Data Protection Policy

EC21 S.A.

Date of application: September 23 2019

Concerns: All staff members

I. Scope

EC21 S.A. (the "**Company**") has set up this data protection policy (the "**Policy**") to comply with Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (the **GDPR** and together with any other applicable national laws and regulations, the **Data Protection Legislation**).

This Policy lays down the principles of Processing Personal Data to ensure that:

- everyone involved in the processing of Personal Data at the Company is fully aware of, and complies with, the requirements of the Data Protection Legislation; and
- Data Subjects will be made aware of their rights under the Data Protection Legislation.

II. Defined terms

The following defined terms are used in this Policy:

- **Board** means the board of directors of the Company;
- **Data Processor** has the meaning set out in clause IX;
- **Data Protection Legislation** has the meaning set out in clause I above;
- **Data Protection Officer** is the compliance officer of the Company;
- **Data Subject** means an identified or identifiable individual whose Personal Data is being Processed;
- **EEA** means the European Economic Area;
- **GDPR** means Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC;
- **Material Change** has the meaning set out in clause XVIII;
- **Material Breach** has the meaning set out in clause XVII;
- **Personal Data** means any information relating to a Data Subject, e.g. a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual;
- **Processing** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

- **Relevant Persons** means (i) directors, authorised persons and shareholders of the Company and (ii) employees and natural persons who are directly involved in the provision of services to the Company; and

- **Sensitive Personal Data** means any Personal Data relating to the racial or ethnic origin of the Data Subject, their political opinions, their religious (or similar) beliefs, their physical or mental health condition, details of criminal offences or criminal convictions (including the commission or alleged commission of any offence, any proceedings for any offence committed or alleged to have been committed and the disposal of such proceedings or the sentence of any court in such proceedings) and genetic and biometric data.

III. General principles

All Relevant Persons and other authorised third parties who have access to any Personal Data held by or on behalf of the Company must adhere to the Policy.

The Company only Processes Personal Data which is directly relevant to its dealings with a given Data Subject. That Personal Data will be Processed in accordance with the Data Protection Legislation and the Policy.

Personal Data collected by the Company is generally collected in order to:

- Ensure that the Company can facilitate efficient transactions with, and perform its obligations and exercise its rights under contracts with, third parties including its customers, partners, associates and affiliates;

- Efficiently manage its employees, contractors, agents and consultants;

- Efficiently and effectively manage its business; and

- Meet all relevant obligations imposed by law.

An explanation of the lawful grounds for which Personal Data may be processed by the Company is provided.

Personal Data may be disclosed within the Company and may be passed from one department to another in accordance with the Data Protection Principles and the Policy and only to those reasonably requiring access to that Personal Data so that they can achieve the purpose for which the Personal Data was collected and is being Processed.

IV. Data protection principles

Any person Processing Personal Data must comply with the following core principles:

- **Lawfulness, fairness and transparency:** Processing must be fair, transparent and lawful. In particular, the Processing must be based on a lawful ground and the Data Subject has been informed of how and why its Personal Data will be Processed upon or before collecting it.

- **Purpose limitation:** Personal Data must be Processed only for specified and lawful purposes and in a manner, which is compatible with those purposes.

- **Data minimisation:** The Personal Data that is processed must be adequate, relevant and limited to the minimum data necessary to achieve the lawful purposes for which it is Processed.

- **Accuracy:** Personal Data must be accurate and, where appropriate, kept up-to-date. Any Personal Data which is incorrect must be rectified as soon as possible.

- **Data retention:** Personal Data must be kept for no longer than is necessary for the lawful purpose for which it is Processed.

- **Rights of Data Subjects:** Data Subjects will have the right to see copies of their Personal Data, have inaccuracies corrected, object to the processing of their Personal Data, withdraw their consent to the Processing or have their Personal Data deleted if it is no longer required by the Company for another important reason.

- **Security:** Personal Data must be protected against unauthorised or unlawful Processing, accidental loss, destruction or damage through appropriate technical and organisational measures.

- **International data transfers:** Personal Data must not be transferred to a country or territory outside of the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the Processing.

- **Accountability:** The Company and its third-party service providers are responsible for and shall demonstrate their compliance with the Policy.

V. Consent

Personal data must only be Processed by the Company if the purpose of the processing satisfies one of the lawful grounds permitted under the Data Protection Legislation. There are various legitimate reasons for which Personal Data can be collected and used. One such reason is that the individual has consented to the use of their data. Other applicable reasons are described in clause VIII.

