Turkish DP Authority publishes an explanatory document on the "Use of Agentic Artificial Intelligence"

14 April 2026

On 12 March 2026, the Turkish Data Protection Authority (**Authority**) published a document titled Agentic Artificial Intelligence (**Document**), which provides a general overview of Agentic Artificial Intelligence (**Agentic AI**) systems, the functions of artificial intelligence agents (**AI Agents**) within these systems, as well as their potential use cases and associated risks. We have summarized the key highlights below.

➢ Agentic AI Systems

At the outset, AI systems were generally designed to perform predefined and repetitive tasks. Over time, however, the scope of their application has expanded, and they have come to be used in more complex functions. Within this evolution, AI systems have become capable of evaluating alternative courses of action to achieve specific objectives and of operating across different contexts.

As a result of these developments, today, the concept of "Agentic AI" has come to the forefront. In the Document, Agentic AI systems are defined as "***integrated systems capable of assessing environmental conditions in order to achieve specific objectives, adapting to changing circumstances, and initiating actions autonomously at varying levels.***"

The Document provides several examples of **Agentic AI systems.** These include:

- Logistics systems that dynamically replan delivery routes based on traffic and weather conditions,
- Cybersecurity systems that detect and mitigate anomalous network activities, and
- Customer support systems that manage support requests and provide initial responses based on user interactions.

By contrast, the Document also provides the following examples of non-agentic AI systems:

- A spam filter designed to classify unsolicited emails,
- A chatbot that responds to employees' inquiries based on the company handbook, and
- A resume screening tool that ranks candidates based on historical recruitment data.

➢ AI Agents in Agentic AI Systems

Agentic AI systems carry out decision-making and action processes through AI Agents. In the Document, an AI Agent is defined as "***an autonomous entity that perceives its environment, responds to it, and acts in accordance with specified objectives***."

AI Agents process data from their environment to achieve their objectives and may use various tools for this purpose. For example, an AI Agent assigned with organizing a conference identifies the requirements, research suitable venues, and plans and executes the necessary steps.

Agentic AI systems, in turn, deploy multiple AI Agents to achieve specific objectives, managing their tasks, interactions, and decision-making and action processes within a broader system framework.

In the Document, this relationship is likened to that between a head chef and the cooks in a restaurant. The head chef (Agentic AI system) determines the menu, plans the preparation and service processes, and coordinates the kitchen's operations, while the cooks (AI Agents) perform more narrowly scoped tasks, such as executing a specific stage of a process.

Multi-Agent Systems: In situations involving complex objectives, Multi-Agent Systems, where multiple AI Agents operate in a coordinated manner, come into play. These systems break down tasks into smaller components, resulting in a more efficient and flexible structure.

Within this framework, Multi-Agent Systems can be regarded as a subcategory or specific implementation of Agentic AI systems. While Agentic AI systems generally refer to structures capable of autonomous action, Multi-Agent Systems denote a more specific architecture based on the coordinated operation of multiple AI Agents.

➢ Potential Risks to Personal Data Protection in the Context of Agentic AI Systems

In the Document, the Authority provides examples of potential risks to personal data protection within the scope of Agentic AI systems. We have summarized these below for ease of reference:

Expansion and Variability in Data Usage: Agentic AI systems may alter their data usage over time while performing their tasks and incorporate datasets that were not initially anticipated. This may expand the scope of data processing activities, making compliance with the principles of purpose limitation and data minimization more challenging, and may weaken the link between data processing and its legal basis. Accordingly, the relationship between the defined data processing purposes and the corresponding activities, as well as the connection to the legal basis, should be continuously assessed throughout the

operation of the system.

- **Risks Concerning Special Category Personal Data:** The processing of special category personal data within Agentic AI systems may increase the risk of harm to individuals or expose them to discrimination.

- **Risk of Bias and Discrimination:** Training Agentic AI systems on large and unstructured datasets may result in the reflection of existing social or cultural biases in system outputs, thereby increasing the risk of discrimination against individuals.

