenbezogene Daten“, „Verarbeitung“ (und „verarbeiten“) sowie „besondere Kategorien personenbezogener Daten“ haben die gleiche Bedeutung wie in dem jeweils anwendbaren Datenschutzrecht.
* „EWR“ bezeichnet den Europäischen Wirtschaftsraum.
* „USA“ bezeichnet die Vereinigten Staaten von Amerika.
* „EK“ bezeichnet die Europäische Kommission.
* „EU-Datenschutzrecht” bezeichnet (a) die Datenschutz-Grundverordnung der EU (Verordnung 2016/679) (DSGVO), (ii) die Datenschutzrichtlinie für elektronische Kommunikation der EU (Richtlinie 002/58/EK) sowie (iii) alle Gesetze, die ein EU-Mitgliedstaat auf der Grundlage oder gemäß den vorgenannten Vorschriften erlassen hat, jeweils in der von Zeit zu Zeit geänderten oder ersetzten Fassung.
* „Schweizerisches Datenschutzrecht“ bezeichnet für den Zeitraum von 1992 bis Dezember 2022 das schweizerische Bundesgesetz über den Datenschutz (DSG) und ab dem 1. Januar 2023 das novellierte schweizerische Bundesgesetz über den Datenschutz (novelliertes DSG) von 2020, jeweils in der von Zeit zu Zeit geänderten oder ersetzten Fassung.
* „UK-Datenschutzrecht“ bezeichnet die aus den Richtlinien über Datenschutz, Schutz der Privatsphäre und elektronische Kommunikation (mit Änderungen etc.) (EU Exit) 2019/419 übernommene Datenschutzgesetzgebung, ergänzt durch die Vorschriften des Datenschutzgesetzes von 2018 (UK-DSG) und der UK-DSGVO (beibehaltene Richtlinie (EU) 2016/679 (UK-DSGVO) gemäß dem entsprechenden Abschnitt des Vertrags mit der Europäischen Union (Austrittsvertrag von 2018), jeweils in der von Zeit zu Zeit geänderten oder ersetzten Fassung.
* „US-Datenschutzrecht“ bezeichnet (a) das Verbraucherdatenschutzgesetz von Kalifornien von 2018 (CVDSG), in der jeweils geltenden Fassung, integriert durch das Datenschutzgesetz von Kalifornien von 2020 (KDSG) sowie die entsprechenden Ausführungsverordnungen, (b) das Verbraucherdatenschutzgesetz von Virginia von 2021 (VVDSG), (c) das Verbraucherdatenschutzgesetz von Colorado von 2021 (CVDSG), (d) das Datenschutzgesetz von Connecticut von 2022 (CDSG) und (e) das Verbraucherdatenschutzgesetz von Utah von 2022 (UVDSG), jeweils in der von Zeit zu Zeit geänderten oder ersetzten Fassung.
* „Hydrafacial“ bezeichnet die Hydrafacial LLC.
* „Gerät“ bezeichnet das Gerät Hydrafacial Syndeo nebst System und Software.
* „Verbraucher“ bezeichnet eine Person, die eine Behandlung durch das Gerät erhält.
* „Kunde“ bezeichnet eine Klinik oder ein Zentrum, die beziehungsweise das Behandlungen mit dem Gerät anbietet.
* „Befugte Nutzer“ bezeichnet Kunden, die mit Kunden verbundenen Unternehmen sowie deren jeweilige Mitarbeiter, Subunternehmer oder Berater, die Behandlungen mit dem Gerät durchführen.

1. *Beziehung der Parteien untereinander:* Hydrafacial (der Verantwortliche) setzt den Kunden (den Auftragsverarbeiter) für die Verarbeitung der in Ziffer 14 dieser DVV bezeichneten personenbezogenen Daten (die „Daten“) für die in Ziffer 16 dieser DVV genannten oder von den Parteien anderweitig schriftlich vereinbarten Zwecke ein (die „zulässigen Zwecke“). Der Kunde darf die Daten nicht für andere als die zulässigen Zwecke halten, verwenden oder offenlegen. Der Kunde darf die Daten nicht kaufen oder verkaufen. Jede der Parteien hält sich an die ihr nach dem einschlägigen Datenschutzrecht obliegenden Verpflichtungen gebunden.
