MAPEI®

ADHESIVES • SEALANTS • CHEMICAL PRODUCTS FOR BUILDING

# POLICY ON THE PROCESSING-PROTECTION AND DESTRUCTION OF PERSONAL DATA

Effective Date:
7 October 2016

# TABLE OF CONTENTS

## I. LEGISLATION, PURPOSE, AND SCOPE

This Policy on the Processing-Protection and Destruction of Personal Data is issued in accordance with the Constitution of Republic of Turkey, the Personal Data Protection Law No. 6698 enacted on 7 April 2016, (Hereinafter referred to as the "Law") and other relevant legislation, in order to establish an announce the principles and obligations of our Company regarding all personal data of our customers, potential customers, employees, visitors, probationary employees, employees, shareholders and authorities of the persons or institutions with whom we cooperate and/or from whom we receive services, all other third parties sharing personal data with us and/or coming into contact in a way resulting in personal data sharing, which are processed by automated or non-automated means, provided that it is a part of any data recording system.

This Policy shall be published on the official website of our Company.

## II. OUR BASIC PRINCIPLES ON THE PROCESSING OF PERSONAL DATA

In Article 4 of the Law, procedures, and principles on the processing of personal data are regulated in parallel with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data No. 108 and with the European Data Protection Directive No 95/46/EC.

Pursuant to the Law, the general principles to be complied with in the processing of personal data are as follows:

- Being in compliance with the law and bona fides,
- Being accurate and up to date, if necessary,
- Being processed for specified, explicit, and legitimate purposes,
- Being relevant, limited and proportionate to the purposes for which they are processed
- Being retained for a period specified in the relevant legislation or necessitated by the purposes for which they are processed.

In this context, principles on the processing of personal data are considered at the core of all processing activities of personal data, carrying out of the data processing activities in accordance with these principles is adopted as the company policy.

## III. III. PROCESSING OF PERSONAL DATA

### Personal Data

Personal Data means any information related to the identified or identifiable natural person.

Processing of personal data may be carried out on the basis of at least one of the conditions specified in Article 5 of the Law.

Accordingly, Personal data of the data subject may be processed in the presence of one of the following conditions;

- Explicit consent of the data subject,
- Being clearly provided for by the laws,
- It is mandatory for the protection of life or physical integrity of the person or of any other person who is bodily incapable of giving his consent or whose consent is not deemed to be legally valid,
- Processing of personal data belonging to the parties of a contract is necessary provided that it is directly related to the establishment or fulfillment of that contract,
- It is mandatory for the data controller to be able to perform his legal obligations,
- The data concerned is made available to the public by the data subject himself,
- Data processing is mandatory for the establishment, exercise or protection of any right,
- It is mandatory for the legitimate interests of the controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject.

The conditions for the processing of personal data, namely cases that make the processing of personal data lawful, are stipulated by the law numerus clausus and these conditions shall not be extended.

If the processing of personal data is based on one of the conditions listed above, then there is no need to obtain explicit consent from the person concerned.

**Personal Data Of Special Nature**

Personal data of special nature is the data that, if found out, could give rise to discrimination or victimization against the person concerned.

Therefore, they must be more strictly protected than other personal data.

Personal data of special nature may be processed upon the explicit consent of the person concerned or in the limited circumstances set out in the Law.

Personal data of special nature is set forth in the Law numerus clausus. These are; race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership to associations, foundations or trade-unions, health, sexual life, convictions and security measures, and the biometric and genetic data of persons.

It is not possible to extend the personal data of a special nature by analogy.

The Law makes a distinction among the personal data of special nature Accordingly, processing of the personal data regarding health and sexual life and those relating to health and sexual life which may be processed without seeking explicit consent of the data subject are regulated differently.

Pursuant to the Law, personal data of special nature may be processed in the following cases other than the explicit consent of the data subject.

- Personal data of special nature other than that of health and sexual life may be processed only in cases stipulated by the Law.
- Personal data regarding health and sexual life may be processed in order to protect public health, to provide preventive medicine, medical diagnosis, treatment, and

care services, to plan and manage health services and financing by the persons and authorized institutions and organizations who are under a confidentiality obligation

In this context, conditions on the processing of personal data are considered at the core of all processing activities of personal data, carrying out of the data processing activities in accordance with these conditions is adopted as the company policy.