VI. Processing purposes

This clause describes the lawful grounds for Processing which are most likely to be relevant to the Company's Processing. If anyone Processing is unable to satisfy one of these grounds he should contact the Data Protection Officer.

The legal grounds for Processing non-sensitive Personal Data include:

- Where the Data Subject has given their consent to the Processing;
- Where the Processing is in the Company's legitimate interests and does not cause unwarranted prejudice to the Data Subject;
- Where the Processing is necessary for the performance of a contract to which the Data Subject is a party, or for the taking of steps (at the request of the Data Subject) with a view to entering into an agreement; or
- Where the processing is required by law.

Sensitive Personal Data is subject to stricter legal controls and the circumstances in which it can be processed are more limited than in respect of other Personal Data. The legal grounds for processing sensitive Personal Data include:

- Where the Data Subject has given their explicit consent (note the requirements for valid consent described above and the potential difficulties of getting valid consent in an employment context);
- Where the processing is necessary for the purposes of carrying out the obligations and exercising rights of the Company or the Data Subject in the field of employment law or social security law;
- For the purposes of occupational health or the assessment of the working capacity of an employee;
- For equal opportunity purposes, where the processing is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained (although there is no such legal ground in Luxembourg); or
- Where the Processing is necessary for the purpose of, or in connection with, any legal proceedings, obtaining legal advice, or establishing, exercising or defending legal rights.

VII. High risk processing activities

Wherever the processing of Personal Data is likely to result in a high risk to the Data Subject (for example, where it is particularly intrusive to a Data Subject's privacy), the Company will need to, before carrying out the processing activity, perform an assessment of the potential impact of the intended processing on the rights and freedoms of the Data Subject. The impact assessment should be conducted by the Data Protection Officer.

The monitoring or profiling of Data Subjects, video surveillance of Data Subjects and the processing of sensitive Personal Data on a large scale are examples of processing activities that might present a high-risk.

VIII. Fair processing information

Any forms (whether paper-based or web-based) that gather data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed.

Regardless of how Personal Data is obtained (whether it is obtained from the Data Subject or from a third party), the Data Subject must be provided with certain information about the processing of their Personal Data by the Company. This information must be provided at or before the time at which the Personal Data is collected (or, if the Personal Data is obtained from a third party, within a reasonable time of obtaining the Personal Data or at the time of the first communication with the Data Subject, whichever is earlier).

The information provided to the Data Subject must include the following:

- The identity and contact details of the Company and the Data Protection Officer;
- The categories of Personal Data collected in relation to the Data Subject;
- If the Personal Data is not obtained from the Data Subject, the source of the Personal Data;
- The purpose for which Personal Data will be processed, including the legal ground for the processing. If the legal ground involves legitimate interests, a description of those legitimate interests must also be provided;
- If the Personal Data is processed based on the Data Subject's consent, an explanation of the Data Subject's right to withdraw their consent at any time;
- The categories of Personal Data that may be disclosed to third parties and the reasons for these disclosures;
- If the Processing is a contractual requirement, whether the Data Subject is obliged to provide the Personal Data on that basis, and the possible consequences of a failure to provide the information;
- Any intention to transfer the Personal Data outside the EEA and information about the level of protection that will be afforded to the transferred data (including details of how the legal requirements for the transfer will be satisfied);
- Information about the existence of any automated decision making (for example, profiling) undertaken by the Company based on the Personal Data, including details of the logic involved and its impact on the Data Subject;

- The period for which the Personal Data will be retained, or (if it is not possible to provide a specific time period) the criteria that will be used to determine the retention period;

- A general description of the Company's policies and practices with respect to protecting the confidentiality and security of Personal Data;

- The existence of the Data Subject's rights; and

- Any other information that is necessary to guarantee that the Processing is fair in the circumstances.

This information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language that will be easy for the Data Subject to understand.

If any of the information described above changes after it has been provided to the Data Subject, the Data Subject must be provided with an updated copy of the information.

