

Issued Date / Hazırlık Tarihi:	3.11.2025
Revision Date / Revizyon Tarihi:	-
Revision No / Revizyon No:	0
Confidentiality level / Gizlilik Seviyesi:	L2
Document No/Dokuman No	POL.16

1. OVERVIEW, PURPOSE AND SCOPE

We, Martur Fompak International, conduct business in respect of Personal Data protection and have zero-tolerance to any breach of applicable privacy laws. With this Policy, we aim to promote a safe, respectful and ethical work environment in which our employees' and all Business Partners' Personal Data are protected. In general, Martur Fompak International can either process your personal data as independent data controllers, or as data processors or joint controllers.

Therefore, we expect all our employees, including directors, Executive Committee members, and members of Board of Directors as well as all Business Partners, such as customers, suppliers, contractors, and consultants, to comply with and act in line with this Policy and to always do business in accordance with our Global Code of Conduct. By this Policy, we actively prevent and prohibit such or similar conduct.

2. DEFINITIONS

Applicable laws and regulations refer to including, but are not limited to, the EU General Data Protection Regulation ("GDPR") 2016/679, the Turkish Personal Data Protection Law No. 6698 ("KVKK"), the Morocco Personal Data Protection Law No.09-08, the Algerian Law No.18-07 on the Protection of natural persons in the processing of personal data, local and specific rules/laws regarding to Personal Data.

Consent refers to any freely given, specific, informed, and unambiguous indication of the Data Subject's wishes by the Data Subject in the form of a declaration or other clear affirmative action by which the Data Subject signifies agreement to Personal Data relating to him or her being processed.

Data Breach refers to a potential or confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

Data Controller refers to any natural or legal person, whether governed by private or public law, including public authorities, institutions and their territorial structures, which determines the purposes and means of processing Personal Data or which is so designated in a normative act.

Data Processor refers to any natural or legal person, public authority, agency or other body processing Personal Data on behalf of the Data Controller.

Data Protection Authority refers to the authority with official responsibility for the protection of Personal Data, which has as its main objective the protection of the fundamental rights and freedoms of natural persons, and in particular their right to private, family and private life with respect to the processing of Personal Data and the free movement of such data.

Data Subject refers to any identified or identifiable natural person whose Personal Data are processed.

Personal Data refers to any information relating to an identified or identifiable natural person an identifiable person is a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity.

Processing refers to any operation or set of operations which is performed upon Personal Data or sets of Personal Data, whether or not by automatic means, such as: collecting, recording, organizing, structuring, storing (storing on any medium), adapting or altering, retrieving, consulting, using, , disclosing by transmission, disseminating or otherwise making available, alignment or combination, restriction, erasure or destruction of data.

Third Party refers to a natural or legal person, public authority, agency or body other than the Data Subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor are authorized.

3. DOMAIN OF APPLICATION

3.1 Territorial area of application

This Policy applies to the processing of Personal Data collected by us, regardless of whether the processing takes place in Türkiye, in European Union or not.

3.2 Material application domain

This Policy applies to processing activities carried out by Martur Fompak International.

All types and categories of Personal Data processed in the course of our activities will fall within the scope of this Policy. These types and categories including but not limited to : Personal Data collected from visitors, employees, job applicants, authorized personnel of Business Partners and other third parties etc.

This Policy covers both automated and manual types of processing.

4. PROCESSING PRINCIPLES

4.1 General principles

The processing of Personal Data will be carried out in accordance with the applicable laws and regulations as well as with the provisions of this Policy and, in particular, in compliance with the following rules:

- Personal Data must be obtained fairly and lawfully and in compliance with the Data Subject's right of information, unless such information is not necessary due to exceptions provided by law, and must only be processed if the Data Subject has given his or her consent unequivocally or if the processing has another legal basis.
- Personal Data must be collected only for specific, explicit and legitimate purposes and must not be processed in a way incompatible with that purpose(s) or must not be kept longer than necessary for the purpose(s) for which it was obtained, by incorporating the principles of privacy by design (for certain purposes) and by privacy by default (for default protection). Personal Data will be made available to third parties only for this purpose(s) or for other purposes provided for by applicable laws and regulations.
- Adequate technical and organizational controls and procedures shall be implemented to ensure the security of Personal Data and to prevent unauthorized access or disclosure, potential harm that could result from accidental or unlawful alteration, accidental or unlawful destruction or accidental loss of data, and against all other unlawful forms of processing.
- The collection of Personal Data must be adequate, relevant and not excessive in relation to the purpose(s) for which the data are collected and/or further processed.
- Procedures must be put in place to ensure prompt responses to enquiries from Data Subjects to ensure that they can properly exercise their rights of access, rectification and objection to the processing unless otherwise provided for by applicable laws and regulations.

4.2 Sensitive data

Sensitive data includes all Personal Data relating to including but not limited to Data Subject's :

- racial or ethnic origin, political opinions or religious or philosophical beliefs;
- trade union membership;
- physical or mental health or sexual state or sex life information;
- genetic, biometric data, criminal and other legal history;
- health-related data;
- data concerning a person's sex life or sexual orientation;

Processing of sensitive data is prohibited unless including but not limited to:

- the Data Subject's express consent to the processing of such sensitive data has been obtained;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- processing is carried out in the course of legitimate activities, with appropriate safeguards, by a foundation, association or any other body not seeking profit for political, philosophical, religious or trade-union purposes and provided that the processing relates solely to the members of the body or persons who have regular contact with it in connection with the purpose(s) and that the personal data are not disclosed to a third party without the consent of the Data Subjects ;
- processing relates to personal data which are manifestly made public by the data subject;
- processing when is necessary for the establishment, exercise or defense of legal claims ;
- processing when is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health services.