## IV. DATA TRANSFER

### 1. Domestic Transfer

The personal data collected in order to process under the general principles set out in the Law may be transferred to third parties with the explicit consent of the data subject in accordance with the provision of Article 8 of the Law.

The Law seeks similar conditions for the processing of personal data and transferring such data in the country.

This article also provides for the conditions under which the personal data may be transferred to third parties without the explicit consent of the data subject.

On the other hand, processing of the personal data within the country in accordance with the law does not mean that such data may be directly transferred. Namely, the conditions set out in Article 5 and 6 should also be sought for the transfer.

In this context, one of the following conditions is required for the transfer of personal data. These conditions are;

- Obtaining explicit consent of the data subject,
- Being clearly provided for by the laws
- It is mandatory for the protection of life or physical integrity of the person or of any other person who is bodily incapable of giving his consent or whose consent is not deemed to be legally valid,
- Processing of personal data belonging to the parties of a contract is necessary provided that it is directly related to the establishment or fulfillment of that contract,
- It is mandatory for the data controller to be able to perform his legal obligations,
- The data concerned is made available to the public by the data subject himself,
- Data processing is mandatory for the establishment, exercise or protection of any right,
- It is mandatory for the legitimate interests of the controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject

The personal data of special nature may be transferred within the country if the explicit consent of data subject is obtained and/or it is clearly provided for by the laws in terms of personal data other than health and sexual life. Personal data regarding health and sexual life may be processed in order to protect public health, to provide preventive medicine, medical diagnosis, treatment, and care services, to plan and manage health services and financing by the persons and authorized institutions and organizations who are under a confidentiality obligation.

Unlike the fact that personal data can only be data of a natural person, the "data controller" and "data processor" can be either a natural or legal person.

Any natural and legal person processing personal data is either a data controller or data processor according to the purposes and methods of data processing.

In this context, the regulations contained in Article 8 of the Law must be complied with in order for data transfer of any kind between the persons fall in these two categories in question.

## 2. Transfer of Personal Data Abroad

Pursuant to Article 9 of the Law, personal data may be transferred abroad if;

- The data subject has given explicit consent pursuant thereto
- Satisfying of the conditions specified in the Law (Conditions set out in Paragraph 2 of Article 5 and Paragraph 3 of Article 6 of the Law) in the data transfer to the countries having an adequate level of protection (countries considered to be secure by the Board),
- If the conditions specified in the Law are satisfied (Conditions set out in Paragraph 2 of Article 5 and Paragraph 3 of Article 6 of the Law) in the data transfer to the countries having no adequate level of protection, undertaking adequate protection in writing and obtaining the consent of the board.

The Law seeks similar conditions for the processing of personal data and transferring such data abroad. Furthermore, it is stipulated therein that the additional measures should be taken in the transfer of personal data abroad.

In case of explicit consent of the data subject, the personal data may be transferred abroad.

In cases other than explicit consent, the Law provides for different provisions in the transfer of the personal data abroad according to whether there is an adequate level of protection in the country to where the transfer is made.

### a. If there is an Adequate Level of Protection

Personal Data may be transferred abroad if;

- Being clearly provided for by the laws,
- It is mandatory for the protection of life or physical integrity of the person or of any other person who is bodily incapable of giving his consent or whose consent is not deemed to be legally valid,
- Processing of personal data belonging to the parties of a contract is necessary provided that it is directly related to the establishment or fulfillment of that contract,
- It is mandatory for the data controller to be able to perform his legal obligations,
- The data concerned is made available to the public by the data subject himself,
- It is mandatory for the establishment, exercise or protection of any right,
- It is mandatory for the legitimate interests of the controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject.

When it comes to the personal data of special nature, in case of an adequate level of protection in the country to where the personal data is transferred the personal data other than that of health and sexual life may be transferred if it is clearly provided for by the Law, personal data of individuals regarding their health and sexual life in the countries having an adequate level of protection may be transferred without explicit consent of the data subject in order to protect public health, to provide preventive medicine, medical diagnosis, treatment, and care services, to plan and manage health services and financing by the persons and authorized institutions and organizations who are under a confidentiality obligation.

