DATA PROTECTION POLICY

1. OBJECTIVE

Mavi respects the privacy of all individuals that have entrusted us with their personal data. Mavi collects, stores and processes Personal Data about individuals such as employees, customers, business partners, suppliers and other third parties (“Data Subjects”) for a variety of purposes.

This Data Protection Policy (“**Policy**”) outlines how Mavi seeks to protect such Personal Data and helps ensure that we understand the principles governing the use of Personal Data. It also describes how Mavi collects, handles and stores Personal Data to meet and comply with all applicable laws and regulations and delegated national legislation (together "**Data Protection Law**")**.**

Mavi’s objective is to protect the Data Subjects by obtaining, collecting, handling, sharing, using and processing their Personal Data in accordance with applicable Data Protection Law. This Policy is a guideline for how data should be collected, handled and processed, based on its sensitivity and importance.

2. SCOPE

This Policy covers Mavi Giyim San. ve Tic. A.Ş., including Mavi Management, all employees of Mavi Giyim San. ve Tic. A.Ş. and its subsidiaries and affiliates (“**Mavi**”) in all countries and regions.

This Policy is applicable to all Employees who handle the Personal Data of individuals (such as, e.g., other employees, customers or contact persons of business partners).

3. DEFINITION

Term	**Meaning**
Employee(s)	All those employed or engaged in any capacity by Mavi. For the purposes of this Policy, the word Employees extends to include the following categories: Board Members, Employees (full time, fixed term, part time and temporary), and contract workers.
Controller	A Controller is a person or organisation that determines the purposes for which, and the manner in which, any Personal Data are processed, establishing practices and implementing policies in line with the Data Protection Law.
Data Protection	This term refers to the relationship during the processing of Personal Data, the associated expectations of privacy and the legal protection surrounding them.

Data Subject	The individual to whom Personal Data relates such as an employee, customer, investor, supplier, shareholders, etc.
Data Protection Authority	Data Protection Authorities are independent public authorities that supervise, through investigative and corrective powers, the application of the Data Protection Law in relevant countries.
Personal Data	Personal Data means any information (or a combination of information) from which a living person can be directly or indirectly identified as well as information containing statements about a person (e.g. Name, salary information, marital status, sick leave dates)
Personal Data Breach	This is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.
Processing	Processing includes obtaining, recording or holding Personal Data, or carrying out any operation or set of operations on Personal Data including organising, amending, retrieving, using, disclosing, erasing or destroying data. Processing also includes sharing or transferring Personal Data to third parties and accessing of Personal Data held by a Controller or Processor.
Processor	A Processor is any person or organisation that processes Personal Data on behalf of and/or on instruction of a Controller.

4. POLICY

4.1 Definition and Importance of Data Protection

Data protection is a set of strategies and processes which can be used to secure the privacy, availability, and integrity of the individuals' data. All individuals have rights pertaining to the way in which their Personal Data are processed. The term "Data Protection" in this Policy refers to the relationship between the collection and processing of Personal Data, the corresponding rights to privacy which Data Subjects have and the legal protection surrounding Personal Data (according to Data Protection Law).

4.2 Definition of Personel Data

Personal Data refers to any information that relates to an individual.

Personal Data means any data (or a combination of data) from which a living individual can be identified directly or indirectly. Personal Data can be factual, or it can be an opinion about an individual, their actions

and behaviour. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute Personal Data.

Personal Data can cover various types of information, such as name-surname, date of birth, email address, phone number, address, physical characteristics, or location data – once it is clear to whom that information relates, or it is reasonably possible to find out.

Should it determined by the applicable Data Protection Law, stricter conditions for processing special categories of Personal Data must be observed. "Special Categories of Personal Data", including but not limited to, information related to a person's race or ethnicity, political opinions, religion, religious or philosophical beliefs, physical or mental health, sexual life, biometric data for the purpose of uniquely identifying a natural person, genetic data and data concerning a natural person's sex life or sexual orientation, which could be differ within the applicable local law. Conditions for processing Special Categories of Personal Data under applicable law must be followed.

