

AI usage rules for employees

Clarify approved tools, information boundaries and responsibilities in one document.

1. Document owner and scope

Company: [COMPANY NAME]

Responsible team / manager: [TEAM AND ROLE]

Effective date: [DATE] · Internal version: [VERSION]

A general working template for employees, interns, consultants and external providers acting for the company. It applies after the authorised company team completes and approves it.

2. What do we use AI for?

- We use permitted information for research, ideas, draft text and summaries.
- We use approved examples for analysis, presentations and meeting preparation.
- We check the output before use. The tool does not replace professional judgement or required managerial approval.

3. Approved tools and accounts

Tool / account type / permitted use: [LIST]

Team responsible for new tool approval: [TEAM]

- We use only company-approved tools and account types for work. Personal account use needs separate approval.
- We report a new tool, extension or integration to the responsible team first.
- We do not upload company information before data use, retention, access and training settings are assessed. Turning off model training, where available, does not by itself establish lawful processing or cross-border transfer safeguards.

Quick check

Is the tool approved? Is this information permitted in this account? Who will verify the output? If an answer is unclear, we consult the responsible team.

Protecting information and output

4. What information do we not share?

The following information is not entered into general-purpose public AI tools without written company approval for the data and use, and the required conditions being met:

- Personal information: Identity, contact, employee records, health, salary, bank and payment details.
- Customer and partner information: Lists, contracts, quotations, prices, complaints, purchase history and correspondence.
- Confidential company information: Costs, profitability, budgets, strategy, unpublished product details and internal reports.
- Access information: Passwords, API keys, session details and confidential access links. Confidential source code also requires separate assessment.

Changing names is not necessarily anonymisation. If other details still identify someone, the information may remain personal data. International personal data transfers require separate assessment of the applicable legal conditions [1].

5. How do we verify the output?

- We compare numbers, units and calculations with the original records.
- We check that sources exist, support the statement and are current.
- We review material legal, financial, health-related or technical conclusions with the relevant expert.
- An authorised person reads text intended for customers or the public. We do not share invented sources, unverified success claims or content with unclear usage rights.

6. Who approves which output?

Work employees may use after checking: [WORK TYPES]

Work requiring manager / expert approval and responsible roles: [WORK AND ROLES]

The company separately defines areas such as customer documents, official statements, contracts, important financial analysis, employee assessments and automated actions. Permission to prepare a draft with allowed data does not automatically authorise sending it or executing an action.

Reporting, review and records

7. What do we do if something looks wrong?

Reporting team / role: [TEAM AND ROLE]

Internal contact channel: [CHANNEL]

- We stop sharing further information and stop the relevant action.
- We notify the responsible team without delay. We record the tool, time, information type and observed incident, without copying confidential information into another tool.
- We preserve incident records. We delete a conversation or file only under the responsible team's instructions, and do not conceal the incident.

For a breach involving personal data being unlawfully obtained by others, the controller notifies the Turkish Board without delay and within 72 hours of becoming aware. Notification to affected people and incident records are also addressed [2]. Employees report internally immediately; they do not wait for that deadline or assume legal assessment or notification authority.

8. When do we review the rules?

Last review: [DATE]

Next review: [DATE]

Responsible team: [TEAM]

- We reassess the rules when tools, accounts, integrations, data use or working processes change.
- We do not wait for the planned review date if a task is unclear or a new risk appears. We share the current version with employees.

9. Reading and internal implementation record

I have read these company-approved rules. If anything is unclear, I will consult the designated responsible team.

Name: _____ Date: _____

Signature / internal record: _____

This record is not explicit consent under the Turkish KVKK, a transfer agreement or a provider contract. The general template needs adaptation to the company's systems and obligations; it is not legal advice or a completed compliance document.

A framework for your company

Defining tools, roles, information boundaries and approvals around real company work is a separate engagement. Responsible AI Use service: <https://dogancoban.com/en/ai-use-policy>

Sources · checked on 13 October 2026

1. Turkish Data Protection Authority — International transfers

<https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim>

2. Turkish Data Protection Authority — Breach notification, decision 2019/10

<https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi>