EY Law Alert

Guidance on Data Protection and Artificial Intelligence in the AIFC

The Astana International Financial Centre (the "AIFC") prepared the Guidance on Data Protection and Artificial Intelligence ("AI") in the AIFC (the "Guidance") based on the AIFC's Data Protection Regulations No. 10 of 2017 (the "Data Protection Regulations") and Data Protection Rules No. 1 of 2018 (the "Data Protection Rules").

The Guidance is applied for providing information on the Provisions and the Data Protection Rules as well as considering the issues of the AI use in the AIFC. Please note that the Guidance is not legally binding.

The better the question.
The better the answer.
The better the world works.

This review is intended for presenting the key provisions of the Guidance and their importance for the companies operating within the AIFC. The Guidance defines the key aspects to be accepted to guarantee the maximally safe data use in the AI context.

Personal data and sensitive personal data

The Guidance focuses on the need to protect personal data defined as "any data referring to an identifiable natural person". Sensitive personal data include information about racial and ethnic origin, political and religious creed, health, biometry and other categories requiring special protection.

AI strategy

According to the provisions of the Guidance, entities are required to develop the AI strategy to demonstrate the commitment of the top management of companies to ethical and responsible use of AI. The strategy may:

- Define AI functions in the entity;

- Establish ethical principles for acquiring, implementing and using AI-based solutions;

- Define unacceptable uses of AI;

- Develop AI tools to facilitate implementation of management measures;

- Set up internal policies and procedures for AI;

- Secure technical infrastructure for legal, responsible and high-quality implementation and use of AI;

- Communicate the issues of the AI strategy, policies and procedures to the employees and stakeholders on a regular basis;

- Consider new legal and regulatory developments applicable to AI.

Key concepts relevant to AI

According to the provisions of the Guidelines, for complete understanding of the application of the Data Protection Rules and the Data Protection Regulations it is necessary to grasp the following concepts that are applicable to AI:

Personal data and AI

- Personal data include those personal data that are generated and output by AI-based systems.

- AI developers and operators are required to secure compliance of the personal data collection and processing with the Data Protection Regulations.

Processing and AI

- Processing relates to any operation performed by an AI-based system with personal data, including collection, analysis, output, storage and removal.

- AI-based systems are required to be developed based on the confidentiality principles by default, with data protection being implemented during the entire data processing life cycle.

Sensitive personal data and AI

- AI-based systems that analyse and output sensitive personal data are required to implement protection measures, including intensified encryption, access control and anonymization methods to protect these data from unauthorized access and leakage.

Data Controller, Data Processor and AI

- An AI developer or operator may constitute a data controller if such developer or operator defines the personal data processing objectives and facilities.

- If the AI-based system processes data on behalf of a third party, it operates as a data processor.

- The AI-based systems need to be configured to comply with the Data Protection Regulations.

Principles of data processing by AI-based systems

The Guidance highlights the importance of complying with the following principles:

- **Transparency and explainability:** Data subjects are required to be informed on the way their data are processed and be able to challenge the automated solutions.

- **Fairness and non-discrimination:** AI-based systems' algorithms are subject to regular non-discrimination testing of results and are adjusted to eliminate the identified biases.

- **Responsibility:** Mechanisms should be in place to allow holding AI developers and operators accountable for the data processing actions performed by the AI-based system.

- **Anonymization:** The AI-based systems are required to use advanced anonymization methods to secure protection from re-identification attempts.

