**CONTRATO DE TRATAMIENTO DE DATOS**

1. *Definiciones:* En el presente Contrato de Tratamiento de Datos ("CTD"), los siguientes términos tendrán el significado que se indica a continuación:

* "País Adecuado" un país que la Comisión Europea, la Oficina del Comisario de Información o el Comisario Federal de Protección de Datos e Información (según proceda) han determinado que garantiza un nivel de protección adecuado para su ámbito de competencia respectivo.
* "Legislación sobre Protección de Datos Aplicable" legislación sobre protección de datos y privacidad aplicable, lo que incluye, cuando proceda, la Ley de Protección de Datos de EE.UU., la Ley de Protección de Datos de la UE, la Ley de Protección de Datos del Reino Unido y la Ley de Protección de Datos de Suiza.
* “Responsable del tratamiento”, “encargado del tratamiento”, “interesado”, “datos personales”, “tratamiento” (y “tratar”) y “categorías especiales de datos personales” tendrán el significado que se les atribuye en la Ley de Protección de Datos aplicable.
* “EEE” significa Espacio Económico Europeo.
* “EEUU” significa Estados Unidos de América.
* “CE” significa Comisión Europea.
* “Ley de Protección de Datos de la UE“: a) el Reglamento general de protección de datos de la UE (Reglamento 2016/679) (RGPD); ii) la Directiva sobre la privacidad y las comunicaciones electrónicas de la UE (Directiva 002/58/CE) y iii) todas y cada una de las leyes de los Estados miembros de la UE elaboradas en virtud o de conformidad con cualquiera de las anteriores; en cada caso, según se modifiquen o sustituyan cada cierto tiempo.
* "Ley Suiza de Protección de Datos" la Ley federal suiza de protección de datos (LFPD) de 1992 hasta diciembre de 2022 y, a partir del 1 de enero de 2023, la Ley federal suiza revisada de protección de datos (LFPD revisada) de 2020, en su versión modificada o sustituida en cada momento.
* "Ley de Protección de Datos del Reino Unido", se refiere a la legislación sobre la privacidad de datos adoptada por el Reglamento 2019/419 sobre protección de datos, privacidad y comunicaciones electrónicas (enmiendas, etc.) (salida de la UE), complementada por lo dispuesto en la Ley de protección de datos de 2018 (DPA del Reino Unido) y el RGPD del Reino Unido (Reglamento retenido (UE) 2016/679 (RGPD del Reino Unido) de conformidad con la sección de la Unión Europea (Ley de Retirada de 2018), en su versión modificada o sustituida en cada momento.
* “Ley de Protección de Datos de EE.UU.”: a) la Ley de privacidad del consumidor de California de 2018 (CCPA), modificada e integrada por la Ley de derechos de privacidad de California de 2020 (CPRA) y los siguientes reglamentos de aplicación; b) la Ley de protección de datos del consumidor de Virginia de 2021 (VCDPA); c) la Ley de privacidad de Colorado de 2021 (CPA); d) la Ley de privacidad de datos de Connecticut de 2022 (CTDPA) y e) la Ley de privacidad del consumidor de Utah de 2022 (UCPA); en cada caso en su versión modificada o sustituida según proceda.
* "Hydrafacial", significa Hydrafacial LLC
* "Dispositivo", significa el dispositivo, sistema y software de Hydrafacial Syndeo.
* "Consumidor", quien recibe un tratamiento a través del Dispositivo.
* "Cliente", clínica o centro que proporciona tratamientos con el Dispositivo.
* "Usuarios Autorizados" se refiere al Cliente, sus filiales y sus respectivos empleados, contratistas o consultores que realicen tratamientos con el Dispositivo.

