Applicable Data Protection Laws

Capitalized terms used and not defined herein have the meanings ascribed to them in the DPA or the Agreements, as applicable.

European Economic Area:

European Union regulations and EEA Member State laws, other than GDPR, requiring a contract governing the processing of personal data, identical to or substantially similar to the requirements specified in Article 28 of the GDPR.

United Kingdom:

The UK Data Protection Act 2018.

Brazil:

The Brazil's General Data Protection Law, Lei Geral de Proteção de Dados ("LGPD"). For the sake of clarity, the Company's obligations to Customer under the DPA are only those express obligations imposed by LGPD on a Data Processor (operador) for the benefit of a Data Controller (controlador) (each, as defined under LGPD). Pursuant to the Company's obligations under LGPD, a new Section 1.6 shall be added to the DPA to read as follows :

> **1.6** Each party is responsible to fulfil its respective obligations under the LGPD, and Customer will only issue Processing instructions, as set forth in Section 1.3 of this DPA, that enable the Company to fulfill its LGPD obligations.

State of California, United States:

The California Consumer Privacy Act of 2018 ("CCPA"). The Company's obligations to Customer under the DPA are those that the CCPA requires that a Business have in place with a Service Provider (each, as defined under CCPA). Pursuant to the Company's obligations under CCPA, a new Section 1.6 shall be added to the DPA to read as follows:

> **1.6** The Company will not collect, sell, retain, disclose or use the Personal Information of the Consumer for any purpose other than pursuant to the Agreements, or as otherwise permitted by CCPA. The Company certifies that it understands and will comply with the restrictions set forth in this Section 1.6.

The terms used in the applicable provisions of the DPA shall be replaced as follows: "Personal Data" shall mean "Personal Information"; "Controller" shall mean "Business"; "Processor" shall mean "Service Provider"; and "Data Subject" shall mean "Consumer".

South Africa:

The Protection of Personal Information Act ("POPIA"). For the sake of clarity, the Company's obligations to Customer under the DPA are only those express obligations imposed by POPIA on an Operator for the benefit of a Responsible Party (each, as defined under POPIA). Pursuant to the Company's obligations under POPIA, Section 9.1 of the DPA hereby is deleted in its entirety and replaced with the following in lieu thereof:

> "The Company will immediately notify Customer after becoming aware of reasonable grounds to believe that the Personal Information of a Data Subject has been accessed or acquired by any unauthorised Person (as defined under POPIA)."

The terms used in the applicable provisions of the DPA shall be replaced as follows: "Personal Data" shall mean "Personal Information"; "Controller" shall mean "Responsible Party"; and "Processor" shall mean "Operator."

Russian Federation

Federal Law dated July 27, 2006 No. 152-FZ "On Personal Data" and secondary legislation promulgated hereunder, as amended.

Ukraine:

The Law of Ukraine "On Personal Data Protection" No. 2297-VI of 01 June 2010, as amended.

Appendix on Additional Safeguards to EU Standard Contractual Clauses (EU SCCs)

1. In accordance with the July 16, 2020 decision of the Court of Justice of the European Union (CJEU) in Case C-311/18 *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*, and without prejudice to any provisions of the DPA, the Company will undertake commercially reasonable additional safeguards that are necessary to secure Personal Data transferred on the basis of EU Standard Contractual Clauses to those countries whose laws are likely to have a substantial adverse effect on the level of data protection offered by the EU Standard Contractual Clauses and required under the GDPR.
2. The Company's TOMs are published at: https://trustyoursupplier.com/wp-content/uploads/2021/08/Chainyard-Security-Technical-and-Organizational-Measures-TOMs-v1.0-03.10.2021-1.pdf such as encryption, access controls, or similar technologies, as applicable, to protect Customer Personal Data against any Processing for national security or other government purposes that are determined to be massive or disproportionate, considering the type of processing activities and the Company's scope of responsibility.
3. In the event of any such request for access to Customer Personal Data by a government or regulatory authority:

a. The Company will notify Customer of such request to enable the Customer to take all necessary actions to communicate directly with the relevant authority and respond to such request. If the Company is prohibited by law to notify the Customer of such request: (i) it will make good faith efforts to challenge such prohibition, as determined in its sole discretion taking into consideration the nature of the processing and its means and resources; and (ii) it commits to providing the minimum amount of information permissible when responding, based on a reasonable interpretation of the order; and
b. if, regardless of all such efforts, the Company is prohibited by law to notify the Customer, upon request of the Customer and in accordance with applicable law, the Company will provide to such Customer general information relative to any such request received from a government or regulatory authority during the preceding twelve (12)-month period.