Mar 2024

Kazakhstan: Legal regulation of personal data protection in the AIFC

The interest of business, especially foreign investors, in the Astana International Financial Centre (AIFC) has been growing steadily over the past years. In the framework of the AIFC, Kazakhstan has, for the first time in the post-Soviet space, introduced a special jurisdiction based on the principles of the laws of England and Wales. The AIFC aims to attract investments to the Kazakhstan economy, develop local capital markets, and create effective projects in the sphere of production and services. As of February 7, 2024, 2,537 companies are registered in the AIFC.[1] The regulatory framework of the AIFC has been actively developing. In this article, Yekaterina Khamidullina, Partner at AEQUITAS Law Firm, considers the legal regulation of personal data protection in the AIFC, the basis of which is formed by the AIFC Data Protection Regulations (the Regulations) and the AIFC Data Protection Rules.

Collab Media / Essentials collection / istockphoto.com

Both acts were developed after the adoption of the well-known General Data Protection Regulation (GDPR), which is evaluated by many experts in the personal data protection sphere as a 'gold standard' or a reference model of protection of personal data in Europe and abroad considering the extraterritorial effect of the GDPR.

We believe that the developers of the AIFC acts in the personal data protection sphere used the GDPR model as a reference. Together with the Data Protection Rules, the Regulations may be characterized as a 'simplified' brief version of the GDPR. As the AIFC acts drastically differ from the Kazakhstan Law on Personal Data and its Protection (the Law), we will not conduct a comparative analysis of the personal data protection regulation in Kazakhstan and the AIFC, which may become the subject of our separate analysis in the future. In this article, we will focus on the key aspects of the AIFC regulation as compared with the GDPR.

Key concepts of the Regulations

The AIFC acts do not provide for such concepts common for the Kazakhstan business as an owner or an operator of a base containing personal data as specified in the Law. Instead, by analogy with the GDPR, the Regulations provide for the concepts of a 'person,' 'data controller,' and 'data processor.'

In the AIFC, 'personal data' means any data relating to an identifiable individual. A 'person' includes any individual, registered organization, or public association without the formation of a legal entity, including a company, partnership, unincorporated association, government, or state.

Understood as a data controller is any person in the AIFC who determines independently or together with other persons the purposes and facilities of processing personal data. A data processor is any person who processes personal data on behalf of the controller.

'Sensitive personal data' includes data relating directly or indirectly to racial or ethnic origin, political views or affiliation, philosophical or religious beliefs, information on criminal records, trade union membership, health or sexual life, and activities in communities. The definition of the concept of sensitive personal data is very similar to the concept of special categories of personal data stipulated by Article 9.1 of the GDPR.

'Third party' means any person other than a data subject, controller, processor, or person authorized to process personal data under the direct control of the controller or the processor.

A data protection commissioner may be any qualified and experienced individual approved by the Board of Directors of the AIFC Authority after consultation with the AIFC Governor. Functions of the Commissioner include administration of the Regulations and the Data Protection Rules and the prevention, detection, and restriction of behavior that may contradict the AIFC acts in the data protection sphere. The data protection commissioner must facilitate awareness-raising activities and contribute to a better understanding of the issues of data protection in the AIFC, the requirements of the Regulations, the Data Protection Rules, and other laws administered by the data protection commissioner.

Similarities between provisions of the AIFC acts and the GDPR

The Regulations provide for the key principles of personal data processing similar to those stipulated by the GDPR, including legality, justness, accuracy, minimization of personal data, restriction of purposes of personal data processing, limitation of storage, and security.

The controller may process sensitive personal data if a data subject has provided their consent and, in some other cases, stipulated by the Regulations. Such cases are similar to the exceptions stipulated for the processing of special categories of personal data under the GDPR.

The controller must make and keep records stipulated by the Data Protection Rules and notify the data protection commissioner of any operations relating to personal data processing. In turn, the data protection commissioner is liable for keeping the Register of Notices for the above operations.

The GDPR provides for restrictions on the transfer of personal data to countries outside the EEA whose laws do not provide for requirements on data protection. According to the Regulations, transferring personal data outside the AIFC is not allowed if another jurisdiction fails to ensure a sufficient level of protection. Schedule 2 of the Data Protection Rules sets out the list of jurisdictions with sufficient levels of personal data protection, which includes 32 countries mostly located in Europe.

It is allowed to transfer data to the jurisdictions that do not provide for a sufficient level of protection in certain cases, including as follows: (i) in case of permission issued by the data protection commissioner; (ii) in case of the presence of a written data subject's consent; (iii) if the data transfer is required to perform a contract, a party to which is a data subject, or upon a request of the data subject concerning a potential contract, a party to which the subject intends to become; (iv) transfer is required to complete or perform a contract entered into in the interests of a data subject between the controller and a third party; (v) transfer is required to perform a legal obligation binding upon the controller, or in case transfer takes place according to a request of the regulatory authority, police, or any other governmental authority of any jurisdiction; or (vi) transfer is required to protect vital interests of a data subject, and in some other cases.

In general, the above cases are similar to the provisions stipulated by the GDPR.

Certain differences between the AIFC acts and the GDPR

One of the distinguishing features of the Regulation is that the processing of sensitive personal data is allowed in the AIFC, among other things, in case this is required to ensure compliance with requirements on counteraction against the legalization of illegally gained proceeds and financing of terrorism, as well as accounting, auditing, and regulatory requirements.

