chimera

PERSONAL DATA PROTECTION POLICY

Table of Contents

1. Purpose and Scope

This Chimera Personal Data Protection Policy ("Policy"), which is part of the Chimera Code of Ethics, aims to provide a compliance framework and coordinate compliance activities for Chimera for complying with Legislation on the protection and processing of personal data. In this context, the objective is to ensure the personal data processing activities by Chimera to be carried out in compliance with the principles of lawfulness, good faith, and transparency.

All employees, directors and officers of Chimera shall comply with this Policy, which is an integral part of Chimera Code of Ethics. Chimera also expects and takes necessary steps to ensure that all of its Business Partners - where applicable - comply with and/or act in accordance with this Policy.

2. Definitions

Business Partner	: Suppliers, customers and other third parties with whom the company has a business relationship and all kinds of representatives, subcontractors, consultants, etc. acting on behalf of the company, as well as their employees and representatives.
Chimera	: Chimera Mühendislik Anonim Şirketi
Explicit Consent	: Consent related to a specific subject, based on information and expressed with a free will.
Anonymization	: Making personal data unrelated to an identified or identifiable natural person under any circumstances, even when by matching with the other data.
Data Subject	: A real person of whom personal data are processed. (customers, visitors, employees and employee candidates, etc.).
Personal Data	: Any information related with an identified or identifiable real person.
Processing of Personal Data	: Any activity performed on data such as obtaining personal data by fully or partially automatic means or non-automatic means that are part of a data registration system; recording, storage, retention, revision, modification, disclosure, transfer, receiving of data, rendering the data obtainable or classification or prevention of use.
Legislation	: All of the relevant legislation in force in Turkey and relevant countries regarding the protection of personal data, especially the Law on the Protection of Personal Data No.6698.
Special Categories of Personal Data	: Race, ethnic origin, political view, philosophical belief, religion, religious sect or other beliefs, clothing style, association, foundation or union membership, health, sexual life, criminal convictions, and security measures as well as biometric and genetic data are special categories of personal data.
VERBİS	: Data Controllers Registry Information System

Data Processor	: A real or legal person that processes personal data for and on behalf of the data controller based on the authorization granted by the data controller.
Data Controller	: A real or legal person who determines the objectives and means of personal data processing and is responsible for the establishment and management of the data recording system.

3. General Principles

Breach of this Policy may result in significant consequences for Chimera, its associated executives and employees including legal, administrative, and criminal penalties based on the Legislation in the region of operation, and, most significantly, the breach may result in serious harm to the reputation of Chimera.

One of the most important issues for Chimera is to act in accordance with the Legislation and the general principles set out in the Legislation with regards to processing of personal data. In this regard, Chimera is expected to follow the guidelines outlined below when processing personal data in compliance with the Legislation.

Chimera carries out the personal data processing practices within the scope of its activities in accordance with the Chimera Personal Data Protection and Processing Policy.

3.1. Processing of personal data in accordance with the law and principle of good faith

The general rule of trust and good faith in compliance with the Legislation must be adhered to on the subject of personal data processing. In this context, personal data should be processed in accordance with general principles of law, good-will and general morality to the extent required by business activities and limited to these activities.

3.2. Ensuring that personal data is accurate and up-to-date when required

Systems must be established, and necessary measures must be taken to ensure that the personal data being processed are accurate and up-to-date while taking account of data subjects' rights.

3.3. Processing of personal data for specific, explicit and legitimate purposes

Personal data must be processed for legitimate and lawful purposes. Chimera must only process personal data in connection with their activities and to the extent necessary. Prior to personal data processing operations, the purposes for processing personal data should be determined.

3.4. Being limited, proportionate and relevant to the purpose of processing

Personal data must be processed adequately for carrying out the determined purposes and processing of personal data that is not necessary for fulfilling the purposes must be avoided.

3.5. Storing for the Period Stipulated in the Relevant Legislation or the Period Required for the Processing Purpose

Personal data must only be stored for the period stipulated in the relevant Legislation or for the period required for the personal data processing purpose.

In this regard, firstly determination must be made whether a certain period is stipulated for the storage of personal data in the relevant Legislation, if any period is determined, this period should be complied with. If no period is determined, personal data must be stored for the period required for carrying out the purpose of the processing. Personal data must be erased, destructed, or anonymized in case the period expires or the reason for its processing no longer exists. Personal data must not be stored based on the possibility of future use.

4. Application of the Policy

4.1. Processing Personal Data Based on The Data Processing Conditions

4.1.1. Execution of Personal Data Processing Activities Based on the Personal Data Processing Conditions Specified in the Legislation

As a rule, personal data must be processed based on at least one of the conditions specified in the Legislation. Determination should be made on whether the personal data processing activities carried out by the company's business units are based on at least one of the conditions. Personal data processing activities that do not meet this requirement should not be included in the processes.