**b. For Data Transfer to the Countries Having No Adequate Level of Protection**

- At least one of the conditions listed in Articles 5 and 6 of the Law must be satisfied,
- The data controllers located in Turkey and relevant foreign country must undertake an adequate level of protection in writing,
- The consent of the Board must be obtained

In this context, our Company has adopted as the Company policy to act in compliance with the provisions described above, and personal data may be transferred provided that it complies with the above-mentioned conditions to MAPEI SPA, institutions and organizations permitted and/or mandated by the provisions of the legislation, our program partners and the banks, persons and companies from which we receive services and/or to which you are directed for your purchase of services, the persons and organizations we receive services and cooperate with to carry out our activities, the persons, companies and our units and personnel that can take precautions and furnish medical attention within the scope of the measures to be taken in particular in relation to health problems as well as the other third parties who are responsible for data security measures such as protection of your personal data, prevention of unauthorized access, and prevention of unlawful processing, and who provide support.

## V. DATA COLLECTION CHANNELS

The personal data may be collected by our Company verbally, in writing or electronically through forms such as application, registration and order forms, by means of our websites and emails, mobile apps, other forms collected, health reports, computer systems, programs and software, agreements, applications, forms, offers, audio and video recordings, cookies used by our computer to identify you during website visits and similar instruments, via our employees, administrative units, departments, secretariat, reception, security units, program and business partners and companies from which we receive services.

## VI. PURPOSES OF DATA PROCESSING

The purposes and legal grounds for the processing and transferring of personal data are; to fulfill legal and contractual obligations as well as to maintain customer relations, to update contact information, to open and track the customer records in the system, to provide all of our services, to maintain after-sale services, to fulfill financial obligations including billing transactions, to fulfill the personnel services and legal obligations pursuant thereto, to ensure that our relevant units can contact with you and your

general satisfaction, to determine the needs, to ensure the legal and actual security of our company, employees, customers and those concerned, to set our strategies, to provide our services in accordance with the requirements of legislation, contract, and technology, to improve our services, to carry out promotional activities, to make analyzes, to issue all the documents and records in line with the purpose of processing, to fulfill the retention, reporting and informing obligations set out by legislation, relevant regulatory authorities and other authorities, to benefit from domestic and international programs and to fulfill other requirements in accordance with the legislation.

## VII. OUR RESPONSIBILITIES

### 1. Obligation of Clarification

The law grants the data subject with a right to be informed about by whom, for what purposes and for which legal grounds their data are to be processed, for what purposes and to whom the data may be transferred, and these issues are considered under the obligation to inform of the data controller.

Accordingly, our Company, the data controller, has assumed the obligation to inform on the followings;

- The identity of the controller and of his representative, if any,
- For what purposes the personal data is processed,
- To whom and for what purposes the personal data may be transferred,
- Methods and legal ground of collection of the personal data,
- Other rights listed in Article 11 of the Law
- It adopted as the Company policy to act in accordance with the relevant obligation.
- In this context, you can find our Obligation of Clarification at the link .....

### 2. The obligation on the Security of Personal Data

In accordance with Article 12 of the Law on the security of personal data, our Company, the data controller, shall be obliged to

- Prevent unlawful processing of personal data,
- Prevent unlawful access to personal data,
- Ensure the retention of personal data

In order to fulfill these obligations, the data controller is obliged to take all necessary technical and organizational measures for providing an adequate level of security.

If the personal data is processed by any other legal and natural person on behalf of the data controller, then the data controller shall be severally liable to take necessary measures together with these persons.

The Law also introduces an auditing responsibility for the data controller regarding the security of personal data.

The data controller shall be obliged to perform the necessary audits or have them performed in his own institution or organization with the aim of implementing the provisions of this Law.

Therefore, the data controller may perform this audit by himself or through any third party.

On the other hand, data controllers and processors shall not disclose the personal data that they learn to third parties contrary to the provisions of the Law, and not use them for the purposes other than that of processing. This obligation shall survive after their retirement from the office.

Lastly, in the event that the personal data which is being processed is illegally obtained by others, the data controller shall promptly inform the data subject and the Board of this situation. The Board, if required, may announce the situation on its own website or through any method that it deems appropriate.