4.3 Outsourcing

Where processing is carried out by a processor on behalf of Martur Fompak International, a processor shall be chosen which will provide sufficient technical security and organizational measures to ensure that the processing will be carried out in accordance with this Policy and it shall be ensured that the processor will comply with these measures.

4.4 Data transfers outside the regulated jurisdiction

Martur Fompok International shall ensure that transfer of Personal Data outside the regulated jurisdiction, such as the transfer of data from the EU to non-EU countries that are not considered to afford the same protection of Personal Data as EU laws, are based on a mechanism approved by the competent data protection authority.

Depending on the local jurisdictions, these approved mechanisms may include:

- the use of standard contractual clauses in agreements with any 3rd parties,
- the use of "binding corporate rules" (i.e., an internal data transfer policy that allows the entity to transfer data to other jurisdictions, provided they are approved by the relevant Data Protection Authority);
- the use of a data transfer regime to take necessary safeguards for the transfer of Personal Data.

4.5 Accountability

We are required to demonstrate the measures we have taken to ensure compliance with applicable laws and regulations, as well as to demonstrate the effectiveness of those measures ('the accountability principle').

4.6 Implementing actions

Training programs are being implemented for the employees who are involved in the processing of Personal Data and to develop the tools used for the processing of Personal Data with regard to the principles contained in this Policy.

In order to prevent any serious consequences of violations of data protection laws, compliance programs and related controls are being implemented, which are reasonably designed to prevent, detect, monitor and address potential violations of the data protection applicable laws and regulations.

5. INDIVIDUAL RIGHTS REGARDING PERSONAL DATA

Applicable laws and regulations provides that Data Subjects must be informed about the processing of their Personal Data at the time of data collection. Although there may be exceptions to this rule, these are rare. These information are:

- the identity and contact details of the data controller and, where applicable, his representative;
- the contact details of the Data Protection Officer, where applicable;
- the purposes for which Personal Data are processed and the legal basis of the processing;
- the legitimate interests pursued by data controller or a third party;
- the recipients or categories of recipients of the Personal Data;
- the period for which the Personal Data will be stored or, if this is not possible, the criteria used to determine this period;
- the existence of the right to request from data controller, in respect of Personal Data relating to the Data Subject, access to or rectification or erasure of Personal Data relating to the Data Subject or restriction of processing or the right to object to processing, as well as the right to data portability
- the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing carried out on the basis of consent prior to the withdrawal of consent;
- the right to lodge a complaint before a supervisory authority;
- whether the provision of personal data is a legal or contractual obligation.

In accordance with applicable laws and regulations, if the Data Controller intends to further process Personal Data for a purpose other than that for which it was collected, it shall provide the Data Subject, prior to such different and new processing, with information about this new purpose and any relevant additional information.

In case of processing of Personal Data, Data Subjects have the right, upon written request:

- to obtain a copy of the public version of them from Martur Fompok International upon request and within a reasonable time;
- to request information about the Personal Data stored in relation to them, including information as to how the Personal Data have been collected;
- to obtain a list of the recipients or categories of recipients to whom their Personal Data are transferred;
- to obtain information as to the purpose(s) of the collection of their Personal Data and of the transfer of their Personal Data;
- to rectify Personal Data when inaccurate ;
- to object to the processing of their Personal Data on compelling legitimate grounds relating to their particular situation, unless otherwise provided for by the applicable law;
- to request the erasure of their Personal Data, where this is legally possible and for legitimate reasons;
- to receive the Personal Data they have provided to Martur Fompok International in a structured, commonly used and machine-readable format and have the right to transmit this data to another data controller.

6. IMPLEMENTING ACTIONS

Training programs are being implemented for the employees who are involved in the processing of Personal Data and to develop the tools used for the processing of Personal Data with regard to the principles contained in this Policy.

In order to prevent any serious consequences of violations of data protection laws, compliance programs and related controls are being implemented, which are reasonably designed to prevent, detect, monitor and address potential violations of the data protection applicable laws and regulations.

7. REPORT CHANNELS

Data Subject can convey all their reports using our Ethics Hotline that operates 24/7, offering a confidential and, where legally permissible, anonymous channel to report concerns:

- Ethics Website [EthicsPoint - Martur Fompok](#)
- Ethics Hotline Number (free of charge) [EthicsPoint - Martur Fompok](#)
- Ethics QR Code



- Legal and Compliance Team

8. AUTHORITY AND RESPONSIBILITIES

This Policy is published by our Legal and Compliance Team, and we are responsible for ensuring the compliance with this Policy by all our employees, including directors, Executive Committee members, and members of Board of Directors as well as all Business Partners who experience or witness any conduct they believe to be in conflict with this Policy, should report with assurance of confidentiality and protection from retaliation as outlined in this Policy. In addition, they are also expected to align with and actively support these principles by promoting a Workplace where everyone is valued and treated with dignity and respect.

9. VIOLATIONS AND CONSEQUENCES

By this Policy, we actively prevent and prohibit such or similar conduct. Our zero-tolerance principle means; if such a conduct does occur, we will look into and review every allegation of violation, take appropriate action in response. If there is a discrepancy between the local regulations, applicable in the countries where our company operates, and this Policy, subject to such practice not being a violation of the relevant local laws and regulations, the stricter of the two, supersedes.

Violation of this Policy may result in significant disciplinary actions including dismissal. If this Policy is violated by Business Partners or any third parties, their contracts may be terminated.

This Policy will be periodically reviewed by the Legal and Compliance Team to ensure compliance with new or revised laws and regulations.