

Personal Data Protection Policy

Under Turkish Personal Data Protection Law No. 6698 · Last revised: 27.10.2026

Company	AltınSoft Bilişim Teknolojileri Tic. Ltd. Şti.	Tax Office / No	Babaeski / 0640383341
MERSIS No	0064038334100001	Trade Registry No	3171
Phone	+90 850 303 81 59	Email	destek@altinsoft.com
Registered Email (KEP)	altinsoft.bilisim@hs01.kep.tr	Hosting Provider Certificate No	YS-388
Address	Fevzi Çakmak Mah. Gazi Mustafa Kemal Bulvarı No:30 Veli Abalı Apt. D:8 Babaeski / Kırklareli – Türkiye		

This Policy explains the principles and rules that AltınSoft Bilişim Teknolojileri Tic. Ltd. Şti. (“ALTINSOFT”), as data controller, applies to the processing and protection of personal data under the Turkish Personal Data Protection Law No. 6698 (“KVKK”) and its secondary legislation. Information for users of the Site and the customer panel is also provided in the Privacy and Security Policy published on the Site. This English version is provided for convenience; in case of any discrepancy, the Turkish version prevails.

1. Purpose

The purpose of this Personal Data Protection Policy (the “Policy”) is to set out the methods and rules applied so that the personal data held by ALTINSOFT is processed lawfully and protected, and so that data subjects can exercise their rights.

2. Scope

This Policy covers all personal data processed, wholly or partly by automated means or by non-automated means that form part of a data filing system, of natural persons whose personal data ALTINSOFT processes in the course of its activities, such as customers, prospective customers, Site visitors, job applicants, employees, office visitors, company shareholders and representatives, and the employees and officers of suppliers and service providers.

3. Definitions

Explicit Consent	Consent relating to a specific subject, based on information and given of one’s free will.
Recipient Group	The category of natural or legal persons to whom personal data is transferred by the data controller.
Biometric Data	Data obtained through technical processing of a person’s physical characteristics, such as the face or fingerprint, that allows the person to be identified.
Personal Data	Any information relating to an identified or identifiable natural person.

Processing of Personal Data	Any operation performed on personal data, such as obtaining, recording, storing, retaining, altering, reorganising, disclosing, transferring, taking over, making available, classifying or preventing the use of the data.
Board	The Personal Data Protection Board.
Special Categories of Personal Data	Data relating to a person's race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance and dress, membership of associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, as well as biometric and genetic data.
Data Subject (Relevant Person)	The natural person whose personal data is processed.
Data Controller	The person who determines the purposes and means of processing personal data and is responsible for establishing and managing the data filing system. For the purposes of this Policy, the data controller is ALTINSOFT.
Data Processor	The natural or legal person who processes personal data on behalf of the data controller on the basis of the authority granted by it.

4. Processing of Personal Data

4.1 General Principles

In accordance with Article 4 of the KVKK, ALTINSOFT processes personal data:

- lawfully and fairly,
- accurately and, where necessary, kept up to date,
- for specified, explicit and legitimate purposes,
- in a manner that is relevant, limited and proportionate to the purposes of processing,
- retaining it for the period laid down in the relevant legislation or required for the purpose of processing.

Personal data whose retention period has expired or whose purpose of processing no longer exists is deleted, destroyed or anonymised ex officio or at the request of the data subject.

4.2 Categories of Personal Data Processed

Category	Examples	Data subject group
Identity	Name, surname, Turkish ID number, tax ID number, date of birth, identity document details	Customer, employee, job applicant, supplier officer
Contact	Address, email address, phone number	All groups
Customer transaction	Order, cart, invoice and service records, support requests, live chat messages	Customer, prospective customer
Financial	Payment and refund records, masked card number and card token issued by the payment institution, IBAN, payroll and payment details	Customer, employee, supplier
Transaction security	IP address, session and login records, two-factor authentication records, traffic data, server and domain name details	Customer, Site visitor, employee

Category	Examples	Data subject group
Identity verification	Image of identity document, photo and video of the face, verification result	Customer
Marketing	Message consent records, campaign and event details, past purchase details, visit statistics collected through cookies	Customer, prospective customer, Site visitor
Personnel file	Employment start and termination notifications, payroll details, CV details	Employee, job applicant
Professional experience	Education details, certificates, previous employer details	Employee, job applicant
Legal transaction	Information in court and enforcement files, correspondence with competent authorities	All relevant groups
Risk management	Collection follow-up details, abuse and fraud control records	Customer
Physical premises security	Office security camera recordings	Employee, office visitor
Special category data	Biometric data: matching of the face image with the photo on the document during identity verification	Customer

