**ACCORD DE TRAITEMENT DES DONNEES**

1. *Définitions :* Dans le présent accord de traitement de données, les termes suivants ont la signification suivante :

* « Pays adéquat » : pays considéré comme offrant un niveau de protection adéquat par la Commission européenne, l’*Information Commissioner’s Office* ou le Préposé fédéral à la protection des données et à la transparence (selon le cas) pour leur domaine de compétence respectif.
* « Législation applicable en matière de protection des données » : législation applicable en matière de protection des données et de respect de la vie privée, comprenant, le cas échéant, la législation américaine sur la protection des données, la législation de l’UE sur la protection des données, la législation britannique sur la protection des données et la législation suisse sur la protection des données.
* « Responsable du traitement », « sous-traitant », « personne concernée », « données à caractère personnel », « traitement » (et « processus ») et « catégories particulières de données à caractère personnel » ont le sens qui leur est donné dans la législation applicable en matière de protection des données.
* « EEA » désigne l’Espace économique européen.
* « CE » désigne la Commission européenne.
* « Législation de l’UE sur la protection des données » : (a) le règlement général de l'UE sur la protection des données (règlement 2016/679) (RGPD) ; (ii) la directive de l'UE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive 2002/58/CE) ; et (iii) toutes les lois des États membres de l'UE adoptées en vertu de ces textes ou portant application de ceux-ci ; dans chaque cas, tels que modifiés ou remplacés de temps à autre.
* « Législation suisse sur la protection des données » : la loi fédérale suisse sur la protection des données (LPD) de 1992 jusqu'en décembre 2022 et, depuis le 1er janvier 2023, la loi fédérale suisse révisée sur la protection des données (LPD révisée) de 2020, telle que modifiée ou remplacée de temps à autre.
* « Législation britannique sur la protection des données » : la législation sur la protection des données adoptée par les règlements 2019/419 sur la protection des données, la vie privée et les communications électroniques (modifications, etc.) (sortie de l'UE) complétés par les dispositions du *Data Protection Act* [loi sur la protection des données] de 2018 (DPA) et du RGPD britannique (règlement maintenu (UE) 2016/679 (RGPD britannique) conformément à l’article 3 de la loi de 2018 sur l'Union européenne (loi de sortie de 2018), tels que modifiés ou remplacés de temps à autre.
* « Législation américaine sur la protection des données » : le *California Consumer Privacy Act* de 2018 (CCPA), tel que modifié et intégré par le *California Privacy Rights Act* de 2020 (CPRA) et les règlements d'application suivants ; (b) *Virginia Consumer Data Protection Act* de 2021 (VCDPA), (c) *Colorado Privacy Act* de 2021 (CPA), (d) *Connecticut Data Privacy Act* de 2022 (CTDPA) et (e) *Utah Consumer Privacy Act* de 2022 (UCPA), dans chaque cas, tels que modifiés ou remplacés de temps à autre.
* « Hydrafacial » désigne Hydrafacial LLC.
* « Appareil » désigne l’appareil, le système et le logiciel Syndeo d’Hydrafacial.
* « Consommateur » désigne la personne qui reçoit un traitement utilisant l’Appareil.
* « Client » désigne la clinique ou l’institut qui fournit des traitements utilisant l’Appareil.
* « Utilisateurs autorisés » désigne le client, ses affiliés, et leurs employés, sous-traitants ou consultants respectifs qui réalisent des traitements utilisant l’Appareil.

