(Annex 13)

Data Privacy and Protection Policy

CIRCONTROL, S.A. (hereinafter the Entity) is committed to due diligence and compliance with the Data Protection regulations.

The following notice contains detailed information on the Privacy and Personal Data Protection Policy in compliance with the provisions of Article 13 of Regulation (EU) 2016/679 of the European Parliament and of the Council 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 (**General Data Protection Regulation or GDPR**) and Article 11 of Organic Law 3/2018 of 5 December 2018 on the Protection of Personal Data and Guarantee of Digital Rights (**PDPL GDR**).

Information about the Data Controller and contact details of the Data Protection Officer/Delegate (DPO/DPD):

- **Identity: CIRCONTROL, S.A.**
- **Address/Postcode:** c.Innovació 3. VILADECAVALLS (08232) - SPAIN
- **Phone**: +34 93.736.29.40
- **Email:** jhuguet@circontrol.com
- **DPO/DPD contact details:** Jordi Huguet
- **Channel:** http://www.corporate-ethicline.com/circontrol/

Purpose of the data processing

The Entity will process the information provided by the data subjects for the following purposes:

- **To manage** your attention, visit and meeting at our facilities.
- To manage the provision and performance of contracted **services and products**.
- **To manage any type of request or suggestion** with respect to our professional services submitted to us by data subjects.
- **For informative and commercial communications**: we process your data in order to inform you about activities, articles of interest and general information related to our activity and the services/products contracted.
- **To manage data provided by candidates for a job position** through their Curriculum Vitae (CV) or other means for the purpose of the selection and recruitment process.
- To ensure the safety and security of our offices, facilities and people through **access control, video surveillance systems** and other access control/identification systems.

- **To comply with the legal provisions** that apply to the Entity and its activities in **the areas of health, equality and occupational risk prevention**.
- **To manage and control the operation of the internal mechanisms, policies and protocols** established by the Entity **for regulatory compliance purposes and the management of complaint channels for this purpose**.
- **All the processing that is applicable to us for due compliance with regulations** and official/sectorial requirements **to which our activity is subject**.

The processing of your data for the aforementioned purposes will be carried out in the strictest compliance with the Data Protection regulations and the Policy that we are setting out in detail for the correct purposes and development of your attention, and for the management of the aforementioned purposes. You may exercise your rights at any time (see specific section).

Data storage criteria

- **Management of services/products contracted with the Entity**: the personal data provided in service contracts, offers and/or proposals, as well as those of other persons whose intervention is necessary, will be retained for as long as the contracted services are in force. At the end of the provision of the contracted service(s), the personal data will be retained in the cases that could result in liabilities with the Entity and/or in compliance with other regulatory frameworks applicable to the Entity or a regulation with the rank of law that requires their conservation. Personal data will be kept in a way that allows the identification and exercise of the rights of those affected and in compliance with the legal and organisational technical measures necessary to ensure their confidentiality and integrity.
- **Curriculum Vitae management**: As a general rule, the Entity keeps your Curriculum Vitae for a maximum period of one year. At the end of this period, the data will be automatically destroyed, in compliance with the principle of data quality.
- **Management of employment contracts:** personal data will be kept, in any case, during the time that the employment relationship is in force and, at the end of it, in cases that could result in liabilities between the parties and when required by a regulation with the rank of law.
- **Others:** the rest of the data and information provided by the user by any means will be kept for as long as necessary to fulfil the purpose for which they were collected.

Legitimisation
The legal basis that enables the Entity to process the personal data of users, customers and/or potential customers under the following titles:

- The consent of the data subjects for the processing and management of any request for information or inquiry about our services and products.
- Consent given by job applicants for recruitment and selection purposes.
- The framework for the provision and/or contracting of services/products with the Entity.
- Legitimate interest in sending you informative, commercial and/or promotional offers related to the activity of the Entity and the services/products contracted via email or any other means.
- Compliance with legal obligations and internal regulatory compliance procedures.
- Legitimate interest in ensuring the safety of offices, facilities and people.

