

## PRIVACY POLICY

### 1. DEFINITIONS

- 1.1. **Controller** – AmRest Holdings, SE with its registered seat in Madrid, Paseo de la Castellana 163, 28046 Madrid, Spain.
- 1.2. **Personal Data** – any information about a natural person, identified or identifiable by one or several factors defining his/her physical, physiological, genetic, psychic, economic, cultural or social identity, including the IP of the device, location data, online identifier and information collected through cookie files and other similar technologies.
- 1.3. **Policy** – this Privacy Policy.
- 1.4. **GDPR** – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC.
- 1.5. **Website** – an online service run by the Controller at the address <https://www.amrestcsr.com>
- 1.6. **User** – any natural person visiting the Website or using one or more services or functionalities described in the Policy.

### 2. DATA PROCESSING IN CONNECTION WITH THE USE OF THE WEBSITE

- 2.1. In connection with the User's use of the website, the Controller collects data with the scope necessary to provide its respective services and collects information about the User's activity on the Website. The detailed rules and purposes of processing the personal data collected during the use of the Website by the User are described below.

### 3. PURPOSES AND LEGAL BASIS OF DATA PROCESSING AT THE WEBSITE

#### USE OF THE WEBSITE

- 3.1. Personal data of all the persons using the Website (including the IP address or other identifiers and information collected through cookie files and other similar technologies) who are not registered Users (i.e. persons with no profile on the Website) are processed by the Controller:
  - 3.1.1. to provide services electronically to provide Users with an access to the content collected on the Website – in this case, the legal basis for the processing is that processing is necessary for the performance of a contract (Article 6(1)(b) of GDPR);
  - 3.1.2. to determine and pursue possible claims or defend against claims – the legal basis for the processing is the legitimate interest pursued by the Controller (Article 6(1)(f) of GDPR) to protect its rights.

## 4. PERIOD OF PERSONAL DATA PROCESSING

- 4.1. The period of data processing by the Controller depends on the type of provided service and the purpose of the processing. In principle, data are processed for the entire period of providing the service or fulfilling a purchase order until the moment of withdrawing consent or filing an effective objection to the data processing in the cases where the legal basis for the processing is the Controller's legitimate interest.
- 4.2. The data processing period may be extended if processing is necessary to determine and pursue possible claims or defend against claims and, after that time, only when and to the extent required by law. After the elapse of the processing period, the data are irreversibly deleted and anonymized.

## 5. RIGHTS CONNECTED WITH PERSONAL DATA PROCESSING

### RIGHTS OF USERS

- 5.1. The users have the following rights:
  - 5.1.1. **right to information on personal data processing** – on that basis, the Controller provides the person making the request with information about data processing, including first of all about the purposes and legal grounds for the processing, the scope of the data held, entities to which they are disclosed and the planned date for deleting the data;
  - 5.1.2. **right of Access or the right to receive a copy of the data** – on that basis, the Controller provides a copy of the data processed to a person making the request;
  - 5.1.3. **right to rectification** – the Controller is obligated to remove any non-compliance or errors in personal data processed and supplement them if they are incomplete;
  - 5.1.4. **right to erasure** – on that basis, one may demand deleting the data whose processing is no longer necessary to achieve any of the purposes for which they were collected;
  - 5.1.5. **right to restriction of the processing** – if such a request is made, the Controller stops performing any operations on the personal data except for those to which the data subject has given consent and except storing them in accordance with the adopted retention rules or until the reasons for restricting the processing disappear (e.g. the supervisory authority issues a decision permitting further data processing);
  - 5.1.6. **right to data portability** – on this basis, to the extent that the data are processed in connection with an executed contract or given consent, the Controller delivers the data provided by the data subject in a machine-readable format. Is it also allowed to request that the data are transmitted to another entity on condition, though, that both the Controller and the other entity have the technical capabilities to do so;
  - 5.1.7. **right to object to personal data processing for marketing purposes** – the user has the right to object at any time to personal data processing for marketing purposes without the obligation to justify such an objection;
  - 5.1.8. **right to object to data processing for other purposes** – the user may object at any time to personal data processing carried out on the basis of the Controller's legitimate interest (e.g. for analytical or statistical purposes or for reasons connected with protecting property);
  - 5.1.9. **right to withdraw consent** – if data are processed on the basis of a given consent, the user may withdraw it at any time, which does not have, however, any effect on the lawfulness of processing based on consent before its withdrawal.