4.3 Legal Grounds

Personal data is processed, under Article 5 of the KVKK, with the explicit consent of the data subject or, without explicit consent, in the following cases:

- It is expressly provided for by law,
- It is necessary to protect the life or physical integrity of a person who is unable to express consent due to actual impossibility or whose consent is not legally valid, or of another person,
- Processing of personal data of the parties to a contract is necessary, provided that it is directly related to the conclusion or performance of that contract,
- It is necessary for ALTINSOFT to fulfil its legal obligation,
- The data has been made public by the data subject,
- Data processing is necessary for the establishment, exercise or protection of a right,
- Data processing is necessary for the legitimate interests of ALTINSOFT, provided that it does not harm the fundamental rights and freedoms of the data subject.

Special categories of personal data are processed, under Article 6 of the KVKK and subject to adequate measures determined by the Board, with the explicit consent of the data subject or in the following cases: it is expressly provided for by law; it is necessary to protect the life or physical integrity of a person unable to express consent due to actual impossibility; it relates to data made public by the data subject and is in line with the intention to make it public; it is necessary for the establishment, exercise or protection of a right; health data is processed by persons under a duty of confidentiality or by authorised institutions for the purposes listed in the law; it is necessary to fulfil legal obligations in the fields of employment, occupational health and safety and social security. Biometric matching during customers' identity verification is based on explicit consent; consent is given by reading the information in the verification email and starting the verification.

4.4 Purposes of Processing

- Concluding and performing contracts, providing services and carrying out post-contract services,
- Managing communication and relations with customers; handling requests, complaints and support processes,
- Identity determination and verification, prevention of fraud and abuse, operation of secure payment and collection systems,
- Carrying out finance, accounting and invoicing activities,
- Fulfilling legal and administrative obligations, providing information to competent authorities and institutions, carrying out audit activities,
- Conducting legal proceedings, lawsuits and enforcement proceedings; detecting and preventing unlawful transactions,
- Ensuring the security of information systems and physical premises and business continuity,
- Sending campaign, announcement and promotional messages where consent has been given,
- Managing relations with service providers and business partners,
- Assessing job applications, recruitment, and carrying out employees' personnel, wage and fringe benefit processes, training and occupational health and safety obligations,
- Keeping data accurate and up to date, and announcing changes in legislation and policies.

4.5 Collection of Personal Data

Personal data is collected electronically or physically, by automated or non-automated means, through the forms on the Site and the customer panel, live chat, email, phone, social sign-in options (Google, Microsoft, GitHub), payment and identity verification service providers, cookies, job applications, contracts, public institutions and security cameras in the office.

4.6 Transfer of Personal Data

Personal data may be transferred, limited to the purposes in 4.4 and in accordance with Articles 8 and 9 of the KVKK, to the following recipient groups:

- Competent public institutions and organisations, judicial authorities, the Social Security Institution,
- Licensed payment institutions (iyzico, PayTR) and banks,
- E-invoice service providers (Paraşüt, BirFatura),
- Identity verification (Veriff), SMS and email delivery (Netgsm, Mutlucell, Resend) service providers,
- Data centre and infrastructure providers (including OVH),
- Analytics and security service providers (Google Analytics where consent has been given; Cloudflare Turnstile, Google reCAPTCHA),
- Persons and organisations providing legal, accounting and audit services.

Transfers abroad. Personal data may be transferred abroad to countries for which the Board has issued an adequacy decision; where there is no adequacy decision, by providing one of the appropriate safeguards listed in Article 9 of the KVKK, such as standard contractual clauses; or in the incidental cases listed in the law. The server service purchased by a customer is provided at the data centre in the country the customer chose when ordering.

4.7 Retention Periods and Destruction

Personal data is retained for the period laid down in the relevant legislation or required for the purpose of processing. The main periods are: 5 years under Tax Procedure Law No. 213 and 10 years under Turkish Commercial Code No. 6102 for invoices, books and accounting records; 1 to 2 years for traffic data under Law No. 5651 and the related regulation; 3 years from the withdrawal of consent for commercial electronic message consent records; 10 years from the end of employment for employee personnel files; and, for camera recordings, as long as the recording system takes to overwrite them (or until an incident under investigation is concluded). Data whose period has expired is deleted, destroyed or anonymised in accordance with the Regulation on the Deletion, Destruction or Anonymisation of Personal Data.