4.3 Data Protection Principles

Processing includes all operations such as collection, organisation, structuring, storage, alteration, consultation, use, communication, combination, restriction, erasure or destruction etc. of Personal Data.

Personal data may be collected, processed and used only in compliance with the following general data privacy principles.

- **Accountability**: Mavi ensures and demonstrates that the key principles and rules of Data Protection Law are met.
- **Lawfulness, Fairness and Transparency:** Mavi only processes Personal Data lawfully, fairly and in a transparent manner and informs Data Subjects on how and why their data (transparency) that the processing matches the description given to the Data Subjects (fairness) and that the processing uses one of the legal bases set forth in the Data Protection Law (lawfulness).
- **Purpose Limitation:** Mavi specifies what the Personal Data collected will be used for (prior to collecting it) and limits the processing of that Personal Data to only what is necessary to meet the specified purpose.
- **Data Minimization:** Personal Data is collected adequately, relevant and limited only to what is necessary for the purposes for which they are processed, ensuring that the period for which the personal data are stored is limited to a strict minimum.
- **Accuracy:** Mavi has processes in place to ensure that Personal Data is accurate and kept up to date.
- **Storage Limitation:** Personal Data is kept in such a way which enables Mavi to identify the Data Subject for no longer than is necessary for the purposes for which the Personal Data are processed.
- **Security/Integrity and Confidentiality:** Mavi uses appropriate technical and organisational measures to protect the integrity and confidentiality of Personal Data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

4.3.1 Accountibility

Monitoring

There may be significant implications for Personal Data Breaches or non-compliance with Mavi's legal responsibilities under the Data Protection Law. It is Mavi's responsibility to process all Personal Data in accordance with legal obligations and the principles of Data Protection.

In the event that Mavi does not meet the accountability requirements, there may not be only a risk of non-compliance with Data Protection Law and other laws, but also a significant reputational risk.

Mavi assesses compliance with this Policy in two regards:

1. Compliance in relation to the protection of Personal Data in general.
2. The effectiveness of Data Protection measures related to operational practices.

Mavi does reviews on a regular basis and control the continuous improvement of its processes.

Personal data breach reporting

It is Mavi's responsibility to report a Personal Data Breach to the relevant Supervisory Authority, when legally required, within 72 hours unless otherwise specified by the applicable law of becoming aware of the breach, and without any undue delay.

When it is suspected that a Personal Data Breach has taken place involving personal data for which Mavi is responsible (as Controllers) Compliance Executives must be informed immediately. Compliance Executives shall decide whether outsourcing is required. If required, Compliance Executive shall revert the assessment to respective person. If the incident results in a risk for Data Subjects, it must be reported to the applicable supervisory authority within 72 hours (of becoming aware of the incident) unless otherwise specified by the applicable law by receiving guidance of Compliance Executives.

Training

All Employees must complete Data Protection training relevant to their position assigned by Mavi.

Human Resources Division of each country must ensure that new joiners to Mavi receive training as part of the onboarding process. Further training must be provided on a periodic basis or whenever there is a substantial change in the law or policy and procedures in this regard.

Responsibility

Each Employee who handles Personal Data has a responsibility to handle and process the Personal Data in line with this Policy and the Data Protection Law.

There are positions in Mavi with specific areas of responsibility:

- **Management Board** is ultimately responsible for ensuring that Mavi meets its legal obligations.
- **Head of Departments** have overall responsibility for ensuring compliance with Data Protection Law regarding the protection of personal data, limited to its own field of activity, and all kinds

of international agreements to which all countries in which Mavi operates, and to control compliance and to follow up, to ensure that internal sanctions are enforced in accordance with internal regulations when necessary, and the day-to-day implementation of this Policy.

- **The Head of Information Technology** is responsible for:
    - Ensuring that all systems, services and equipment used for storing data meet acceptable security standards
    - Performing regular checks and scans to ensure security hardware and software is functioning properly
    - Evaluating any third-party services Mavi is considering using to retain or process Personal Data

Data protection by design

Mavi seeks to structure internal processes to have Data Protection principles embedded into every stage of Processing activities. Data Protection by design means that, both before and during any Processing activity Mavi carries out, appropriate technical and organisational measures must be implemented to integrate safeguards into the Processing. Mavi will always aim to implement appropriate technical and organisational measures both at the time of determination of the means for Processing and at the time of the Processing itself in order to ensure the principle of Data Minimization is met.