In this context, principles on the security of personal data are considered at the core of our all activities and the utmost care is shown to ensure the security of personal data and it is adopted as the Company policy.

## 3. The obligation on the Responding to the Application Lodged by the Data Subject

The data controllers shall be obliged to respond to the requests which are lodged by the data subject in writing and by other means determined by the Board as soon as possible depending on the nature of the and within 30 (thirty) days of the receipt at the latest and free of charge.

However, the data controller may charge a fee in the tariffs set by the Board from the applicant if the request necessitates any cost.

If the data controller accepts the request or rejects it by providing justified grounds pursuant thereto, it shall notify the data subject of its response in writing or electronically.

In the event that the request containing in the application is accepted, then the data controller shall do what is necessary for the concerned request.

If the application has resulted from the fault of the data controller, the charge shall be refunded to the data subject.

In cases where the application is rejected, the response is found to be insufficient or the application is not replied in a timely manner; the data subject may lodge a complaint before the Board within 30 (thirty) days as from the date on which he became aware of the response and in any circumstances within 60 (sixty) days from the application date.

In this context, compliance with the obligations regarding responding to the applications lodged by the data subjects is set to as the Company policy.

## 4. The obligation on Erasure, Destruction or Anonymization of the Personal Data in Case of the Disappearance of the Grounds that Entail the Processing

Erasure of Personal Data; shall mean a process of making personal data inaccessible and non-reusable for the relevant users in any way.

Data controllers shall be obliged to take any technical and organizational measures

to ensure that the erased personal data can be inaccessible and non-reusable for the relevant users.

Destruction of Personal Data; shall mean a process of making personal data inaccessible, irretrievable, and non-reusable by any person in any way.

Data controllers shall be obliged to take any technical and organizational measures required for the destruction of personal data.

Anonymization of Personal Data shall mean a process making of personal data non-associable with any identified or identifiable natural person in no way even by matching with other data. For personal data to be anonymized, personal data must be made non-associable with identified or identifiable natural person in spite of the use of appropriate techniques in terms of the registry medium and the relevant field of activity such as retrieving and matching personal data with another data by the data controller, receiver or receiver groups.

Data controllers shall be obliged to take any technical and organizational measures required for the anonymization of personal data.

In the event that the grounds that entail the processing have disappeared despite having been processed in accordance with the law, the erasure, destruction, and anonymization of such data ex officio or upon the request of the data subject is adopted as our Company policy, and the destruction processes are also presented below.

### 5. 5. The obligation on the Implementation of the Board's Resolutions

If the Board finds an infringement as a result of the examination made upon complaint or ex officio in cases where it finds out an infringement, then the Board shall resolve that the identified infringements shall be remedied by the data controller and notify the concerned persons of this resolution. The data controller has to implement this resolution without undue delay and no later than thirty days of the notification.

## VIII. RIGHTS OF DATA SUBJECT

Under Article 11 of the Law, the data subject shall have the following rights, which he may exercise any time by applying to the data controller;

- To learn whether or not her personal data has been processed;
- To request information if his personal data are processed,
- To learn the purpose of his data processing and whether this data is used for intended purposes,
- To know the third parties to whom his personal data is transferred at home or abroad,
- To request rectification in case personal data are processed incompletely or inaccurately,
- To request erasure or destruction of personal data,
- To request notification of the rectification, erasure or destruction to the third parties to whom personal data has been transferred,

- To object to the occurrence of any result that is to detriment of the person concerned by means of the analysis of personal data exclusively through automated systems,
- To request compensation for the damage arising from the unlawful processing of his personal data.
- Our Company has adopted as the Company policy to act in compliance with the rights of the concerned persons, Data Subjects may submit their request regarding their above-mentioned rights by filling out this form which can be found at ..... ..... and signing with a wet signature, to the address " Beştepeler Mah., Nergis Sok., Via Flat İş Merkezi, No.7/2, Daire:48, Söğütözü/ANKARA-TURKEY".