1. *Relación entre las Partes:* Hydrafacial (el responsable del tratamiento) designa al Cliente (el encargado del tratamiento) para tratar los datos personales descritos en el párrafo número 14 de este CTD (los "Datos") para los fines descritos en el párrafo número 16 de este CTD o según acuerden las partes por escrito (los "Fines Permitidos"). El Cliente no conservará, utilizará ni comunicará los Datos para ningún fin distinto de los Fines Permitidos. El Cliente no comprará ni venderá los Datos. Cada una de las Partes cumplirá con sus respectivas obligaciones en virtud de la Legislación sobre Protección de Datos Aplicable
2. *Transferencias internacionales y legislación sobre localización de datos:* Los Datos introducidos, a los que el Cliente y sus Usuarios Autorizados acceden a través del Dispositivo, están alojados en EE.UU. y las cláusulas contractuales tipo aplicables aprobadas ("CCT") en [\*enlace a las CCT\*] ("Página Web de las CCT") se considerarán incorporadas al presente CTD a fin de cumplir con la Legislación sobre Protección de Datos Aplicable. En caso de que el Cliente solicite un ejemplar íntegramente cumplimentado, puede suscribir la versión prefirmada correspondiente que se encuentra en la Página Web de las CCT y enviar una copia por correo electrónico a dpo@hydrafacial.com. En aquellos países no pertenecientes al EEE ("Terceros Países") en los que se aplique una restricción legal al almacenamiento y la transferencia de Datos en virtud de una ley de localización de datos, los Datos no se transferirán ni se alojarán fuera del territorio local y se almacenarán en servidores locales. Antes de transferir datos a EE.UU., Hydrafacial ha tomado las medidas razonables para velar por que los datos transferidos estén sujetos a un nivel de protección sustancialmente equivalente al que tienen en el país de origen. En cuanto a los Datos procedentes del Reino Unido (“RU”) o Suiza las referencias en este apartado 3 a: a) el "EEE" se sustituirá por el "Reino Unido" o "Suiza", según proceda; b) la "Ley de Protección de Datos de la UE" se sustituirá por la "Ley de Protección de Datos del Reino Unido" o la "Ley Suiza de Protección de Datos", según proceda; y c) la "CE" se sustituirá por la "Oficina del Comisario de Información" o el "Comisario Federal de Protección de Datos e Información", según proceda.
3. *Seguridad y confidencialidad*: Teniendo en cuenta la naturaleza del tratamiento, Hydrafacial y el Cliente aplicarán las medidas técnicas y organizativas apropiadas para contar con un nivel de seguridad adecuado a los riesgos (como se indica en el artículo 32 del Reglamento General de Protección de Datos de la UE) con el fin de proteger los Datos de i) su destrucción accidental o ilícita, y ii) la pérdida, alteración, comunicación o acceso no autorizados a los Datos (una "Violación de la Privacidad"). El Cliente se asegurará de que todos los Usuarios Autorizados que traten los Datos se hayan comprometido expresamente mantener la confidencialidad.
4. *Subtratamiento:* Teniendo en cuenta la naturaleza del tratamiento, cuando los Usuarios Autorizados pudieran ser considerados como subencargados del tratamiento en virtud de la Legislación sobre Protección de Datos Aplicable, el Cliente deberá cumplir, al menos, los requisitos y condiciones establecidos en el presente CTD únicamente para los Fines Permitidos.
5. *Cooperación y derechos de los interesados*: Teniendo en cuenta la naturaleza del tratamiento, el encargado del tratamiento ayudará al responsable del tratamiento a través de medidas técnicas y organizativas apropiadas, en la medida en que sea posible y, cuando sea necesario, el Cliente prestará asistencia razonable y oportuna a Hydrafacial para que pueda responder a: i) Cualquier solicitud de un interesado para ejercer sus derechos en virtud de la legislación aplicable en materia de protección de datos (incluido su derecho de acceso, rectificación, oposición, supresión y portabilidad de los datos, según proceda) y ii) cualquier otra correspondencia, solicitud o reclamación que se reciba de un interesado, autoridad reguladora u otro tercero en relación con el tratamiento de los datos. En caso de que se reciba una solicitud, correspondencia, consulta o reclamación de este tipo que se dirija directamente al Cliente, este deberá informar sin demora a Hydrafacial y proporcionarle todos los detalles al respecto.
6. *Evaluación, consulta y asistencia* Teniendo en cuenta la naturaleza del tratamiento, en caso necesario, el Cliente prestará su colaboración para que Hydrafacial pueda a) realizar cualquier evaluación de impacto sobre la protección o transferencia de datos y b) consultar a las autoridades de control competentes antes del tratamiento cuando así lo exija la Legislación sobre Protección de Datos Aplicable.
7. *Violación de privacidad*: Si el Cliente tiene conocimiento de que se ha producido una Violación de Privacidad, procederá a informar inmediatamente a Hydrafacial y le proporcionará la información y cooperación razonables para que pueda cumplir con sus obligaciones en materia de notificación de violaciones de privacidad en virtud de la Legislación sobre Protección de Datos Aplicable. Asimismo, el Cliente tomará las medidas y acciones que sean razonablemente necesarias para mitigar los efectos de la Violación de Datos y mantendrá informado al Cliente de todos los avances materiales que se produzcan en relación con la misma. Se aplicarán los mismos requisitos a los subencargados del tratamiento.
8. *Supresión o devolución de datos*: Al finalizar el contrato se podrá solicitar al Cliente que proporcione a Hydrafacial un certificado de no conservación de datos.
9. *Control de conformidad:* El Cliente permitirá que Hydrafacial (o su representante) inspeccione o audite sus procedimientos y documentación para asegurar el cumplimiento de las obligaciones establecidas en el presente Contrato de Tratamiento de Datos.
10. *Informes de Transparencia*: Hydrafacial no comunicará ni proporcionará acceso a ningún Dato a ninguna autoridad gubernamental a menos que lo exija la ley. La política de Hydrafacial para atender las solicitudes de las autoridades públicas en relación con los Datos ("Solicitudes Legales"), junto con el Informe de Transparencia de Hydrafacial sobre Solicitudes Legales, está disponible en [\*enlace\*]. Hydrafacial procederá a: a) examinar la legalidad de las Solicitudes Legales y oponerse a ellas cuando sea lícito y apropiado y b) cuando la Solicitud Legal no cumpla con lo dispuesto en el artículo 46 del RGPD o con cualquier otra disposición pertinente para la transferencia lícita de datos personales, informará de ello a la autoridad pública (en cada caso en la medida exigida por la Legislación sobre Protección de Datos Aplicable a la Solicitud Legal).

