

EMERGING LEGAL AND ETHICAL CONSIDERATIONS IN GENERATIVE ARTIFICIAL INTELLIGENCE: A DATA PROTECTION PERSPECTIVE

Legal Insight

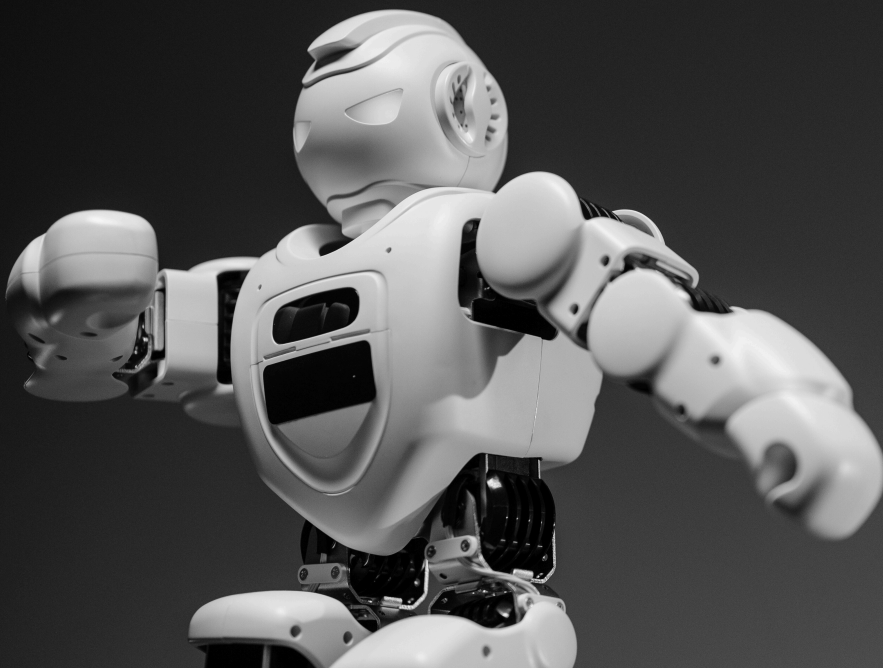
Prepared By.

Atty. Yalçın TORUN LL.M., Atty. Kaan ÇIRPAN LL.B.

Torun Law Firm

Table of Content

Introduction to Generative AI	01	Conclusion	12
Key Privacy Considerations When Using Generative AI	04	About Our Law Firm	13
Legal Framework under the Turkish Personal Data Protection Law (KVKK)	09		
Core Concepts and Definitions in Artificial Intelligence	10		





Introduction to Generative AI

Generative AI holds infinite potential — and equally infinite responsibility.

Generative Artificial Intelligence (AI) marks a significant milestone in the evolution of intelligent systems, capable of autonomously generating content such as text, images, audio, and code. These technologies, powered by large-scale machine learning models, are not only redefining the boundaries of human-machine interaction but are also introducing complex challenges related to data privacy, algorithmic bias, and regulatory oversight.

As AI technologies increasingly mediate digital experiences and influence decision-making across various sectors, law firms must adopt a forward-looking perspective. This includes not only understanding the capabilities and risks associated with generative AI but also ensuring compliance with national and international legal frameworks that aim to protect personal data and uphold fundamental rights.



EY AI Sentiment Index (2025) reveals that in Türkiye 82% of respondents reported having used AI technology at least once in the preceding six months.

52%

According to Deloitte Türkiye's "Digital Consumer Trends 2024" report, individual use of generative AI in Türkiye has surpassed global averages. 52% of individuals use generative AI tools actively.

39%

Regarding data security perceptions, only 39% believe current AI technologies are safe and secure, while just 29% find it easy to understand how companies protect personal data.