To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, a pre- Data Protection Impact Assessment ("DPIA") check must be completed before starting a project and if it is required a full DPIA must be conducted.

4.3.2 Lawfulness, fairness and transparency

Mavi is responsible for understanding the context in which the Personal Data processing occurs as part of its day-to-day operations and help ensure that the processing is done fairly and in line with the Data Protection Law, and it could be clearly described to Data Subjects.

Mavi always processes Personal Data lawfully, fairly and transparently in accordance with the Data Subject's rights.

With regards to third-party suppliers/contractors that process Personal Data on Mavi's behalf, in accordance with the Data Protection Law, Mavi shall:

- engage the services of third-party suppliers/contractors who can demonstrate compliance with Data Protection Law;
- put in place prescribed contractual arrangements with third party suppliers/contractors which meet the requirements of Data Protection Law; and
- demonstrate to the local data protection authorities, if necessary, that Mavi has complied with these legal obligations.

Personal data collection and notification

Mavi shall only collect Personal Data where it is necessary for lawful purposes or explicitly allowed.

Mavi will only collect Personal Data from Data Subjects where:

- The processing is required by applicable local law or under an international treaty;
- It is necessary to do so for business purposes and for Mavi to enter into or perform its contractual obligations with Data Subjects;
- The nature of Mavi's business purposes means it is within [reasonable] legitimate interests to Process the Personal Data, and Mavi is not prejudicing the Data Subject by Processing the Personal Data;
- The consent of the individuals has been obtained and the relevant consent is freely given and gathered according to the rules in applicable local law;
- The collection is carried out under emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person;
- Other reasons, which are explicitly allowed by the relevant applicable local law.

Mavi provides Data Subjects with information regarding the processing of their personal data in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

4.3.3 Purpose limitation: Processing for limited purposes

Personal Data collected for one purpose can usually not be used for a different purpose, unless otherwise required by applicable local law or the relation between the parties.

Mavi processes Personal Data for purposes specifically permitted under Data Protection Law. Data Subjects will be notified of those purposes when Mavi first collects the Personal Data or as soon as possible thereafter.

4.3.4 Data minimization: Adequate, relevant and non-excessive processing

Personal Data should only be processed where it isn't reasonably feasible to carry out the processing in another manner and by taking into account the Data Minimization principles (Annex 1 – Data Minimization.). Where possible, it is preferable to use anonymous data. Where Personal Data is needed, it should be adequate, relevant, and limited to what is necessary for the purpose. Processing should only use as much Personal Data as is required to successfully accomplish a particular purpose. Personal Data not needed for the purpose of Personal Data processing should not be collected and/or processed.

4.3.5 Accuracy: Ensuring that personal data is accurate

It is aimed to ensure that Mavi's systems and processes for identifying inaccurate information are robust and to act quickly to update or erase any inaccurate Personal Data.

Mavi will always endeavour to ensure that Personal Data we hold is accurate and kept up to date.

The Data Subjects may ask to correct inaccurate Personal Data relating to them.

4.3.6 Storage limitation: Timely processing and data retention

It is aimed to not keep the Personal Data for any longer than is necessary in accordance with Data Protection Law.

Mavi also takes all reasonable steps to anonymise, destroy or erase all Personal Data from the systems (electronic/paper-based) which is no longer required. All Employees should ensure that they are familiar with the destruction concept.

4.3.7 Security/integrity and confidentiality: Security of personal data

Mavi has taken adequate safeguards to ensure the confidentiality and security of the Personal Data of Data Subjects. Personal Data held are subject to a level of security that is appropriate for the potential risk.

Mavi has implemented appropriate technical, physical and organizational measures to protect Personal Data against accidental or unlawful destruction or accidental loss, damage, alteration, unauthorised disclosure or access as well as all other forms of unlawful processing (including, but not limited to, unnecessary collection) or further processing.

