

Information on the Use of Electronic Monitoring System

We hereby inform you that the electronic monitoring system (surveillance camera system) is operated. The electronic monitoring systems of the store are managed by the executive staff of Oboler Ltd.

We inform you that the rules for recording, using, and retaining image and sound recordings are governed by the provisions of Act CXXXIII of 2005 on the Rules of Personal and Property Protection and Private Investigation Activities (Szvtv.), as well as the provisions of Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (Info Act). The operation of the electronic monitoring system is carried out based on the explicit consent specified in Section 30 (2) of the Szvtv., as detailed below, for the protection of human life, physical integrity, and property, to prevent and detect violations and accidents, to catch offenders in the act, and to provide evidence of violations. We draw your attention to the fact that entering the premises monitored by cameras after being informed by this notice constitutes explicit consent to data processing.

Scope of Data Processed: The facial images, voices, and other personal data of customers appearing in the image and sound recordings.

The electronic monitoring system operates 24 hours a day, seven days a week. The recordings are stored on a server located in the security service room for three working days.

To ensure the secure handling of personal data, the protection of data stored on the server is provided by personal usernames and passwords, which allow for determining who accessed the data and when.

Authorized employees of Oboler Ltd. are entitled to view the live feed from the cameras. The recordings of the cameras may be viewed by the company's executives, the store manager, or, in the event of their unavailability, the current duty manager of the company.

Stored recordings of the operated camera surveillance and recording system can only be accessed by authorized personnel for the purpose of proving violations against human life, physical integrity, and property, identifying the offender, or investigating other incidents or accidents affecting life or physical integrity.

Oboler Ltd. records in a logbook the name of the person accessing the recordings, the reason for accessing the data, and the time of access.

Data transfer is only possible in the context of ongoing procedures regarding unlawful conduct or breach of obligations, to the authorities or courts conducting such proceedings. The scope of data transferred may include recordings containing relevant information created by the camera system and the names of individuals possibly appearing in the recordings.

We inform you that individuals whose rights or legitimate interests are affected by the recording of image and sound may request a copy of the recordings made about them by the electronic monitoring system. Additionally, in accordance with applicable legal provisions, they may request the deletion of the recordings. Furthermore, those whose rights or legitimate interests are affected by the recording of image and sound may, within three working days

from the recording, request that the data not be destroyed or deleted by Merse and Merse Ltd. by providing proof of their rights or legitimate interests.

We also inform you that you may request information about the processing of your personal data at any time from the executive officer of Oboler Ltd. You may also request the correction or blocking of your personal data in accordance with applicable legal provisions. Additionally, you may object to the processing of your personal data.

We inform you that in the event of a violation of your rights, you may turn to the courts in accordance with the provisions of the relevant laws. Furthermore, anyone may file a complaint with the National Authority for Data Protection and Freedom of Information, alleging that a violation of rights occurred or that there is an imminent threat of such a violation in connection with the processing of personal data.

Premises Monitored by Cameras (Based on Camera Numbers):

- Entrance door camera
- Camera installed in the waiting area

The primary purpose of monitoring is the protection of the store's assets, equipment, and inventory, as well as the assets brought into the store by its guests. For this reason, monitoring the entrances, cash registers, and common areas of the commercial unit is particularly justified. Another purpose of monitoring is to prevent accidents occurring in the premises of the store and to uncover their circumstances. Additionally, monitoring serves the purpose of asset protection concerning high-value items often left unattended by customers.

According to Act XXII of 1992, the then Labour Code, the employer has the right to monitor employees during working hours concerning their job responsibilities. Accordingly, a camera surveillance system may be legally applied in compliance with the following legal conditions, and it is not necessary to obtain the employee's consent for this purpose. However, monitoring must not violate human dignity or personal rights, and the employee's private life cannot be monitored. Monitoring cannot aim to observe the employee's behavior or habits; it cannot aim to check work performance or intensity. If the employee's life or physical integrity is at risk at the workplace, recordings showing the full figure of the employee may be made.

In line with the principles of accountability and proportionality, data protection obligations must be fulfilled:

- **Accountability:** It must be demonstrable that the employee has been adequately informed and that the security of data obtained during monitoring has been ensured and processed appropriately.
- **Proportionality:** Personal data obtained during monitoring must be necessary for the legitimate interest of the data controller. The principle of proportionality is violated if the interests of the data subject are of higher order (e.g., fundamental rights, respect for private life).

Guarantee requirements must be adhered to, which means that camera monitoring should primarily serve the protection of life, physical integrity, personal freedom, the guarding of dangerous substances, business, payment, banking, and securities secrets, and asset protection.

Thus, the placement of cameras must not violate human dignity, and the principle of purpose limitation must be observed, which means:

- The field of view of the cameras must be set to focus exclusively on areas consistent with the purpose of monitoring.
- Recordings stored for more than three days require a valid justification; otherwise, they must be irreversibly deleted.
- Access to the recordings must be regulated so that only decision-makers can access them and exclusively for the appropriate purpose.

The obligation to provide information must also be met, which must naturally be provable during an official inspection. The employer is obliged to inform employees about the existence of monitoring and the following:

- The legal basis for data processing.
- The placement of individual cameras (shown positions) and their purpose (e.g., cash return, threats, aggressive behavior).
- The areas monitored by the cameras: sales area, warehouse, items: inventory, papers.
- That the employer conducts the monitoring recorded by the given camera.
- The person operating the electronic monitoring system: Anita Merse.
- The location of recording storage: server - 3 days / and duration.
- Data security measures concerning storage: the database automatically deletes itself after three days.
- Authorized persons for accessing the data: superior authorities and the employer may use the recordings for decision-making purposes.
- What rights employees have regarding the electronic monitoring system and how they can exercise these rights, i.e., if the employer wishes to ensure adherence to rules or investigate the commission of a crime using camera surveillance (where prior notification would thwart the proof), they must reckon with the fact that under the new Civil Code, individuals depicted in such recordings are entitled to compensation for any violations of personal rights. However, the affected individual may invoke their personal rights, but these cannot be used for purposes incompatible with societal functions, meaning they cannot prevent their employer from using these recordings as evidence.

Forms of Damage:

- Internal data loss (intentional or negligent deletion). Data leakage is primarily a matter of data security, which also entails data protection measures. From a data security perspective, three categories of protection can be distinguished to prevent data leakage: physical, administrative, and logical protection.

Physical protection aims to make access to the network and entry to the store's computers difficult. This form of protection applies to live human protection, security systems, alarms, locks, lightning protection, backup power supply, and camera surveillance.

The second form of protection is **administrative protection**, which practically means setting internal regulations at the organizational level for how to handle and use the internal IT network. This includes password policies, backup protocols, and internal network protocols (online email systems).

Logical protection includes all measures used to safeguard an already established system. This includes access permission/authorization issues and network security concerns such as firewalls, remote access, or wireless network configurations. This category also includes defense against malicious programs and user-run software.

In accordance with the above, I order compliance with the above to protect human life, physical integrity, personal freedom, business, payment, banking, and patient record secrecy, as well as asset protection. I acknowledge and accept the above by signature:

- 1.
- 2.
- 3.

Budapest, November 9, 2022

Dr. István Rozsos