Key Privacy Considerations When Using Generative AI



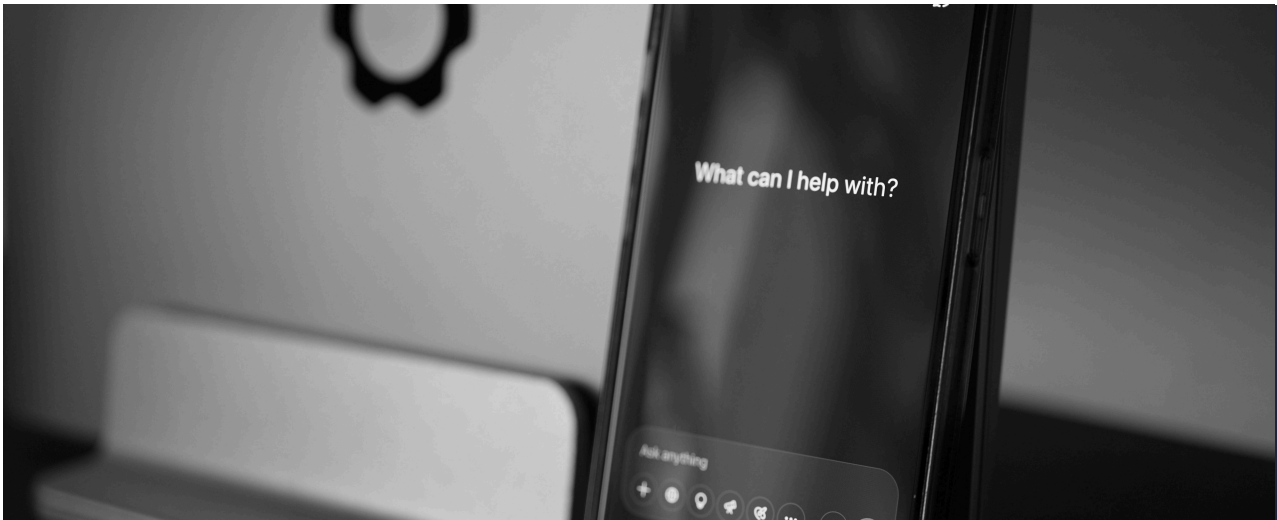
As generative artificial intelligence systems increasingly permeate everyday digital experiences, individuals must take a proactive role in safeguarding their personal data. Below are essential recommendations that reflect global privacy standards, ethical considerations, and practical digital hygiene:



1. Understand What You Share

- Before entering any prompt, consider whether it contains personally identifiable information (PII) such as your name, email address, national ID, medical data, financial records, client information, or legal case details.
- Generative AI models may temporarily retain or learn patterns from prompts – even when no direct storage is stated.
- Rule of thumb: If you wouldn't publish it online, don't paste it into an AI prompt.





2. Review the Tool's Privacy Policy

- Always read and verify the privacy policy and terms of service of any AI platform you use.

Check:

- Whether data is stored or used for model training.
- How long data is retained.
- Who the data may be shared with (third-party processors, affiliates, etc.).
- Choose tools that are transparent, open-source, GDPR-compliant, and provide clear opt-out mechanisms for data processing.



3. Be Cautious When Using AI for Third Parties

If you are an attorney, consultant, HR professional, educator, or healthcare provider, never enter third-party data (e.g., client files, student records, patient data) into AI tools unless you have:

- Explicit consent,
- A valid legal basis (such as legitimate interest or contract performance),
- And the tool complies with local data protection laws.

This is particularly critical in jurisdictions governed by GDPR and Türkiye's KVKK.



4. Use Anonymous or Synthetic Inputs

When possible, mask or generalize personal identifiers:

- Replace names with initials.
- Use placeholder dates or case IDs.
- Reframe sensitive facts abstractly before querying.

