Article 1 – Data Controller

The joint Data Controllers are:

- **"Swipe S.r.l."**, with registered office at Via Sclafani 40B, 95024 Acireale (CT), VAT No. 06009700870, Email: privacy@swiperest.com, Certified Email (PEC): swipe@pec.it, owner of the Swiperest platform, registered with the Companies Register of the Chamber of Commerce of South East Sicily;
- **"Treezor SA"**, a simplified joint-stock company incorporated under French law, registered with the Paris Trade and Companies Register under number 807 465 059, with registered office at 33 avenue de Wagram, 75017 Paris, accredited as an electronic money institution (CIB: 16798), authorized to provide payment services.

The Joint Controllers inform you that your personal data will be processed in full compliance with applicable legislation and solely for the purposes and in the manner set out below, in accordance with the principles of personal data protection established by Regulation (EU) 2016/679 (GDPR).

Article 2 – Methods and Purposes of data Processing

We inform you that your data will be processed using the following means:

- Electronic form or by means of computerized or automated tools for the following purposes:
  - Compliance with legal and contractual obligations;
  - Use of services offered by Swipe S.r.l. (interactive and personalized advertising services with a reward mechanism through the allocation of reward points convertible into money);
  - Use of services offered by Treezor SA (opening of a digital payment account, management of the fund transfer system, issuance of a virtual or physical debit card, management of payment statements and related authorizations or limitations);
  - Administrative and accounting purposes related to service agreements;
  - Compliance with obligations arising from laws, regulations, EU legislation, and provisions issued by authorities legally empowered to do so or by supervisory and control bodies.

The provision of data is required by legal and contractual obligations; therefore, refusal to provide such data, in whole or in part, may result in the inability to provide the requested services.

Article 3 – Personal Data Subject to processing

The personal data subject to processing include identification and contact data provided by you, such as, by way of example and not limitation: first name, last name, date and place of birth, city of residence, email address, spoken language, education level, employment, marital status, OTP, and password.

Article 4 – Processing Methods

The processing of your personal data will be carried out in accordance with the principles of fairness, lawfulness, transparency, and protection of your confidentiality and rights. Processing will be carried out both electronically and in paper form. Your data will be collected and stored in both electronic databases and paper archives. Processing will be carried out by implementing appropriate security measures to safeguard the confidentiality, integrity, and completeness of the data processed, pursuant to Article 32 of the GDPR and in accordance with the instructions provided by the Joint Controllers.

Article 5 - Data Security

Your personal data will be processed using automated tools for the time strictly necessary to achieve the purposes for which they were collected, in compliance with the principles of necessity and proportionality, avoiding the processing of personal data where operations can be performed using anonymous data or other methods.We have adopted specific security measures to prevent data loss, unlawful or improper use, and unauthorized access.

Article 6 – Legal Basis

The Company processes optional user data based on consent, given through explicit acceptance of this Privacy Policy and in relation to the purposes and methods described herein. The lawfulness of the processing carried out by the Data Controllers is

ensured pursuant to Article 6(1)(a), (b), and (c) of the General Data Protection Regulation.

Article 7 – Categories of Recipients

Without prejudice to communications carried out in compliance with legal and contractual obligations, all collected and processed data may be communicated exclusively for the purposes indicated above to the following categories:

- Public or private entities to whom communication is required or permitted by law or necessary for the performance of obligations;
- Data Processors (entities supporting the organization in the provision of services);
- Authorized Persons (employees and collaborators).

Data will not be disclosed to unspecified parties through making them available or accessible.

Article 8 – Duration of Processing

Data will be retained for the period strictly necessary to achieve the purposes for which they were collected, in accordance with the principles of data minimization, storage limitation, and rational archive management. For processing based on consent, data will be retained until consent is withdrawn. If the data subject considers that the purpose of processing has been fulfilled, they may exercise their rights by submitting a formal request to the indicated address.

Article 9 – Retention Period

Data required for contractual and accounting purposes shall be retained for the time necessary to manage the commercial and accounting relationship. Where retention is no longer justified, data will be immediately deleted or anonymized. In any case, data processed for commercial communications will be retained for a maximum of 5 years, after which, unless otherwise agreed, they will be deleted or anonymized. If deletion is not possible (for example, because data are stored in backup archives), they will be securely retained, anonymized, and excluded from further processing until deletion.

Article 10 – Data Subject Rights

Pursuant to Regulation (EU) 2016/679 (GDPR) and applicable national legislation, the data subject may, within the limits and under the conditions set out by current law, exercise the following rights:

- **Article 15 – Right of Access:** the right to obtain from the data controller confirmation as to whether or not personal data concerning them are being processed;
- **Article 16 – Right to Rectification:** the right to obtain from the data controller the rectification of inaccurate personal data concerning them;
- **Article 17 – Right to Erasure ("Right to be Forgotten"):** the right to obtain from the data controller the erasure of personal data concerning them;
- **Article 18 – Right to Restriction of Processing:** the right to obtain from the data controller restriction of processing where the accuracy of the personal data is contested, where the processing is unlawful, or where the data subject has objected to the processing;
- **Article 19 – Right to Notification:** the right to receive from the data controller notification in the event of rectification or erasure of personal data or restriction of processing;
- **Article 20 – Right to Data Portability:** the right to receive personal data concerning them from a data controller in a structured, commonly used and machine-readable format, and to transmit those data to another data controller without hindrance;
- **Article 21 – Right to Object:** the right to object at any time to the processing of personal data, including processing for direct marketing purposes;
- **Article 22 – Automated Individual Decision-Making, including Profiling:** the right not to be subject to a decision based solely on automated processing, including profiling.

Requests must be submitted to: **Swipe S.r.l.**, Via Sclafani 40B
95024 Acireale (CT), Email: privacy@swiperest.com, Certified Email (PEC): swipe@pec.it.

These rights may also be exercised by writing to Dr. Andrea D'Urso, acting as DPO (Data Protection Officer), at privacy@swiperest.com.

Without prejudice to any other administrative or judicial remedy, the User also has the right to lodge a complaint with the Italian Data Protection Authority (Garante per la Protezione dei Dati Personali – www.garanteprivacy.it) if they believe that their personal data protection rights have been violated.

Article 11 – Data Transfer

Personal data are stored on servers located within the European Union. However, the Data Controller reserves the right, where necessary, to transfer servers outside the EU. In such case, the Data Controller ensures that any transfer of data outside the EU will be carried out in compliance with applicable legal provisions, including through the adoption of Standard Contractual Clauses approved by the European Commission and the implementation of Binding Corporate Rules for intra-group transfers.