

SİMSOFT TEKNOLOJİ ANONİM ŞİRKETİ

PERSONAL DATA PROTECTION AND PROCESSING POLICY

INDEX

1. Purpose	2
2. Scope	2
3. Our Fundamental Principles	2
4. Conditions for Processing Personal Data.....	2
5. Processing Activities Arising from Defence Industry Legislation	2
6. Transfer of Personal Data	2
7. Retention and Destruction	3
8. Data Security.....	3
9. Procedure to Be Followed in the Event of a Data Breach.....	3
10. Rights of the Data Subject and Application	3
11. Entry into Force and Updates.....	4

1. Purpose

SİMSOFT TEKNOLOJİ ANONİM ŞİRKETİ (the "Company") regards the protection of personal data as a fundamental corporate responsibility. This Policy has been prepared in order to disclose to the public the principles under which our Company processes personal data, how data subjects may exercise their rights, and the technical and administrative measures taken by our Company.

2. Scope

This Policy applies to all natural persons whose personal data are processed by our Company, including in particular our Company's employees, employee candidates, interns, customers and prospective customers, project authorities and prime contractors and their representatives, suppliers, subcontractors and business partners and their employees, visitors and website users.

3. Our Fundamental Principles

- We process personal data lawfully and in accordance with the rule of good faith.
- We ensure that the data we process are accurate and, where necessary, kept up to date.
- We process data for specified, explicit and legitimate purposes and do not use them for other purposes.
- We keep the data we process relevant, limited and proportionate to the purpose, and we do not collect data that are not needed.
- We retain data for the period provided for in the legislation or necessary for the purpose for which they are processed; upon expiry of that period, we erase, destroy or anonymise them.
- We inform data subjects before commencing the processing activity.

4. Conditions for Processing Personal Data

We process personal data on the basis of one of the conditions listed in Article 5 of the Law. In processing activities based on explicit consent, we present explicit consent texts as documents separate from Privacy Notices, and we ensure that consent is given freely, relates to a specific matter and may be withdrawn at any time. We process special categories of personal data only where the conditions set out in Article 6 of the Law are met and by taking the adequate measures determined by the Personal Data Protection Board (the "Board").

5. Processing Activities Arising from Defence Industry Legislation

Our Company operates within the scope of Law No. 5202 on Defence Industry Security and the Defence Industry Security Regulation. Personal data processing activities carried out for the purposes of ensuring facility and project security, protecting classified information, documents, projects and materials, conducting personnel security clearance processes, and managing visit and access operations are based on the legal basis of being expressly provided for by law. Data processed within this scope are processed limited to the purposes and periods set out in the relevant legislation; data within the scope of Law No. 7315 on Security Investigation and Archive Research are not processed or transferred for purposes other than their intended purpose.

6. Transfer of Personal Data

We transfer personal data only in connection with the processing purpose and in accordance with the conditions set out in Articles 8 and 9 of the Law. We enter into written contracts regulating obligations relating to the protection of

personal data with the parties from whom we obtain services in their capacity as data processors, and we audit these parties at intervals determined by us.

7. Retention and Destruction

We retain personal data for the periods determined for each data category in our Personal Data Retention and Destruction Policy. Data whose retention period has expired are erased, destroyed or anonymised in periodic destruction intervals not exceeding six months. Destruction operations are recorded in minutes.

8. Data Security

In order to prevent the unlawful processing of and unlawful access to personal data and to ensure their safekeeping, we take the necessary technical and administrative measures, including access authorisation and an authorisation matrix, encryption, up-to-date security software, network security, record keeping and log management, backup, penetration tests, physical security measures, confidentiality undertakings, regular awareness training and periodic audits. Our information security management system and our personal data compliance programme are operated in an integrated manner.

9. Procedure to Be Followed in the Event of a Data Breach

Where personal data are obtained by others through unlawful means, we notify the Board without delay and within seventy-two hours at the latest from the date on which we become aware of the situation. We also notify the affected data subjects within the shortest reasonable time. Other notification obligations required by legislation are fulfilled separately.

10. Rights of the Data Subject and 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 rectification if they have been processed incompletely or inaccurately; to request their erasure or destruction within the framework of the conditions set out in Article 7 of the Law; to request that the rectification, erasure and destruction operations be notified to the third parties to whom the personal data have been transferred; to object to the occurrence of a result to your detriment by means of the analysis of the processed data exclusively through automated systems; and to claim compensation for damage 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, together with documents evidencing your identity, in writing to the address 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 previously notified to us and 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 depending on the nature of the request and within thirty days at the latest. Where the operation requires an additional cost, a fee may be charged in accordance with the tariff determined by the Personal Data Protection Board.

11. Entry into Force and Updates

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