

SİMSOFT TEKNOLOJİ ANONİM ŞİRKETİ

CCTV RECORDINGS AND PHYSICAL PREMISES SECURITY PRIVACY NOTICE

INDEX

1. Identity of the Data Controller	2
2. Scope of Application	2
3. Your Personal Data Processed	2
4. Monitored Areas.....	2
5. Processing Purposes and Legal Bases	3
6. Method of Collection	3
7. Transfer	3
8. Retention Period.....	3
9. Technical and Organisational Measures Taken	4
10. Layered Notice	4
11. Your Rights as a Data Subject and Method of Application	4
12. Effective Date and Updates	5

1. Identity of the Data Controller

Pursuant to Personal Data Protection Law No. 6698 (the "Law"), your personal data are processed by SİMSOFT TEKNOLOJİ ANONİM ŞİRKETİ (the "Company") in its capacity as data controller, within the scope set out below.

Trade Name	SİMSOFT TEKNOLOJİ ANONİM ŞİRKETİ
Address	Üniversiteler Mah. İhsan Doğramacı Blv. ODTÜ Teknokent SATGEB Bölge Ortak Bina 1. Kat AR-GE Ofisi 06800 ODTÜ Çankaya/Ankara/TÜRKİYE
Telephone	+90 850 840 00 46
E-mail	kvkk@simsoft.com.tr
Registered Electronic Mail (KEP)	simsoft@hs02.kep.tr
Website	www.simsoft.com.tr

2. Scope of Application

This Privacy Notice applies to all natural persons entering our Company's head office and branches, as well as its production, development, training and test facilities. This includes employees, interns, visitors, representatives of customers and project authorities, personnel of suppliers and subcontractors, and employees of cargo, service and similar service providers.

Our Company operates in the defence industry, and physical security measures are implemented at our facilities within the scope of Defence Industry Security Law No. 5202 dated 29/6/2004, the Defence Industry Security Regulation, and Law No. 5188 on Private Security Services dated 10/6/2004. CCTV monitoring and entry-exit recording form part of these measures.

3. Your Personal Data Processed

Data Category	Data Processed
Physical Premises Security	Footage obtained through the closed-circuit camera system; date and time of entry and exit, access card or visitor card records
Identity	For visitors, name and surname; identity verification by presentation of an identity document
Contact	For visitors, telephone number and e-mail address
Professional Information	Information on the institution represented by the visitor, and the visitor's title and position
Other	Purpose of the visit, the department or person to be met, records relating to electronic devices brought into the facility; Personnel Security Clearance information where required under the relevant legislation

No audio recording is made by the camera system, no biometric data are processed, and no facial recognition or similar automated identification analysis is performed on the recordings.

4. Monitored Areas

CCTV monitoring is carried out at facility entry and exit points, garden and car park areas, corridors, loading and dispatch areas, server and system rooms, and at the entrances of controlled areas where classified information, documents and materials are kept.

No CCTV monitoring is carried out in areas that may disproportionately affect the privacy of individuals. In this context, areas such as changing rooms, enclosed sections of rest areas, places of worship, the infirmary and toilets

are excluded from monitoring. CCTV recordings are not used for the purpose of measuring employee performance or continuous surveillance of employees.

5. Processing Purposes and Legal Bases

Processing Purpose	Legal Basis	Article of the Law
Ensuring the security of facilities, personnel, visitors and materials; preventing and detecting unauthorised entry, theft, sabotage and similar incidents	Necessary for the legitimate interests of the data controller, provided that the fundamental rights and freedoms of the data subject are not harmed	Art. 5/2-f
Ensuring facility security and access to controlled areas, and protecting classified information, documents and materials, within the scope of defence industry security legislation	Expressly provided for by law; necessary for the data controller to comply with its legal obligations	Art. 5/2-a, Art. 5/2-ç
Fulfilling obligations arising from legislation on private security services	Necessary for the data controller to comply with its legal obligations	Art. 5/2-ç
Implementing occupational health and safety measures, and investigating occupational accidents and emergency incidents	Necessary for the data controller to comply with its legal obligations; necessary for the legitimate interests of the data controller, provided that the fundamental rights and freedoms of the data subject are not harmed	Art. 5/2-ç, Art. 5/2-f
Establishment, exercise or protection of a right, and establishing evidence in judicial and administrative proceedings	Necessary for the establishment, exercise or protection of a right	Art. 5/2-e
Receiving and evaluating visit requests and notifying them to the competent authorities pursuant to the legislation	Expressly provided for by law; necessary for the data controller to comply with its legal obligations	Art. 5/2-a, Art. 5/2-ç

6. Method of Collection

Footage is collected by automated means through the closed-circuit camera system installed at our facilities; entry-exit and visitor records are collected by partially automated means through access control systems and visitor registration procedures.