2. *Internationale Gesetze betreffend die Übermittlung und Lokalisierung von Daten:* Die vom Kunden und seinen befugten Nutzern in das Gerät eingegebenen oder von dem Gerät abgerufenen Daten werden in den USA gehostet. Die geltenden anerkannten Standardvertragsklauseln („SVK”) unter [\*Link zu den SVK\*] („SVK-Webseite“) gelten entsprechend dem anwendbaren Datenschutzrecht als in diese DVV einbezogen. Sofern der Kunde eine vollständige ausgefertigte Version benötigt, kann er die vorab unterzeichnete Version auf der SVK-Webseite gegenzeichnen und eine Kopie an dpo@hydrafacial.com senden. In Ländern außerhalb des EWR („Drittländer”), in denen Datenspeicherung und Datenübermittlung rechtlichen Einschränkungen kraft geltender Datenlokalisierungsgesetze unterliegen, werden die Daten nicht außerhalb des lokalen Territoriums übertragen oder gehostet und nur auf lokalen Servern gespeichert. Vor der Übermittlung von Daten in die USA hat Hydrafacial angemessene Schritte unternommen, um sicherzustellen, dass die übermittelten Daten ein Schutzniveau genießen, das im Wesentlichen dem entspricht, das im Ursprungsland geboten wird. Was Daten aus dem Vereinigten Königreich („UK”) oder der Schweiz anbelangt, ist bei Verweisen in dieser Ziffer 3 auf (a) den „EWR” stattdessen „UK” oder „Schweiz”, (b) „EU-Datenschutzrecht“ stattdessen „UK-Datenschutzrecht” oder „schweizerisches Datenschutzrecht“ und (c) die „EK” stattdessen „Datenschutzbeauftragter“ oder „Bundesbeauftragter für den Datenschutz und die Informationsfreiheit“ einzusetzen.
3. *Sicherheit und Vertraulichkeit*: In Anbetracht der Art der Verarbeitung werden Hydrafacial und der Kunde geeignete technische und organisatorische Maßnahmen ergreifen, um für ein Sicherheitsniveau zu sorgen, das den Risiken angemessen ist (wie in Artikel 32 der Datenschutz-Grundverordnung der EU geregelt) und die Daten vor (i) zufälliger oder rechtswidriger Zerstörung und (ii) Verlust, Änderung, unbefugter Offenlegung und unbefugtem Zugriff („Verstoß gegen die Datensicherheit“) zu schützen. Der Kunde hat sicherzustellen, dass alle seine befugten Nutzer, die die Daten verarbeiten, sich ausdrücklich zur Wahrung der Vertraulichkeit verpflichtet haben.
4. *Unterauftragsverarbeitung:* In Anbetracht der Art der Verarbeitung hat der Kunde in Fällen, in denen befugte Nutzer nach dem einschlägigen Datenschutzrecht als Unterauftragsverarbeiter gelten, zumindest sicherzustellen, dass die Anforderungen und Bedingungen dieser DVV erfüllt werden und die Verarbeitung nur für die zulässigen Zwecke erfolgt.
5. *Kooperation und Rechte der Betroffenen*: In Anbetracht der Art der Verarbeitung hat der Auftragsverarbeiter den Verantwortlichen soweit möglich durch geeignete technische und organisatorische Maßnahmen zu unterstützen; der Kunde hat Hydrafacial in angemessenem Umfang und zeitnah zu unterstützen, um es Hydrafacial zu ermöglichen, auf (i) Anforderungen von Betroffenen auf Ausübung ihrer Rechte nach dem einschlägigen Datenschutzrecht (beispielsweise des Rechts auf Zugang, Berichtigung, Widerspruch, Löschung oder Datenübertragbarkeit) oder (ii) Korrespondenz, Ersuchen oder Beschwerden von Betroffenen, Regulierungsbehörden oder dritten Parteien in Zusammenhang mit der Verarbeitung der Daten zu antworten. Wird ein Ersuchen, eine Korrespondenz, eine Anfrage oder eine Beschwerde direkt an den Kunden gerichtet, hat der Kunde Hydrafacial unverzüglich zu informieren und alle diesbezüglichen Angaben zur Verfügung zu stellen.