In this case, the controller must obtain the data protection commissioner's permission, allowing the controller to process sensitive personal data and apply relevant protective measures to such processing. The permission is obtained on a fee-paid basis following the procedure stipulated by the Regulations.

Most of the requirements relating to the safe processing of personal data are similar in both acts. However, unlike the GDPR, the Regulations do not expressly provide for the possibility of data pseudonymization or encryption.

According to the Regulations, data subjects enjoy most of the rights stipulated by the GDPR, including the right to be informed of the collection and use of their data, as well as to access data; delete their data (right to be forgotten); rectify inaccuracies; object against processing; and file a complaint to the data protection commissioner. However, certain rights of data subjects specified in the GDPR are not stipulated by the Regulations, including the right to data portability and the right to object against profiling and automated decision-making.

According to the GDPR, 'profiling' means any form of automated processing of personal data implying the use of personal data to evaluate certain personal aspects relating to an individual, specifically, for analysis or forecasting of aspects relating to such individual's work performance, economic conditions, health, their personal preferences, interests, reliability, behavior, location, or movements (Article 4(4) of the GDPR).

Considering the rapid development of IT, artificial intelligence (AI), mass collection, and processing of data via the internet and social networks, to date, the issue of profiling and automated decision-making based on the received personal data seems to be hot. Western countries have encountered many high-impact judicial proceedings on this issue, leading to multimillion-dollar fines imposable on certain major corporations.

Schedule 3 to the Data Protection Rules determines the maximum amounts of fines which may be applied for violating the Regulations. Thus, in case of providing unreliable or misleading information, a person may be imposed a fine in the amount of $5,000. In case of processing sensitive personal data in violation of conditions or prohibitions stipulated in a permit, the fine will be $10,000.

In case of the personal data transfer to the territory of a jurisdiction failing to ensure an adequate level of protection of such personal data, a person may be fined $20,000. The maximum fine in the amount of $25,000 is stipulated for a failure to fulfill the instructions on compliance with the AIFC legislation on the protection of personal data administered by the data protection commissioner.

Additional comments

We believe that the AIFC acts in the data protection sphere will be updated and improved in the course of the development of the AIFC. The current laws of the AIFC are based on the Kazakhstan Constitution and consist of: (i) the Constitutional Law on the AIFC; (ii) the AIFC acts, which do not contradict the Constitutional Law on the AIFC and may be based on the principles, rules, and precedents of the laws of England and Wales and/or standards of the leading world financial

centers adopted by the AIFC bodies within the authorities granted by the Constitutional Law on the AIFC; and (iii) current laws of Kazakhstan, which apply to the extent not regulated by the Constitutional Law on the AIFC and the AIFC acts.

In light of the above, the companies registered in the AIFC should keep in mind that the Law and other subordinate acts of Kazakhstan in the personal data protection sphere may theoretically apply to their activities not regulated by the Regulations and the Data Protection Rules. We believe that in this case, it will be necessary to rely on the future judicial practice of the AIFC Court. Analysis of public judgments posted on the website of the AIFC Court shows the absence of judicial cases involving violations of the AIFC acts in the personal data protection sphere[2].

It is worth mentioning that, when issuing judgments in disputes where the parties selected the AIFC laws as the governing law, justices relied upon the acts and judgments of the AIFC, rules of English law, and sometimes referred to the judgments of English courts. For example, among the reviewed judicial cases, there are cases relating to labor disputes under employment contracts regulated by the AIFC Employment Regulations. In these judgments, the justices did not apply the rules of the Kazakhstan Labor Code. According to our findings, justices of the AIFC Court applied the Kazakhstan legislation when considering cases where the parties selected the Kazakhstan laws as the governing law.

Even if we allow for a theoretical possibility of applying the Law, it would be complicated to do this in practice because a major part of the key concepts of the Regulations is absent in the Law. For example, it is not possible to draw an analogy between the controller and an owner of a base containing personal data because these persons have completely different sets of duties.

Analysis of the Kazakhstan judicial practice also shows that there are very few court judgments relating to violations in the personal data protection sphere. A major part of the publicly available cases was primarily connected with the protection of honor, dignity, and business reputation, and the claimants additionally referred to the violation of requirements on personal data protection.

We previously mentioned that the justices of the AIFC Court tend to refer to the English court judgments, which, unlike the Kazakhstan courts, are highly experienced in resolving disputes in the personal data protection sphere. Provisions of the GDPR had been incorporated into the laws of England and Wales before the UK's exit from the EU, and they are commonly known as the UK GDPR. The UK legal regulation of data protection is very similar to the EU regulation, and

when resolving disputes in the personal data protection sphere, the AIFC justices are more likely to rely upon the laws of the AIFC and English laws than upon the Kazakhstan legislation.

Over the past few years, there have been many violations of requirements on personal data protection, which were extensively discussed by the Kazakhstan mass media. We recommend that companies registered in the AIFC treat personal data protection issues with due care and diligence to mitigate the risk of violations and liability.

Yekaterina Khamidullina Partner
y.khamidullina@aequitas.kz
AEQUITAS Law Firm, Almaty

---

1. See: https://publicreg.myafsa.com/roc/
2. As of January 16, 2024, 98 judicial cases over the years 2019-2023 were posted on the website of the AIFC Court.