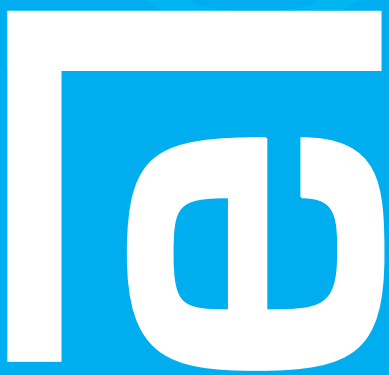
COMPLIANCE

DATA PRIVACY POLICY



www.egebant.com.tr

DATA PRIVACY POLICY

1. PURPOSE AND SCOPE

Egebant is committed to protecting the confidentiality of all stakeholders with whom it has commercial business relations, including its customers, suppliers, employees, and subcontractors. Based on this principle, the Company has adopted this Data Privacy Policy ("Policy").

2. DEFINITIONS

Applicable Data Protection Laws refer to all laws and regulations in force in Türkiye regarding privacy or data protection (including the Law on the Protection of Personal Data) that are applicable to the processing of Personal Data.

Personal Data means any information relating to an identified or identifiable natural person ("Data Subject"). Identification may occur by reference to a name, identification number, location data, online identifiers, or one or more factors specific to the physical, physiological, genetic, psychological, mental, economic, cultural, or social identity of a Data Subject.

Employee means all permanent employees, officers, full-time or part-time employees, relevant third-party consultants, and temporary workers who act on behalf of Egebant entities and are subject to this Policy.

Process / Processing means any operation performed on Personal Data, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination or otherwise making available, international transfer, alignment or combination, restriction, erasure, or destruction.

Data Processor means any person or unit that processes Personal Data on behalf of Egebant and is subject to this Policy.

Data Breach means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

Security Measures mean legal, organizational, or technical measures aimed at the integrity, availability, and confidentiality of Personal Data, intended to prevent, mitigate, or remedy Data Breaches.

Special Categories of Personal Data mean Personal Data relating to a Data Subject's race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health, sex life, sexual orientation, or criminal convictions.

3. RESPONSIBILITIES

- Employees are required to comply with this Policy when processing Personal Data in the course of normal business activities.
- Senior management within the Company is responsible for ensuring compliance with this Policy, including maintaining an appropriate governance structure and allocating the necessary resources for compliance and implementation.
- If Employees suspect or become aware that this Policy conflicts with any local law or regulation, or that any Company practice violates this Policy, they must promptly inform the Company through the Ethics channels.
- The Company may implement additional policies, procedures, or practices in order to ensure compliance with this Policy and/or Applicable Data Protection Laws.

4. GENERAL POLICY

a. The Company makes every effort to process Personal Data in accordance with this Policy and Applicable Data Protection Laws. Where Applicable Data Protection Laws provide a higher level of protection than this Policy, the Company must comply with such laws and regulations.

b. Core Principles

- Lawfulness and Purpose Limitation

The Company must process Personal Data only for lawful, fair, and specified, explicit, and legitimate business purposes, and on an appropriate legal basis under Applicable Data Protection Laws. Such legal basis may include the Data Subject's explicit consent, performance of a contract, steps taken prior to entering into a contract, legal obligations, or the Company's legitimate interests that do not override the interests or fundamental rights and freedoms of Data Subjects. Where Applicable Laws or internal policies require the Company to obtain explicit consent prior to processing certain Personal Data, the Company will obtain such consent and respect the Data Subject's decision. The Company must keep records showing that consent has been obtained and that withdrawals of consent are implemented.

- Data Minimization

The Company must limit the processing of Personal Data to the minimum amount of information necessary to achieve the defined purpose(s). Where possible, the Company should use data that does not identify Data Subjects. Access to such information must be limited to need. The Company will minimize the scope of processing, access, and storage of Personal Data required for the defined purpose(s). Access will be limited to those who need to know. Except for limited exceptions, Personal Data must not be made accessible to an indefinite number of persons.

- Maintaining Accuracy and Quality

The Company must always maintain the integrity of Personal Data processing activities and take necessary steps to ensure that Personal Data are accurate, complete, up to date, and reliable for their intended use.