6. *Bewertung, Beratung und Unterstützung* In Anbetracht der Art der Verarbeitung hat der Kunde, falls erforderlich, mit Hydrafacial zusammenzuarbeiten, damit Hydrafacial vor der Verarbeitung (a) Datenschutzfolgenabschätzungen oder Datenübermittlungsfolgenabschätzungen vornehmen und (b) sich mit den zuständigen Aufsichtsbehörden beraten kann, soweit dies nach dem einschlägigen Datenschutzrecht erforderlich ist.
7. *Verstöße gegen die Datensicherheit*: Wenn der Kunde einen Verstoß gegen die Datensicherheit erkennt, hat er Hydrafacial unverzüglich davon in Kenntnis zu setzen, Hydrafacial ausreichende Informationen darüber zur Verfügung zu stellen und mit Hydrafacial zusammenzuarbeiten, um die in Fällen von Verstößen gegen die Datensicherheit nach dem einschlägigen Datenschutzrecht gegebenenfalls erforderlichen Meldungen zu tätigen. Der Kunde hat auch alle bei angemessener Betrachtung notwendigen Maßnahmen und Schritte einzuleiten, um die Auswirkung des entsprechenden Verstoßes gegen die Datensicherheit zu mildern und Kunden über alle wichtigen Entwicklungen in Zusammenhang mit dem Verstoß gegen die Datensicherheit auf dem Laufenden zu halten. Die gleichen Anforderungen gelten auch für Unterauftragsverarbeiter.
8. *Löschung oder Rückgabe der Daten*: Der Kunde kann gegebenenfalls aufgefordert werden, Hydrafacial bei Vertragsablauf eine Bestätigung der Einstellung der Datenspeicherung vorzulegen.
9. *Prüfung der Einhaltung von Vorgaben:* Der Kunde hat Hydrafacial (oder einem Bevollmächtigten von Hydrafacial) die Möglichkeit einzuräumen, ihre Verfahren und Dokumentationen einzusehen oder zu prüfen, um sicherzustellen, dass die in dieser Vereinbarung über Datenverarbeitung aufgeführten Verpflichtungen eingehalten werden.
10. *Transparenzberichte:* Hydrafacial wird staatlichen Behörden keinen Zugang zu Daten gewähren, sofern nicht eine entsprechende gesetzliche Verpflichtung dazu besteht. Die Strategie von Hydrafacial für den Umgang mit Anforderungen von Behörden in Bezug auf Daten („Rechtliche Anforderungen“) und der Transparenzbericht von Hydrafacial über rechtliche Anforderungen können unter [\*Link\*] eingesehen werden. Hydrafacial wird (a) die Rechtmäßigkeit von rechtlichen Anforderungen prüfen und diese anfechten, soweit dies rechtmäßig ist und angezeigt erscheint, und (b) in Fällen, in denen rechtliche Anforderungen nicht Art. 46 DSGVO oder anderen einschlägigen Vorschriften für die rechtmäßige Übermittlung von personenbezogenen Daten entsprechen, die Behörde entsprechend informieren (soweit dies nach dem einschlägigen Datenschutzrecht bei rechtlichen Anforderungen erforderlich ist).

**Anlage I - Informationssicherheitskontrollen**

1. *Sicherheitskontrollen*:
2. Hydrafacial hat zur Unterstützung ihres Datenschutzes die folgenden Datenschutz- und Datensicherheitsrichtlinien und Verfahren eingeführt:

* Richtlinien für Informationssicherheit: als Vorgaben für das Management und zur Unterstützung der Informationssicherheit entsprechend den Unternehmensanforderungen sowie den einschlägigen Gesetzen und Verordnungen.
* Organisation der Informationssicherheit: zur Schaffung eines Netzwerks, um bei Hydrafacial die Einführung und Durchführung von Informationssicherheitsmaßnahmen zu initiieren und zu kontrollieren.
