CONTENTS

1. PURPOSE

Mavi Giyim San. ve Tic. A.Ş. ("Mavi") attaches importance to the privacy of all real persons whose personal data is processed. Mavi collects, stores and processes Personal Data about natural persons such as employees, customers, business partners, suppliers and other third parties ("Data Subjects") for various purposes.

This Personal Data Processing and Protection Policy ("**Policy**") describes how Mavi tries to protect the relevant Personal Data, and includes explanations to help us understand the principles governing the use of Personal Data. This Policy also explains how Mavi collects, processes and stores Personal Data in order to comply with all relevant legal regulations and fulfill the requirements under the Personal Data Protection Law No. 6698.

2. SCOPE

This Policy is related to the data of groups of individuals whose personal data are processed by the Company, wholly or partially by automated means or non-automated means which form part of a data filing system.

3. DEFINITIONS

For the purposes of this Policy;

a. **"Explicit consent"** means freely given, specific and informed consent.
b. **"Anonymization"** means rendering personal data impossible to link with an identified or identifiable natural person, even through matching them with other data.
c. **"Employees"** means any and all people employed in any capacity at Mavi.
d. **"Legal and Compliance Managers" means** any and all Legal and Compliance Department employees, who report to the Head of Legal and Compliance and are authorized by the Head of Legal and Compliance.
e. **"Data subject"** means any natural person whose personal data are processed.
f. **"Personal data"** means any information related to an identified or identifiable natural person.
g. **"Processing of personal data"** means any operation which is performed on personal data, wholly or partially by automated means or non-automated means which form part of a data filing system, such as collection, recording, storage, protection, alteration, adaptation, disclosure, transfer, retrieval, making available for collection, categorization, preventing the use thereof.
h. **"Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
i. **"PDPL"** or **"Law"** means the Personal Data Protection Law No. 6698.
j. **"Board"** means the Personal Data Protection Board.
k. **"Authority"** means the Personal Data Protection Authority.
l. **"Special Categories of Personal Data"** means personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, religious sect or other belief, appearance, membership to associations, foundations or trade-unions, data concerning health, sexual life, criminal convictions and security measures, and the biometric and genetic data.
m. **"Policy"** means the Personal Data Protection and Processing Policy.
n. **"Data processor"** means the natural or legal person who processes personal data on behalf of the data controller upon its authorization.
o. **"Data filing system"** means the system where personal data are processed by being structured according to specific criteria.
p. **"Data controller"** means the natural or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data filing system.

4. ROLES AND RESPONSIBILITIES

All Mavi employees are responsible for the implementation, dissemination and sustainability of the principles set out in this Policy.

The following roles at Mavi have specific responsibilities:

- **Board of Directors** is responsible for ensuring that Mavi fulfills its legal obligations.
- **Directors of the Departments** have general responsibilities, limited to their own fields of activity, which include ensuring, controlling and monitoring compliance with the Personal Data Protection Law regarding the protection of personal data and ensuring that internal sanctions and this Policy are implemented on a daily basis, if necessary, in accordance with internal regulations.
- **Legal and Compliance Managers** will facilitate compliance with the Personal Data Protection Law and act as the go-to persons for both employees and third parties regarding daily issues and questions related to Personal Data Protection. Legal and Compliance Managers are generally responsible for monitoring personal data protection project processes and the daily implementation of this Policy.

Unit Directors of the Global Information Technologies Department are generally responsible for ensuring that all systems, services and equipment used to store data meet acceptable security standards and for performing regular checks and scans to ensure that security hardware and software are running properly.

5. IMPLEMENTATION

Personal Data, *as explained in the Definitions section of the Policy*, means any information relating to an identified or identifiable natural person. Examples of Personal Data include name and surname, date of birth, e-mail address, phone number and address (when it is clear who the relevant information belongs to or when it is reasonably possible to find it), and processes include more examples.

Special Categories of Personal Data, *as explained in the Definitions section of the Policy*, means personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, religious sect or other belief, appearance, membership to associations, foundations or trade-unions, data concerning health, sexual life, criminal convictions and security measures, and the biometric and genetic data. Processing of Special Categories of Personal Data is subject to stricter rules compared to processing of Personal Data. Rules regarding the processing of these data are also regulated in the Policy on Protection and Processing of Special Categories of Personal Data.

5.1. General Principles Regarding the Processing of Personal Data

Personal Data may only be processed in accordance with the general principles listed below.

5.1.1. Lawfulness and fairness

Lawfulness and fiarness means the obligation to act in accordance with the principles set forth by laws and other legal regulations while processing personal data. Mavi aims to act in accordance with legal regulations and ethical rules in the processing of personal data. In this context, it strives to prevent any consequences that the data subject does not expect and does not need to expect.

5.1.2. Being accurate and kept up to date where necessary

Mavi strives to ensure that personal data is accurate and, where necessary, up-to-date. Mavi's communication channels are open to ensure that the personal data of the data subjects are kept accurate and up-to-date. The active duty of care to ensure that personal data is accurate and, where necessary, up-to-date is valid if Mavi produces a conclusion relevant to the data subject based on these data.

5.1.3. Being processed for specified, explicit and legitimate purposes

The legitimate purpose means that the data processed by the data controller is related to the work it performs or the service it offers and is necessary for these purposes, and Mavi processes personal data to the extent that it is related to the activities it carries out and is necessary for these purposes.

5.1.4. Being relevant, limited and proportionate to the purposes for which they are processed.

Personal Data should only be processed if processing is not reasonably possible in any other way and by taking into account the principles of Data Minimization. In cases where Personal Data need to be processed, processing must be adequate, relevant and limited to what is necessary for the purpose of processing. Only the amount of Personal Data that is needed for the successful fulfilment of a specific purpose should be processed. Personal Data that are not needed for the purpose of processing should not be collected and/or processed.

5.1.5. Being stored for the period laid down by relevant legislation or the period required for the purpose for which the personal data are processed.

In addition to the retention periods determined by the data controller in accordance with the principle of storing personal data for only a limited period based on purpose of processing, there are also retention periods stipulated in the relevant legislation which the data controller needs to comply with. Accordingly, Mavi complies with the retention period (if any) stipulated in the legislation for the relevant personal data, and in cases where no such period is stipulated, Mavi stores the data only for the period necessary for the purpose of processing. If there is no valid reason for further storage of data, that data is disposed in accordance with the Storage and Disposal Policy.

5.2. Conditions for processing Personal Data

As per Article 5 of the Law, Mavi may process personal data without seeking the explicit consent of the data subject only in cases where one of the following conditions is met:

a) It is expressly provided for by the laws.

b) It is necessary for the protection of life or physical integrity of the person himself/herself or of any other person, who is unable to explain his/her consent due to the physical disability or whose consent is not deemed legally valid.

c) Processing of personal data of the parties of a contract is necessary, provided that it is directly related to the establishment or performance of the contract.

d) It is necessary for compliance with a legal obligation to which the data controller is subject.

e) Personal data have been made public by the data subject himself/herself.

f) Data processing is necessary for the establishment, exercise or protection of any right.

g) Processing of data is necessary for the legitimate interests pursued by the data controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject.

5.3. Legal Obligations

The main legal obligations that Mavi must comply with in its capacity as data controller are as follows.

5.3.1. Obligation to Inform

In order for Mavi to fulfill its obligation to inform, persons whose personal data is processed are informed, at least, about the conditions listed in Article 10 of the Law, in accordance with the Communique On Principles And Procedures To Be Followed In Fullfillment Of The Obligation To Inform.

Mavi aims to inform Data Subjects in a transparent, intelligible and easily accessible manner by using clear and plain language.

5.3.2. Obligation to Take Necessary Technical and Administrative Measures to Ensure Data Security

Mavi acts in accordance with the Information Security Policy and takes the following measures to prevent the unlawful processing of, and unlawful access to, personal data and to protect personal data:

- Network and application security is provided.
- A closed system network is used for personal data transfer via network.
- Key management is implemented Security measures are taken as needed in connection with procurement, development and maintenance of information technology systems.
- The security of the personal data stored in the cloud is provided.
- Disciplinary regulations are in place for employees that include data security provisions.
- Training and awareness studies are carried out periodically for employees on data security..
- An authority matrix has been developed for employees.
- Access logs are kept regularly.
- Corporate policies on access, information security, use, storage and disposal have been prepared and implemented. Data masking measures are applied when necessary.
- Privacy commitment are executed.
- Permissions of employees whose role is changed or who quit their jobs are revoked accordingly.
- Up-to-date antivirus software are used.
- Firewalls are used.
- Data security provisions are integreated into employee contracts.
- Extra security measures are taken for personal data transferred via paper, and the relevant documents are sent in a document classified as confidential.
- Policies and procedures regarding personal data security have been established.
- Security issues related to personal data are reported quickly.
- Security of personal data is monitored.

- Necessary security measures are taken for physical exits containing personal data. Physical environments where personal data are stored are secured against external risks (fire, flood, etc.).
- Environments where personal data are stored are secured.
- The amount of personal data is reduced as much as possible.
- Personal data is backed up, and the personal data back-ups are kept in a secure environment.
- User account management and access control systems are implemented and monitored.
- Periodic and/or spontaneous internal audits are carried out.
- Log records are kept without user intervention.
- Existing risks and threats have been identified.
- Protocols and procedures regarding the security of special categories of personal data are identified and implemented.
- When sending special categories of personal data via e-mail, these data are encrypted and sent by using Registered Electronic Mail (KEP) or corporate mail account.
- If personal data is sent via electronic mail, it is sent in encrypted form and using KEP or corporate mail account. Intrusion detection and prevention systems are in place.
- Penetration testing is performed.
- Cyber security measures have been taken and are continuously monitored.
- Encryption done..
- Data security practices of data processing service providers are audited periodically.
- It is ensured that service providers processing data have appropriate level of data security awareness.
- Software designed to prevent loss of data are used.

5.3.3. Reporting personal data breaches

Mavi is responsible for reporting Personal Data Breaches to the Authority, when legally required, without undue delay and within 72 hours after becoming aware of a breach.

In the event that a Personal Data Breach involving personal data for which Mavi may be held liable is suspected to have occurred, the Legal and Compliance Managers must be notified immediately.

5.3.4. Obligation to Receive and Respond to Requests from Data Subjects

Each person has the right to request to the data controller about him/her;

a) to learn whether his/her personal data are processed or not,

b) to demand for information as to if his/her personal data have been processed,

c) to learn the purpose of the processing of his/her personal data and whether these personal data are used in compliance with the purpose,

d) to know the third parties to whom his personal data are transferred in country or abroad,

e) to request the rectification of the incomplete or inaccurate data, if any,

f) to request the erasure or destruction of his/her personal data under the conditions referred to in Article 7,

g) to request reporting of the operations carried out pursuant to sub-paragraphs (d) and (e) to third parties to whom his/her personal data have been transferred,

h) to object to the occurrence of a result against the person himself/herself by analyzing the data processed solely through automated systems,

i) to claim compensation for the damage arising from the unlawful processing of his/her personal data.

Data Subjects may exercise their rights by using the contact details provided in Mavi's information texts. Mavi may request additional information to verify the identity of Data Subjects.

Mavi will conclude the requests of Data Subjects to exercise their rights without undue delay and within 30 days from the date of receipt of a request.

5.4. Personal Data Transfers

5.4.1. Transfer of Personal Data in Türkiye

Personal data may be shared with domestic recipient groups by taking the measures determined by the Personal Data Protection Board and based on one of the conditions set out in section 5.3.4. of the Policy.

5.4.2. Transfer of Personal Data Abroad

Your personal data may be transferred abroad by taking the measures determined by the Personal Data Protection Board based on one of the following conditions. Personal data may be transferred abroad by data controllers and data processors without explicit consent of the data subject upon the existence of one of the legal conditions specified in this Policy and if:

I. adequate protection is provided in the country where personal data are to be transferred, sectors within the country or international organizations.

II. Adequate protection is not provided, upon provision of one of the assurances listed below, provided that the data subject is also entitled to exercise his/her rights and to seek legal remedy in the country where the personal data are to be transferred;

A. The existence of an agreement that is not an international agreement between public institutions and organizations or international organizations abroad and public institutions and organizations or professional organizations with public institution status in Turkey, and the Board's permission for transfer.

B. The existence of binding company rules approved by the Board, which contain provisions regarding the protection of personal data that the companies within the group of companies engaged in joint economic activities are obliged to comply with.

C. The existence of a standard contract declared by the Board, which contain matters such as data categories, purposes of data transfer, recipient and recipient groups, technical and administrative measures to be taken by the data recipient, and additional measures taken for special categories of personal data.

D. Existence of a written commitment letter, which contain provisions to provide adequate protection, and the Board's permission for transfer.

III. Where adequate protection or an appropriate assurance is not provided, the Personal Data may be transferred abroad if:

A. The data subject gives explicit consent to the transfer, provided that he/she is informed about the possible risks.
B. The transfer is required for the performance of a contract between the data subject and the data controller or for the implementation of pre-contractual measures taken at the request of the data subject.
C. The transfer is required for the establishment or performance of a contract between the data controller and another natural or legal person for the benefit of the data subject.
D. The transfer is required to protect a major public interest.
E. The transfer of personal data is required for the establishment, exercise or protection of a right.
F. Transfer of personal data is necessary for the protection of life or physical integrity of the person himself/herself or of any other person, who is unable to explain his/her consent due to the physical disability or whose consent is not deemed legally valid.
G. Transfer is done from a registry that is open to the public or to persons with a legitimate interest, provided that the conditions required for accessing the registry in the relevant legislation are met and the person with a legitimate interest requests it.

5.5. Destruction of Personal Data

As per Article 7 of the Law and the "*By-Law on the Erasure, Destruction and Anonymization of Personal Data*", personal data is disposed in case the reasons for processing it no longer exist or upon the request of the data subject, even though it has been processed in accordance with the provisions of the relevant Law. Such erasure, destruction and anonymization processes are carried out according to our Company's "Personal Data Storage and Disposal Policy", without prejudice to the relevant legislation.

6. SANCTION

Action may be taken and/or one or more provisions of the sanctions included in the relevant contracts may be applied by initiating legal and administrative legal proceedings against any personnel, stakeholders and third parties who violate the rules and processes regarding personal data protection and information security, including especially this Policy.

7. MAKING CHANGES TO THE POLICY

In the event that PDP regulations are amended in a manner which affect the provisions of this Policy or when deemed necessary by the Company, this Policy may be accordingly changed, reviewed and re-approved.

8. RELEVANT DOCUMENTS

HO.PO.02 Personal Data Storage and Disposal Policy
LC.PO.05-Policy on Processing and Protection of Special Categories of Personal Data
IT.PO.01-Information Security Policy

9. REVISION HISTORY

Rev. No.	Date	Reason
00	01.04.2022	Initial Publication
01	04.06.2024	Revision
02	20.01.2025	Revision