- **Risk of Autonomy and Control:** The increasing level of autonomy in Agentic AI systems may enable them to initiate actions without human intervention; this may reduce the predictability and controllability of system outputs, potentially leading to unintended outcomes.

- **Technical Design and Operational Risks:** The complex architecture of Agentic AI systems, operational disruptions arising from AI Agents, susceptibility to misuse, and challenges in technical verification processes may give rise to risks concerning the reliability and effectiveness of the systems.

- **Inference-Based Data Usage and Challenges in Data Anonymization:** The ability of Agentic AI systems to correlate data from different sources may lead to the inference of more sensitive information about individuals from limited or non-personal data and to the re-identification of anonymized data, thereby complicating anonymization processes.

- **Lack of Transparency, Explainability, and Accountability:** The multi-step and distributed nature of decision-making processes in Agentic AI systems may hinder the traceability of which actions are carried out at each stage and on the basis of which data, thereby negatively affecting the transparency and explainability of personal data processing activities. Additionally, the involvement of multiple AI Agents and various actors may complicate the clear allocation of responsibility and accountability, making it difficult to determine which party is responsible for potential breaches or harm.

- **Risk to the Accuracy of Personal Data and Hallucinations:** In Agentic AI systems, particularly through the use of generative AI models, outputs that are erroneous yet convincing -commonly referred to as “hallucinations”- may be generated. Such outputs may lead to subsequent decisions based on incorrect information, thereby jeopardizing the accuracy of personal data.

- **Risk to Security and System Resilience:** The integration of Agentic AI systems with multiple data sources, tools, and digital environments may expand the attack surface and give rise to new security vulnerabilities.

In conclusion, the effective management of risks to personal data protection in the use of Agentic AI systems requires careful planning in system design, data usage processes, and administrative measures. These risks necessitate the effective implementation of data protection regulations.

➢ What Measures Should Be Taken?

In the Document, the Authority emphasizes the importance of adopting **a risk-based approach** to personal data protection in Agentic AI systems, taking into account the systems' level of autonomy, intended purpose, and architectural characteristics. Within this framework, the main measures that may be implemented are summarized below:

- **Human Oversight:** In light of the increasing level of autonomy, it is important to establish meaningful human involvement and oversight mechanisms to ensure that the systems operate in accordance with specified objectives, ethical principles, and societal expectations.

- **Transparency and Explainability:** Appropriate explainability and traceability mechanisms should be incorporated from the design phase to ensure that system operations, the data used, and the rationale underlying decision-making are comprehensible.

- **Ensuring Data Accuracy:** To maintain the reliability of system outputs, it is important to monitor the currency and accuracy of the data used throughout the process, particularly where outputs are used as inputs for subsequent processes.

- **Clarification of Roles and Responsibilities:** Clearly defining the roles, responsibilities, and authorities of developers, deployers, and other relevant actors can support the effective management of system-related risks.

- **Privacy by Design and Privacy by Default:** Adopting the principles of "privacy by design" and "privacy by default," as well as the use of privacy-enhancing technologies, can contribute to addressing risks to personal data protection at an early stage.

- **Risk Assessment Mechanisms:** Assessing data protection risks that may arise throughout the system lifecycle and, where necessary, utilizing tools such as Data Protection Impact Assessments (DPIAs) can be beneficial.

- **Governance and Awareness:** Aligning internal data governance processes with Agentic AI systems and providing training and awareness initiatives for individuals who use or manage such systems, can contribute to strengthening data security.

Bora Yazıcıoğlu
bora@yazicioglulegal.com

Nafiye Yücedağ
nafiye@yazicioglulegal.com

Ece Oğur
eceogur@yazicioglulegal.com

This note does not constitute legal advice. It has been prepared and shared for informational purposes only. Should you wish to obtain legal advice on the matter, we kindly ask you to contact us.