**ACORDO SOBRE TRATAMENTO DE DADOS**

1. *Definições:* No presente Acordo sobre Tratamento de Dados ("ATD"), os seguintes termos terão os seguintes significados:

* "País Adequado" um país que a Comissão Europeia, o Gabinete do Comissário da Informação ou o Comissário Federal da Proteção de Dados e Informação (conforme aplicável) determinaram como assegurando um nível adequado de proteção para a respetiva área de competência.
* "Lei Aplicável à Proteção de Dados" leis aplicáveis à proteção de dados e à privacidade, incluindo, quando aplicável, a Lei de Proteção de Dados dos EUA, a Lei de Proteção de Dados da UE, a Lei de Proteção de Dados do Reino Unido e a Lei de Proteção de Dados da Suíça.
* " Responsável pelo Tratamento", "Subcontratante", "Titular dos Dados", "dados pessoais", "tratamento" e "categorias especiais de dados pessoais" terão os significados dados na Lei Aplicável à Proteção de Dados.
* “EEE” significa Espaço Económico Europeu.
* “EUA” significa Estados Unidos da América.
* “CE” significa Comissão Europeia.
* “Lei de Proteção de Dados da UE” (a) o Regulamento Geral sobre a Proteção de Dados da UE (GDPR) (Regulamento 2016/679) (GDPR); (ii) a Diretiva de Privacidade Eletrónica da UE (Diretiva 002/58/CE); e (iii) toda e qualquer legislação dos Estados-Membros da UE feita ao abrigo, ou nos termos, de qualquer das anteriores; em cada caso, conforme emendada ou substituída de tempos a tempos.
* "Lei Suíça sobre a Proteção de Dados" a Lei Federal Suíça sobre a Proteção de Dados (FADP) de 1992 até Dezembro de 2022, e a partir de 1 de Janeiro de 2023, a Lei Federal Suíça (revista) sobre a Proteção de Dados (FADP revista) de 2020, tal como alterada ou substituída de tempos a tempos.
* "Lei de Proteção de Dados do Reino Unido" a legislação sobre privacidade de dados adotada pelos Regulamentos 2019/419 sobre Proteção de Dados, Privacidade e Comunicações Eletrónicas (Alterações, etc.) (EU Exit), complementada pelos termos do Data Protection Act 2018 (UK DPA) e do UK GDPR (Retained Regulation (EU) 2016/679 (UK GDPR) nos termos do artigo da União Europeia (Withdrawal Act 2018), conforme alterado ou substituído de tempos a tempos.
* " Lei de Protecção de Dados dos EUA" (a) a Lei da Privacidade do Consumidor da Califórnia de 2018 (CCPA), emendada e integrada pela Lei dos Direitos de Privacidade da Califórnia de 2020 (CPRA) e seguintes regulamentos de implementação; (b) a Lei da Proteção de Dados do Consumidor da Virgínia de 2021 (VCDPA); (c) a Lei da Privacidade do Colorado de 2021 (CPA); (d) a Lei da Privacidade de Dados de Connecticut de 2022 (CTDPA); e (e) a Lei da Privacidade do Consumidor de Utah de 2022 (UCPA); em cada caso, emendada ou substituída de tempos a tempos.
* “Hydrafacial” significa Hydrafacial LLC
* “Dispositivo”, significa o dispositivo, sistema e software Hydrafacial Syndeo.
* “Consumidor”, quem recebe um tratamento de Dispositivo.
* “Cliente”, clínica ou centro que fornece tratamentos de Dispositivos.
* “Utilizadores Autorizados" significa Cliente, as suas afiliadas, e os seus respetivos empregados, contratantes ou consultores que realizam tratamentos de Dispositivos.