1. *Relation entre les parties*: Hydrafacial (le responsable du traitement) désigne le client (sous-traitant) pour traiter les données à caractère personnel décrites à l’article 14 du présent accord (les « données ») aux fins décrites à l’article 16 du présent accord ou à toute autre fin convenue par écrit entre les parties (la « finalité autorisée »). Le client n’a pas le droit d’utiliser ou de communiquer les données à d'autres fins que la finalité autorisée. Le client n’a pas le droit d’acheter ou de vendre les données. Chacune des parties doit se conformer à ses obligations respectives en vertu de la législation applicable en matière de protection des données.
2. *Transferts internationaux et législation sur la localisation des données* :les données saisies et consultées par le client et ses utilisateurs autorisés au moyen de l'Appareil sont hébergées aux États-Unis et les clauses contractuelles types applicables approuvées (les « CCT ») consultables ici : [\*lien vers les CCT\*] (la « page des CCT ») sont réputées faire partie du présent accord pour se conformer à la législation applicable en matière de protection des données. Si le client a besoin d’un exemplaire complet signé, il peut contresigner la version applicable pré-signée disponible sur la page des CCT et en envoyer une copie par courrier électronique à l'adresse dpo@hydrafacial.com. Dans les pays situés en dehors de l'EEE (les « pays tiers ») dans lesquels existe une restriction légale sur le stockage et le transfert de données en vertu d'une loi sur la localisation des données, les données ne seront pas transférées ou hébergées en dehors du territoire national et seront stockées sur des serveurs locaux. Avant de transférer les données aux États-Unis, Hydrafacial a pris des mesures raisonnables pour s'assurer que les données transférées font l’objet d’un niveau de protection sensiblement équivalent à celui qui existe dans leur pays d'origine. Pour les données provenant du Royaume-Uni ou de la Suisse, il convient de remplacer dans le présent paragraphe 3 les références à : (a) l’« EEE » par « Royaume-Uni » ou « Suisse » selon le cas ; (b) « législation de l’UE sur la protection des données » par « législation britannique sur la protection des données » ou « législation suisse sur la protection des données » selon le cas, et (c) « CE » par « *Information Commissioner’s Office* » ou « préposé fédéral à la protection des données et à la transparence » selon le cas.
3. *Sécurité et confidentialité* : en fonction de la nature du traitement, Hydrafacial et le client doivent mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque (telles que spécifiées à l'article 32 du Règlement général sur la protection des données de l'UE) afin de protéger les données (i) contre la destruction accidentelle ou illicite, et (ii) contre la perte, l'altération et la divulgation non autorisée des données ou l'accès à celles-ci (« atteinte à la confidentialité des données »). Le client s'assurera que tous les utilisateurs autorisés qui traitent des données se sont expressément engagés à en respecter la confidentialité.
4. *Sous-traitance ultérieure* :en fonction de la nature du traitement, lorsque les utilisateurs autorisés peuvent être considérés comme des sous-traitants en vertu de la législation applicable en matière de protection des données, le client doit au minimum veiller au respect des obligations et conditions figurant dans le présent accord uniquement pour les finalités autorisées.
5. *Coopération et droits des personnes concernées* : en fonction de la nature du traitement, le sous-traitant doit assister le responsable du traitement en prenant des mesures techniques et organisationnelles appropriées, dans la mesure du possible et, si nécessaire, le client doit fournir une assistance rapide et raisonnable à Hydrafacial pour lui permettre de répondre à : (i) toute demande d'une personne concernée qui souhaite exercer ses droits en vertu de la législation applicable en matière de protection des données (y compris les droits d'accès, de rectification, d'opposition, d'effacement et de portabilité des données, le cas échéant) ; et (ii) toute autre correspondance, demande ou réclamation émanant d'une personne concernée, d'une autorité de régulation ou d'un tiers en rapport avec le traitement des données. Si cette demande, correspondance, requête ou réclamation est adressée directement au client, ce dernier en informera Hydrafacial dans les plus brefs délais en lui fournissant tout le détail.
6. *Évaluation, consultation et assistance* : en fonction de la nature du traitement, le client devra coopérer, le cas échéant, pour permettre à Hydrafacial (a) de réaliser des évaluations de la protection des données ou de l'impact d’un transfert ; et (b) de consulter les autorités de contrôle compétentes avant le traitement lorsque cela est exigé par la législation applicable en matière de protection des données.
7. *Atteintes à la confidentialité des données* : si le client prend connaissance d’une atteinte à la confidentialité des données, il doit en informer immédiatement Hydrafacial en lui fournissant les informations nécessaires et sa coopération raisonnable pour permettre à Hydrafacial de se conformer à ses éventuelles obligations de notification au titre de la législation applicable en matière de protection des données. Le client doit également prendre les mesures raisonnablement nécessaires pour limiter les conséquences de cette atteinte à la confidentialité des données et doit tenir le consommateur informé de tout événement important lié à celle-ci. Ces obligations s’appliquent également aux sous-traitants ultérieurs.
8. *Suppression ou restitution des données* : il peut être demandé au client de fournir à Hydrafacial un certificat de non-rétention des données à la fin du contrat.
9. *Contrôle de conformité* : le client autorise Hydrafacial (ou son représentant) à inspecter ou à vérifier ses procédures et sa documentation afin de s'assurer qu’il respecte les obligations figurant dans le présent accord de traitement de données.
10. *Rapports de transparence* : Sauf si la législation l’exige, Hydrafacial ne communiquera pas de données à des autorités gouvernementales et ne leur permettra pas de les consulter. La politique d’Hydrafacial relative aux demandes des autorités publiques portant sur des données (les « demandes légales ») et son rapport de transparence relatif à ces demandes sont disponibles à l'adresse suivante : [\*lien\*]. Hydrafacial s'engage à : (a) examiner la légalité des demandes légales et à les contester lorsqu'il est légal et approprié de le faire ; et, (b) lorsque la demande légale n'est pas conforme à l'art. 46 du GDPR ou à d’autres dispositions pertinentes se rapportant au transfert licite de données à caractère personnel, à en informer l'autorité publique (dans la mesure requise par la législation applicable en matière de protection des données qui s’applique à la demande légale en question).