Recipients
Personal data are not transferred to third parties, except by legal order.

Origin
Personal data is obtained directly from the data subjects and from our partners. The categories of personal data provided to us are:

- Identification data.
- Postal or email addresses.
- Data provided and/or consented by the data subjects themselves related to and necessary for the management and performance of the requested service/product.

Rights
Right of access, rectification and deletion: data subjects have the right to obtain confirmation as to whether or not the Entity is processing personal data concerning them. Data subjects have the right to access their personal data, as well as to request the rectification of inaccurate data or request its deletion when, among other reasons, the data is no longer necessary for the purposes for which it was collected.
Right to limitation and opposition: in certain circumstances, the data subjects may request the limitation of the processing of their data, in which case we will only keep them for the exercise or defence of claims. In certain circumstances, for reasons related to their specific situation, data subjects may oppose the processing of their data. The Entity will stop processing the data in this case, except for imperative legitimate reasons, or for the exercise or defence of possible claims.

Right to revoke the consent given: data subjects have the right to withdraw their consent at any time, except in the case of processing of personal data provided for in the Data Protection regulations or necessary for the provision of the contracted service, which do not require such consent. However, this withdrawal does not have retroactive effects, so it will not affect the lawfulness of the processing based on previously granted consent.
These rights may be exercised in our Channel (see specific section).

Security and control measures
General
In compliance with data protection regulations, the Entity shall process personal data by applying the appropriate technical, legal, organisational and security measures in order to guarantee the confidentiality and integrity of the information it manages in accordance with the provisions of the regulations in force.
Please inform the Data Protection Officer/Delegate through the contact details/Channel established in this Privacy Policy of any security risk of which you have evidence or knowledge, and which may compromise the integrity and confidentiality of personal data and/or confidential information, in order to allow for the necessary measures to be taken to prevent unauthorised processing, loss, destruction or accidental damage.

Cybersecurity
As a specific and complementary concept to the above, the Entity applies cybersecurity measures to prevent and manage possible attacks and fraud by cybercriminals that threaten the privacy and protection of the data that our Entity processes and accesses in the scope of its activities and operations.
In this sense, we would like to warn you that, in the event of possible risk situations due to communications whose content and/or format generate doubts of authenticity, we recommend omitting them and contacting the Data Protection Officer/Delegate using the contact details indicated in this Privacy Policy.
Likewise, any requests you receive from our Entity regarding changes in payment methods, requests for contact details, contact persons, confidential (non-public) information, bank and/or credit card details and/or other official data, must not be fulfilled without direct confirmation from our Entity by an alternative means. We appreciate and require your cooperation with the communication and reporting of any notification in relation to this type of requests and other possible situations of risk of cyber-attacks in which our Entity may be used, as well as any possible security risks that you may be aware of.

Channel

The Entity has implemented a Channel to ensure the highest levels of commitment, rigour and professionalism in terms of security, experience, independence and knowledge in the processing of the communications received.

The Channel, which includes use in the field of Data Protection, has been implemented through a web platform. It has been developed and is managed by an independent external expert to provide and guarantee our aforementioned commitments.

Through the Channel, **you may communicate and process** the exercise of your **Rights** (see previous section) and disclose any indication or knowledge you may have of **possible security breaches, cyber-attacks** and/or **possible breaches or irregularities regarding the Data Protection regulations and this Policy**.

The data to access the Channel are detailed at the beginning of this Policy.

Supervisory authority

In the event of a disagreement with the Entity regarding the processing of your data, you have the right to lodge a complaint with the relevant Data Protection Supervisory Authority. In Spain, this authority is the Spanish Data Protection Agency (www.aepd.es).

Attention and support

Data subjects may communicate any questions regarding the processing of their personal data or the interpretation of our Policy to the Entity by contacting the Data Protection Officer/Delegate (DPO/DPD) at the address indicated at the beginning of this Policy.