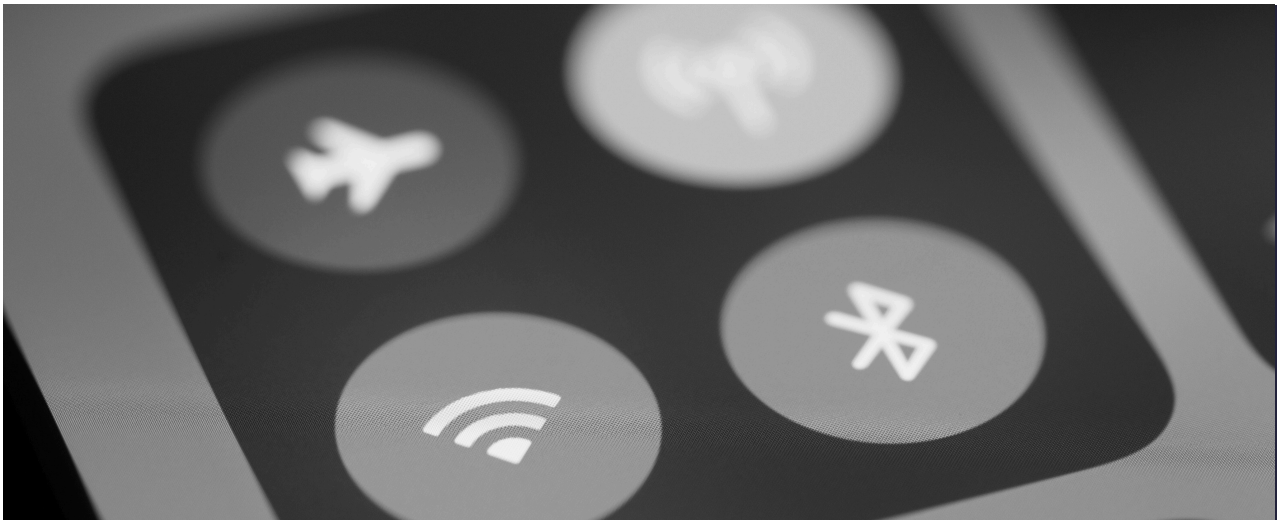
For professional usage, consider using self-hosted open-source LLMs that run locally and do not transmit data externally.



5. Enable Data Usage Controls

Platforms like ChatGPT, Claude, Gemini, or Copilot often provide data control settings:

- Disable chat history or training data contribution.
- Delete past conversations regularly.
- Monitor your account for data breaches or activity logs.



6. Educate Yourself About AI Limitations

Generative AI models may:

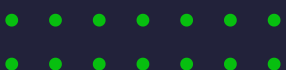
- Fabricate facts (“hallucinations”),
- Misrepresent sources,
- Misunderstand context,
- Reinforce bias based on training data.

Using these tools without understanding their limits may result in unintended privacy or legal violations.



7. Use Secure Networks and Devices

- Access generative AI platforms only from secure networks (VPNs, encrypted Wi-Fi) and avoid public terminals.
- Avoid using unverified AI apps that operate outside the app stores or have no known data policies.





8. Keep Your Professional and Personal Use Separate

If you are a legal, medical, or business professional:

- Avoid cross-contamination between personal queries and sensitive work material.
- Consider using enterprise-grade AI tools with signed data processing agreements (DPAs) and audit trails.



9. Data Rights: EU & Türkiye

- Under GDPR, individuals may request both the deletion of stored prompts or conversations and the export (data portability) of their personal data processed by AI platforms.
- Under Türkiye's KVKK, the right to request deletion or destruction of personal data (including prompts or conversations that contain personal information) is explicitly recognized (Article 11/1-e). However, unlike GDPR, KVKK does not grant a right to data portability; therefore, individuals cannot demand their data to be provided in a structured, machine-readable format.



10. Remember: Privacy Is a Continuous Process

- Protecting your privacy in an AI-powered world requires more than one-time caution.
- Regularly review your settings, update your awareness, and follow the evolving legal landscape on AI and data protection.