* Personalsicherheit: um sicherzustellen, dass für alle Mitarbeiter gut gesorgt und Verständnis für ihre jeweiligen Rollen und Aufgaben gezeigt wird, um sicherzustellen, dass alle Mitarbeiter mit ihren Aufgaben und Verpflichtungen im Bereich Informationssicherheit vertraut sich und diese erfüllen, um sicherzustellen, dass die Interessen der Organisation während des Beschäftigungsprozesses, von der Einstellung bis zum Ausscheiden, gewahrt werden, und um sicherzustellen, dass alle Mitarbeiter einer Verschwiegenheitspflicht unterliegen.
* Datenklassifizierung: dient der Klassifizierung von Informationen und Daten von Hydrafacial, um Aufgaben für deren Schutz angemessen definieren und zuweisen zu können, soll ein angemessenes Niveau von Informations- und Datensicherheit je nach Sensibilitätsstufe und Wichtigkeit für die Organisation sicherstellen und soll unbefugte Offenlegung, Modifizierung, Entfernung oder Zerstörung von auf Medien gespeicherten Informationen verhindern.
* Zugangsmanagement: schafft ein Rahmenwerk für die Kontrolle und Verwaltung von Nutzer-, System- und Applikationszugängen und für die Verantwortlichkeiten der Nutzers, begrenzt den Zugang zu Informationen und Datenverarbeitungseinrichtungen, soll sicherstellen, dass befugte Nutzer Zugang erhalten und unbefugter Zugriff auf Systeme und Dienste verhindert wird, überträgt den Nutzern die Verantwortung für die Sicherung ihre Authentifizierungsdaten und soll unbefugten Zugriff auf Systeme und Applikationen verhindern.
* Physische Sicherheit und Umgebungssicherheit: soll physischen Zugang, Beschädigung oder Störung der Informationen oder Informationsverarbeitungseinrichtungen von Hydrafacial sowie Verlust, Beschädigung, Diebstahl oder Kompromittierung der Vermögenswerte von Hydrafacial und Unterbrechungen des operativen Betriebsablaufs verhindern.
* Operative Sicherheit: soll sicherstellen, dass Informationen und Informationsverarbeitungseinrichtungen sicher betrieben und vor Malware und Datenverlust geschützt werden, soll sicherstellen, dass Sicherheitsereignisse angemessen aufgezeichnet werden und soll sicherstellen, dass die Integrität der operativen Systeme gewahrt bleibt und technische Schwächen nicht ausgenutzt werden können.
* Kommunikationssicherheit: zur Einführung von Kontrollen zum Schutz der Daten in Netzwerken und zugehörigen Einrichtungen, die für die Sicherheit der Daten sorgen sollen, welche innerhalb von Hydrafacial oder an externe Parteien übermittelt werden.
* Beziehungen zu Lieferanten: es soll sichergestellt werden, dass die Vermögenswerte von Hydrafacial geschützt sind, auf die Lieferanten zugreifen können, und dass ein vereinbartes Maß an Informationssicherheit und Dienstleistungserbringung entsprechend den jeweiligen Verträgen mit den Lieferanten gewahrt bleibt.
* Management für Informationssicherheitszwischenfälle: soll ein kohärentes, effektives Konzept für den Umgang mit Informationssicherheitszwischenfällen, und auch mit Störfällen und Schwächen, bereitstellen.
* VPN (virtuelles privates Netzwerk) für Fernzugriff: bietet den Nutzern mehr Sicherheit und Anonymität, wenn sie sich mit webbasierten Diensten und Websites verbinden. Ein VPN verbirgt die tatsächliche öffentliche IP-Adresse des Nutzers und „tunnelt” den Verkehr zwischen dem Gerät des Nutzers und dem Fernserver.
* Verschlüsselung von Daten im Ruhezustand und während der Übermittlung beziehungsweise in Bewegung. Daten im Ruhezustand sind inaktive Daten, die nicht zwischen Geräten und Netzwerken hin und her bewegt werden und meist in Datenarchiven gespeichert sind. Dagegen werden Daten während der Übermittlung zwischen Geräten oder zwei Netzwerkstellen hin und her bewegt.
* Backup- und Wiederherstellungsfunktionen: bezeichnen den Prozess der Duplizierung von Daten und der Datenspeicherung an einem sicheren Ort für den Fall von Verlust oder Beschädigung, so dass die Daten anschließend wieder an – den ursprünglichen oder einen sicheren alternativen Ort – zurückgeführt und erneut operativ genutzt werden.
