KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

RECOMMENDATIONS ON THE PROTECTION OF PERSONAL DATA IN THE FIELD OF ARTIFICIAL INTELLIGENCE

RECOMMENDATIONS ON THE PROTECTION OF PERSONAL DATA IN THE FIELD OF ARTIFICIAL INTELLIGENCE

CONTENT

ABSTRACT

This guide includes recommendations on the protection of personal data within the scope of the Personal Data Protection Law No. 6698 for developers, manufacturers, service providers and decision makers operating in the field of artificial intelligence.

INTRODUCTION

Purpose and Basis

The Turkish Language Association's official Dictionary defines intelligence as "the ability of a person to think, reason, perceive objective facts, judge and draw conclusions". People process the data they collect from the environment through their senses and generate useful information from these data using their intelligence.

Artificial Intelligence ("AI"), on the other hand, focuses on developing algorithms and computer software that are capable of executing tasks associated with humans, such as thinking, interpreting, and making decisions, by way of analyzing such human tasks. [1]

In today's world, major progress has been made on artificial intelligence techniques and applications, and intelligence-based systems have started impacting life in many aspects.

Even though artificial intelligence brings substantial benefits to individuals and society, it should be managed justly in terms of individual's right to request the protection of personal data within the scope of fundamental rights and freedoms. Artificial intelligence works and practices that rely on personal data processing shall comply with the Personal Data Protection Law No 6698 and secondary legislation.

This document contains recommendations on the activities being carried out/to be carried out in the field of artificial intelligence and aims to provide clarity on the protection of personal data within the scope such works.

___

1 Balaban Erdal M., Kartal E. 2018. Veri Madenciliği ve Makine Öğrenmesi Temel Algoritmaları ve R Dili ile Uygulamaları (İkinci Baskı), İstanbul: Çağlayan Kitabevi ve Eğitim Çözümleri

While preparing the document, "Guidelines on Artificial Intelligence and Data Protection" published by Directorate General of Human Rights and Rule of Law, "Recommendation of the Council on Artificial Intelligence" published by OECD and "Ethics Guidelines for trustworthy AI" by Council of Europe were consulted.

Scope

This document provides recommendations on the protection of personal data in artificial intelligence applications for developers, manufacturers, service providers and decision makers in the field of artificial intelligence.

Definitions

For the purposes of this document, the following definitions apply:

Data subject: the natural person, whose personal data are processed,

Law: Personal Data Protection Law No 6698

Personal data: any information relating to an identified or identifiable natural person

Data processor: the natural or legal person, who processes personal data on behalf of the data controller upon its authorization,

Data controller: the natural or legal person, who determines the purpose and means of the processing of personal data and is responsible for the establishment and management of the data filing system,

Developer: the natural or legal person who develops any content and application for the products of artificial intelligence systems,

Manufacturer: the natural or legal person who develops any product such as software and hardware that constitutes artificial intelligence systems

Service provider: the natural or legal person who offers products and/or services using artificial intelligence-based systems, data collection systems, software, and tools.

Recommendations

General Recommendations

- In the process of developing and adopting AI applications, the fundamental rights and freedoms of data subjects should be respected and there should be no violation of any right.

- The right to protection of human dignity should be respected by safeguarding human rights and fundamental freedoms.

- Artificial intelligence and data collection works that rely on processing of personal data should be based on the principles of lawfulness, fairness, proportionality, accountability, transparency, being accurate and up-to-date, specified and limited use of personal data, and data security approach within an approach that protects the fundamental rights and freedoms of individuals.

- An approach, that focuses on avoiding and mitigating the potential risks and considers human rights, functioning of democracy, social and ethical values, should be adopted in processing of personal data.

- Data subjects should be able to have control over the processing activities, considering the effect of processing activities on individuals and society.

- In case a high risk is foreseen in terms of protecting personal data in AI works based on personal data processing, privacy impact assessment should be conducted and compliance of processing activity with laws should be evaluated within this framework.

- In AI works based on personal data processing, compliance with the personal data protection legislation should be ensured from the initial stage and all systems should be developed and administered in line with the data protection principle starting from the design. Within this scope, a data protection compliance program specific to each project should be established and implemented.

- If special categories of personal data are processed while developing and implementing AI technology based on personal data processing, technical and administrative measures should be implemented more strictly taking into account the special rules for processing such data.

- If the same result can be achieved without processing personal data in the development and implementation of AI technologies, anonymization of personal data should be preferred while processing data.

- The status of being a data controller or a data processor of different stakeholders of AI works based on data processing should be determined at the beginning of the project and their legal relationships should be brought into compliance with data protection legislation.

Recommendations for Developers, Manufacturers and Service Providers

- In the design phase, an approach, based on data privacy, should be adopted in line with national and international regulation and/or documents.

- Possible adverse consequences on human rights and fundamental freedoms should be assessed, and a precautionary approach based on appropriate risk prevention and mitigation measures should be adopted.

- In all phases of data processing activity, including data collection; fundamental rights and freedoms should be considered, and the risk of discrimination or other negative effects and prejudices that may affect data subjects should be prevented.

- Data usage should be minimized by assessing the quality, nature, origin, amount, category, and content of the personal data and accuracy of the developed model should be monitored constantly.

- De-contextualised algorithm models[2] should be adequately evaluated with regards to the risk of adverse effects on individuals and society.

- Academic institutions, which can contribute to design human-rights based, ethically and socially-oriented AI applications and to detect potential bias, should be contacted; and independent experts and institutions should be consulted in areas where transparency and stakeholder participation might be difficult.

---

2 De-contextualised algorithm models refer to the use of algorithms originally designed for specific artificial intelligence model for different purposes or artificial intelligence models.

- Individuals should have the right to object to processing activities based on technologies that affect their opinions and personal development.

- Considering the capability of AI systems to analyse and use personal data, rights of the data subjects arising from national and international legislation should be protected in processing of personal data.

- Risk assessment, based on the active participation of individuals and groups likely to be affected by AI practices, should be encouraged.

- Products and services should be designed to ensure that individuals are not subjected to a decision, which will affect them, based on automated processing, regardless of their own opinions.

- Alternatives that interfere less with personal rights should also be offered in the production, and the freedom of choice of users should be guaranteed.

- Algorithms, that ensure accountability for all stakeholders in terms of compliance with personal data protection law starting from the design of products and services throughout their entire life cycle, should be adopted.

- Users should have the right to stop data processing activity, and a system, that allows the erasure, destruction or anonymization of personal data belonging to users, should be designed.

- Individuals that interact with an AI application should be informed about the reasons for the personal data processing activity, details of the methods used in the processing of personal data and the possible consequences; and an effective data processing approval mechanism should be designed for necessary cases.

Recommendations for Decision Makers

- The principle of accountability should be respected in all phases.

- Risk assessment procedures should be adopted for the protection of personal data and an application matrix should be created on the basis of sector/application/hardware/software.

- Appropriate measures, such as codes of conduct and certification mechanisms, should be implemented.

- Sufficient resources should be allocated to monitor whether the AI models are used in different contexts or for different purposes.

- The role of human intervention in decision-making processes should be ensured. The freedom of individuals not to rely on the results of the suggestions provided by AI applications should be protected.

- Supervisory authorities[3] should be consulted when there is a possibility of significantly affecting the fundamental rights and freedoms of data subjects.

- Cooperation between supervisory authorities and other authorized bodies on the subjects of data privacy, consumer protection, promotion of competition, and anti-discrimination should be encouraged.

---

3 Supervisory Authorities means the institutions and bodies authorized to regulate and/or supervise in AI field.

- Researches that measure the human rights, ethical, sociological and psychological impacts of AI applications should be supported.

- Individuals, groups and stakeholders should be informed and actively involved in the debates on what role AI and big data systems should play in shaping social dynamics, and in decision making processes affecting them.

- Appropriate mechanisms based on public software should be promoted in order to create a digital ecosystem that supports secure, fair, legal and ethical sharing of data.

- Investments should be made in digital literacy and education resources to increase data subjects' awareness and understanding of AI applications and their effects.

- To raise personal data protection awareness of application developers, trainings within the framework of data privacy should be encouraged.

Sources

Following documents are recommended for further reading:

- Personal Data Protection Law No 6698

- Convention No 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data

- "Guidelines on Artificial Intelligence and Data Protection" prepared by Council of Europe and Directorate General of Human Rights and Rule of Law (https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8)

- "Recommendation of the Council on Artificial Intelligence" published by OECD (https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449)

-"Ethics Guidelines for Trustworthy AI" published by High-Level Expert Group on Artificial Intelligence that was set up by the European Commission (https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419)

- "White Paper on Artificial Intelligence - a European approach to excellence and trust" published by the European Commission

- Opinion No 4/2020 of EDPS regarding the European Commission's White Paper on Artificial Intelligence (https://edps.europa.eu/sites/edp/files/publication/20-06-19_opinion_ai_white_paper_en.pdf)