

Personal Data Protection Policy

This Policy describes the procedures implemented and adhered to by the Company SOTACIB KAIROUAN, whose registered office is located 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 operations and their protection as the data controller.

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

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

Processing is understood in the sense given by Article 5 of the aforementioned law:

"operations carried out in an automated or manual manner by a natural or legal person, aimed in particular at the collection, recording, storage, organization, modification, exploitation, use, dispatch, distribution, dissemination, or destruction or consultation of 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;
- Clients;
- Subcontractors;
- Users of the Company's website;

And any other person authorizing the Company to process their data.

2. Personal Data Processed:

The Company collects only the personal data necessary for its business activities and legitimate commercial purposes. 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 on family and social status such as data necessary for the allocation of social or other personal benefits, including data on beneficiaries and dependents;
- Information on academic background (educational and professional background, etc.);
- Employment and recruitment information (resume, professional certificates, internship certificates, etc.);
- Financial information (salary, social benefits, bank accounts, granted loans, etc.);
- Health information (medical questionnaire during recruitment, medical records and reports for social security and health insurance purposes, etc.);
- Video surveillance data collected within the Company's premises;
- Biometric data collected during employee attendance in the Company's premises;
- Geolocation data in the context of job performance.

3. Principles of Personal Data Processing:

All personal data processing operations implemented by the Company comply with the applicable national regulations in Tunisia regarding personal data protection, notably the provisions of Organic Law No. 2004-63 of July 27, 2004, on the protection of personal data.

The Company is committed to complying with the applicable regulations for all personal data processing operations it implements. Specifically, it commits to the following principles:

- Personal data is processed transparently, fairly, and with respect for human dignity.
- Personal data is processed respecting privacy and public freedoms.
- Personal data is collected for specified, explicit, and legitimate purposes and limited to what is necessary for the purposes for which it was collected.
- Personal data is retained adequately, relevantly, and 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, given the purposes for which it is processed, is erased or rectified promptly.

4. Security of Processed Personal Data:

The Company implements appropriate technical and organizational measures to ensure a level of security adapted to the risk inherent in its processing operations, to preserve the security of personal data and, in particular, to prevent any destruction, loss, alteration, disclosure, unauthorized intrusion, or access to such data, whether accidental or unlawful.

Furthermore, the Company commits to:

- Prevent the equipment and installations used in personal data processing from being placed in conditions or locations accessible to unauthorized persons;

- Prevent data media from being read, copied, modified, or moved by unauthorized persons;
- Prevent the unauthorized introduction of any data into the information system, as well as any unauthorized access, deletion, or removal of recorded data;
- Prevent the information processing system from being used by unauthorized persons;
- Ensure that the identity of persons who accessed the information system, the data introduced into the system, the time of introduction, and the person who performed it can be verified retrospectively;
- Prevent data from being read, copied, modified, erased, or removed during their communication or transport;
- Backup data by creating secure backup copies.

5. Data Retention Period:

The Company commits to retaining personal data for a period not exceeding that necessary for the purposes for which it is processed and in accordance with the regulations in force and the authorizations granted by the National Personal Data Protection Authority.

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 and the applicable regulations and act only within the limits authorized by the Company. The subcontractor must also have all necessary and appropriate technical means to carry out the tasks assigned to it. The Company and the subcontractor assume civil liability 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;
- For monitoring and managing received complaints;
- Declarations to the state and any public institution 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 subcontracting contracts involving personal data processing. The Company may share and transfer personal data abroad with the Parent Company and 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 with personal data processing that they have the following rights:

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

The Company provides the address of the registered office indicated at the head of this document for any access request.

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

The Company provides the address of the registered office indicated at the head of this document for any objection.

If individuals concerned with personal data processing are not satisfied with the responses provided after opposition, they may file a complaint with the National Personal Data Protection Authority.