## P GDP 08 CLARIFICATION TEXT ABOUT CAMERA RECORDINGS

### 1. PURPOSE and SCOPE

The personal data processing activities carried out by Etiya Bilgi Teknolojileri Yazılım Sanayi ve Ticaret A.Ş. ("Company" or "Etiya") at the entrances of the building facility and within the facility are carried out under the Constitution of the Republic of Turkey, the Law on the Protection of Personal Data ("PDPL") and other relevant national and international legislation. To ensure security as a data controller under the PDPL, Etiya carries out personal data processing activities in the buildings and offices of our Company for the monitoring of the entrances and exits of employees, guests and suppliers, and the critical server room entrance within the offices with the monitoring activity with security cameras. In addition, Etiya carries out personal data processing activities as a data controller by using security cameras and recording guest entrances and exits.

### 2. RESPONSIBLE

Etiya Employees

### 3. IMPLEMENTATION

#### 3.1.CAMERA MONITORING AND RECORDING ACTIVITIES CARRIED OUT AT THE ENTRANCES AND INSIDE ETIYA BUILDINGS AND OFFICES

Etiya processes personal data by taking images with a closed-circuit camera system (CCTV) at the Company's campuses to ensure legal, technical, and commercial occupational safety.

**3.1.1.Legal Basis of Camera Monitoring Activity and Method of Collecting Personal Data**

The camera monitoring and recording activities by Etiya are carried out under Law No. 5188 on Private Security Services and the regulation on the implementation of this law and based on the legal reason based on the legitimate interest of our Company. Personal data are collected electronically through closed-circuit camera systems to ensure the security of Etiya buildings within the framework of the personal data processing conditions specified in Articles 5 and 6 of the KVKK.

**3.1.2 Conducting Monitoring Activities with Security Camera According to KVKK Law**

To ensure security in Etiya buildings and offices, it carries out security camera monitoring activities by the personal data processing conditions listed in the KVKK for the purposes stipulated in the relevant legislation in force.

**3.1.3 Announcement of Monitoring Activity with Camera**

Article 10 of the KVKK by Etiya, under the article, the personal data owner is enlightened. Etiya notifies with more than one method regarding monitoring its lighting with a camera in relation to general issues. Thus, it is aimed at preventing damage to the fundamental rights and freedoms of the personal data owner to ensure transparency and enlightenment of the personal data owner. For camera monitoring activity by Etiya, a notification letter stating that monitoring will be made hung at the entrances of the areas where monitoring is carried out.

**3.1.4 Purpose of Conducting Camera Monitoring Activity and Limitation of Purpose**

Etiya processes personal data in a limited, restrained manner related to the purpose of the process, under Article 4 of the KVKK. Therefore, the purpose of maintaining the monitoring activity with a closed circuit camera by Etiya is limited to the purposes listed in this Policy. In this direction, the monitoring areas, recording periods, locations, and several security cameras are sufficient to achieve the security purpose and are limited to this purpose. It is not subject to monitoring the person’s privacy in areas that may result in interference in excess of security purposes (for example, kitchen, toilets, etc.).

**3.1.5 Ensuring the Security of the Data Obtained**

Under Article 12 of the KVKK, necessary technical and administrative measures are taken by Etiya to ensure the security of the personal data obtained due to the camera monitoring activity.

#### 3.1.6 Retention Period of Personal Data Obtained by Camera Monitoring Activity

Etiya's storage period of personal data with the camera is 30 days.

#### 3.1.7 For Which Purposes the Personal Data Obtained Will Be Transferred to Whom

A limited number of employees have access to the information obtained due to monitoring. Etiya can transfer camera images to authorized public institutions per the legislation to ensure the security of Etiya buildings and offices within the framework of the personal data processing conditions and purposes specified in Articles 8 and 9 of the KVKK. (For example, with the written request of the prosecutor's office or judge during the investigation of an incident) A limited number ofpeople who have access to the records declare that they will protect the confidentiality of the data they access with a confidentiality undertaking.

### 3.2 FOLLOW-UP OF THE ENTRANCES AND EXITS OF GUESTS AND SUPPLIERS CARRIED OUT AT AND WITHIN THE ETIYA BUILDING, OFFICE ENTRANCES

By Etiya, personal data processing activities are carried out to monitor guest entries and exits in Etiya buildings and offices for the purposes specified in this Policy and to ensure data security as a data controller under the KVKK. When obtaining the names and surnames of the persons who come to the Etiya buildings as guests or through the texts hung in Etiya or otherwise made available to the guests, the personal data owners in question are enlightened in this context. The data obtained for guest entry-exit follow-up are processed only for this purpose. The relevant personal data are collected based on the legal reason related to the legitimate interest of our Company within the framework of the personal data processing conditions specified in Articles 5 and 6 of the KVKK and recorded in the data recording system during the visit to the Etiya building and office in the physical environment. Etiya can transfer the personal data collected within the scope of visitinf the Etiya buildings to the authorized public institutions under the legislation to ensure the security of the Etiya buildings and offices within the framework of the personal data processing conditions and purposes specified in Articles 8 and 9 of the KVKK.

### 3.3 PURPOSES OF PROCESSING, CATEGORIZATION, AND STORAGE PERIODS OF PROCESSED PERSONAL DATA

Under Article 10 of the KVKK, Etiya informs the personal data owner which groups of personal data owners process which personal data within the scope of the disclosure obligation, the purposes of processing the personal data of the personal data owner, and the retention periods.