4.4 Rights of the Data Subject

Data Subjects have the right to request access of an overview of their Personal Data, and under certain conditions, rectification and/or erasure of Personal Data in accordance with Data Protection Law. In addition, Data Subjects may also have the right of restriction of processing concerning their Personal Data, the right to object to processing, as well as the right to data portability, when applicable according to local law.

Data Subjects can exercise their right of access, rectification, and/or erasure of Personal Data, right of restriction of processing, and/or right to object to processing as well as to invoke right to data portability, if applicable, by using the contact details specified in the relevant data protection notices. Additional information to verify the Data Subjects' identity can be required.

Data Subjects can withdraw their consent at any time. Withdrawal does not have retroactive effect.

Mavi will deal with any requests from Data Subjects exercising their rights without undue delay, and within 30 calendar days of receipt of such request, unless otherwise required by applicable local law.

4.5 Data Transfers

As Mavi is a global organization, collected data may be transferred internationally. Personal Data may be transferred to other group companies of Mavi and other third-party entities, if reasonably necessary and in accordance with applicable local law.

When Personal Data needs to be transferred to other entities, Mavi will always ensure that these transfers are based on a legal basis. These entities can be companies within Mavi group of undertakings but also third-party entities who process data on behalf of Mavi.

If Mavi engages companies to process data on its behalf Mavi cooperates only with processors who fulfil Mavi's requirements of providing appropriate technical and organizational measures which meet Mavi standards and the requirements of Data Protection Law. Before personal data is processed, data processing agreements will be signed to bind the processor accordingly.

Mavi also complies with any legal restrictions and requirements that apply to the cross-border transfer of personal data.

4.6 Implementation, monitoring and enforcement

Each Mavi Company, through its appropriate bodies, shall adopt this Policy, and through its managers, shall be responsible and accountable for administering and overseeing the implementation of this Policy and supporting guidelines by implementing local directives, guidelines and related documents and processes, considering more stringent or specific local legal requirements.

All Mavi employees shall be trained on the general privacy principles according to their function and responsibility for the processing of personal data.

Compliance Executives help facilitate compliance with Data Protection Law and acts as a point of contact for day-to-day issues and questions on Data Protection for both employees, third parties and the Data Protection Officer.

Compliance Executives has overall responsibility for monitoring data protection project processes and the day-to-day implementation of this Policy.

Compliance Executives are, Head of Legal and Compliance and, Senior Manager of Legal and Compliance, whom you may contact from compliance@mavi.com.

4.7 Consequences of Breaching the Policy

Compliance with this Policy and obligations under Data Protection Law is essential for Mavi. Any breach of this Policy may result in disciplinary action being taken, up to and including dismissal.

4.8 Data Protection Officer

Mavi companies that are obligated to appoint a data protection officer will appoint data protection officers in accordance with Data Protection Laws.

The data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of Personal Data pursuant to Data Protection Law.

Pursuant to this assignment, Data Protection Officer for the Mavi Europe AG can be contacted at fox-on Datenschutz GmbH, Pollerhofstr. 33a, 51789 Lindlar, Germany, dsb@fox-on.com.

4.9 Amendment of this Policy

This Policy is owned by the Legal and Compliance Division. It will be reviewed and amended from time to time to reflect changes in applicable laws and Mavi's business requirements.

5. RELATED DOCUMENTS

- Annex-1 Data Minimization

ANNEX-1 DATA MINIMIZATION

Personal data should only be processed where it isn't reasonably feasible to carry out the processing in another manner. Where possible, it is preferable to use anonymous data. Where personal data is needed, it should be **adequate, relevant, and limited to what is necessary for the purpose ('data minimization').**

Therefore, you must ensure the personal data you are processing is:

- **adequate –** sufficient to properly fulfil your stated purpose.
- **relevant –** has a rational link to that purpose; and
- **limited to what is necessary** – you do not hold more than you need for that purpose.

In order to ensure you are complying with data minimization principle you can use below checklist:

Checklist

☐ We only collect personal data we actually need for our specified purposes.

☐ We have sufficient personal data to properly fulfil those purposes.