4.1.2. Execution of Special Categories of Personal Data Processing Activities Based on Special Categories of Personal Data Processing Conditions Stipulated in the Legislation

As a rule, special categories of personal data must be processed based on the conditions specified in the Legislation. Chimera must; ensure that It must be ensured that the special categories of personal data processing activities carried out by the company's business units are in line with these conditions, the necessary technical and administrative measures for the processing of the special categories of personal data must be taken and it must be ensured that the following conditions are met:

i. **Special categories of personal data excluding health and sexual life** can be processed without the explicit consent of data subjects if it is explicitly stipulated in the laws, in other words, if there is an explicit provision in the relevant law regarding the processing of personal data. Otherwise, explicit consent of the data subject should be obtained.
ii. **Special categories of personal data regarding health and sexual life** can be processed without the explicit consent of data subjects for the purposes of the protection of public health, carrying out preventive medicine, medical diagnosis, treatment and care services, planning of financing and management of health services by the persons who are bound with professional secrecy or legally authorized authorities and institutions. Otherwise, explicit consent of the data subject should be obtained.

Processing of special categories of personal data must be carried out in accordance with the provisions set out in the Legislation regarding the processing of special categories of personal data and transfer of data to domestic third parties and abroad. In addition to the above-mentioned

matters, in these cases, personal data processing activities must also be carried out by fulfilling the special requirements set forth in the Legislation.

4.2. Requirements To Be Complied with For Transfer Of Personal Data

Personal data of data subjects should be transferred to third parties in accordance with the purposes and legal basis for personal data processing and by taking the necessary security measures. In this regard, necessary processes for acting in accordance with the conditions stipulated in the Legislation must be designed.

4.3. Obligations Related to The Protection and Processing Of Personal Data

4.3.1. Obligation to Register with VERBİS

Chimera must register with VERBİS as Data Controllers if they are under the obligation to register according to the criteria stipulated in the Legislation. In case of a revision in the registered information, the information in VERBİS must be updated within seven days from the date of revision.

Compliance Officer must be informed twice a year, every 6-month periods (June-December) regarding the updates made by the Chimera in VERBİS.

4.3.2. Obligation to Inform Data Subjects

Data subjects must be informed at the time of collection of personal data in accordance with the Legislation.

In this regard, the personal data collection channels must be determined for the fulfillment of the obligation to inform; data subjects must be informed through the privacy notices which comply with the scope and conditions specific to these collection activities required in the Legislation; the appropriate processes should be designed accordingly by the Chimera.

Company must keep the personal data collection channels up to date as a list and share the list with Compliance Officer twice a year, every 6-month periods (June-December).

4.3.3. Obligation to Ensure the Security of Personal Data

Along with the awareness on the importance of ensuring data security in all aspects within the Chimera, necessary and adequate technical and administrative measures must be taken to prevent unlawful processing of personal data or access to data, and to store data in accordance with the Legislation and in this regard necessary audits must be conducted by the company and/or have audits conducted by a third party.

Within the scope of the measures taken by the company, trainings regarding the Legislation should be given to the employees. The company must provide information to Compliance Officer regarding the trainings carried out in this context.

4.3.4. Audit of the Measures Taken for the Protection of Personal Data

Systems for conducting and having the necessary audits regarding the functioning of the measures taken in terms of technical and administrative measures must be built. These audit results must be reported to the company's compliance department or manager, and the necessary actions must be taken to improve the measures taken.

4.3.5. Measures to be Taken in Case of Unauthorized Disclosure of Personal Data

The data subject and the relevant authorities must be informed as soon as possible in compliance with the Legislation in case the processed personal data is illegally obtained by third parties. In this context, the necessary internal structure in which Compliance Officer take part, must be created within the company.

4.3.6. Obligation to Inform the Data Subject

The data subjects have the right to request information about their processed personal data by applying data controllers whenever they need.

In this context, the necessary procedures and processes must be established and implemented within the company in the matters of designing the necessary application channels in accordance with the Legislation, evaluating the applications, answering the applications within the periods stipulated in the Legislation in order to evaluate the rights of the data subjects and to provide the necessary information to the data subjects.

In the case that the data subjects submit their requests regarding their rights to the company, the relevant request must be responded as soon as possible and within thirty days at the latest.

While concluding the relevant application of the data subject, information shall be provided with a wording and format easily understandable to the data subject. Necessary warnings should be given within the company and awareness must be ensured that data subjects have a right to complain to the relevant authority in the case that the data subject's application is rejected, the response is insufficient, or the application is not responded within the stipulated timeframe.

Data subject applications and the response processes should be kept as a list by the Company and must be shared with Compliance Officer twice a year at 6-month periods (June-December).

In addition, the opinions of Compliance Officer must be taken before any action is taken regarding all kinds of information and document requests from the relevant authorities to the company and all kinds of applications to be made by the company to these authorities.

5. Authority and Responsibilities

All employees and directors of Chimera are responsible for complying with this Policy, implementing and supporting the relevant Chimera’s procedures and controls in accordance with the requirements of this Policy. If there is a discrepancy between the local regulations, applicable in the countries where Chimera operates, and this Policy, the stricter of the two shall prevail, unless such practice is in violation of the relevant local laws and regulations, the stricter of the two, supersede.

If you become aware of any action that you believe is inconsistent with this Policy, the applicable law or the Chimera Code of Ethics, you may seek guidance or report the incident to your line managers. Alternatively, you may report the incident to the Compliance Officer.

Chimera employees may contact the Compliance Officer for their questions regarding this Policy and its application. Violation of this Policy may result in significant disciplinary actions including dismissal. If this Policy is violated by third parties, their contracts may be terminated.