IX. Third party providers

Where the Company instructs a third party to process Personal Data on behalf of the Company (a "**Data Processor**"), the Data Processor must enter into a written agreement with the Company that:

- Provides details of the Processing that they are being instructed to carry out;

- Requires the Data Processor to process the Personal Data only in accordance with the Company's written instructions and to the extent necessary for them to fulfil their obligations to the Company under the agreement;

- Requires the Data Processor to implement appropriate technical and organisational measures and controls to ensure the confidentiality and security of the Personal Data; and

- Imposes any additional Processing obligations required by law. Guidance on the additional legal obligations that the agreement must include can be obtained from the Data Protection Officer.

The agreement should be approved by the Data Protection Officer and signed by both parties before any Personal Data is transferred to the data processor.

When contracting with a Data Processor, it is important that the Company conduct appropriate due diligence both at the outset of the relationship and on a periodic basis thereafter, to ensure that the Data Processor is capable of complying, and does comply, with the requirements of this clause IX.

X. Disclosure of personal data

The Company must ensure that Personal Data is not disclosed to unauthorised third parties. All staff should exercise caution when asked to disclose any Personal Data to a third party. This does not apply to Data Processors.

Personal Data should not be disclosed orally or in writing to third parties without the consent of the Data Subject and approval from the Data Protection Officer.

In some circumstances, disclosure of Personal Data is permitted without the need to obtain the prior consent of the Data Subject. Such disclosures might (depending on the circumstances) be permitted where this is:

- Necessary to safeguard national security;
- Necessary for the prevention or detection of crime, in the substantial public interest, and where obtaining consent from the Data Subject would prejudice that purpose;
- Necessary for the administration of justice;
- Necessary to comply with applicable law; or
- Necessary to protect the vital interests of the Data Subject (this refers to life and death situations), but only where their consent cannot be obtained.

Requests for Personal Data from third parties must be supported by appropriate paperwork and any disclosures must be approved by the Data Protection Officer.

XI. International transfers of personal data

Specific legal requirements apply to the transfer of Personal Data out of the EEA. The "transfer" of data includes sending data to another country or allowing that data to be accessed remotely in another country, regardless of whether the Company transfers Personal Data outside the EEA itself or a data processor does so when acting on the Company's behalf.

Personal Data must not be transferred outside the EEA unless the recipient country ensures an adequate level of protection for the rights and freedoms of Data Subjects. This requirement can be satisfied by:

- The existence of binding corporate rules (relevant to intra-group transfers only);
- The recipient country having been subject to an "adequacy determination" by the European Commission (to date, only a handful of countries are subject to an adequacy determination, such as Switzerland, Canada and Israel);
- The entry into a data transfer agreement between the Company and the non-EEA recipient of the Personal Data which contains standard contractual clauses that have been approved by the European Commission; or
- Certification of a US recipient under the EU-US Privacy Shield scheme.

Before such a transfer takes place, it must first be checked with the Data Protection Officer to determine whether the transfer is lawful.

XII. Retention and disposal of personal data

Personal Data must not be retained for longer than is necessary for the lawful purposes for which it is processed. To achieve this, each category of Personal Data processed by the Company must be subject to a retention period which can be justified by reference to those lawful grounds. Retention periods must be monitored and, upon their expiry, the relevant Personal Data must be deleted or anonymised (so that it is no longer possible to identify the Data Subject to whom the Personal Data relates).

For example, considerable amounts of Personal Data are collected on employees. However, once an employee has left the Company, it will not be necessary to retain all the information held on them because much of this is only required to administer the employment relationship, such as bank details for salary payments. Some Personal Data will need to be kept for longer periods than others, for example where it is necessary to retain certain records in order for the Company to comply with its legal obligations.

Personal Data must be disposed of securely in a way that protects the rights and privacy of Data Subjects and ensures the permanent erasure of the Personal Data (e.g., shredding, disposal as confidential waste, or secure electronic deletion). Hard drives of redundant Personal Data should be wiped clean before disposal.

XIII. Data protection and data security

The Company shall ensure that all its directors, employees, seconded persons, contractors, agents, consultants, partners and other parties working on behalf of the Company comply with the following when Processing:

- Personal Data, whether held electronically or in paper form, must be kept securely at all times. The Company's staff, consultants and authorised third parties must ensure that appropriate technical and organisational measures are in place to prevent unauthorised or accidental access, use, disclosure, loss or damage when Personal Data is being processed (including but not limited to when it is at rest or in transit). Data security measures are set out in the Company's information security policy. Technical measures, for example, include using encryption tools to protect Personal Data held in electronic form. Organisational measures, for example, include storing paper records containing Personal Data in locked cabinets. It is essential that if Personal Data is lost, damaged, compromised, misdirected or stolen, or otherwise processed in an unauthorised manner, that it is reported as an information security incident. Any breach should be immediately reported to the Data Protection Officer who shall ensure that any additional steps or notifications required under the applicable law are adhered to;

- Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of Personal Data in accordance with clause XIV; and

- Personal Data should not be disclosed except in accordance with clauses XI and XII.

