

2025



# ODAS'S POLICY ON PERSONAL DATA PROTECTION LAW AND INFORMATION SECURITY



# Table of Contents

Purpose and Scope	01
Principles and Commitments Regarding the Personal Data Protection Law and Information Security	02
Implementation Principles Regarding the Personal Data Protection Law and Information Security	03
Enforcement	04

## 01 Purpose and Scope

As ODAŞ Elektrik Üretim Sanayi Ticaret AŞ (“ODAŞ”) and its subsidiaries (“ODAŞ Group Companies”), we are aware that all our employees are responsible for information security and that both our group companies and our stakeholders may suffer significant damage in the event of intentional or unintentional loss or misuse of information. With this in mind, we are committed to establishing and maintaining a robust information security management system that protects the confidentiality, integrity and accessibility of our assets in accordance with TS ISO/IEC 27001 and TS ISO/IEC 27019 - Energy Services Industry Information Security Measures Standard, and the Personal Data Protection Law No. 6698 (KVKK) and other relevant legislation.

In this regard, protecting the privacy and confidentiality of the personal data of our employees, customers, and the general public is also an integral part of our Information Security Management System.

## 02 Principles and Commitments Regarding the Personal Data Protection Law and Information Security

**1.** We establish the duties, roles, and responsibilities required for the establishment and operation of the Information Security Management System; we periodically review these authorities, roles, and responsibilities and take all necessary measures to ensure system security.

**2.** Personal data security is managed in line with Company policies by means of technical and administrative measures, with the support of senior management and the participation of all employees.

**3.** The following information is defined as **personal data** by ODAŞ Group Companies in accordance with the Personal Data Protection Law (KVKK) and other applicable legislation. However, this is not limited to the information defined herein; all data that qualifies as personal data as defined by the legislation is considered personal data:

- Account number, username, and password
- ID number and other identification information
- Contact details (address, phone number, email, etc.)
- Financial information (bank account details, credit card details)
- Personal preferences and behavioral data
- Sensitive personal data (health data, biometric data, etc.)

The privacy, integrity, and accessibility of this data are protected.



# POLICY ON PERSONAL DATA PROTECTION LAW AND INFORMATION SECURITY

---

4. ODAŞ Group Companies operate in full compliance with local and international personal data protection regulations such as KVKK (Türkiye), GDPR (European Union), CCPA (United States), and the provisions of international treaties to which the Republic of Türkiye is a party. We monitor relevant legislation, applicable laws, and developments related to contractual and customer requirements, and take necessary measures to ensure their implementation and prevent potential violations.
5. We identify and classify our information assets, determine the risks that may jeopardize them, develop the necessary methods to manage these risks, and implement these methods effectively.
6. ODAŞ **commits** to protecting the privacy, integrity, and security of all personal data collected from our employees, customers, and other third parties, and to protecting the confidentiality of individuals.
7. ODAŞ acts in accordance with the law and principles of integrity in the processing of personal data. Develops and effectively implements the necessary methods to ensure that the personal data processed is accurate and, where necessary, up to date
8. Personal data is processed, stored, and disposed of only for lawful and authorized purposes; it is shared with third parties in accordance with the regulations under the Personal Data Protection Law (KVKK) and other legislation by taking the necessary security measures.
9. Personal data is collected only for lawful, legitimate, and clearly defined purposes. Personal data is processed in a manner that is relevant, limited, and proportionate to these purposes.
10. ODAŞ stores personal data in compliance with the period specified in the relevant legislation or as necessary for the purpose for which it is processed.
11. Processing of data is carried out for clear reasons such as provision of a service, legal obligations, and customer relations.
12. Data is stored on secure servers; and when it is no longer needed, it is deleted, destroyed, or anonymized.
13. Only authorized personnel may access personal data. Access is controlled on a role-based basis. Access to data is granted through multi-factor authentication. We implement AES-256 encryption, firewalls, IDS/IPS systems, up-to-date antivirus software, secure backup and recovery solutions, network segmentation, and log monitoring.
14. Personal data is processed and shared in accordance with the legal processing terms under the Personal Data Protection Law (KVKK) and other relevant legislation.
15. ODAŞ requires **third parties such as dealers, business partners, and service providers** to **fully comply with information security and personal data protection principles** while cooperating with them within the scope of its operations. The qualifications of the parties in their personal data processing procedures are taken into account. **Confidentiality agreements** and **data processing protocols** are signed with all third parties.



