

GUIDE

KVKK Compliance Starter Guide

A starter guide on where to begin with compliance under Turkey's Personal Data Protection Law (KVKK, Law no. 6698) and in what order to take the steps. This guide is for general information and is not legal advice.



GUIDE

ABOUT 7 MIN READ

KVKK

IN THIS GUIDE

1. Key concepts
2. Compliance roadmap
3. How to build the data inventory
4. Notice and explicit consent
5. Data security measures
6. Data subject requests and breach management
7. Starter checklist

01

Key concepts

Personal data

Any information relating to an identified or identifiable natural person.

Data controller

The person or organisation that determines the purposes and means of processing.

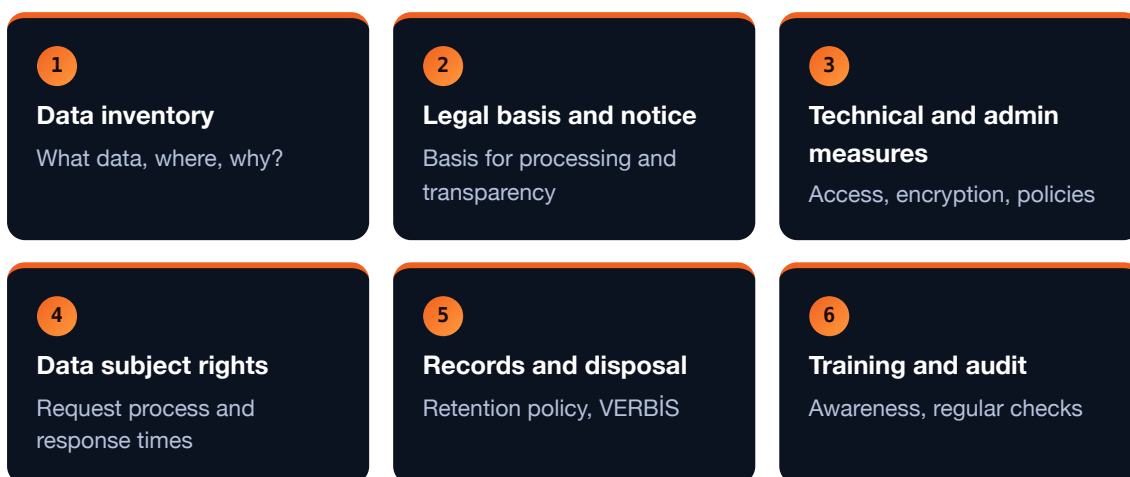
Data processor

A party that processes data on behalf of the controller (e.g. cloud, payroll or e-mail providers).

Data subject

The individual whose data is processed: customer, employee, visitor, candidate, etc.

02 Compliance roadmap



03 How to build the data inventory

The foundation of compliance is knowing which personal data is processed in which process. Work process by process (HR, sales, accounting, website, CCTV, etc.) and record for each:

- Categories of personal data processed (is any of it special-category data?)
- Purpose and legal basis of processing
- Who it is shared with and where (including abroad)
- Retention period and disposal method
- Systems that hold the data and roles with access

04 Notice and explicit consent

The duty to inform applies even when explicit consent is not needed. Explicit consent is not the only legal basis; data processed for performance of a contract or a legal obligation, for example, does not require separate consent. When consent is needed it must be informed, specific and freely given.

In practice: Website forms, cookies and job application processes are the first places most organisations should review.

05 Data security measures

Technical measures

Access authorisation, passwords and multi-factor authentication, encryption, logging, backup, vulnerability management.

Administrative measures

Policies and procedures, confidentiality undertakings, training, controller-processor contracts, audits.

06

Data subject requests and breach management

Requests from data subjects must be answered within the period set by law, at the latest within 30 days, so the request channel and internal process should be defined in advance. In case of a data breach, under Board decisions the Board must be notified as soon as possible and within 72 hours at the latest from when the breach is learned.

Note: VERBİS registration thresholds and deadlines can change; always check current Board decisions.

07

Starter checklist

- | | |
|---|--|
| ☐ Data inventory prepared | ☐ Privacy notices are current and published in the right channels |
| ☐ Retention and disposal policy ready | ☐ Access rights reviewed |
| ☐ Data subject request process defined | ☐ Breach response and notification plan ready |
| ☐ Staff trained on KVKK | ☐ Contracts with processors reviewed |

Let's plan your KVKK compliance together We will assess your current state and build a prioritised compliance plan.

// CONTACT

Get in touch

Share your needs and current situation and we will define the right scope and roadmap together. Fill in our information form or contact us directly.

Troy Bilgi Teknolojileri Ticaret Limited Şirketi

Atatürk Mah. Vedat Günyol Cad. 44M/2

Ataşehir / İstanbul, Türkiye

T 0-216-575 5222 **E** info@troybilgiteknolojileri.com



Scan the QR code for the service page and information form