APPENDIX – Local Jurisdiction Specific – LGPD - BRAZIL

This Appendix supports the Data Privacy Policy 66.01, providing insight in local variations specific to the BRAZIL LGPD.

1. DEFINITIONS UNDER THE LGPD:

Controller or "Controlador"	A Controller determines the purposes and the means of the processing of personal data. It has the power to make high-level decisions about how and why the personal data can be used. It determines matters such as, the content of the data to be collected and used, who it will be collected about and when it will be disclosed and to whom.
"Data Breach" or "Incidente de segurança"	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised. disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Data Subject or "Titular"	An identified or identifiable natural person that the personal data relates to, such as an employee, former employee, retiree, candidate, contractor, corporate contact, website visitor etc.
Data Protection Officer, DPO or "Encarregado de Proteção de Dados"	Person appointed by the Controller and Processor to act as a communication channel between the Controller, the Data Subject and the ANPD.
LGPD or "Lei Geral de Proteção de Dados"	Brazilian general data protection law, Law nº 13.709/2018.

Personal Data or "Dado Pessoal"	Any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified either directly from data, or indirectly, either on its own or together with other data which is in, or may come into, the Controller's possession. For example by reference to a name, identification number, location data, IP address, online identifier or to other factors such as physical or
	economic factors. This term will include any data that can be used to learn, record or decide something about an individual.
Processing ou "Tratamento"	Any operation or set of operations carried out in relation to Personal Data, such as collecting, storing, disclosing, amending and deleting. Processing is widely defined and will in effect cover any activity involving Personal Data, for example, storing CVs, updating employee, customer or supplier records, monitoring employees' internet use or operating a CCTV system which captures Data Subjects' behaviour, etc.
Processor or "Operador"	A processor merely processes the personal data on behalf of the Controller. It is not able to make high-level decisions about how and why the data will be used.
Special Categories of Personal Data or "Dado sensível"	Personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life/sexual orientation, genetic data or biometric data.
Supervisory Authority or ANPD	The independent public authority which is established in Brazil to monitor the application of the LGPD, and to protect the rights of data subjects pursuant to LGPD.

2. DATA BREACH:

2.1. <u>Breach Notification Requirements:</u>

Notification shall be no longer than two business days of becoming aware of the event.

2.1.1. What to do in case of a Data Breach:

i. assess the incident internally - nature, category and number of data subjects affected, category and number of data affected, concrete and probable consequences;

ii. notify the *data breach* to the Company's DPO and, if Company is acting as a Processor, to the Controller;

iii. notify the ANPD and *data subjects*, in case of risk or material damage to those Data Subjects that has been affected by the *personal data breach;*

iv. prepare documentation with the internal assessment of the incident, measures taken and risk analysis, in order to comply with the principle of accountability and accountability.

2.1.2. Notifications require key information including:

i. identification and contact details (Controller, DPO etc.);

ii. indicate that it is a complete, preliminary communication or a complementary communication;

iii. date and time when discovered, extension, circumstance in which the breach occurred, storage location of the data, the categories and approximate number of Data Subjects concerned; description of the nature of the Data Breach; iv. the likely consequences of the Data Breach;

v. the measures taken or proposed by the Company to address the Data Breach, including, where appropriate, measures to mitigate its possible adverse effects; vi. possible problems of cross-border nature; and

vii. other useful information for those Data Subjects that has been affected by the *personal data breach* to protect their data or prevent possible damage.

3. DATA PROTECTION PRINCIPLES:

The LGPD also specifies as principles **free access, prevention and non-discrimination.**

Information on how each term above applies is detailed below:

3.1. Free access

Guarantee to the Data Subjects of facilitated and free of charge consultation about the form and duration of the processing, as well as about the integrity of their Personal Data.

3.2. Prevention

Determines the adoption of measures to prevent the occurrence of damages due to the processing of Personal Data.

3.3. Non-discrimination

Impossibility of carrying out the processing for unlawful or abusive discriminatory purposes.

The Data Subject has the right to request for the review of decisions made solely based on automated processing of personal data affecting her/his interests, including decisions intended to define her/his personal, professional, consumer and credit profile, or aspects of her/his personality (under Article 20 of the LGPD).

And whenever requested to do so, the Company shall provide clear and adequate information regarding the criteria and procedures used for an automated decision, subject to commercial and industrial secrecy.

If there is no offer of the information as provided above, the ANPD may carry out an audit to verify discriminatory aspects in automated processing of Personal Data.

