YAZICIOGLU LEGAL

Turkish DP Authority publishes an explanatory document on the "Use of Generative Artificial Intelligence Tools in Workplaces"

14 April 2026

As you may recall, in our Information Note (**Information Note**) dated 13 January 2026, we reviewed the "the Guideline on Generative Artificial Intelligence and Personal Data Protection" published by the Turkish Data Protection Authority (**Authority**), which provides explanations on Generative Artificial Intelligence (**GenAI**) based on 15 key questions.

The Guideline on Generative Artificial Intelligence and Personal Data Protection provided numerous important explanations on how to ensure compliance with the Personal Data Protection Law in processes involving GenAI.

On 5 March 2026, the Authority published a document (in Turkish) titled "Use of Generative Artificial Intelligence Tools in Workplaces" (**Document**), which provides a general framework for the use of publicly accessible GenAI tools offered by third-parties in workplace settings.

The Authority states that the Document was published to raise awareness among companies, institutions, and organizations, highlight potential risks, and encourage responsible use. We have compiled below the key points from the Document that we consider particularly important.

➢ Uncontrolled Use of GenAI Tools (Shadow AI) and Potential Risks

As is well known, employees today use GenAI tools in the workplace for activities such as drafting emails and texts, summarizing documents, brainstorming, and conducting research. For these purposes, third-party services are often utilized in practice, including chat-based AI applications, coding assistants, and translation or text-generation tools.

In the Document, the Authority defines the concept of "Shadow AI" as "*the use of GenAI tools within an organization or institution by employees in business processes without the knowledge, approval, or corporate control of that organization or institution"*. As noted in the Document, such use may arise from employees' individual initiative. GenAI tools used outside corporate control are stated to pose various risks, including:

- Issues with auditability and accountability,
- The negative impacts of incorrect or misleading AI outputs on decision-making processes,

- Risks related to the protection of intellectual property and trade secrets,
- Damage to corporate reputation and loss of trust,
- Information and cybersecurity risks,
- Unlawful processing of personal data or unauthorized access to such data.

Accordingly, the Document emphasizes that it is important to ensure compliance with obligations regarding **(i)** data security, **(ii)** verification processes, and **(iii)** the protection of personal data when using these tools.

The Document further states that the concept of Shadow AI shares similarities with "Shadow IT" practices, which refer to the business-related use of IT tools and services that are unknown to the organization, unmonitored, or not incorporated into corporate risk management processes.

However, the Document emphasizes that Shadow AI entails risks that must be addressed at multiple levels, particularly in light of the capacity of GenAI tools to directly influence data processing, content generation, and decision-making mechanisms underlying business processes.

➢ Considerations Regarding the Use of GenAI Tools in the Workplace

In the Document, the Authority states that approaches or practices aimed at banning the use of GenAI tools are unlikely to produce effective results and, on the contrary, may encourage their use outside organizational control and visibility. Indeed, such lack of oversight could lead to the organization's confidential information, trade secrets, and personal data being shared with AI systems, including for training purposes (*Although this falls outside the scope of this note, prohibiting the use of AI in public institutions while it continues to be used by public officials would give rise to the same risk, this time in relation to state secrets, and may lead to serious national security issue*).

Accordingly, the Authority emphasizes the importance of adopting guidance-, balance-, and awareness-based approaches rather than prohibitive measures. Within this framework, the main considerations for the use of GenAI tools in workplaces are outlined in the Document as follows:

- **Establishing a clear corporate policy or guidance framework defining the boundaries for the proper and appropriate use of GenAI tools:** Within this scope, it is stated that specifying which GenAI tools may be used and for what purposes, setting out the conditions of use, defining the types of information that may be shared with such tools, establishing guidelines for the use of generated outputs, implementing

data privacy and security measures, and providing employee awareness training would contribute to managing such use in a more controlled and predictable manner.

- **Adopting a careful approach regarding institutionally sensitive information and personal data in employees' interactions with GenAI tools:** The Document highlights that the sharing of data with GenAI tools provided by third parties may pose risks, as it could result in data processing outside the organization's control mechanisms. Accordingly, it is recommended that personal data not be shared unless necessary; where sharing is required, anonymized or generalized information should be used, and particular caution should be exercised when sharing sensitive information, especially of a health, financial, or legal information.

- **The risk of overreliance on outputs generated by GenAI tools and the diminishing role of human judgment:** As noted in the Document, this phenomenon, referred to as "automation bias," may lead users to accept AI-generated outputs without sufficiently questioning their accuracy, resulting in the incorporation of incorrect or misleading information into business processes. Therefore, it is recommended that GenAI outputs should not be used as the sole basis for final decisions and that they be evaluated under human oversight for accuracy and contextual appropriateness.

- **Assessment of measures for data security and access control to ensure the proper management of the use of GenAI tools in business processes:** In this context, it is recommended that employees be allowed to access only those GenAI tools designated by the organization, that the types of information that must not to be shared via such tools be clearly defined, and that access be restricted on a role and need based basis. Additionally, controlling access to external platforms, limiting the use of GenAI tools to corporate devices, and adopting role-based access approaches are suggested as practices that contribute to effective risk management.

- **Raising awareness among employees:** In this context, it is recommended that policies and guidance regarding the use of GenAI be communicated to employees, that easy access to such documents be ensured, and that awareness and training activities be conducted. Additionally, fostering a culture in which employees adopt a critical approach to the accuracy of AI outputs, as well as establishing feedback mechanisms through which they can report encountered issues, is considered to contribute to the identification of risks and the development of a corporate culture of responsible GenAI use.

Our Comment: The increasing use of GenAI tools by employees in business processes may result in their use outside corporate control, giving rise to various risks, particularly with respect

to personal data protection and information security. The Document underlines that the Authority adopts an approach favoring the management of these tools within the framework of corporate policy, awareness, and oversight mechanisms, rather than outright prohibition. Accordingly, it is important for organizations to review or establish internal policies and control mechanisms governing the use of GenAI tools and to implement the necessary governance framework.

Bora Yazıcıoğlu
bora@yazicioglulegal.com

Nafiye Yücedağ
nafiye@yazicioglulegal.com

Ece Oğur
eceogur@yazicioglulegal.com