DATA PROCESSING AGREEMENT

1. *Definitions:* In this Data Processing Agreement ("DPA"), the following terms shall have the following meanings:
   - "Adequate Country" a country that the European Commission, the Information Commissioner's Office or the Federal Data Protection and Information Commissioner (as applicable) have determined as ensuring and adequate level of protection for their respective area of competence.
   - "Applicable Data Protection Law" applicable data protection and privacy laws including, where applicable, US Data Protection Law, EU Data Protection Law, UK Data Protection Law and Swiss Data Protection Law.
   - "Controller", "processor", "data subject", "personal data", "processing" (and "process") and "special categories of personal data" shall have the meanings given in Applicable Data Protection Law.
   - "EEA" means European Economic Area.
   - "US" means United States of America.
   - "EC" means European Commission.
   - "EU Data Protection Law" (a) the EU General Data Protection Regulation (Regulation 2016/679) (GDPR); (ii) the EU e-Privacy Directive (Directive 002/58/EC); and (iii) any and all EU Member State laws made under or pursuant to any of the foregoing; in each case as amended or superseded from time to time.
   - "Swiss Data Protection Law" the Swiss Federal Act on Data Protection (FADP) of 1992 until the December 2022, and from January 1, 2023, onward, the Revised Swiss Federal Act on Data Protection (Revised FADP) of 2020, as amended or superseded from time to time.
   - "UK Data Protection Law" the data privacy legislation adopted by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019/419 as supplemented by the terms of the Data Protection Act 2018 (UK DPA) and the UK GDPR (Retained Regulation (EU) 2016/679 (UK GDPR) pursuant to section of the European Union (Withdrawal Act 2018), as amended or superseded from time to time.
   - "US Data Protection Law" (a) the California Consumer Privacy Act of 2018 (CCPA), as amended and integrated by the California Privacy Rights Act of 2020 (CPRA) and following implementing regulations; (b) the Virginia Consumer Data Protection Act of 2021 (VCDPA); (c) the Colorado Privacy Act of 2021 (CPA); (d) the Connecticut Data Privacy Act of 2022 (CTDPA); and (e) the Utah Consumer Privacy Act of 2022 (UCPA); in each case as amended or superseded from time to time.
   - "Hydrafacial" means Hydrafacial LLC
   - "Device", means the Hydrafacial Syndeo device, system & software.
   - "Consumer", who receives a Device treatment.
   - "Costumer", clinic or center that provides Device treatments.
   - "Authorized Users" means Customer, its affiliates, and their respective employees, contractors or consultants that performs Device treatments.
2. *Relationship of the Parties:* Hydrafacial (the controller) appoints the Customer (the processor) to process the personal data described in the paragraph number 14 of this DPA (the "Data") for the purposes described in the paragraph number 16 of this DPA or as otherwise agreed in writing by the parties (the "Permitted Purpose"). The Customer shall not retain, use, or disclose the Data for any purpose other than for the Permitted Purpose. The Customer shall not buy or sell the Data. Each Party shall comply with its respective obligations under Applicable Data Protection Law.
3. *International Transfers & Data Localization Laws:* The Data entered and accessed by the Customer and its Authorized Users through the Device is hosted in the US and the applicable standard contractual clauses approved ("SCC's") at this location ("SCC's Webpage") shall be deemed incorporated into this DPA in order to comply with the Applicable Data Protection Law. If the Customer requires a fully executed version, it may countersign the applicable pre-signed version on the SCC's Webpage and email a copy dpo@hydrafacial.com. In those countries outside the EEA ("Third Country") where a legal restriction on the data storage and transfer of Data applies by virtu of a data localization law, the Data will not be transferred or hosted outside the local territory and will be stored on local servers. Prior to transferring Data to the US, Hydrafacial has taken the reasonable steps to ensure that the transferred Data is subject to a level of protection substantially equivalent to that provided in the county or origin. For Data originating from the United Kingdom ("UK") or Switzerland references in this Section 3 to: (a) the "EEA" shall be replaced with the "UK" or "Switzerland", as applicable; (b) "EU Data Protection Law" shall be replaced with "UK Data Protection Law" or "Swiss Data Protection Law", as applicable; and (c) the "EC" shall be replaced with the "Information Commissioner's Office" or the "Federal Data Protection and Information Commissioner", as applicable.
4. *Security & Confidentiality*: Taking into account the nature of the processing, Hydrafacial & the Customer shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks (as specified in Article 32 of the EU General Data Protection Regulation) to protect the Data (i) against accidental or unlawful destruction, and (ii) against loss, alteration,