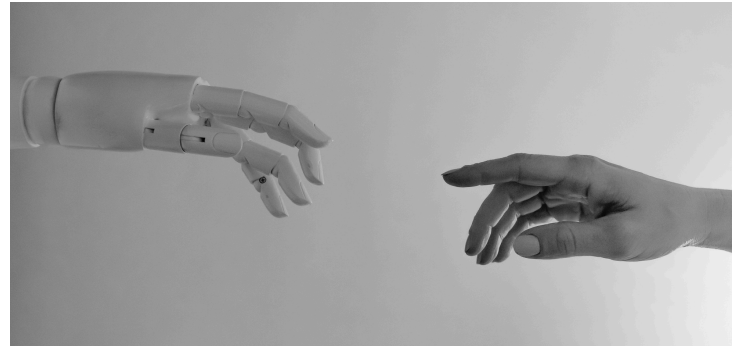
Legal Framework under the Turkish Personal Data Protection Law (KVKK)

The Turkish Personal Data Protection Law No. 6698 (KVKK) **provides the foundational legal basis for personal data processing activities**, including those facilitated by AI systems. Although the KVKK does not explicitly regulate AI technologies, **it applies to all automated data processing activities** involving identifiable individuals.

Key provisions include:

- **Article 4:** Outlines the principles of lawful, fair, accurate, and purpose-bound data processing.
- **Article 10:** Requires clear and transparent information to be provided to data subjects.
- **Article 11(g):** Grants individuals the right to object to decisions made solely through automated processing.
- **Article 12:** Obligates data controllers to implement technical and organizational measures for data security.

In this legal context, human intervention in automated decision-making processes is essential to preserving accountability, transparency, and fairness—principles at the core of both national and international data protection regimes.



Core Concepts and Definitions in Artificial Intelligence

The following is a comprehensive glossary of key terms relevant to AI governance, adapted from internationally recognized standards:

Algorithm: A sequence of instructions designed to perform a specific task or solve a problem.

Big Data: Large-scale datasets that require advanced tools for processing and analysis due to their volume, variety, and velocity.

Artificial Intelligence (AI): The ability of a machine to perform tasks typically requiring human intelligence, such as reasoning, learning, and perception.

AI System: A machine-based system that, with varying levels of autonomy, produces outputs such as predictions or decisions based on input data.

Narrow/Weak AI: AI systems designed to perform a specific task with high competence.

General/Strong AI: Systems capable of performing a broad range of tasks at a level comparable to human intelligence.

Artificial Superintelligence: Hypothetical AI that surpasses human intelligence in all domains, including scientific reasoning and social skills.

Machine Learning: A subset of AI that enables systems to learn from data without explicit programming.

Supervised Machine Learning: A machine learning technique that uses labeled data during training.

Unsupervised Machine Learning: A learning technique using unlabeled data to identify patterns or groupings.

Reinforcement Learning: A process where an agent learns optimal behavior through reward-based feedback.

Deep Learning: A type of Machine Learning using deep neural networks with multiple layers for complex pattern recognition.



Generative AI: AI that creates content (text, images, music) based on input prompts, using trained ML models.

Large Language Model (LLM): An AI model trained on massive text corpora to perform language-based tasks using deep learning.

Natural Language Processing (NLP): A field of AI focused on enabling machines to understand and generate human language.

Prompt: An input or instruction provided to a generative AI system to elicit a desired output.

Hallucination: An instance where a generative AI model produces outputs that appear valid but are factually incorrect.