5. Rights of the Data Subject

Under Article 11 of the KVKK, data subjects have the right to apply to ALTINSOFT to:

1. Learn whether their personal data is processed,
2. Request information if it has been processed,
3. Learn the purpose of processing and whether the data is used in line with that purpose,
4. Know the third parties in Türkiye or abroad to whom personal data is transferred,
5. Request rectification if the data is incomplete or inaccurate,
6. Request deletion or destruction under the conditions in Article 7 of the KVKK,
7. Request that the operations carried out under items (5) and (6) be notified to third parties to whom the personal data has been transferred,
8. Object to a result to their detriment arising from the analysis of the processed data exclusively through automated systems,
9. Claim compensation for damages suffered due to unlawful processing.

Consent given for processing based on explicit consent may be withdrawn at any time; withdrawal does not affect the lawfulness of earlier processing. If the EU General Data Protection Regulation (GDPR) or another data protection law applies to you, you also have the rights granted by that law.

6. Exercising Rights

Data subjects may submit their requests, clearly stating their identity and request, in accordance with the Communiqué on the Procedures and Principles for Applications to the Data Controller: by a wet-signed petition delivered in person, through a notary or by registered post with return receipt to ALTINSOFT's address; by registered email (KEP) to altinsoft.bilisim@hs01.kep.tr; signed with a secure electronic signature or mobile signature; or from the email address registered in ALTINSOFT's system, to destek@altinsoft.com. The KVKK Data Subject Application Form published on the Site may be used for the application.

Applications are concluded free of charge as soon as possible according to their nature and within thirty (30) days at the latest; if the operation entails an additional cost, the fee in the tariff set by the Board may be charged. For a third party to apply on behalf of the data subject, a notarised special power of attorney must be submitted. ALTINSOFT may request additional information to verify that the applicant is the data subject and to clarify the application.

If the application is rejected, the response is found insufficient or no response is given in time, the data subject may file a complaint with the Board under Article 14 of the KVKK.

7. Data Security Measures

Under Article 12 of the KVKK, ALTINSOFT applies the following technical and administrative measures to prevent unlawful processing of and access to personal data and to ensure its safekeeping.

7.1 Technical Measures

- All communication between the Site and users is encrypted with TLS (SSL).
- Customer passwords are stored as irreversible one-way hashes; customers are offered two-factor authentication with passkeys, an authenticator app and backup codes.
- The full card number and card security code are not stored; saved cards are kept with a masked number and a token issued by the payment institution.
- Access to information systems is made with a personal username and password; passwords consist of at least 8 characters and contain letters, numbers and special characters.
- Access rights are limited per person and role in line with the purposes of processing; they are updated when duties change and removed for those who leave. Access and operations are logged.
- Electronic files containing personal data are stored with restricted access rights and/or encryption and transferred encrypted; secret keys belonging to service providers are stored encrypted.
- Firewalls and malware protection are used for network security; security vulnerabilities are monitored and updates are applied.
- Penetration tests are carried out regularly.
- Data masking is applied where necessary.
- Regular backups are taken for data integrity and business continuity.
- Employee computers lock after a period of inactivity and ask for the password again.

7.2 Administrative Measures

- Employees sign a confidentiality and information security agreement on the protection of personal data; sanctions are applied to those who do not comply with their obligations.
- Employees receive training on the protection of personal data at least once a year.
- Before personal data processing begins, the obligation to inform and, where required, the obligation to obtain explicit consent are fulfilled; areas with security cameras are marked with warning signs.
- Contracts with third parties to whom data is transferred safeguard the protection of personal data and security measures.
- Documents and portable storage containing personal data are kept in locked areas; printouts containing personal data are not left on printers and photocopiers; system passwords are not kept in writing in the open.

8. Data Breach Notification

If processed personal data is obtained by others by unlawful means, ALTINSOFT notifies the Board as soon as possible and within 72 hours at the latest, and the relevant persons within a reasonable time, in accordance with Article 12 of the KVKK and the Board's decisions.

9. Entry into Force and Updates

This Policy enters into force on the date it is published on the Site. ALTINSOFT may update the Policy in line with changes in legislation and its activities; the current text is published on the Site with its “Last revised” date.

Contact: destek@altinsoft.com · +90 850 303 81 59 · KEP: altinsoft.bilisim@hs01.kep.tr · Fevzi akmak Mah. Gazi Mustafa Kemal Bulvarı No:30 Veli Abalı Apt. D:8 Babaeski / Kırklareli – Türkiye