**5.1.10. right to lodge a complaint before the competent Supervisory Authority** – if the user believes that the personal data processing breaches the provisions of GDPR or other personal data protection regulations, the data subject has the right to lodge a complaint before the competent Supervisory Authority

## **NOTIFICATION OF REQUESTS ASSOCIATED WITH EXERCISING THE RIGHTS**

**5.2.** A request about exercising the rights of users may be filed:

**5.2.1.** by letter to the address: AmRest Holdings, SE with its registered seat in Madrid, Paseo de la Castellana 163, 28046 Madrid, Spain.

**5.2.2.** by e-mail to the address: [gdpr.amrestholdings@amrest.eu](mailto:gdpr.amrestholdings@amrest.eu)

**5.3.** If the Controller is unable to identify the person filing a request on the basis of the notification made, the Controller will ask the petitioner for additional information. Provision of such data is not mandatory, however failure to provide them will result in a request recognition refusal.

**5.4.** The request may be filed in person or through an attorney-in-fact (e.g. a family member). In view of data security, the Controller encourages data subjects to use a power-of-attorney in the form certified by a notary public or an authorized legal counsel or attorney-at-law, which will significantly accelerate verification of the request's authenticity.

**5.5.** A reply to the request should be provided within one month of its receipt. If it is necessary to extend the deadline, the Controller shall inform the applicant about reasons for the delay.

**5.6.** Where the application is submitted to the Controller electronically, the response is given in the same form unless the applicant requests otherwise. In all other cases the response is given in writing. When the deadline for exercising the request makes it impossible to reply in writing and the applicant's data processed by the Controller allow for contact by electronic means, the response should be provided electronically.

## **RULES OF CHARGING FEES**

**5.7.** The proceeding concerning filed requests is free of charge. Fees may be charged only if:

**5.7.1.** Making requests by the same person that are excessive (e.g. extremely frequent ones) or manifestly unfounded; in such a case, the Controller may demand that fees are paid in the amount of 10 euro.

The above fee includes costs of carrying on communication and costs connected with taking requested actions.

**5.8.** If the data subject challenges the decision to charge fees, the person may lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes the GDPR. In Spain the competent Supervisory Authority is the AEPD ("*Agencia Española de Protección de Datos*").

## **6. DATA RECIPIENTS**

**6.1.** In connection with the implementation of services, Personal Data will be disclosed to external entities, including in particular suppliers responsible for the operation of IT systems, for the provision of website hosting and support services and entities associated with the Controller, including companies from its capital group, for the management of intragroup processes.

- 6.2.** The Controller reserves the right to disclose selected information items referring to the User to relevant authorities or third parties which will demand that they are provided such information pursuant to an appropriate legal basis and in compliance with prevailing laws.

## **7. TRANSFER OF DATA OUTSIDE THE EEA**

- 7.1.** The level of personal data protection outside the European Economic Area (EEA) differs from that guaranteed by the European law. For this reason, the Controller may transmit personal data to places outside the EEA, only when necessary and in any case, after ensuring an adequate protection level, mainly by:

**7.1.1.** cooperating with personal data processors in the states with respect to which a relevant decision of adequacy has been issued by the European Commission;

**7.1.2.** under application of standard contractual clauses issued by the European Commission, which shall include, if applicable, supplementary measures to ensure the protection of the data in the territory into which the personal data will be imported;

- 7.2.** At the data collection stage, the Controller will always inform the User of its intention to transfer personal data outside the EEA.

## **8. PERSONAL DATA SECURITY**

- 8.1.** The Controller conducts an ongoing risk analysis to ensure that personal data are processed in a secure manner, guaranteeing first of all that access to the data is provided only to authorized persons and only to the extent necessary for them to perform their tasks. The Controller makes sure that any operations on personal data are recorded and performed only by authorized employees or collaborators.
- 8.2.** The Controller takes any necessary actions so that also its subcontractors and other cooperating entities guaranteed the application of appropriate security measures in each case when they process personal data on the Controller's behalf.

## **9. CONTACT DATA**

- 9.1.** The Controller may be contacted by e-mail [gdpr.amrestholdings@amrest.eu](mailto:gdpr.amrestholdings@amrest.eu) or by letter sent to the mailing address.

## **10. AMENDMENTS TO THE PRIVACY POLICY**

- 10.1.** The policy is verified on an ongoing basis and updated when needed.