CCTV POLICY AND DISCLOSURE STATEMENT

Document Name : CCTV Policy and Disclosure Statement

Document No Doc- : KV-ANA009

ument Supervisor : Yusuf Söylemez

Publishing De- : IT DEPARTMENT

VERSION HISTORY

Version	Date of Effectiveness	Definition
v1.0	13.06.2017	Initial Publication
v2.0	08.01.2020	Optimization

CCTV POLICY

- INTERNAL DIRECTIVE

Points to Consider When Installing and Operating the Camera Recording System

(1) The company must publish this Policy on its corporate website (online policy regulation) and must put up a notice at the entrances of the areas where the surveillance will take place (on-site disclosure).

(2) The company must sign a letter of undertaking with the security firm that installs and operates the CCTV system, agreeing on the terms governing the protection and processing of personal data. Only a limited number of employees must have access to live camera recordings and the records saved and preserved digitally. Those who have access to the recordings must declare through a non-disclosure agreement that they shall protect the privacy of the data that they access.

(3) The company must take all necessary technical and administrative measures to ensure the security of personal data obtained as a result of the CCTV monitoring activity. Camera recordings must be saved and preserved in secure places that are accessed only by authorized personnel.

(4) It must be ensured that camera recordings are relevant, limited and measured; and in line with these principles, factors such as the number of cameras, surveillance areas, and surveillance hours must be implemented for the purpose of - and solely confined to - effectively ensuring security. In that regard, it must be ensured that cameras are placed only at strategically important locations, and - as a general rule - at entrances and exits.

(5) Areas where surveillance might cause interventions that exceed the purpose of security (for example, places of worship, dressing rooms, restrooms and similar places) must not be subjected to surveillance activities.

(6) It must be checked whether the cameras only record footage from the intended areas. Cameras must not focus on a different area or person.

(7) In the recorded areas, it is obligatory to put up the visual below at prominent locations.

(8) Camera recordings may be transmitted to third persons only under the conditions specified in this Disclosure Statement. Recordings must not be shared on the internet, or transferred to media or third parties other than authorized institutions. All transfers must be listed in an official report, which must then be archived systematically.

(9) While sharing camera recordings, the following documents and information must be added to the report:

(a) The number and location of the camera,

(b) Sharing purposes,

(c) The date, time and other relevant information regarding the shared footage,

(ç) The names of those present at the time the footage is shared (for example, data subject, their lawyer, data controller representative),

(d) And whether the footage has been edited to prevent persons other than the data subject from appearing in it.

(10) Cameras must never record audio.

(11) Cameras must continue recording 24/7. It must be stated in the Disclosure Statement if the cameras record based on motion sensors.

(12) It must be ensured that the recording quality is at a specified level.

(13) In cases where mobile security cameras are used, the individuals in the recorded environment must be informed of the surveillance activity at the time of arriving at the place.

(14) If the camera recordings are to be used for job monitoring, this must be explicitly stated in the disclosure statement regarding the processing of employee personal data.

(15) It must be ensured that camera recordings are only seen by authorized persons, and that screens showing the recordings are not positioned to be visible to visitors or employees.

CAMERA INVENTORY

Camera No.	Location	Active?

REPORT

Incident Details :

Party with whom recordings are shared :

Camera No. :

Camera Location :

Date of Registry :

Sharing Date :

Sample Disclosure Warning

[COMPANY]

ALL ACTIVITIES ARE RECORDED 24/7 IN ORDER TO ENSURE SECURITY IN THIS AREA.

For more information, go to https://snitechnology.net/kvkk.

CAMERA RECORDING DISCLOSURE STATEMENT

I. Data controller

As per the Law No. 6698 on the Protection of Personal Data ("Law"), your personal data is being processed by SNI **TEKNOLOJİ HİZMETLERİ A.Ş.** (“Company”) within the scope specified below.

II. The Manner in Which Personal Data is Collected and its Legal Rationale

This Camera Disclosure Statement notifies you of the fact that camera surveillance equipment is installed in areas belonging to **SNI TEKNOLOJİ HİZMETLERİ A.Ş .’** including in buildings, facilities, premises, workplaces, additional buildings, auditing sites, the environs of the production area, stores, yards, entrance gates, building exteriors, office entrance halls, event halls, diners, cafeterias, visitor lobbies, parking spaces, security cabins, floor corridors, other service areas and areas where the warning sign below is located ("company premises"). The camera surveillance system records and processes individuals and objects that are within the viewing angle of camera equipment. The system continues to function as long as it detects movement thanks to its built-in motion sensors. Visual information and camera recordings are processed through the video surveillance system.