Data subject rights in the context of AI

According to the Data Protection Regulations, data subjects have certain rights that are required to be complied with when such data subjects' personal data are processed by the AI-based systems:

Right to receive information about personal data and correct them

The data subject has the right to obtain from the data controller upon request:

- Written confirmation on whether the personal data are processed

- Information about the processed personal data and its sources

- Correction, removal and blockage of personal data

In the context of AI, these rights are critical since the AI-based systems can generate conclusions and forecasts about people, which may be incorrect and biased.
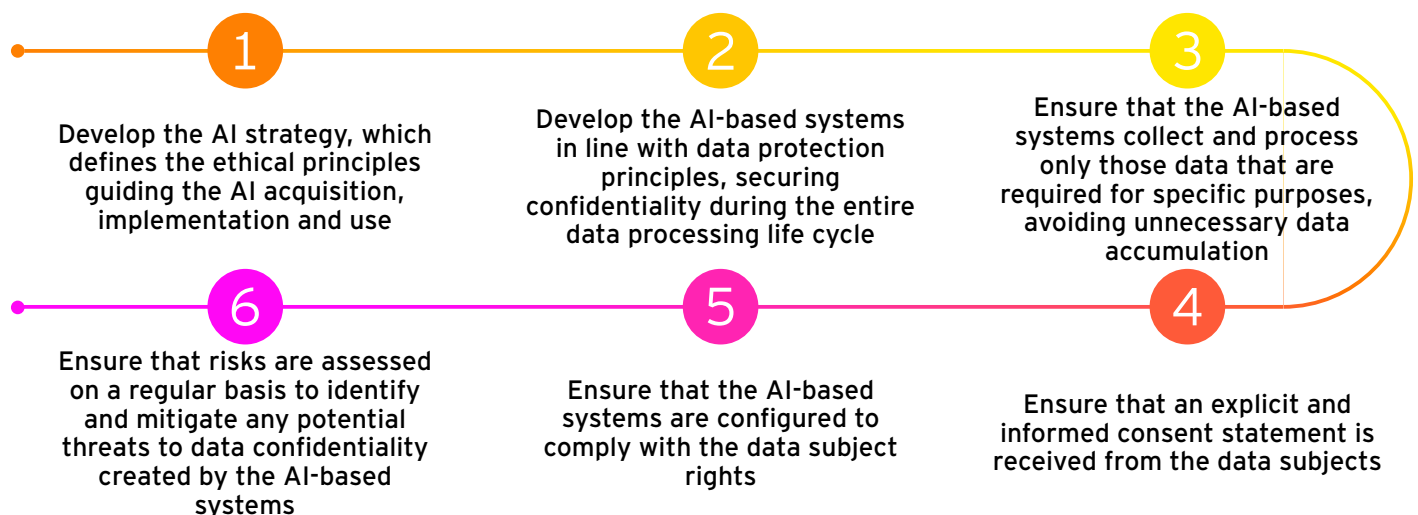
The right to object to personal data processing

The data subject has the right to:

- Object to personal data processing

- Be informed before the moment when the personal data are for the first time disclosed to a third party or used on behalf of a third party for direct marketing purposes and have an explicit right to object to such disclosure or use

These rights are critical in automated decision-making processes where people may challenge their data processing or use in specific AI-driven decisions.

Compliance with the data protection regulations in AI-based systems

To comply with the Data Protection Regulations, entities are required to perform the following steps:

1 Develop the AI strategy, which defines the ethical principles guiding the AI acquisition, implementation and use

2 Develop the AI-based systems in line with data protection principles, securing confidentiality during the entire data processing life cycle

3 Ensure that the AI-based systems collect and process only those data that are required for specific purposes, avoiding unnecessary data accumulation

6 Ensure that risks are assessed on a regular basis to identify and mitigate any potential threats to data confidentiality created by the AI-based systems

5 Ensure that the AI-based systems are configured to comply with the data subject rights

4 Ensure that an explicit and informed consent statement is received from the data subjects

Contacts

Dinara Tanasheva

Partner, Head of Tax and Law Services for Kazakhstan and Central Asia
+7 727 258 5960
dinara.s.tanasheva@kz.ey.com

Nargiz Suleimenova

Senior Associate, Tax & Law

+7 727 258 5960
nargiz.suleimenova@kz.ey.com

Abdigapar Saparbek

Senior Consultant, Tax & Law

+7 727 258 5960
abdigapar.saparbek@ey.com

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

ey.com/kz