**Annexe I – Systèmes de contrôle de la sécurité des données**

1. *Systèmes de contrôle de la sécurité* :
2. Hydrafacial applique les politiques et procédures suivantes à l'appui de son programme de sécurité et de protection des données :

* Politiques de sécurité de l’information : pour apporter une orientation et un soutien à la direction de l’entreprise en matière de sécurité de l'information, conformément aux obligations de l'entreprise et aux lois et réglementations applicables.
* Organisation de la sécurité de l’information : pour mettre en place un cadre de travail permettant de lancer et de surveiller la mise en œuvre et le fonctionnement de la sécurité de l’information chez Hydrafacial.
* Sécurité des ressources humaines : pour garantir que chaque membre du personnel a les compétences nécessaires pour ses fonctions et responsabilités et qu’il les comprend ; pour s’assurer que l’ensemble du personnel a conscience de ses responsabilités et obligations en matière de sécurité de l'information et que chacun les respecte ; pour garantir que les intérêts de l’entreprise sont protégés tout au long du processus d'embauche, depuis la phase de pré-embauche jusqu'à la fin du contrat de travail ; pour s’assurer que l'ensemble du personnel est soumis au devoir de confidentialité.
* Classification des données : pour identifier les catégories d’informations et de données d’Hydrafacial ; pour définir et attribuer les responsabilités correspondantes en vue d’assurer leur protection ; pour garantir un niveau approprié de protection des informations et des données en fonction de leur degré de sensibilité et de leur importance pour l'organisation ; pour empêcher la divulgation, la modification, la suppression ou la destruction non autorisée des informations conservées sur des supports.
* Gestion des accès : pour fournir un cadre de contrôle et de gestion des accès pour les utilisateurs, les systèmes et les applications, ainsi que pour les responsabilités des utilisateurs ; pour limiter l'accès aux informations et aux installations de traitement de ces informations ; pour permettre l'accès autorisé des utilisateurs et empêcher tout accès non autorisé aux systèmes et aux services ; pour rendre les utilisateurs responsables de la protection de leurs informations d'authentification ; pour empêcher tout accès non autorisé aux systèmes et aux applications.
* Sécurité physique et environnementale : pour empêcher tout accès physique non autorisé, tout dommage et toute interférence avec les informations et les installations de traitement de l'information d’Hydrafacial ; pour empêcher la perte, le vol ou la compromission des actifs d’Hydrafacial et l'interruption de ses activités.
* Sécurité des opérations : pour garantir que les informations et les installations de traitement des informations sont exploitées en toute sécurité et sont protégées contre les logiciels malveillants et la perte de données ; pour s’assurer que les incidents de sécurité sont enregistrés de manière appropriée ; pour garantir l'intégrité des systèmes opérationnels et éviter toute exploitation des vulnérabilités techniques.
* Sécurité des communications : pour mettre en place des systèmes de contrôle garantissant la protection de l'information dans les réseaux et les installations correspondantes ; pour garantir la sécurité des informations transférées au sein d’Hydrafacial ou avec des tiers.
* Relations fournisseurs : pour assurer la protection des actifs d’Hydrafacial auxquels les fournisseurs ont accès ; pour maintenir un niveau convenu de sécurité de l'information et de prestation de services conformément aux contrats signés avec les fournisseurs.
* Gestion des incidents liés à la sécurité de l'information : pour garantir une approche efficace et uniforme de la gestion des événements liés à la sécurité de l'information, y compris les incidents et les faiblesses.
* VPN (réseau virtuel privé) pour l’accès à distance : améliore la sécurité et l’anonymat des utilisateurs lorsqu’ils se connectent à des services ou des sites en ligne. Le VPN masque l'adresse IP publique réelle de l'utilisateur et « tunnelise » le trafic entre l'appareil de l'utilisateur et le serveur à distance.
* Cryptage des données au repos ou en transit : également appelé « données en mouvement ». Les données au repos sont des données inactives qui ne sont pas en train de se déplacer pas entre des appareils ou des réseaux et qui sont généralement stockées dans des archives de données. Les données en transit se déplacent quant à elles entre des appareils ou deux points du réseau.
* Capacités de sauvegarde et de récupération : il s'agit du processus de duplication des données et de leur stockage dans un endroit sûr en cas de perte ou de dommage, puis de la restauration de ces données à un certain endroit (celui d’origine ou un autre endroit sûr) pour qu'elles puissent être de nouveau utilisées dans les opérations.
* Firewalls : il s'agit d'un dispositif de sécurité des réseaux qui surveille et filtre le trafic réseau entrant et sortant sur la base de règles de sécurité définies au préalable par l’organisation. Dans sa forme la plus simple, un firewall (pare-feu en anglais) est essentiellement la barrière qui se trouve entre un réseau interne privé et l'Internet public.
* Logiciel antivirus : il s'agit d'un type de logiciel qui permet de prévenir, d’analyser, de détecter et de supprimer les virus sur les ordinateurs.
* Authentification multifactorielle (MFA) : technologie de sécurité qui requiert plusieurs méthodes d'authentification basées sur différentes sources pour vérifier l'identité des utilisateurs au moment de la connexion ou d'une autre transaction.
* Filtrage de sécurité des courriers électroniques : processus qui consiste à bloquer les codes ou liens indésirables ou potentiellement malveillants qui redirigent l'utilisateur vers des sites web suspects. Il bloque les e-mails qui cherchent à pénétrer dans le système pour accéder à des données sensibles.
* Formation de sensibilisation à la sécurité : connaissances et attitude des membres d'une organisation concernant la protection des actifs physiques, et surtout informationnels, de cette organisation.