Your personal data is processed for the purposes of fulfilling the legal obligations of the data controller (monitoring whether occupational safety/security rules are implemented, detecting and preventing unauthorized access to work sites in an effort to ensure information security), ensuring the legitimate interests of the data controller (preserving camera recordings to ensure the security of physical locations, detecting and investigating breaches in workplace rules), and in cases explicitly stated in law (Law No. 5188 on the Private Security Services, Labor Law No. 4857, Law No. on Job Safety and Security).

III. Our Purposes for Processing Personal Data

Your abovementioned personal data shall be processed for the fulfillment of the purposes below that are subject to your transfer of the said data to us:

- Protecting company premises from all kinds of attacks, theft, robbery or other harm that might impact individuals, objects or products present at the premises
- Ensuring the security of company premises, infrastructure, products, and operations, as well as taking measures against potential security breaches
- Informing authorized entities and institutions,

- Ensuring the legal, technical and commercial-business safety of the Company and individuals that are in a business relationship with the Company
- Planning and executing the company's information security processes
- Checking entries/exits to and from the workplace
- Creating and monitoring visitor records
- Planning and/or executing occupational health and/or safety processes, and fulfilling the obligation related to these purposes
- Preventing fire and similar disasters
- Managing the areas located at the company's premises (teknopark, mall, parking spaces, designated areas)
- Detecting and investigating breaches in workplace rules
- Managing emergency management processes,

IV. Transferring Personal Data

In line with the "need to know" and "need to use" principles, our Company strives to process your personal data by ensuring the necessary data minimization and taking the required technical and administrative security measures. We are obligated to share the personal data we process with third parties for a specific set of purposes, since activities such as ensuring the security of company premises, managing and auditing processes related to ensuring compliance with workplace rules, and managing digital infrastructure require a constant stream of data transfer with various stakeholders.

In order to solely fulfill the abovementioned purposes, your personal data may be shared with our shareholders, business partners, subsidiaries and affiliates, holding companies, the companies and shareholders of **SNI BİLİŞİM TEKNOLOJİ SANAYİ VE TİCARET A.Ş.** with which we have a special business partnership for conducting business continuity and information security processes, as well as with our business partners and service providers that run provide, operate, or offer services for our IT infrastructure, our business partners and services providers that offer quality control, complaint management, and risk analysis services, legally authorized public institutions, private persons, organizations and third parties, and exclusively designated third parties in line with the legitimate interests of the data controller, in accordance with the purposes specified in this disclosure statement, and may be processed domestically or internationally. In addition, personal data may be shared with the following parties:

- With security companies or service providers that install or operate the technical infrastructure, for the purpose of ensuring the security of the Company and its premises
- Suppliers for the purpose of storing employee data physically and electronically
- Experts, law firms and auditing companies for the purpose of carrying out auditing and fact-finding activities; as well as public institutions, insurance companies, social support funds and business advisors for the purpose of fulfilling regulatory and contractual obligations
- Authorized administrative and auditing boards and/or other authorized auditing institutions,
- Legal authorities, law enforcement, or public institutions for the purpose of resolving legal conflicts or if it is requested pursuant to legal regulations.

VI. Rights of the Data Subject

In accordance with the Communique on Procedures and Principles of Applying to Data Controllers, you - as the data subject whose personal data is being processed - can contact us using the **kvkk@snitechnology.net** email address or the form at **https://snitechnology.net/kvkk** to exercise your rights as per Article 11 of the Law governing the rights of the data subject (learn whether your personal data is processed or not, request information if your personal data is processed, learn the purpose of your data processing and whether this data is used for intended purposes, know the third parties to whom your personal data is transferred at home or abroad, request the rectification of the incomplete or inaccurate data, if any, request the erasure or destruction of your personal data, request notification of all operations to third parties to whom your personal data has been transferred, object to the processing, exclusively by automatic means, of your personal data, and request compensation for