4. LAWFUL AND FAIR PROCESSING:

4.1. Processing Normal Categories of Personal Data iv.

The LGPD also brings the possibly of four other lawful bases (under Article 7 of the LGPD)j in addition to those specified in the GDPR:

i. for carrying out studies by research entities, ensuring, whenever possible, the anonymization of Personal Data;

ii. for the regular exercise of rights in judicial, administrative or arbitration procedures, the last pursuant to Law No. 9,307, of September 23, 1996 (the "Brazilian Arbitration Law"); iii. to protect the health, exclusively, in a procedure carried out by health professionals, health services or sanitary authorities; or iv. for the protection of credit, including as provided in specific legislation.

4.2. The Company must document the legal basis being relied on for each type of processing of Personal Data in a Records of Processing Activities and these must be made transparent to the Data Subjects in an applicable Privacy Notices to ensure the processing is lawful and transparent.

4.3. Processing Special Categories of Personal Data

Some data is considered more sensitive than other data as it can more easily be used to prejudice against an individual. This data is classed as Special Categories of Personal Data; under the LGPD, we must only collect, share and otherwise process this type of data if, in addition to being able to rely on a lawful justification for processing Personal Data we can also satisfy a specific condition (under Article 11 of the LGPD). These means at least one of the following conditions must be met:

a) when the Data Subject or her/his legal representative specifically and distinctly consents, for the specific purposes:

b) without consent from the Data Subject, in the situations when it is indispensable for:

   i. Controller's compliance with a legal or regulatory obligation;

ii. shared processing of data when necessary by the public administration for the execution of public policies provided in laws or regulations;

iii. studies carried out by a research entity, whenever possible ensuring the anonymization of sensitive personal data;

iv. the regular exercise of rights, including in a contract and in a judicial, administrative and arbitration procedure, the last in accordance with the terms of Law No. 9,307, of September 23, 1996 (the "Brazilian Arbitration Law");

v. protecting life or physical safety of the Data Subject or a third party;

vi. to protect the health, exclusively, in a procedure carried out by health professionals, health services or sanitary authorities;

vii. ensuring the prevention of fraud and the safety of the Data Subject, in processes of identification and authentication of registration in electronic systems, respecting

the rights mentioned in Art. 9 of the LGPD and except when fundamental rights and liberties of the Data Subject which require protection of personal data prevail. Note that the LGPD and the GDPR states similar definition of what is a Special Category data.

5. INDIVIDUAL RIGHTS:

5.1. Individual Rights

In addition to the Data Subject GDPR rights, LGPD also guarantees that the Data Subject, at any time and by means of request, has the right to obtain from the Controller the following:

i. anonymization, blocking or deletion of unnecessary or excessive data or data processed in noncompliance with the provisions of the LGPD; ii. deletion of Personal Data processed with the consent of the data subject, except in the situations provided in Art. 16 of the LGPD; and iii. information about public and private entities with which the Controller has shared data.

5.2. Data Subject Access

Data subjects may make subject access requests ("SARs") at any time to find out more about the Personal Data which the Company holds about them, what it is doing with that Personal Data, and why.

Under the LGPD, responses to SARs shall normally be made in a simplified format, immediately or by means of a clear and complete declaration that indicates the origin of the data, the nonexistence of registration, the criteria used and the purpose of the processing, subject to commercial and industrial secrecy, **within fifteen days of receipt**.

If it is impossible to immediately adopt the measure mentioned above, the Company shall send a reply to the Data Subject to communicate that the Company is not the data processing agent and indicate, whenever possible, who the agent is; or indicate the reasons of fact or of law that prevent the immediate adoption of the measure.

ANPD may provide differently regarding the time periods provided for specific sectors.

Information and the data may be provided, at the Data Subject's discretion by electronic means that is safe and suitable for this purpose or in printed form.

When processing originates from the consent of the Data Subject or from a contract, the Data Subject may request a complete electronic copy of her/his personal data, subject to commercial and industrial secrecy, in accordance with regulations of the national authority, in a format that allows its subsequent use, including for other processing operations.

According to LGPD, the Company may not charge a fee for handling any SARs, even in case of additional copies of information.

5.3. Data Protection Officer

The Data Protection Officer's activities under the LGPD consist of:

i. accepting complaints and communications from Data Subjects, providing explanations and adopting measures; ii. receiving communications from ANPD and adopting measures;

iii. orienting entity's employees and contractors regarding practices to be taken in relation to personal data protection; and

iv. carrying out other duties as determined by the Controller or set forth in complementary rules.