1. Le client doit appliquer des mesures organisationnelles et techniques appropriées conformément à la législation applicable en matière de protection des données, notamment pour protéger les données contre tout traitement illégal ou non autorisé et contre la perte, la destruction ou les dommages accidentels.

**Annexe II – Précisions concernant le traitement des données**

1. *Catégories de personnes concernées* : (i) consommateur ; (ii) utilisateur autorisé ; (iii) client.
2. *Catégories de données traitées* : (i) coordonnées des personnes concernées et renseignements relatifs à leur compte, tels que leur nom complet, leur numéro de téléphone, leur adresse électronique, leur titre et leur adresse IP ; (ii) historique et résultats des traitements de données**.**
3. *Catégories particulières de données* : aucune catégorie particulière de données n’est traitée dans l’Appareil.
4. *Finalité du traitement* : les données à caractère personnel seront traitées lorsque cela est nécessaire pour la fourniture des services liés à l’Appareil. Elles pourront faire l'objet des traitements de base suivants : collecte, divulgation par communication et consultation. En particulier, (i) si le consommateur souhaite créer un compte, le client et l'utilisateur autorisé saisissent ses coordonnées dans l’Appareil pour lui permettre de recevoir un SMS/e-mail et de terminer son processus d'enregistrement ; (ii) les consommateurs ont la possibilité de communiquer leur historique de traitement au client et à son utilisateur autorisé. De même, lorsqu'ils utilisent l’Appareil, les clients et les utilisateurs autorisés ont la possibilité de synchroniser leur compte dans l’application avec l’Appareil afin d’obtenir un historique de traitement des prestataires. Les clients et les utilisateurs autorisés verront des données agrégées concernant les traitements dispensés, et aucune information personnelle identifiable concernant des consommateurs ne sera associée aux traitements que le client et l'utilisateur autorisé peuvent consulter.
5. *Durée du traitement* : les données à caractère personnel peuvent être traitées pendant toute la durée du contrat concernant les services liés à l’Appareil.