



Turkish Data Protection Authority's Approach in the Field of Artificial Intelligence

Authors: Gönenç Gürkaynak Esq., Ceren Yıldız, Noyan Utkan and Derya Başaran, ELIG Gürkaynak Attorneys-at-Law

On September 15, 2021, the Turkish Data Protection Authority (“DPA”) published its Recommendation on the Protection of Personal Data in the Field of Artificial Intelligence¹ (“Recommendation”) on its website. The Recommendation is basically regarding the protection of personal data for developers, manufacturers, service providers and decision makers operating in the field of artificial intelligence.

The Recommendation which is prepared based on the “Guidelines on Artificial Intelligence and Personal Data Protection²” published by the Directorate General of Human Rights and Rule of Law, “Recommendation of the Council on Artificial Intelligence³” of OECD and “Ethics Guidelines for Trustworthy AI⁴” of the European Council consists of three headings; (i) General Recommendation, (ii) Recommendation for Developers, Manufacturers and Service Providers, and (iii) Recommendation for Decision Makers.

I. DPA's General Recommendation

In the Recommendation, DPA firstly recommends basic data protection related matters in order to make sure that the artificial intelligence applications are in line with the relevant legislation.

- During the development and implementation of artificial intelligence applications, the fundamental rights and freedoms of data subjects should be respected and violations of right should not be allowed.
- The protection of human rights and fundamental freedoms and the right to protection of human dignity should be taken into consideration.
- Artificial intelligence and data collection studies which are based on personal data processing should be in line with certain principles (i.e. compliance with laws, fairness, proportionality, accountability, transparency, correct and updated personal data, specific and limited purpose of personal data use, and data security) within an approach that protects the fundamental rights and freedoms of individuals.
- In the processing of personal data, a perspective which focuses on the prevention and mitigation of potential risks and which takes into consideration the human rights, the function of democracy, and social and ethical values should be adopted.
- Data subjects should be able to control the data processing activity.
- In case a high risk is foreseen in terms of protection of personal data, a privacy impact assessment should be applied and compliance of data processing with laws should be decided within this framework.

¹ Available at <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/25a1162f-0e61-4a43-98d0-3e7d057ac31a.pdf>

² Available at <https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8>

³ Available at <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>

⁴ Available at <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>

- From the first stage on the artificial intelligence studies based on personal data processing, the personal data protection legislation should be complied with and all systems, starting from designing, should be developed and managed according to the data protection principles. In this context, a data protection compliance program should be established and applied, specific to each project.
- In case special categories of personal data is being processed while developing and applying artificial intelligence technologies based on personal data processing, technical and administrative measures should be applied more strictly by considering the rules for processing special categories of personal data.
- If the same result could be achieved without processing personal data, anonymization should be preferred.
- The status of data controller or data processor of different stakeholders of artificial intelligence studies should be determined at the beginning of the project and their legal relationship should be in compliance with the data protection legislation.

II. DPA's Recommendation for Developers, Manufacturers and Service Providers

DPA defines “developer” as real or legal person, who develops content and applications for all kinds of products belonging to artificial systems, “manufacturer” as the real or legal person, who produces all kinds of products such as software and hardware that constitute artificial intelligence systems, and “service provider” as the real or legal person, who provides products and/or services using artificial intelligence based systems, data collections systems, software and devices.

- During the design, personal data privacy which is in line with national and international regulations and/or documents should be considered.
- An appropriate risk prevention and mitigation measures should be adopted.
- At each stage of data processing, including data collection, the risk of discrimination or other negative effects and prejudices that might occur on the data subjects should be prevented by considering the fundamental rights and freedoms.
- Minimum data usage should be adopted by evaluating the quality, nature, source, amount, category and content of the used personal data, and the developed model should constantly be monitored.
- Algorithm models taken out of context should carefully be evaluated for the risk of causing adverse effects on the individuals and society. Algorithm models taken out of context is defined as an algorithm which is first designed for an artificial intelligence model and later used for another purpose or artificial intelligence model.
- Academic institutions which could contribute to designing of human rights based, ethical and socially oriented artificial intelligence applications should be contacted, and opinions of the objective experts and organizations should be received in the areas where transparency and stakeholder participation might be difficult.

- The individuals should have the right to object to the actions based on technologies which effect their opinions and personal development.
- Considering the power of artificial intelligence systems to analyze and use the personal data, the rights of the data subjects arising from national and international legislation should be protected in the processing of personal data.
- Risk assessment should be encouraged, based on the active participation of individuals and groups which are most likely to be affected by the practices particularly.
- The products and services should be designed to ensure that the individuals are not subjected to a decision that would affect them based on automated processing, regardless of their own opinions.
- Alternatives should be offered which interfere less with personal rights in the production, and the users' freedom of choice should be guaranteed.
- Algorithms should be adopted to ensure accountability for all stakeholders in terms of compliance with personal data protection law, starting from the designing of the products and services throughout their life-cycle.
- Users should have the right to stop data processing and option to delete, destruct or anonymize persona data.
- The persons who are interacted with the practice should be informed about the reasons for the personal data processing; the details of the methods used in the personal data processing, the possible conclusions and an effective data processing approval mechanism should be designed for the necessary cases.

III. DPA's Recommendation for Decision Makers

- The principle of accountability should be adopted for all the stages.
- Risk assessment procedures for protection of personal data should be adopted and implementation of a matrix should be established on the basis of sector/practice/hardware/software.
- Appropriate measures, such as codes of conduct and certification mechanisms, should be adopted.
- Adequate resources should be allocated by decision makers to monitor whether artificial intelligence models are used for a different context or purpose.
- The role of human intervention in decision making processes should be established. The freedom of individuals not to trust the results of the suggestions presented by the artificial intelligence applications should be protected.
- Supervisory authorities should be consulted when there is a possibility of affecting the data subjects' fundamental rights and freedoms significantly.
- On data privacy, consumer protection, competition promotion and anti-discrimination subjects, cooperation between the supervisors and other authorized bodies should be encouraged.



- The practice researches based on measuring the human rights, ethical, sociological and psychological effects of artificial intelligence applications should be supported.
- Individuals, groups and stakeholders should be informed and they should actively be involved in discussing the role that artificial intelligence, along with big data systems, would play in shaping social dynamics and in the decision making processes that affect them.
- Appropriate open software based mechanisms should be encouraged to create a digital ecosystem which supports a safe, fair, legal and ethical data sharing.
- Investment should be made in the digital literacy and educational resources to raise awareness about understanding artificial intelligence applications and implications for the data subjects.
- Trainings should be encouraged within the framework of data privacy in order to raise awareness of personal data protection for application developers.

The DPA's aim with this Recommendation is to provide clarity on the protection of personal data. Therefore, this study might be considered as a roadmap in terms of data protection for the developers, manufacturers, service providers and decision makers operating in the artificial intelligence field.

Article contact: Gönenc Gürkaynak, Esq.

Email: gonenc.gurkaynak@elig.com

(First published by Mondaq on September 21, 2021)