unauthorised disclosure of, or access to the Data (a "Privacy Breach"). Customer shall ensure that any Authorized Users who process the Data have expressly agreed to maintain confidentiality.

5. *Subprocessing:* Taking into account the nature of the processing, where Authorized Users could be considered as sub-processors under the Applicable Data Protection Law, the Customer shall at least ensure compliance with the requirements and conditions set out in this DPA only for the Permitted Purposes.
6. *Cooperation and Data Subjects' Rights*: Taking into account the nature of the processing, the processor shall assist the controller by appropriate technical and organisational measures, insofar as this is possible and, where necessary, the Customer shall provide reasonable and timely assistance to Hydrafacial to enable it to respond to: (i) any request from a data subject to exercise his or her rights under applicable data protection law (including his or her rights of access, rectification, objection, erasure and data portability, as applicable); and (ii) any other correspondence, request or complaint received from a data subject, regulatory authority or other third party in connection with the processing of the data. In the event that any such request, correspondence, enquiry or complaint is made directly to the Customer, the Customer shall promptly notify Hydrafacial with full details thereof.
7. *Assessment, Consultation & Assistance* Taking into account the nature of the processing, in case needed, the Customer shall provide cooperation to enable Hydrafacial to (a) conduct any data protection or transfer impact assessments; and (b) consult competent supervisory authorities prior to processing where required by Applicable Data Protection Law.
8. *Privacy Breaches*: If the Customer becomes aware of a Privacy Breach, the Customer shall immediately notify Hydrafacial and provide Hydrafacial with reasonable information and cooperation to enable Hydrafacial to comply with any breach notification obligations it may have under applicable data protection law. The Customer shall also take such measures and actions as are reasonably necessary to mitigate the effects of the Data Breach and shall keep the Customer informed of all material developments in connection with the Data Breach. The same requirements shall apply to sub-processors.
9. *Deletion or Return of Data*: The Customer may be asked to provide Hydrafacial with a certificate of non-retention of data at the end of the contract.
10. *Check of Compliance:* The Customer shall allow its procedures and documentation to be inspected or audited by Hydrafacial (or its nominee) to ensure compliance with the obligations set out in this Data Processing Agreement.
11. *Transparency Reports* Hydrafacial will not disclose or provide access to any Data to any governmental authority unless required to do so by law. Hydrafacial's policy for dealing with requests from public authorities in relation to Data ("Legal Requests"), together with Hydrafacial's Transparency Report on Legal Requests, is available at this location. Hydrafacial will: (a) review the legality of the Legal Requests and challenge them where it is lawful and appropriate to do so; and (b) where the Legal Request does not comply with Art. 46 of the GDPR or any other relevant provision for the lawful transfer of personal data, inform the public authority thereof (in each case to the extent required by the Applicable Data Protection Law applicable to the Legal Request).