1. *Relação entre as Partes:* A Hydrafacial (o responsável pelo tratamento) nomeia o Cliente (o subcontratante) para tratar os dados pessoais descritos no parágrafo número 14 do presente ATD (os "Dados") para os fins descritos no parágrafo número 16 do presente ATD, ou conforme acordado por escrito entre as partes (a "Finalidade Autorizada"). O Cliente não deverá reter, utilizar, ou divulgar os Dados para qualquer outro fim que não seja para a Finalidade Autorizada. O Cliente não comprará nem venderá os Dados. Cada Parte deverá cumprir as respetivas obrigações, ao abrigo da Lei de Proteção de Dados Aplicável.
2. *Leis de Transferências Internacionais e Localização de Dados:* Os Dados introduzidos e acedidos pelo Cliente e os seus Utilizadores Autorizados, através do Dispositivo, são alojados nos EUA e as cláusulas contratuais-tipo (“CCT”) aplicáveis, aprovadas em [\*link para as CCT\*] ("Página Web das CCT") serão consideradas incorporadas no presente ATD, a fim de cumprir a Lei de Proteção de Dados Aplicável. Se o Cliente necessitar de uma versão integralmente assinada, pode assinar a versão pré-assinada aplicável na página web das CCT e enviar uma cópia por correio eletrónico para dpo@hydrafacial.com. Nos países fora do EEE ("País Terceiro") onde se aplica uma restrição legal ao armazenamento e transferência de Dados em virtude de uma lei de localização de dados, os Dados não serão transferidos ou alojados fora do território local e serão armazenados em servidores locais. Antes da transferência de Dados para os EUA, a Hydrafacial tomou as medidas razoáveis para assegurar que os Dados transferidos estão sujeitos a um nível de proteção substancialmente equivalente ao fornecido no condado ou origem. Para dados originários do Reino Unido ("Reino Unido") ou da Suíça, as referências nesta Secção 3 são (a) o "EEE" será substituído por "Reino Unido" ou "Suíça", conforme o caso; b) a "Lei sobre a Proteção de Dados da UE" será substituída por "Lei de Proteção de Dados do Reino Unido" ou "Lei de Proteção de Dados da Suíça", conforme o caso; e c) a "CE" será substituída pelo "Gabinete do Comissário de Informação" ou pelo "Comissário Federal de Proteção de Dados e Informação", conforme o caso.
3. *Segurança e Confidencialidade*: Tendo em conta a natureza do tratamento, a Hydrafacial e o Cliente implementarão medidas técnicas e organizacionais adequadas para garantir um nível de segurança adequado aos riscos (tal como especificado no Artigo 32 do Regulamento Geral de Proteção de Dados da UE) para proteger os Dados (i) contra a destruição acidental ou ilegal, e (ii) contra a perda, alteração, divulgação não autorizada ou acesso aos Dados (uma "Violação de Privacidade"). O cliente deverá assegurar que quaisquer Utilizadores Autorizados que tratem os Dados tenham concordado expressamente em manter a confidencialidade.
4. *Tratamento por Subcontratantes:* Tendo em conta a natureza do tratamento, onde os Utilizadores Autorizados poderiam ser considerados como subcontratantes, ao abrigo da Lei de Proteção de Dados Aplicável, o Cliente deverá pelo menos assegurar o cumprimento dos requisitos e condições estabelecidos neste ATD, apenas para as Finalidades Autorizadas.
5. *Cooperação e Direitos dos Titulares dos Dados*: Tendo em conta a natureza do tratamento, o subcontratante prestará assistência ao responsável pelo tratamento, através de medidas técnicas e organizacionais adequadas, na medida do possível, e, se necessário, o Cliente prestará assistência razoável e atempada à Hydrafacial para que esta possa responder: (i) a qualquer pedido de um titular dos dados para exercer os seus direitos, ao abrigo da legislação aplicável de proteção de dados (incluindo os seus direitos de acesso, retificação, objeção, apagamento e portabilidade dos dados, conforme aplicável); e (ii) qualquer outra correspondência, pedido ou reclamação recebida de um titular dos dados, autoridade reguladora ou outro terceiro relacionado com o tratamento dos dados. No caso de qualquer pedido, correspondência, inquérito ou reclamação ser feito diretamente ao Cliente, o Cliente deverá notificar imediatamente a Hydrafacial com todos os seus detalhes.
6. *Avaliação, Consulta e Assistência* Tendo em conta a natureza do tratamento, em caso de necessidade, o Cliente deverá prestar cooperação para permitir à Hydrafacial (a) realizar quaisquer avaliações de proteção de dados ou de impacto da transferência; e (b) consultar as autoridades de supervisão competentes antes do tratamento, quando exigido pela Lei de Proteção de Dados Aplicável.
7. *Violação de Privacidade*: Se o Cliente tomar conhecimento de uma Violação de Privacidade, o Cliente deverá notificar imediatamente a Hydrafacial e fornecer à Hydrafacial informações e cooperação razoáveis, para permitir à Hydrafacial cumprir qualquer obrigação de notificação de violação que possa ter, ao abrigo da lei de proteção de dados aplicável. O Cliente deverá também tomar as medidas e ações razoavelmente necessárias para mitigar os efeitos da Violação de Dados e manter o Cliente informado de todos os desenvolvimentos materiais relacionados com a Violação de Dados. Os mesmos requisitos são aplicáveis aos subcontratantes.
8. *Apagamento ou Devolução de Dados*: O Cliente pode ser instado a fornecer à Hydrafacial um certificado de não retenção de dados no final do contrato.
9. *Verificação de Conformidade:* O Cliente deverá permitir que os seus procedimentos e documentação sejam inspecionados ou auditados pela Hydrafacial (ou pelo seu nomeado) para assegurar o cumprimento das obrigações estabelecidas no presente Acordo de Tratamento de Dados.
10. *Relatórios de Transparência* A Hydrafacial não divulgará, nem dará acesso, a quaisquer Dados a qualquer autoridade governamental, a menos que tal seja exigido por lei. A política da Hydrafacial para tratar os pedidos das autoridades públicas em relação a Dados ("Pedidos Legais"), juntamente com o Relatório de Transparência sobre Pedidos Legais da Hydrafacial, está disponível em [\*link\*]. A Hydrafacial: (a) irá rever a legalidade dos Pedidos Legais e contestá-los quando for lícito e apropriado fazê-lo; e (b) quando o Pedido Legal não estiver em conformidade com o Art. 46 do RGPD, ou qualquer outra disposição relevante para a transferência legal de dados pessoais, irá informar a autoridade pública do facto (em cada caso, na medida exigida pela Lei de Proteção de Dados Aplicável ao Pedido Legal).