### 3.4 DELETION, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA

Although Etiya has processed the personal data subject to this Policy under the provisions of the relevant law as regulated in Article 138 of the Turkish Criminal Code and Article 7 of the KVKK, the personal data shall be deleted, destroyed, or anonymized according to Etiya's own decision or upon the request of the personal data owner if the reasons requiring processing disappear.

#### 3.4.1 Etiya, Obligation to Delete, Destroy, and Anonymize Personal Data

Although Personal Data has been processed under the provisions of the relevant law as regulated in Article 138 of the Turkish Criminal Code and Article 7 of the KVKK, the personal data shall be deleted, destroyed, or anonymized under the decision of Etiya or upon the request of the personal data owner in case the reasons requiring the processing disappear. In this context, Etiya fulfills its obligation by the methods described in this section.

#### 3.4.1.1 Deletion and Destruction Techniques of Personal Data

Although Etiya has been processed under the relevant law provisions, it may delete or destroy personal data on its own decision or upon the request of the personal data owner if the reasons requiring the processing disappear. The most commonly used erasure or destruction techniques by Etiya are listed below:

##### 3.4.1.1.1 Physical Destruction

Personal data can also be processed by non-automated means, provided they are part of any data recording system. When deleting/destroying such data, the method of physically destroying personal data in a way that Etiya can't use afterward is applied.

#### 3.4.1.1.2 Secure Deletion from Software

When deleting/destroying data processed by fully or partially automated means and stored in digital environments, methods are used to delete the data from the relevant software so that it cannot be recovered again

#### 3.4.1.1.3 Securely Erased by Expert

In some cases, Etiya may hire an expert to delete personal data on its behalf. In this case, the personal data is securely deleted/destroyed by the expert in the field in such a way that it cannot be recovered again.

### 3.4.1.2 Techniques for Anonymizing Personal Data

Anonymization of personal data means that personal data cannot be associated with an identified or identifiable natural person under any circumstances, even by matching it with other data. Etiya can anonymize personal data when the reasons that require processing personal data processed in accordance with the law are eliminated. Under Article 28 of the PDPL, personal data that has been anonymized may be processed for research, planning, and statistics purposes. Such processing is outside the scope of the PDPL, and the explicit consent of the personal data owner will not be sought. Personal data processed by anonymization will be outside the scope of PDPL. The most commonly used anonymization techniques by Etiya are listed below.

#### 3.4.1.2.1 Masking

Data masking is the method of anonymizing personal data by removing the basic determinant information of personal data from the data set. Example: Transforming the personal data owner into a data set where it becomes impossible to identify the personal data owner by removing information such as the name that enables the identification of the personal data owner, the TC Identity Number, etc.

#### 3.4.1.2.2 Aggregation

Many data are aggregated with the data aggregation method, and personal data cannot be associated with any person. Example: Revealing that there are as many as X years old Z employees without showing the age of the employees individually.

#### 3.4.1.2.3 Data Derivation

With the data derivation method, more general content is created from the content of personal data, and it is ensured that personal data cannot be associated with any person. Example: Specifying ages instead of dates of birth; designation of the region of residence instead of the street address.

#### 3.4.1.2.4 Data Mixing

The data mixing method ensures that the values in the personal data set are mixed and the link between the importance and the people is broken. Example: Changing the nature of the voice recordings so that the data owner cannot be associated with the sounds. Physical Space Security Information: Personal data related to records and documents taken at the entrance to the physical space, during the stay in the physical space; camera records, fingerprint records and records taken at the security point, which are obviously belonging to a natural person whose identity is determined or identified; which are processed partially or completely automatically or as part of the data recording system. Audiovisual Information: These are the data contained in the documents that are copies of the documents containing personal data and the voice recordings (except for the records included within the scope of the Physical Space Security Information) and photographic and camera records, which belong to a natural person whose identity is determined or identifiable by a real person.

## 3.5 THE RIGHTS OF THE PERSONAL DATA OWNER LISTED IN ARTICLE 11 OF THE KVK LAW

We inform you that personal data owners have the following rights under Article 11 of the PDPL:

- To learn whether their personal data is processed or not,
- If their personal data has been processed, to request information about it,
- To learn the purpose of processing personal data and whether they are used per their purpose,
- To know the third parties to whom their personal data are transferred at home or abroad,
- To request the correction of personal data if it is incomplete or incorrectly processed and to request that the transaction carried out within this scope be notified to third parties to whom their personal data is transferred,

- To request the deletion or destruction of personal data if the reasons requiring the processing disappear even though it has been processed under the provisions of the Law and other relevant laws, and to request that the transactions carried out within this scope and in case their personal data are processed incompletely or incorrectly to be notified to the third parties to whom their personal data is transferred,
- To object to the occurrence of a result against him by analyzing the processed data exclusively using automated systems,
- Requesting compensation for the damage in case of damage due to unlawful processing of personal data.

You can submit your applications for your rights listed above to our Company by filling out the Data Owner Application Form, which you can access through our general clarification text in the **Etiya Privacy Policy.** Depending on the nature of your request, your applications will be concluded free of charge as soon as possible and within thirty days at the latest; however, if the transaction requires an additional cost, you may be charged a fee according to the tariff to be determined by the Personal Data Protection Board.

**4. FORMS, RECORDS, SCHEMES**

**5. REFERENCE DOCUMENTS**