## 03 Implementation Principles Regarding the Personal Data Protection Law and Information Security

**16.**Data owners (customers, employees, visitors, etc.) have the following rights under Article 11 of the Personal Data Protection Law (KVKK):

- **Request for information:** The right to know whether their personal data has been processed, to request information about such processing if it has occurred, to learn the purpose of the processing and whether the data is being used in accordance with that purpose, and to learn the identity of third parties with whom the data has been shared within the country and/or abroad
- **Correction:** Requesting the correction of data if it is incomplete or improperly processed, requesting that the correction request be communicated to third parties within the country and/or abroad
- **Deletion/Destruction:** Under the scope of Article 7 of the Personal Data Protection Law (KVKK), the right to request the deletion or destruction of personal data when the reasons requiring the processing of such data no longer exist, and the right to request that a request for correction be communicated to third parties within and/or outside the country
- **Objection:** Objecting to a result that is unfavorable based on the analysis of the data by automated systems,
- **Claim for compensation:** Claiming compensation for damages incurred due to unlawful processing of data

**17.**ISO/IEC 27001 does not directly regulate the rights of data owners; however, it defines the **technical and managerial infrastructure required for the secure implementation of these rights**. In this regard, the following practices have been implemented:

- Special identity verification and registration mechanisms are used for **access requests**.
- **Data correction and deletion processes** are carried out in a traceable and auditable manner in accordance with the requirements of ISO 27001 for "asset management," "access control," "modification management," and "log management".
- **Permanent deletion** or **anonymization** procedures are applied to the records that have been deleted or for which processing has been stopped.
- **Data owners' applications** are handled within the framework of procedures defined under the Information Security Management System, responsible persons, and service level agreements (SLA).
- A centralized request tracking system is established to record, review, and report the outcome of all requests.
- Operations such as access, correction, and deletion are performed **by authorized persons** and **recorded**.

**18.**Our customers may submit their requests regarding their personal data:

- to the e-mail address [[kvkk@odas.com.tr](mailto:kvkk@odas.com.tr)],



# POLICY ON PERSONAL DATA PROTECTION LAW AND INFORMATION SECURITY

- Through the official Personal Data Protection Authority (KVKK) application form published by the Personal Data Protection Authority ("Authority"), (Through the relevant personal application form issued by ODAŞ),
- to the address of ODAŞ, "Barbaros Mah. Başak Cengiz Sok. Varyap Meridian No.1D / Villa 4 34746 Batı Ataşehir – Istanbul" either physically or through a notary public after the verification of their identity,
- through the call center after the verification of their identity. Applications shall be answered free of charge within **30 days at the latest, in accordance with the Personal Data Protection Law (KVKK)**. However, if the procedure also incurs a cost, the fee specified in the tariff determined by the Board may be charged.

**19.**In case of a personal data breach, customers, authorized institutions, and the Personal Data Protection Board shall be notified **within 72 hours at the latest**. The root cause of the case is investigated, and the necessary technical and managerial improvements are implemented to prevent recurrence.

**20.**Recognizing the fact that people are the most critical factor in ensuring information security, we organize regular data privacy and security training, awareness-raising training, seminars, and various awareness programs for our employees and, when necessary, other stakeholders involved in the data processing process; and we also monitor the results of these programs.

**21.**We draft business continuity plans and test them to ensure that our operations and responsibilities to our stakeholders are not interrupted in the event of any adverse circumstances.

**22.**To ensure that our Information Security Management System operates in accordance with standards, we develop procedures and instructions, establish control points, and regularly set objectives, measure effectiveness, monitor, and review them in line with our philosophy of continuous improvement.

**23.**Information Security and Personal Data Protection processes are audited at least once a year through **internal and/or external audits**.

## 04 Enforcement

ODAŞ's Policy on Personal Data Protection Law and Information Security has entered into force as of 25.07.2025, pursuant to the Board of Directors' Decision dated 25.07.2025 and numbered 2025/10. The effective date and version information of the Policy shall be clearly stated in the document. The Policy is published and made available on internal company systems and the corporate website.

ODAŞ Ethics Committee is responsible for implementing, monitoring, and assessing the effectiveness of the Policy. Within this scope, ODAŞ Ethics Committee identifies risks in the implementation of policies, reviews the ethics reports received, monitors the system's effectiveness regarding violations, and recommends corrective actions when necessary. Recommendations for revisions are prepared by the ODAŞ Ethics Committee and implemented by the Board of Directors. Updated versions of the Policy are clearly communicated to all employees and relevant stakeholders.





# Contact Us

## Headquarters

Barbaros Mh. Başak Cengiz Sk.  
Varyap Meridian Sitesi No:1/D Villa 4  
Bati Ataşehir / Istanbul

## Get in Touch

[info@odasenerji.com](mailto:info@odasenerji.com)

## Website

[www.odas.com.tr](http://www.odas.com.tr)

## Tel

+ 90 216 474 1 474