- Retention and Deletion of Personal Data

The Company must not retain Personal Data longer than necessary. Personal Data must be destroyed or anonymized in accordance with applicable Company Policies and records retention schedules, including the Company's Records Retention Policy. Company Policies and retention programs must consider the Company's business needs, legal obligations, and scientific, statistical, or historical research requirements.

c. Data Subject Rights

- The Company must assess requests from Data Subjects regarding their rights related to Personal Data, including access, restriction, data portability, erasure, objection, or withdrawal of consent.
- The Company must respond to such requests within one month and make efforts to fulfill the request within the time period specified in the Data Subject Rights Policy.
- The Company is not obliged to fulfill a request unless it can legally link the requestor to the Personal Data concerned, or if the request is manifestly unfounded or excessive due to its repetitive nature.

d. Ensuring Appropriate Security and Reporting Security Breaches

- The Company must apply Security Measures to ensure the security of data, particularly in processing activities involving transmission of Personal Data via wireless networks, portable devices, or media. Such measures must take into account the processing activity, the nature of the Personal Data, and the cost and feasibility of implementing the Security Measures.
- Security Measures must be defined through written security policies and procedures.
- Employees must immediately report a security breach to the Egebant IT Department and ensure that security breaches are recorded in accordance with the Company's Data Breach Policy.

e. Disclosure of Personal Data

- The Company must disclose Personal Data only to law enforcement or courts, or to business partners, suppliers, or customers, where specifically authorized and only if such disclosure complies with the laws and regulations in force in Türkiye and/or Applicable Data Protection Laws.
- To ensure the confidentiality and security of Personal Data, the Company must carefully select Data Processors, subject them to contractually committed controls, and comply with all applicable Data Protection Laws.

f.International Transfer of Personal Data

The Company may transfer Personal Data only in accordance with the conditions set forth in applicable Data Protection Laws.

g. Training

Employees who process Personal Data as part of their roles or functions must be trained regularly in accordance with this Policy. Training must be adapted to the relevant employee's role or function.

h. Monitoring and Records

- The Global Data Protection Officer and local Data Protection Officers must conduct periodic reviews and audits to ensure compliance with this Policy.
- The Company must maintain records of data processing activities. Records must be provided to supervisory authorities upon request.

i**. Compliance and Waivers**

- Requirements introduced by this Policy may be waived only in exceptional cases and subject to conditions, after obtaining management approval.
- Any Employee who fails to comply with this Policy may be subject to disciplinary actions, including termination of employment.

5. INTELLECTUAL PROPERTY RIGHTS AND PROTECTION

All intellectual and industrial property owned by or developed by the Company is considered confidential information and must be protected. This includes patents, utility models, industrial designs, trademarks, copyrights, software, algorithms, technical drawings, reports, processes, know-how, trade secrets, and all other intangible assets constituting the Company's intellectual property.

Employees, consultants, and all third parties acting on behalf of the Company:

- may not copy, reproduce, share, or disclose the Company's intellectual property elements to third parties without authorization,
- may use intellectual property information obtained during the performance of their duties only to the extent required by the work and within the scope of authorization.
- are obliged to act in accordance with internal Company regulations and applicable legislation.

a.Intellectual Property Rights of Third Parties

The Company adopts as a fundamental principle respect for the intellectual and industrial property rights of customers, suppliers, business partners, consultants, and other third parties.

Accordingly:

- Third-party intellectual property such as patents, copyrights, trademarks, software, designs, technical documents, trade secrets, and similar elements may be used only within the framework of legal basis, contractual provisions, and permissions,
- Copying, reproducing, modifying, distributing, or sharing third-party intellectual property elements without a license, agreement, or explicit written permission is prohibited,
- Unauthorized disclosure of third-party confidential information or information of an intellectual property nature is considered a confidentiality breach under this Policy.

All inventions, designs, software, documents, and similar works developed within the Company are deemed to belong to the Company in accordance with applicable legislation and internal Company regulations, and where necessary, shall be legally protected.

Information and documents containing intellectual property are regarded as confidential data under this Policy and are protected against unauthorized access, disclosure, loss, or misuse through appropriate technical and organizational Security Measures.

In the event of non-compliance with this Policy, disciplinary procedures may be applied to the relevant person(s), and where necessary, legal and criminal remedies may be pursued.

6. INFORMATION

If you have any questions or concerns regarding this Policy or confidentiality matters in general, please contact the IT Department.