* Firewalls: sind Netzwerksicherheitsvorkehrungen, die den eingehenden und ausgehenden Verkehr entsprechend den vorher festgelegten Sicherheitsrichtlinien einer Organisation überwachen und filtern. In ihrer einfachsten Form ist eine Firewall eine Barriere zwischen einem privaten internen Netzwerk und dem öffentlichen Internet.
* Antivirus-Software: bezeichnet eine bestimmte Art von Software, die dazu dient, Viren auf einem Computer zu verhindern, zu scannen, zu identifizieren und zu löschen.
* Mehrstufige Authentifizierung (MA): bezeichnet eine Sicherheitstechnologie, die mehrere Methoden der Authentifizierung aus voneinander unabhängigen Kategorien von Berechtigungsnachweisen einsetzt, um die Identität eines Nutzer für ein Login oder eine sonstige Transaktion zu verifizieren.
* Sicherheitsfilterung für E-Mails: bezeichnet den Prozess der Blockierung unerwünschter und potenziell schädlicher Codes und Links, die den Nutzer zu verdächtigen Websites lenken und verhindert E-Mails, die versuchen, in das System zu gelangen, um auf sensible Daten zugreifen zu können.
* Schulung für Sicherheitsbewusstsein: zielt auf das Wissen und die Einstellung der Organisationsmitglieder in Bezug auf den Schutz der physischen und insbesondere der Informationsgüter der Organisation ab.

1. Der Kunde hat nach dem einschlägigen Datenschutzrecht angemessene technische und organisatorische Maßnahmen zu ergreifen. Dazu gehört auch, für Schutz vor unbefugter oder rechtswidriger Verarbeitung, zufälligem Verlust, Zerstörung und Beschädigung zu sorgen.

**Anlage II – Einzelheiten zur Datenverarbeitung**

1. *Kategorien von Betroffenen****:*** (i) Verbraucher, (ii) befugte Nutzer, (iii) Kunden.
2. *Verarbeitete Datenkategorien:* (i) Vertrags- und Kontoinformationen der Betroffenen, wie beispielsweise vollständiger Name, Telefonnummer, E-Mail-Adresse, Rolle und IP-Adresse, (ii) Behandlungshistorie und Erfolgsbilanz**.**
3. *Besondere Datenkategorien****:*** Mit dem Gerät werden keine besonderen Datenkategorien verarbeitet.
4. *Zweck des Verarbeitungsprozesses:* Personenbezogene Daten werden verarbeitet, soweit dies erforderlich ist, um die Gerätedienste erbringen zu können. Für die verarbeiteten personenbezogenen Daten kommen die folgenden grundsätzlichen Verarbeitungsaktivitäten in Betracht: Erhebung, Offenlegung durch Kommunikation und Abruf. Insbesondere handelt es sich um folgende Verarbeitungsprozesse: (i) sofern der Verbraucher ein Konto erstellen möchte, geben der Kunde und der befugte Nutzer Ihre persönlichen Angaben in das System des Geräts ein, woraufhin der Verbraucher eine SMS/E-Mail erhält und den Anmeldevorgang abschließen kann, (ii) Verbraucher haben die Möglichkeit, Ihre Behandlungshistorie mit dem Kunden und dem befugten Nutzer zu teilen. Entsprechend haben der Kunde und der befugte Nutzer bei der Verwendung des Geräts die Möglichkeit, Ihr App-Konto mit dem Gerät zu synchronisieren, um eine Aufzeichnung der Behandlungshistorie des Mitteilenden zur Verfügung zu haben. Kunden und befugte Nutzer können aggregierte Daten über die von ihnen durchgeführten Behandlungen abrufen. Mit den Behandlungsinformationen, die Kunden und befugte Nutzer abrufen können, sind jedoch keine personenbezogenen, identifizierbaren Daten der Verbraucher verknüpft.
5. *Dauer der Verarbeitung:*Personenbezogene Daten können verarbeitet werden, solange der Vertrag mit Hydrafacial Device Services läuft.