**Anexo I - Controlos de Segurança da Informação**

1. *Controlos de segurança*:
2. A Hydrafacial sustenta as seguintes políticas e procedimentos de apoio ao seu programa de privacidade e segurança:

* Políticas de segurança da informação: Fornecer orientação de gestão e apoio à segurança da informação, de acordo com os requisitos empresariais, e leis e regulamentos relevantes.
* Organização da segurança da informação: Estabelecer um quadro para iniciar e controlar a implementação e operações de segurança da informação na Hydrafacial.
* Segurança dos recursos humanos: Garantir que todos os trabalhadores estejam devidamente preparados e compreendam as suas funções e responsabilidades. Garantir que todos os trabalhadores estejam conscientes e cumpram as suas responsabilidades e obrigações em matéria de segurança da informação. Garantir que os interesses da organização são protegidos durante todo o processo de emprego, desde a pré-contratação até à rescisão. Garantir que todos os trabalhadores estejam sob o dever de confidencialidade.
* Classificação dos Dados: Identificar a informação e classificação de dados de Hydrafacial, e definir e atribuir responsabilidades apropriadas para assegurar a sua proteção. Garantir um nível adequado de proteção da informação e dos dados, de acordo com o seu nível de sensibilidade e importância para a organização. Evitar a divulgação, modificação, remoção ou destruição não autorizadas de informações armazenadas em meios de comunicação.
* Gestão do acesso: Fornece o quadro para o controlo e gestão do acesso do utilizador, sistema e aplicações, e responsabilidades do utilizador. Limitar o acesso à informação e às instalações de processamento de informação. Garantir o acesso autorizado dos utilizadores e impedir o acesso não autorizado aos sistemas e serviços. Responsabilizar os utilizadores pela salvaguarda dos seus dados de autenticação. Impedir o acesso não autorizado a sistemas e aplicações.
* Segurança física e ambiental: Impedir o acesso físico não autorizado, danos e interferências com a informação e instalações de processamento de informação da Hydrafacial. Prevenir a perda, dano, roubo ou comprometimento dos bens da Hydrafacial, e a interrupção operacional.
* Segurança operacional: Garantir que as instalações de informação e processamento de informação são operadas de forma segura, protegidas contra malware e perda de dados. Garantir que os eventos de segurança sejam devidamente registados. Garantir a manutenção da integridade operacional do sistema, e evitar a exploração de vulnerabilidades técnicas.
* Segurança das comunicações: Estabelecer controlos para a proteção da informação em redes e instalações associadas. Garantir a segurança da informação a transferir no interior da Hydrafacial e com entidades externas.
* Relações com fornecedores: Garantir a proteção dos bens de Hydrafacial aos quais os fornecedores têm acesso. Manter um nível acordado de segurança da informação e de prestação de serviços, em conformidade com os acordos com os fornecedores.
* Gestão de incidentes de segurança da informação: Garantir uma abordagem consistente e eficaz à gestão de eventos de segurança da informação, incluindo incidentes e fragilidades.
* VPN (rede virtual privada) para acesso remoto: Aumenta a segurança e o anonimato dos utilizadores quando estes se ligam a serviços e sites baseados na web. Uma VPN esconde o endereço IP público real do utilizador e o tráfego dos "túneis" entre o dispositivo do utilizador e o servidor remoto.
* Criptografia de dados em repouso e em trânsito: Também conhecidos como dados em trânsito. Os dados em repouso referem-se a dados inativos que não transitam entre dispositivos ou redes e tendem a ser armazenados em arquivos de dados. Por outro lado, os dados em trânsito transitam entre dispositivos ou dois pontos de rede.
* Capacidade de backup e recuperação: É o processo de duplicar dados e armazená-los num local seguro em caso de perda ou dano, e depois restaurar esses dados para um local - o original ou uma alternativa segura - para que possam ser novamente utilizados em operações.
* Firewalls: É um dispositivo de segurança de rede que monitoriza e filtra o tráfego de entrada e saída da rede, com base nas políticas de segurança previamente estabelecidas por uma organização. No seu conceito mais básico, uma firewall é essencialmente a barreira que se situa entre uma rede interna privada e a Internet pública.
* Software antivírus: é um tipo de software utilizado para prevenir, verificar, detetar e eliminar vírus de um computador.
* Autenticação multi-factor (AMF): É uma tecnologia de segurança que requer múltiplos métodos de autenticação, de categorias independentes de credenciais, para verificar a identidade de um utilizador para efetuar um login ou outra transação.
* Filtragem de segurança do correio eletrónico: É o processo de bloqueio de códigos ou ligações indesejados, ou potencialmente maliciosos, que redirecionam o utilizador para sítios Web suspeitos. Impede as mensagens de correio electrónico que procuram entrar no sistema para obter acesso a dados sensíveis.
* Formação de sensibilização para a segurança; É o conhecimento e a atitude que os membros de uma organização possuem relativamente à proteção do património físico, e especialmente informativo, dessa organização.

