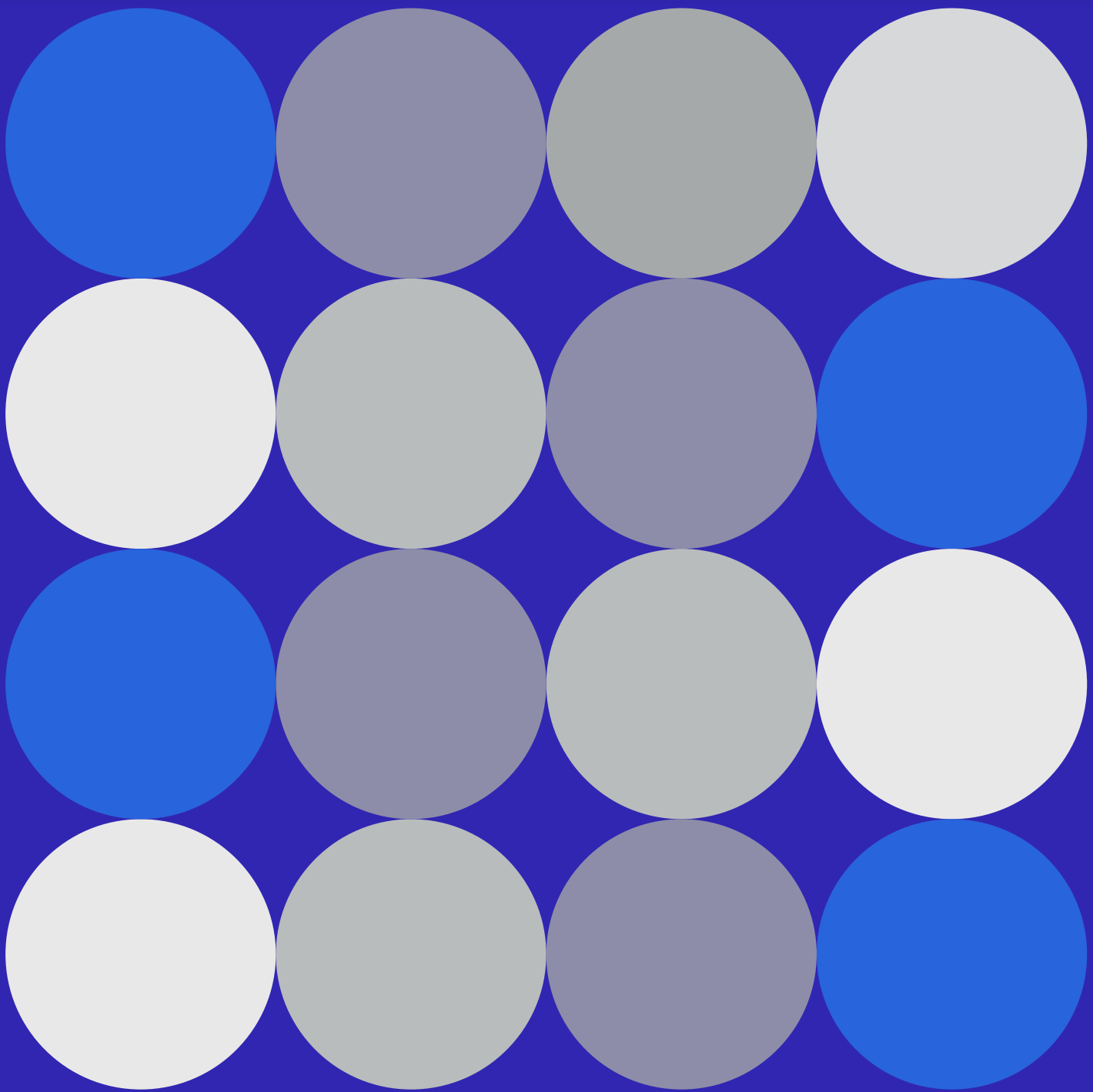
PERSONAL DATA PROTECTION. STATE OVERSIGHT AND LEGISLATIVE UPDATES.

GRATA INTERNATIONAL



PERSONAL DATA PROTECTION. STATE OVERSIGHT AND LEGISLATIVE UPDATES.

On 11 February 2024, Kazakhstan put into effect the Law 'On the Introduction of Amendments and Supplements to Certain Legislative Acts On Information Security, Informatization, and Digital Assets' (hereinafter - the 'Law'), dated 11 December 2023, No. 44-VIII ZRK. This Law introduces notable changes and supplements to the existing legislation, specifically the Law 'On Personal Data and Protection Thereof', dated 21 May 2013, No. 94-V (hereinafter - the 'Personal Data Law').

