The Turkish Data Protection Authority Publishes Guidance on the Use of Generative AI Tools in the Workplace

A. Introduction

Generative Artificial Intelligence ("**GenAI**") refers to AI systems trained on large-scale datasets that are capable of producing content in various formats, including text, images, video, audio, and software code, in response to user-provided prompts or instructions. These systems are increasingly used in the workplace to support information access, content creation, and a broad range of operational activities.

The Personal Data Protection Authority ("**Authority**") has published a document entitled Use of Generative AI Tools in the Workplace, setting out a general framework for the use of third-party, publicly accessible GenAI tools in professional settings.

The document is accessible here.

B. Assessment Under Data Protection Law

When employees use GenAI tools to draft e-mails and other texts, summarise documents, or produce work materials, they often share information that constitutes personal data with these systems, frequently without being aware of doing so.

It is therefore essential that personal data processing activities carried out through GenAI systems comply with the Personal Data Protection Law No. 6698 ("**Law**").

Entering customer information, employee data, or internal correspondence into a GenAI tool constitutes a personal data processing activity. In such cases, the employer acts as the data controller in respect of that processing activity.

Under Article 12 of the Law, data controllers are required to implement the necessary technical and organisational measures to ensure the security of personal data. Accordingly, the sharing of personal data through GenAI tools in the course of employees' work increases the risk of a data breach and may result in the employer's liability as data controller.

This risk is particularly acute in relation to GenAI tools used outside the employer's oversight and control, commonly referred to as Shadow AI, which may result in personal data being processed unlawfully, accessed by unauthorised parties, or used for purposes other than those for which it was collected.

C. Recommended Measures for Data Controllers

While acknowledging the benefits that GenAI tools can bring, the document emphasises that data controllers must establish clear and comprehensive rules governing their use in the workplace.

In this regard, the following measures are recommended for data controllers:

(i) Establishing an internal policy that sets out which GenAI tools may be used and for what purposes, what types of data may be submitted as inputs, and the rules applicable to the use of outputs generated by these tools;

(ii) Using anonymised or pseudonymised data when interacting with GenAI tools wherever possible, and exercising particular caution with sensitive categories of data such as health data, customer data, and financial information;

LBF Partners
Esentepe Mah. Büyükdere Cad. No:108/1 K:7 34394 Şişli İstanbul Türkiye

(iii) Reviewing the privacy policies of permitted GenAI tools to assess the purposes for which data is processed, the circumstances in which it may be transferred to third parties, and the applicable retention periods;

(iv) Restricting access to external platforms, limiting the use of GenAI tools to corporate devices only, and implementing access control mechanisms;

(v) Communicating internal policies and rules on GenAI use to employees and conducting regular training and awareness activities.

These measures are critical not only for fulfilling data controllers' obligations under Article 12 of the Law, but also for compliance with the obligations set out under Article 7 and the relevant provisions of the Cyber Security Law No. 7418.

D. Conclusion

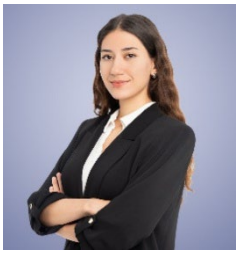
While the document does not in itself create new legal obligations, it merits careful consideration as it clarifies how existing obligations apply to GenAI use cases and signals that this area is increasingly prominent on the Authority's supervisory agenda. The Authority's position is not that GenAI tools should be prohibited outright, but rather that their use should be governed by clear rules, supported by appropriate security measures, and accompanied by employee awareness initiatives.

Data controllers that have not yet adopted a corporate GenAI policy should consider using the document as a starting point for their compliance efforts. Establishing a clear internal policy on the use of GenAI tools in the workplace, including rules on data security and access control, is an important step towards fulfilling obligations arising under personal data protection law.

For further information and support, please contact us.

Elif Çopur Çelebi
Partner

e.copur@lbfpartners.com



Büşra Karabudak
Associate

b.karabudak@lbfpartners.com