1. O Cliente deverá utilizar medidas técnicas ou organizacionais adequadas de acordo com a Lei de Proteção de Dados Aplicável, incluindo proteção contra tratamento não autorizado ou ilegal e contra perda, destruição ou danos acidentais.

**Apêndice II - Informações Adicionais sobre o Tratamento de Dados**

1. *Categorias de titulares dos dados****:*** (i) Consumidor; (ii) Utilizador Autorizado; (iii) Cliente.
2. *Categorias de dados tratados:* (i) Contacto e informação de conta dos titulares dos dados, tais como nome completo, número de telefone, endereço de correio eletrónico, função e endereço IP; (ii) Histórico e desempenho do tratamento.
3. *Categorias especiais de dados****:*** Nenhuma categoria especial de dados é tratada dentro do Dispositivo.
4. *Finalidade da operação de tratamento:* Os dados pessoais serão tratados sempre que necessário para a prestação dos serviços do Dispositivo. Os dados pessoais tratados podem ser sujeitos às seguintes atividades básicas de tratamento: recolha, divulgação por comunicação e consulta. Em particular, as operações de tratamento incluem (i) Se o Consumidor desejar criar uma conta, o Cliente e o Utilizador Autorizado introduzem os seus dados no sistema do Dispositivo para que o Consumidor receba um SMS/e-mail e conclua o processo de registo. (ii) Os Consumidores têm a opção de partilhar o seu histórico de tratamento com o Cliente e o Utilizador Autorizado. Da mesma forma, ao utilizar o Dispositivo, os Clientes e o Utilizador Autorizado terão a opção de sincronizar a sua conta de aplicação com o Dispositivo, de modo a ter um registo do histórico de tratamento dos fornecedores. Os Clientes e o Utilizador Autorizado irão ver dados agregados sobre os tratamentos que forneceram, e nenhuma informação pessoalmente identificável dos Consumidores será associada aos tratamentos que o Cliente e o Utilizador Autorizado virem.
5. *Duração do tratamento:*Os dados pessoais podem ser tratados durante a vigência do contrato com os serviços do Dispositivo de Hydrafacial.