This notice is intended to inform you about the processing of the personal data that you voluntarily provide, in compliance with the applicable personal data protection legislation. This notice is provided pursuant to the European General Data Protection Regulation (also referred to as the **"GDPR"**) and the applicable Italian legislation (hereinafter collectively referred to as the **"Applicable Legislation"**).
This notice may be amended, supplemented and/or updated, including as a result of changes to the applicable personal data protection legislation.

1. Data Controller.

The Data Controller is Alps Blockchain S.p.A., with registered office at Vicolo Liceo 1, 38122 Trento (TN), Italy, Italian tax code and VAT number 02515120224, Trento Economic and Administrative Index (REA) no. TN-230317 (hereinafter also the **"Data Controller"** or simply the **"Controller"**).
For any clarification or information, or to exercise the rights set out in this Privacy Notice, the Data Controller may be contacted at the following details: tel. +39 333 2663836, email: amministrazione@alpsblockchain.com, certified email (PEC): info@pec.alpsblockchain.com.

2. Personal data processed.

When an application is submitted, the personal data voluntarily included by the candidate in their *curriculum vitae* or in other documents provided (for example, a cover letter), including identification and contact data and information relating to educational qualifications and professional experience, or disclosed to the Data Controller by third parties expressly authorised by the candidate, will be collected for the purpose of selecting personnel suitable for the positions available with the Data Controller (hereinafter collectively, the **"Data"**).
Candidates are requested not to include in those documents any data revealing their health status, racial or ethnic origin, religious beliefs, political opinions, sex life, or any other information qualifying as special-category data under Article 9 of the GDPR. Any special-category data provided by the data subject will be deleted immediately unless accompanied by a written declaration of consent to its processing under Article 9(2)(a) of the GDPR. In any event, where explicit consent has been given, any special-category data provided will be processed by the Data Controller only where strictly necessary for the recruitment process (for example, to establish whether the candidate belongs to a protected category). Data subjects are also requested not to disclose data relating to criminal convictions and offences, as defined by the legislation in force. Any such data provided by the data subject will be deleted immediately.

3. Purposes and legal bases of processing.

In view of the above, the Data will be processed for the purposes and on the legal bases set out below.

	PURPOSE	LEGAL BASIS
a.	The Data will be processed by the Data Controller to respond to specific requests from the candidate and to carry out activities preparatory and functional to establishing an employment and/or collaboration relationship. These include, by way of example, receiving and recording the candidate's *curriculum vitae* in the Data Controller's databases; assessing the information contained in the candidate's *curriculum vitae* to determine their potential suitability for an employment relationship with the Data Controller; arranging interviews; and carrying out related formalities.	The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the data subject's request prior to entering into a contract [Article 6(1)(b) GDPR]. Where the candidate voluntarily includes special-category data in their CV, the legal basis for processing is the data subject's explicit consent, provided at the same time (for example, by including it at the end of the CV or

		in the body of the accompanying email) [Article 9(2)(a) GDPR].

4. Data retention period.

The Data Controller will retain the Data for the time necessary to fulfil the purposes of the processing, in accordance with the storage-limitation principle. More specifically, the Data Controller retains:

- the Data (including *curricula vitae*) processed for the purposes specified in point a. of the preceding table, where the application is submitted in response to a specific vacancy, only for the period necessary to select a candidate for that vacancy and, in any event, for no longer than 36 months after receipt of the application. In the case of an unsolicited application (or the general submission of a *curriculum vitae* at the company's premises without responding to any specific vacancy), the Data (including *curricula vitae*) will be processed for 36 months after receipt, during which time the Data Controller may use them to contact the candidate about positions considered compatible with their profile. At the end of this retention period, the Data will be deleted unless the candidate has been selected for the position.

5. Nature of the provision of Data.

The provision of Data is optional. However, any refusal to provide all or part of the Data may make it impossible for the Data Controller to respond to the candidate's requests and/or assess the application. The inclusion of special-category data in the curriculum vitae is always optional and is not solicited. Such data will be considered solely to establish whether the candidate belongs to a protected category. Failure to provide such data will therefore have no consequences, except that it will not be possible to establish whether the candidate belongs to a protected category.

6. Methods of processing the Data.

The Data will be processed manually and/or by electronic means in accordance with the principles of lawfulness, purpose limitation, data minimisation and storage limitation, using appropriate technical and organisational security measures to protect the Data against unauthorised or unlawful access, destruction, and accidental loss of integrity or confidentiality.

For recruitment purposes, the Data Controller does not use automated decision-making or monitoring systems. In carrying out internal management and organisational activities, the Data Controller may use artificial intelligence tools to support its processes. These tools operate under the constant supervision of authorised personnel and are never used to make decisions based solely on automated processing that produce legal effects concerning the data subject or similarly significantly affect them. The Data are therefore not subject to any fully automated decision-making process or profiling within the meaning of Article 22 of the GDPR.

7. Recipients of the Data.

The processing is carried out by personnel of the Data Controller who are specifically authorised on the basis of their respective duties, as well as by processors specifically appointed in writing, within the scope of their respective functions and in accordance with the Data Controller's instructions. Appropriate measures are used to ensure the security and confidentiality of the processed Data. A list of processors is available upon request.

The Data may also be disclosed to the following categories of recipients:

- recruitment agencies, bodies and temporary-employment companies;
- companies or professionals engaged in the judicial or out-of-court protection of the Data Controller's rights;
- persons, entities or public authorities to which the Data must be disclosed, in their capacity as independent data controllers, pursuant to a legal provision or an order issued by those authorities.

8. **Transfers to third countries or international organisations.**

The Data are processed within the European Economic Area (EEA). The Data Controller does not transfer the Data to third countries or international organisations. Should a transfer outside the EEA become necessary for technical or organisational reasons, it will take place only to countries ensuring an adequate level of protection under Article 45 of the GDPR or subject to appropriate safeguards under Article 46 of the GDPR (in particular, standard contractual clauses adopted by the European Commission). The data subject may obtain a copy of those safeguards by contacting the Data Controller at the details provided above. **Rights of the data subject.**

The individual to whom the Data relate, in their capacity as data subject, may exercise the rights listed below by submitting a request to the Data Controller using the contact details provided in paragraph 1 above:

- obtain confirmation as to whether or not personal data concerning them are being processed and, where that is the case, obtain access to the data and relevant information, together with a copy of the personal data undergoing processing;
- request and obtain the updating of personal data, the rectification of inaccurate data or the completion of incomplete data;
- request and obtain the erasure of personal data where: a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; b) the data subject objects to processing based on the Data Controller's legitimate interests and there are no overriding legitimate grounds for continuing the processing; c) the data have been unlawfully processed; or d) the Data Controller is required to erase the data in order to comply with a legal obligation;
- request and obtain restriction of processing where: a) the accuracy of the data is contested, for the period required by the Data Controller to carry out the necessary checks; b) the Data Controller's processing is unlawful and the data subject opposes erasure and requests restriction of their use instead; c) the data are required by the data subject for the establishment, exercise or defence of a legal claim, although the Data Controller no longer needs them for processing purposes; or d) verification is pending as to whether the Data Controller's legitimate grounds override those of the data subject;
- where data have been rectified or erased or processing has been restricted, have such rectification, erasure or restriction communicated to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort;
- where processing is based on a contract and carried out by automated means, request and receive the personal data concerning them in a structured, commonly used and machine-readable format and, where technically feasible, have those data transmitted directly by the Data Controller to another controller;
- object, in whole or in part, on legitimate grounds relating to their particular situation, to the processing of personal data concerning them, even where relevant to the purpose of collection;
- where processing is based on the data subject's consent, withdraw consent at any time, easily and without impediment, using, where possible, the same channels used to give consent;
- lodge a complaint with the Italian Data Protection Authority under Article 77 of the GDPR or seek an appropriate judicial remedy if they consider that the processing of personal data concerning them infringes the GDPR. The Italian Data Protection Authority is located at Piazza Monte Citorio 121,

Rome, Italy; fax: (+39) 06 69677 3785; telephone: (+39) 06 696771; email: garante@gpdp.it; certified email (PEC): protocollo@pec.gpdp.it.