# IX. DESTRUCTION OF PERSONAL DATA

## 1. Grounds Entailing Destruction of Personal Data

- Amendment and abolishment of the provisions of the relevant regulations on which the processing thereof is based,
- The disappearance of the purpose entailing the processing or storage thereof,
- Withdrawal of the explicit consent by the data subject in cases where the processing of personal data is only carried out on the basis of explicit consent,
- Acceptance of the application by the Institution, which was lodged for the deletion or destruction of his personal data by the data subject under his rights pursuant to Article 11 of the Law,
- In cases where our Company rejects any application lodged by the data subject claiming the deletion, destruction or anonymization of his personal data, where it deems the response given to be insufficient or where it fails to respond within the period of time as prescribed by the Law, that he has made a complaint before the Board and that the request pursuant thereto has been accepted by the Board,
- Expiration of the maximum period of time entailing the storage of personal data, and the absence of any conditions that justify the storage of personal data for any longer period of time,

Personal data shall be deleted or destroyed by our Company upon the request of the data subject or deleted, destroyed or anonymized ex officio in the foregoing cases.

## 2. 2. Destruction Methods of Personal Data

### 2.1 Erasure of Personal Data

**Personal Data on Servers**

For the personal data on the servers, those of which the required period of retention has expired, the system administrator shall remove the access authority of the relevant users and erase them.

**Personal Data in Electronic Medium**

The personal data in an electronic medium, those of which the required period of retention has expired shall be made inaccessible and non-reuseable in any way for other employees (relevant users) except the database administrator.

**Personal Data in Physical Medium**

The personal data in a physical medium, those of which the required period of retention has expired shall be made inaccessible and non-reuseable in any way for other employees except for the unit manager responsible for the document archive

Furthermore, such personal data shall be blackened out by drawing/painting/erasing so that such data cannot be read.

**Personal Data in Portable Medium**

The personal data in Flash-based retention environments, those of which the required period of retention has expired, shall be encrypted by the system administrator and the data shall be retained in safe mediums with encryption keys by granting access only to the system administrator.

## 2.2 Destruction of Personal Data

**Personal Data in Physical Medium**

Personal data in hardcopies, those of which the required period of retention has expired shall be irretrievably destroyed in paper shredders.

**Personal Data in Optical/Magnetic Medium**

The personal data in optical and magnetic medium those of which the required period of retention has expired shall be physically destroyed by melting, burning or pulverizing. In addition, the magnetic medium shall be made illegible by passing it through a dedicated device and exposing it to a high level of the magnetic field.

## 2.3 Anonymization of Personal Data

Anonymization of Personal Data shall mean a process making of personal data non-associable with any identified or identifiable natural person in no way even by matching with other data.

For personal data to be anonymized, personal data must be made non-associable with identified or identifiable natural person in spite of the use of appropriate techniques in terms of the registry medium and the relevant field of activity such as retrieving and matching personal data with another data by the data controller or any third parties.

.

### 3. Retention and Destruction Periods

Regarding the personal data being processed by our Company within the scope of its activities; retention periods on a personal data basis regarding personal data within the scope of the activities carried out depending on the Processes shall be included in the Data Processing Inventory; retention periods on a data category basis shall be included in during registration to VERBIS; retention periods on a Process basis shall be included in this policy, and are listed below table.

| Process | Retention Period | Destruction Period |
|---|---|---|
| All Transactions other than retentions and transactions required by the legislation, and those specified below | 5 Years | In the first periodic destruction process following the end of the retention period |
| Contracts | 10 Years following the end of the contract | In the first periodic destruction process following the end of the retention period |
| Communication Activities | 10 Years following the end of the activity | In the first periodic destruction process following the end of the retention period |
| Management of the Human Resources Processes | 10 Years following the end of the activity | In the first periodic destruction process following the end of the retention period |
| Tracking Systems | 10 Years | In the first periodic destruction process following the end of the retention period |
| Management of Hardware and Software Processes | 2 Years | In the first periodic destruction process following the end of the retention period |
| Visitor Registration | 2 Years following the end of the activity | In the first periodic destruction process following the end of the retention period |
| Security Camera Records | 2 Years | In the first periodic destruction process following the end of the retention period |

### 4. Periodic Destruction Interval

In accordance with Article 11 of the relevant Regulation, the Company has determined the periodic destruction interval to be 6 (six) months. Accordingly, the Company shall perform periodic destruction process in June and December every year.

## X. THIS POLICY IS ISSUED IN ORDER TO ESTABLISH AND ANNOUNCE THE PRINCIPLES AND LIABILITIES OF OUR COMPANY.