☐ We periodically review the data we hold and delete anything we don't need (observe legal retention periods).

So, you should identify the minimum amount of personal data you need to fulfil your purpose. You should hold that much information, but no more.

This is the first of three principles about data standards, along with accuracy and storage limitation.

The accountability principle means that you need to be able to demonstrate that you have appropriate processes to ensure that you only collect and hold the personal data you need.

How do we decide what is adequate, relevant and limited?

So, to assess whether you are holding the right amount of personal data, you must first be clear about why you need it

You may need to consider this separately for each individual, or for each group of individuals sharing relevant characteristics. You should in particular consider any specific factors that an individual brings to your attention.

You should periodically review your processing to check that the personal data you hold is still relevant and adequate for your purposes and delete anything you no longer need. This is closely linked with the storage limitation principle.

When could we be processing too much personal data?

You should not have more personal data than you need to achieve your purpose. Nor should the data include irrelevant details.

> **Example:** You need the e-mail address of a business partner's employee, because you need to send the invoice or shipping details, but you don't need their blood type information.

If you need to process particular information about certain individuals only, you should collect it just for those individuals – the information is likely to be excessive and irrelevant in relation to other people.

> **Example:** You may need the business phone number of a business partner's employee, but you don't need their home phone number.

You must not collect personal data on the off-chance that it might be useful in the future. However, you may be able to hold information for a foreseeable event that may never occur if you can justify it.

> **Example:** If you receive a list which contains home addresses of the all employees by accidentally you must not keep this list in case you would need that information in the future.

If you are holding more data than is actually necessary for your purpose, this is likely to be unlawful within the scope of GDPR (as all of the lawful bases have a necessity element) as well as a breach of the data minimization principle. Individuals will also have the right to erasure (according to applicable local laws).

When could we be processing inadequate personal data?

If the processing, you carry out is not helping you to achieve your purpose then the personal data you have is probably inadequate. You should not process personal data if it is insufficient for its intended purpose. In some circumstances you may need to collect more personal data than you had originally anticipated using, so that you have enough information for the purpose in question.

Data may also be inadequate if you are making decisions about someone based on an incomplete understanding of the facts. In particular, if an individual asks you to supplement incomplete data under their right to rectification, this could indicate that the data might be inadequate for your purpose.

Obviously, it makes no business sense to have inadequate personal data – but you must be careful not to go too far the other way and collect more than you need.

What about the adequacy and relevance of opinions?

A record of an opinion is not necessarily inadequate or irrelevant personal data just because the individual disagrees with it or thinks it has not taken account of information, they think is important.

However, in order to be adequate, your records should make clear that it is opinion rather than fact. The record of the opinion (or of the context it is held in) should also contain enough information to enable a reader to interpret it correctly. For example, it should state the date and the author's name and position.

If an opinion is likely to be controversial or very sensitive, or if it will have a significant impact when used or disclosed, it is even more important to state the circumstances or the evidence it is based on. If a record contains an opinion that summarizes more detailed records held elsewhere, you should make this clear.

Blacking out

Personal data not needed for the purpose of personal data processing should not be collected and/or processed or blacking out process should be applied.

Blacking out means **non-restorably scratching out, painting and blurring personal data that are not / no longer needed for processing** (see Annex-1 for an example of blacking out data on printed media, and Annex-2 and Annex-3 for examples of electronic media).

We should also follow the above rules for the identity card photocopies we obtained previously for various reasons or we keep in our files, drawers and as attached to agreements. **In any case, religion and blood type data must be blacked out** on photocopies that we are obliged to keep and as far as their documentation is not required by local laws (see Annex-2).

Please contact us at gdpr@mavi.com for any questions or if you hesitate on any matter.

ANNEX-1: An Example of Blacking Out Data on Printed Media


CERTIFICATE

[redacted]

Mavi Europe AG [redacted]

has successfully participated in the

„Data Protection for Employees (GDPR)"

online training session.

fox-on DATENSCHUTZ

www.fox-on.com

12.05.2020

ANNEX-2: An Example of Blacking Out Data Electronically:

ANNEX-3: An Example of Blacking Out Data Electronically: