Personal Data Protection Policy

This Policy describes the procedures implemented and respected by the Company SOTACIB, headquartered at Immeuble Alysse, Angle de la rue du Lac Tanganyika et le passage du Lac Neusiedl, Les Berges du Lac, 1053, Tunis, hereinafter referred to as "The Company" in the context of personal data processing and their protection as a data controller.

The Company aims to build a relationship based on trust and mutual interest with its employees, customers, suppliers, subcontractors, and any other persons concerned by the processing of personal data. Consequently, the Company is determined to protect their personal data and privacy.

The term "personal data" corresponds to the definition given by Article 4 of the Organic Law 2004-63 of July 27, 2004, on the protection of personal data, namely "all information regardless of its origin or form that allows directly or indirectly to identify a natural person or makes them identifiable, except for information related to public life or considered as such by law."

The term "processing" means as given by Article 5 of the aforementioned law: "operations carried out in an automated or manual manner by a natural or legal person, which aim, in particular, to collect, record, store, organize, modify, exploit, use, send, distribute, disseminate, destroy, or consult personal data, as well as any operations related to the exploitation of databases, indexes, directories, files, or interconnection."

1. Scope of the Policy:

The Company applies this policy to its:

- Employees;
- Directors;
- Visitors;
- Suppliers;
- Customers;
- Subcontractors;
- Users of the Company's website;
- And to any other person authorizing the Company to process their data.

2. Personal data processed:

The Company collects only the personal data necessary to carry out its activity and legitimate business objectives. It may collect and process the following personal data:

- Personal information such as name and surname, home address, phone number, ID card number, email address, etc.;

- Information about family and social status such as data necessary for the granting of social benefits or other personal advantages, including data on beneficiaries and dependents;
- Information on academic training (school and university curriculum, professional background, etc.);
- Information related to employment and recruitment (resume, professional certificates, internship certificates, etc.);
- Financial information (salary, social benefits, bank accounts, loans granted, etc.);
- Health-related information (medical questionnaire during recruitment, medical files and reports for social security and health insurance purposes, etc.);
- Video surveillance data collected within the Company's premises;
- Biometric data collected during employee check-in within the Company's premises;
- Geolocation data as part of employment.

3. Principles of personal data processing:

All personal data processing carried out by the Company complies with the national regulations applicable in Tunisia regarding the protection of personal data, particularly the provisions of Organic Law No. 2004-63 of July 27, 2004, on the protection of personal data.

The Company is committed to respecting the applicable regulations for all personal data processing operations it implements.

More specifically, it commits to respecting the following principles:

- Personal data is processed transparently, fairly, and with respect for human dignity.
- Personal data is processed with respect for privacy and public freedoms.
- Personal data is collected for specific, explicit, and legitimate purposes and only as necessary for the purposes for which they were collected.
- Personal data is stored adequately, relevantly, and is limited to what is necessary for the purposes for which it is processed.
- Personal data is kept up-to-date, and all reasonable measures are taken to ensure that inaccurate data, considering the purposes for which it is processed, is erased or rectified without delay.

4. Security of processed personal data:

The Company implements appropriate technical and organizational measures to ensure a level of security suitable to the risk inherent in its processing operations, preserving the security of personal data and, in particular, preventing any destruction, loss, alteration, disclosure, intrusion, or unauthorized access to such data, accidentally or unlawfully.

Furthermore, the Company commits to:

- Preventing the equipment and installations used in the processing of personal data from being placed in conditions or locations allowing unauthorized persons to access them;
- Preventing data media from being read, copied, modified, or moved by unauthorized persons;
- Preventing unauthorized introduction of any data into the information system, as well as any knowledge, erasure, or deletion of recorded data;
- Preventing the information processing system from being used by unauthorized persons;
- Ensuring that the identity of persons who have accessed the information system, the data entered into the system, the moment of entry, and the person who performed it can be verified afterwards;
- Preventing data from being read, copied, modified, erased, or deleted during their communication or transport;
- Backing up data by creating secure backup copies.

5. Data retention period:

The Company commits to retaining personal data for no longer than necessary for the purposes for which it is processed, in accordance with the regulations in force and the authorizations granted by the National Authority for the Protection of Personal Data.

6. Subcontracting:

When the Company entrusts certain processing operations or their entirety to third parties under a subcontracting contract, it commits to carefully selecting the subcontractor. The subcontractor must comply with the provisions of this policy, as well as the regulations in force, and must act only within the limits authorized by the Company. The subcontractor must also have all the necessary and appropriate technical means to carry out its assigned tasks. The Company and the subcontractor shall be civilly liable in case of violation of the provisions of this policy.

7. Use of personal data:

Personal data may be processed and/or transferred abroad for the following purposes:

- Human resources management: recruitment, employment, administration of benefit programs, salary management, training, performance management and promotion planning, risk management, and personnel protection, etc.;
- Insurance or tax requirements;
- In the context of monitoring and managing received complaints;

- Declarations made to the State and any public establishment or public authority entitled to require the presentation of certain data;
- Legal or regulatory purposes.

8. Transfer of personal data:

The Company may share and transfer personal data with third parties for business needs or in the context of subcontracting contracts involving the processing of personal data.

The Company may share and transfer personal data abroad with the Parent Company, as well as the group's subsidiaries.

Similarly, the Company may transfer personal data when required by law or compelled by a subpoena or court order.

9. Rights of data subjects:

The Company informs individuals concerned by the processing of personal data that they have the following rights:

- Right of access: the right granted to the data subject, their heirs, or their guardian to consult all personal data concerning them, as well as the right to correct, complete, rectify, update, modify, clarify, or erase them when they are inaccurate, ambiguous, or their processing is prohibited. The right of access also includes the right to obtain a copy of the data in a clear language and consistent with the content of the records, and in an intelligible form when processed using automated methods.

The Company provides the address of the headquarters indicated at the top of this document for any access request.

- Right to object: The data subject, their heirs, or their guardian have the right to object at any time to the processing of personal data concerning them for valid, legitimate, and serious reasons, except in cases where processing is provided by law or required by the nature of the obligation.

The Company provides the address of the headquarters indicated at the top of this document for any objections.

In case individuals concerned by the processing of personal data are not satisfied with the responses received after opposition, they can file a complaint with the National Authority for the Protection of Personal Data.