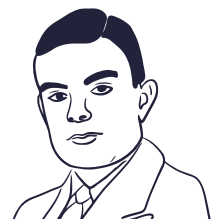
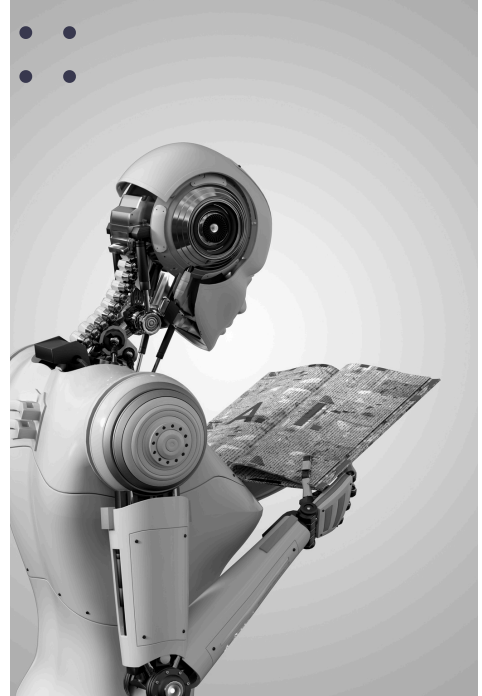
Deepfake: Synthetic audio-visual content generated by AI that mimics real people or events, often misleadingly.

Human-Centric AI: An AI development philosophy that emphasizes respect for human rights, welfare, and autonomy.

AI Developer: An entity responsible for creating content or applications for AI systems.

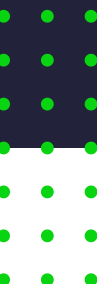
AI Manufacturer: A producer of hardware or software components of AI systems.

AI Service Provider: An entity offering AI-based services or products through various technical systems.



“Instead of trying to produce a program to simulate the adult mind, why not rather try to produce one which simulates the child’s?”

— Alan Turing, **Computing Machinery and Intelligence (1950)**



Conclusion



Generative AI is no longer a futuristic concept—it is an active force shaping how individuals, businesses, and institutions interact with information, create value, and make decisions. Yet, this transformative potential comes with heightened responsibilities. The ability of AI systems to process, generate, and even infer personal data underscores the urgency of embedding privacy, transparency, and accountability into every stage of their design and use.

From a legal perspective, frameworks such as the EU's GDPR and Türkiye's KVKK provide essential safeguards. While both regimes empower individuals to demand deletion of their personal data, only GDPR extends this to data portability—illustrating how privacy rights evolve differently across jurisdictions. This makes compliance not just a matter of national law, but of navigating diverse regulatory landscapes with precision and foresight.

For law firms, the challenge—and opportunity—lies in guiding clients through this complexity:

- Ensuring that data protection principles are respected when adopting AI tools.
- Educating individuals and organizations about their rights and responsibilities.
- Advocating for a human-centric approach to AI governance where innovation serves human dignity and rights, rather than undermining them.

In this sense, the legal profession is not only a guardian of compliance but also a strategic partner in building trust. By combining deep legal expertise with technological literacy, law firms can help shape an AI-powered future that is both innovative and just.



About Our Law Firm



Torun Law Firm is a forward-looking legal practice based in Ankara, Türkiye, with a proven track record of combining deep legal expertise with a modern, innovative approach. Founded on principles of integrity, professionalism, and client-centered service, our firm provides high-level counsel across multiple practice areas, including:

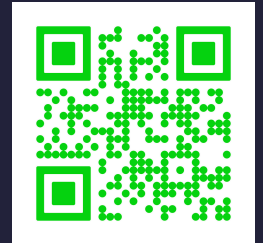
- International Investment and Arbitration
- Data Protection and Privacy Law
- Commercial and Corporate Law
- Mergers and Acquisitions
- Trademark and Patent Representation

We believe that the role of the legal profession extends beyond compliance: it is about building trust, safeguarding rights, and enabling innovation in a rapidly evolving world. With an international outlook and strong local expertise, we serve as a reliable partner to individuals, corporations, and institutions navigating the complexities of law in the digital age.

Atty. Yalçın TORUN LL.M., Atty. Kaan ÇIRPAN LL.B.

Contact Us

Join us on the journey where law safeguards innovation and technology shapes the future.



+90 (505) 621-9992 | +90 (312) 432-5678



en.torunhukukburosusu.com



info@torunhukukburosusu.com



Kızılırmak District, 1443rd Street,
No:25, 1071 Plaza Block B Suite
27, Çankaya / Ankara