7. Transfer

Your CCTV and entry-exit records may be viewed only by a limited number of our authorised employees and private security officers, and are not routinely shared with third parties. The records may be transferred, in accordance with the conditions set out in Article 8 of the Law, to public institutions and organisations authorised by law and to judicial authorities in the event of an investigation into a security incident, occupational accident or suspected crime; to the competent authorities during inspections conducted under defence industry security legislation; and to our domestic suppliers providing maintenance and technical support services for the system.

8. Retention Period

CCTV footage is retained for 1 month from the date of recording and is automatically deleted by the system at the end of this period. Visitor and entry-exit records are retained for 1 year from the date of recording.

Where a particular recording constitutes evidence in connection with a security incident, occupational accident, disciplinary process, administrative investigation or legal dispute, only the relevant recording is segregated and

retained until the conclusion of the process and the finalisation of the decision; in such case, the reason for segregating the recording is documented in minutes. Upon expiry of the retention period, your personal data are erased, destroyed or anonymised within the periodic destruction intervals, not exceeding six months, set out in our Personal Data Retention and Destruction Policy.

9. Technical and Organisational Measures Taken

- Access to the recordings is restricted to a limited number of persons authorised in writing, and access authorisations are reviewed periodically.
- Access to the recordings is logged, specifying the person accessing, the date, the time and the reason for access.
- The systems on which the recordings are kept are located in physically protected areas and are protected against unauthorised access.
- Personnel with access authorisation sign a confidentiality undertaking and receive regular awareness training.
- Warning signs notifying the presence of monitoring are displayed in the monitored areas.

10. Layered Notice

The obligation to inform is fulfilled through the layered notice method adopted by the Personal Data Protection Authority. Warning signs placed visibly in the monitored areas constitute the first layer, and this Privacy Notice constitutes the second layer. The text is accessible at facility entrances and on our website.

11. Your Rights as a Data Subject and Method of Application

Pursuant to Article 11 of the Law, you have the right to learn whether your personal data are processed; to request information in this regard if they have been processed; to learn the purpose of processing and whether they are used in accordance with that purpose; to know the third parties to whom they are transferred domestically or abroad; to request their rectification if they are incomplete or inaccurately processed; to request their erasure or destruction within the framework of the conditions set out in Article 7 of the Law; to request that rectification, erasure and destruction operations be notified to third parties to whom the personal data have been transferred; to object to the occurrence of a result against you by means of the analysis of the processed data exclusively through automated systems; and to request compensation for damages in the event that you suffer damage due to unlawful processing.

You may submit your requests concerning your rights, in accordance with the Communiqué on the Procedures and Principles for Applications to the Data Controller, by completing the Data Subject Application Form published on our website and sending it, together with documents evidencing your identity, in writing to Üniversiteler Mah. İhsan Doğramacı Blv. ODTÜ Teknokent SATGEB Bölge Ortak Bina 1. Kat AR-GE Ofisi 06800 ODTÜ Çankaya/Ankara/TÜRKİYE, with your secure electronic signature or mobile signature, or to kvkk@simsoft.com.tr via the e-mail address you have previously notified to us and which is registered in our system, or to simsoft@hs02.kep.tr via your Registered Electronic Mail (KEP) address. Your application will be concluded free of charge as soon as possible and at the latest within thirty days, depending on the nature of the request. Should the process require an additional cost, the fee set out in the tariff determined by the Personal Data Protection Board may be charged.

In your request concerning CCTV recordings, specifying the facility where the recording was made, the date and approximate time range, and information enabling us to identify you in the recording will facilitate the conclusion of your application. Where other persons also appear in the footage subject to the request, the assessment is made while protecting the rights of third parties.

12. Effective Date and Updates

This text entered into force in 2026. The Company reserves the right to update the text in line with legislative amendments, decisions of the Personal Data Protection Board and changes in its processing activities. The current text is published on our website.