XIV. Data Subject's rights

Data Subjects are entitled to exercise certain rights in respect of their Personal Data. These rights include access to the Personal Data held by the Company about them, the right to require the rectification of their data (where it is incorrect) and in certain circumstances the right to object to the Processing of their Personal Data or to require it to be erased.

Data Subjects have a number of legal rights in relation to their Personal Data. These rights include:

- The right to obtain information regarding the processing of their Personal Data and access to the Personal Data which the Company holds about them (or which is held on the Company's behalf);

- The right to receive a copy of any Personal Data which the Company processes about them, including (in some circumstances) the right to receive Personal Data in a structured, commonly used electronic format and/or request that this Personal Data are transmitted to a third party where this is technically feasible;

- The right to request that the Company rectify their Personal Data if it is inaccurate or incomplete;

- The right to request that the Company erase their Personal Data in certain circumstances. This may include (but is not limited to) circumstances in which:

    - it is no longer necessary for the Company to retain their Personal Data for the purposes for which it was originally collected;
    - the Company is only entitled to process the Data Subject's Personal Data with their consent (i.e. because no other lawful ground for processing the Personal Data applies), and the Data Subject withdraws their consent; and
    - the right to lodge a complaint with the relevant data protection authority, if the Data Subject thinks that any of their rights have been infringed by the Company.

- Keep a look out for any requests by Data Subjects to exercise any of the rights described above. Data controllers are legally obliged to respond to these requests within one month of receiving such a request. Please refer all actual or suspected requests by a Data Subject to exercise any of the rights described above to the Data Protection Officer without delay.

Requests to exercise these rights should be sent to the Data Protection Officer upon receipt.

XV. Recording keeping

Accurate and up to date records of the Processing carried out by the Company must be maintained within the organisation. These records must include:

- Details of the controller and of the Data Protection Officer;
- The purposes of the Processing;
- The categories of Data Subjects and the categories of Personal Data;
- The categories of recipients of Personal Data;
- The categories of transfers of Personal Data to countries outside the EEA;
- The envisaged time limits for erasure of the Personal Data (where possible); and
- A general description of the technical and organizational security measures adopted by the Company.

XVI. Roles and responsibilities

The Board is ultimately responsible for ensuring that the Company meets its legal obligations as applicable.

The Data Protection Officer is responsible for:

- Keeping the Board updated about data protection responsibilities, risks and issues;
- Reviewing all data protection procedures and related policies;
- Arranging data protection training and advice for employees;
- Handling all data protection queries for employees;
- Dealing with all requests from individuals to see the data the Company holds about them (Subject Access Requests); and
- Checking and approving any contracts or agreements with Date Processors.

XVII. Escalation procedure

Where a potential breach of this Policy is identified, the Data Protection Officer must be informed.

The Data Protection Officer, upon receiving a report of a potential breach will assess whether the breach is material (a "**Material Breach**").
Where the breach is a Material Breach, the Data Protection Officer shall inform the Manager who will consider what appropriate action to take.

Where the breach is not a Material Breach the Data Protection Officer may take such steps as the Data Protection Officer considers appropriate.

The Data Protection Officer will maintain a record of all actual and potential breaches received in relation to this Policy.

XVIII. Monitoring and review of this Policy

The quality and appropriateness of the execution arrangements and this Policy will be monitored on an ex-ante and an ex-post basis by the Company and the Data Protection Officer.

Ex-post monitoring: The Company will also review on a regular basis whether this Policy is effective, i.e., whether the processes are applied correctly. In the course of this review a significant event that could impact the lawfulness of the Processing under this Policy shall be considered a Material Change. Where a Material Change has occurred, the Company shall consider making changes to the Policy. The review will be carried out by the Company and the Data Protection Officer.

Review of the Policy: This Policy will be reviewed and amended, if necessary, annually taking into account the results of the above-mentioned monitoring and ad-hoc when the results of the monitoring constitute a Material Change.