PERSONAL DATA PROCESSING AND PRIVACY POLICY

The purpose of this document is to ensure the protection of corporate information and personal data at Akmerkez Gayri Menkul Yatırım Ortaklığı A.Ş./ Üçgen Bakım ve Yönetim Hizmetleri A.Ş. (“Company”) in terms of confidentiality, integrity, and accessibility, and to determine the principles of methods and processes of the Information Security Management System for processing and protection of personal data.

- It is the shared responsibility of all employees to protect the reliability and image of the organization by protecting personal data.
- The PPD Committee is responsible for creating, implementing, and ensuring the effectiveness of policies, procedures and instructions.
- The organization aims to ensure the security of all physical and electronic information assets used in the provision of IT services in order to ensure that basic and supportive business activities continue with minimal downtime.
- In contracts with third parties, we ensure compliance with LPPD requirements.
- Privacy, integrity, retention, and accessibility of information are the main principles when processing, transmitting and maintaining personal data.
- The processing of personal data in physical/electronic form is carried out according to access authorization matrices. No employee can gain unauthorized access to personal data.
- All employees are regularly given awareness training on protection of personal data.
- The PPD Committee meets at least 2 times a year or as per legal or contractual necessities, takes the necessary decisions, implements such decisions, and measures their effectiveness.
- Access and data organization logs are kept for all data processed by the organization including personal data to ensure data security.
- Backups are created for all data processed by the organization including personal data and the validity of the business continuity is verified by performing return tests from the backup.
- Access rights, including to the media where personal data is processed, are regularly checked and verified. This ensures the confidentiality of the company's information in personal and electronic communications and in information exchanges with third parties.

- Personal data inventory is kept up-to-date as required by law and relevant regulations, and the registration statement is updated within 7 days in the event of practices that may change the registration statement.
- The requests of data subjects are handled carefully and answered within the period required by the law.
- Risk assessment is performed for all data processed by the organization including personal data as well as the media and system where such data are processed and action plans are developed to mitigate risks.
- The organization takes administrative and technical measures to prevent data breaches. Possible violations despite the measures are evaluated within the framework of procedures and managed in accordance with legal requirements.
- The organization ensures that all policies, procedures and instructions are easily accessed by employees.
- Lacking practices are identified by conducting an internal audit within the organization and corrective-preventive activities are planned.