Appendix I - Information Security Controls

12. *Security controls*:

12.1. Hydrafacial maintains the following policies and procedures in support of its privacy and security program:

- Information security policies: To provide management direction and support for information security in accordance with business requirements, and relevant laws and regulations.
- Organization of information security: To establish a framework for initiating and controlling information security implementation and operations at Hydrafacial.
- Human resource security: To ensure that all workforce members are well suited for, and understand, their roles and responsibilities. To ensure that all workforce members are aware of, and that they fulfill, their information security responsibilities and obligations. To ensure that the organization's interests are protected throughout the employment process, from pre-employment to termination. To ensure that all workforce is under the duty of confidentiality.
- Data Classification: To identify Hydrafacial's information and data classification, and to define and assign appropriate responsibilities for ensuring their protection. To ensure an appropriate level of protection for information and data in accordance with their sensitivity level and importance to the organization. To prevent the unauthorized disclosure, modification, removal or destruction of information stored on media.
- Access management: Provides the framework for user, system and application access control and management, and user responsibilities. To limit access to information and information processing facilities. To ensure authorized user access and to prevent unauthorized access to systems and services. To make users accountable for safeguarding their authentication information. To prevent unauthorized access to systems and applications.
- Physical and environmental security: To prevent unauthorized physical access, damage and interference with Hydrafacial's information and information processing facilities. To prevent loss, damage, theft or compromise of Hydrafacial's assets, and interruption of its operations.

- Operations security: To ensure that information and information processing facilities are operated securely, protected from malware and loss of data. To ensure that security events are recorded appropriately. To ensure that operational system integrity is maintained, and exploitation of technical vulnerabilities is avoided.
- Communications security: To establish controls for the protection of information in networks and their associated facilities. To ensure the security of information being transferred within Hydrafacial and with external parties.
- Supplier relationships: To ensure protection of Hydrafacial assets that are accessible by suppliers. To maintain an agreed-upon level of information security and service delivery in accordance with supplier agreements.
- Information security incident management: To ensure a consistent and effective approach to managing information security events, including incidents and weaknesses.
- VPN (virtual private network) for remote Access: Adds security and anonymity to users when they connect to web-based services and sites. A VPN hides the user's actual public IP address and "tunnels" traffic between the user's device and the remote server.
- Encryption of data at rest and in transit: Also known as data in motion. Data at-rest refers to inactive data not moving between devices or networks and tends to be stored in data archives. On the other hand, data in-transit is moving between devices or two network points.
- Backup and recovery capabilities: Is the process of duplicating data and storing it in a secure place in case of loss or damage, and then restoring that data to a location — the original one or a safe alternative — so it can be again used in operations.
- Firewalls: Is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet.
- Antivirus software: is a kind of software used to prevent, scan, detect and delete viruses from a computer.
- Multi-factor authentication (MFA): Is a security technology that requires multiple methods of authentication from independent categories of credentials to verify a user's identity for a login or other transaction.
- Email security filtering: Is the process of blocking unwanted or potentially-malicious code or links that redirect the user to suspicious websites. It prevents emails that seek entry into the system to get access to sensitive data.
- Security awareness training; Is the knowledge and attitude members of an organization possess regarding the protection of the physical, and especially informational, assets of that organization.

12.2. The Customer shall use appropriate technical or organisational measures according to the Applicable Data Protection Law, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Appendix II – Details on the Data Processing

13. *Categories of data subjects*: (i) Consumer; (ii) Authorised User; (iii) Costumer.
14. *Categories of data processed*: (i) Contact & Account Information of the data subjects, such as full name, phone number, email address, role and IP address; (ii) Treatment History & Performance.
15. *Special categories of data*: No special categories of data are processed within the Device.
16. *Purpose of processing operation*: Personal data will be processed where necessary for the provision of the Device services. Personal data processed may be subject to the following basic processing activities: collection, disclosure by communication and consultation. In particular, the processing operations include (i) If the Consumer wishes to create an account, the Customer and the Authorised User enter their details into the Device system so that the consumer receives a SMS/e-mail and completes the registration process. (ii) Consumers have the option to share their treatment history with the Customer & Authorised User. Similarly, when using the Device, Customers & Authorised User will have the option to synchronise their application account with the Device in order to have a record of the providers' treatment history. Customers & Authorised User will see aggregated treatment data about the treatments they have provided, and no personally identifiable information of Consumers will be associated with the treatments that the Customer & Authorised User sees.
17. *Duration of processing*: Personal data may be processed for the duration of the contract with Hydrafacial Device services.