**Apéndice I - Controles de seguridad de la información**

1. *Controles de seguridad*:
2. Hydrafacial cuenta con las siguientes políticas y procedimientos para respaldar su programa de privacidad y seguridad:

* Políticas de seguridad de la información: Proporcionar orientación y soporte a la gestión de la seguridad de la información de acuerdo con los requisitos de la empresa y las leyes y reglamentos pertinentes.
* Organización de la seguridad de la información: Establecer un marco para iniciar y controlar la implantación y el funcionamiento de la seguridad de la información en Hydrafacial.
* Seguridad de los recursos humanos: Asegurarse de que todos los miembros de la plantilla están bien preparados y comprenden sus funciones y responsabilidades. Asegurarse de que todos los miembros de la plantilla conocen y cumplen sus responsabilidades y obligaciones en materia de seguridad de la información. Velar por la protección de los intereses de la organización durante todo el proceso de contratación, desde la fase previa a la contratación hasta su extinción. Velar por que toda la plantilla esté sujeta al deber de confidencialidad.
* Clasificación de datos: Determinar la clasificación de la información y los datos de Hydrafacial, y definir y asignar las responsabilidades adecuadas para su protección. Asegurar un nivel adecuado de protección de la información y los datos de acuerdo con su nivel de sensibilidad y su importancia para la organización. Impedir la comunicación, modificación, eliminación o destrucción no autorizadas de la información almacenada en soportes.
* Gestión de acceso: Proporciona el marco para el control y la gestión del acceso de los usuarios, sistemas y aplicaciones, así como las responsabilidades de los usuarios. Limitar el acceso a la información y a las instalaciones de tratamiento de la información. Asegurar el acceso autorizado de los usuarios e impedir el acceso no autorizado a los sistemas y servicios. Responsabilizar a los usuarios respecto a la custodia de su información de acceso. Impedir el acceso no autorizado a sistemas y aplicaciones.
* Seguridad física y medioambiental: Evitar el acceso físico no autorizado, daños e injerencias en la información de Hydrafacial y las instalaciones de tratamiento de información. Evitar la pérdida, daño, robo o amenaza de los activos de Hydrafacial y la interrupción de sus operaciones.
* Seguridad de las operaciones: Velar por que la información y las instalaciones de tratamiento de la información funcionen de forma segura, protegidas de programas maliciosos y de la pérdida de datos. Asegurarse de que los incidentes de seguridad se registran adecuadamente. Velar por el mantenimiento de la integridad del sistema operativo y evitar que se aprovechen las vulnerabilidades técnicas.
* Seguridad de las comunicaciones: Establecer controles para la protección de la información en las redes y sus medios conexos. Velar por la seguridad de la información que se transfiere dentro de Hydrafacial y a partes externas.
* Relaciones con los proveedores: Velar por la protección de los activos de Hydrafacial a los que tienen acceso los proveedores. Mantener un nivel convenido de seguridad de la información y prestación de servicios conforme a los acuerdos con establecidos con los proveedores.
* Gestión de incidentes de seguridad de la información: Asegurar que se utiliza un enfoque coherente y eficaz en la gestión de los hechos relacionados con la seguridad de la información, incluidos los incidentes y los puntos débiles.,
* VPN (red privada virtual) para acceso remoto: Proporciona a los usuarios seguridad y anonimato cuando se conectan a servicios y sitios web. Una VPN oculta la dirección IP pública real del usuario y "tuneliza" el tráfico entre el dispositivo del usuario y el servidor remoto.
* Cifrado de datos en reposo y en tránsito: También denominados datos en movimiento. Los datos en reposo se refieren a datos inactivos que no se mueven entre dispositivos o redes y tienden a almacenarse en archivos de datos. En cambio, los datos en tránsito se mueven entre dispositivos o entre dos puntos de la red.
* Capacidad de copia de seguridad y recuperación: Es el proceso de duplicar datos y almacenarlos en un lugar seguro en caso de pérdida o daño, para después restaurar esos datos en una ubicación –la original o una alternativa segura– con el fin de que se puedan volver a utilizar en las operaciones.
* Cortafuegos: Es un dispositivo de seguridad de red que supervisa y filtra el tráfico de red entrante y saliente basándose en las políticas de seguridad previamente establecidas de una organización. En su forma más básica, un cortafuegos es esencialmente la barrera que se sitúa entre una red interna privada e y la internet pública.
* Software antivirus: Es un tipo de software utilizado para prevenir, escanear, detectar y eliminar virus de un ordenador.
* Autenticación multifactor (AMF): Es una tecnología de seguridad que requiere múltiples métodos de autenticación a partir de categorías independientes de credenciales con el fin de verificar la identidad de un usuario para realizar un inicio de sesión u otra operación.
* Filtrado de seguridad del correo electrónico: Es el proceso de bloqueo de código no deseado o potencialmente malicioso o de enlaces que redirigen al usuario a sitios web sospechosos. Evita los correos electrónicos que pretenden entrar en el sistema para acceder a datos sensibles.
* Sensibilización en materia de seguridad: Es el conocimiento y la actitud de los miembros de una organización con respecto a la protección de los activos físicos de dicha organización, especialmente de la información.

1. El Cliente utilizará las medidas técnicas u organizativas apropiadas de acuerdo con la Legislación sobre Protección de Datos Aplicable, incluida la protección contra el tratamiento no autorizado o ilícito y contra la pérdida, destrucción o daño accidentales.

**Apéndice II - Información detallada sobre el Tratamiento de Datos**

1. *Categorías de interesados:* i) Consumidor; ii) Usuario Autorizado; iii) Cliente.
2. *Categorías de datos tratados:* i) Información de contacto y cuenta de los interesados, como el nombre completo, número de teléfono, dirección de correo electrónico, puesto y dirección IP; ii) historial de tratamiento y rendimiento**.**
3. *Categorías especiales de datos****:*** En el Dispositivo no se tratan categorías especiales de datos.
4. *Finalidad de la operación de tratamiento:* Los datos personales se tratarán cuando sea necesario para la prestación de los servicios del Dispositivo. Los datos personales tratados podrán ser objeto de las siguientes operaciones básicas de tratamiento: recogida, transmisión mediante comunicación y consulta. Concretamente, las actividades de tratamiento comprenden: i) cuando el Consumidor desea crear una cuenta, el Cliente y el Usuario Autorizado introducen sus datos en el sistema del Dispositivo para que el consumidor reciba un SMS/correo electrónico y complete el proceso de registro; ii) se ofrece a los Consumidores la opción de compartir su historial de tratamiento con el Cliente y el Usuario Autorizado. Del mismo modo, al utilizar el Dispositivo, los Clientes y Usuarios Autorizados podrán sincronizar su cuenta de la aplicación con el Dispositivo para disponer de un registro del historial de tratamiento de los proveedores. Los Clientes y Usuarios Autorizados verán datos agregados sobre los tratamientos que han proporcionado, y no se asociará ninguna información personal identificable de los Consumidores con los tratamientos que vea el Cliente y Usuario Autorizado.
5. *Duración del tratamiento:*Los datos personales se podrán tratar mientras dure el contrato con los servicios del Dispositivo Hydrafacial.