Key changes include:

1. Introduction of the concept of 'personal data security breach'.
2. Effective 1 July 2024, a new requirement mandates that the Ministry of Digital Development, Innovation, and Aerospace Industry of Kazakhstan (Digital Development Ministry) be notified of any breaches in personal data security.
3. Collecting and processing physical copies of identity documents is now prohibited.
4. The Digital Development Ministry is authorised to implement governmental oversight to ensure compliance with personal data legislation.

The amendments introduced to the Personal Data Law require businesses to adopt a more responsible approach to collecting and processing personal data. The law empowers the Digital Development Ministry to conduct unscheduled inspections of business entities to ensure compliance with the requirements of the Personal Data Law. Such inspections are initiated based on specific facts and circumstances concerning a particular business entity, such as complaints from individuals. The Digital Development Ministry should take a decision to conduct an unscheduled inspection and register it with the Legal Statistics and Special Records Committee of the General Prosecutor's Office of Kazakhstan. During the inspection, the Digital Development Ministry assesses the business entity's compliance with the requirements outlined in the inspection checklist. For matters related to personal data legislation, the checklist consists of 33 requirements. However, only some requirements are mandatory for some business entities. Following the state inspection, the Digital Development Ministry issues a report and a corrective order to address any identified violations according to the inspection checklist. Apart from the state inspection, a business entity may face administrative penalties if grounds for administrative offences are found.

The annex hereto provides an overview of the latest amendments and supplements to the Personal Data Law.

How can liability risks be minimised and compliance with personal data legislation ensured?

To minimise the risks of potential breaches of personal data protection legislation and ensure compliance, companies need:

1. Define the objectives of processing restricted personal data.
2. Establish procedures for processing, distributing, and accessing restricted personal data.
3. Define the procedure for blocking restricted personal data when requested by the data subject.
4. Approve a list of personal data necessary and sufficient for carrying out the tasks at hand.
5. Maintain a database within the territory of Kazakhstan where restricted personal data are stored.
6. Adopt a policy for collecting, processing, and protecting personal data.
7. Identify business processes containing restricted personal data.
8. Differentiate between publicly accessible and restricted personal data.
9. Specify the individuals responsible for collecting and processing personal data or having access to them.
10. Appoint a person responsible for organising the personal data processing (for legal entities).
11. Ensure the installation of information security devices and software updates on technical devices processing restricted personal data.
12. Implement the maintenance of (1) event logs of database management systems when processing restricted personal data and (2) user activity logs for those having access to restricted personal data.
13. Implement the use of integrity control measures for restricted personal data.
14. Implement cryptographic information security tools and encryption for storing and transmitting personal data.
15. Implement user identification and/or authentication measures when working with restricted personal data.
16. Have the ability to demonstrate the protection of personal data in countries where cross-border personal data transfer occurs.

Meeting these requirements is a complex task that companies' IT departments should perform jointly with legal experts to minimize negative consequences and risks.

This overview is provided for informational purposes only. While it offers a general understanding, it does not constitute legal advice. For comprehensive guidance tailored to your specific situation, we encourage you to contact GRATA Law Firm at almaty@gratanet.com .

Best Regards,

GRATA Law Firm

1. PERSONAL DATA SECURITY BREACH

The Law introduced a new concept of 'personal data security breach'[1] recognised as "a breach of personal data protection resulting in unlawful dissemination, alteration, or destruction, unauthorised dissemination of transmitted, stored, or otherwise processed personal data, or unauthorised access to them".

The developers of the Law introduced this concept because they deemed it necessary to identify personal data leaks that can seriously harm individuals' rights and interests.

Based on the 'personal data security breach' concept in the Personal Data Law, data security means the state of their protection from unlawful and unauthorised access and processing, including alteration, destruction, transmission, dissemination, and storage of personal data. According to Articles 22 and 25 of the Personal Data Law, compliance with the obligations of the owner[2] and operator[3] protects such security. Organisational, technical, and legal measures that the owner, operator, and third party[4] must take and comply with ensure personal data security. These measures include having rules, procedures, and internal policies for collecting, processing, storing, and transmitting data, regulating access to personal data, establishing protection measures, and other measures.

2. PERSONAL DATA SECURITY BREACH NOTIFICATION

Starting from 1 July 2024, the Law introduced a new obligation for the owner and operator to notify the competent authority (Digital Development Ministry) of any personal data security breach within one business day of its discovery.[5] The notice must include the contact information of the person responsible for the organisation of personal data processing (if applicable). Subsequently, the competent authority forwards information about the personal

[1] Article 1.11.1 of the Law 'On the Introduction of Amendments and Supplements to Certain Legislative Acts On Information Security, Informatization, and Digital Assets', dated 11 December 2023, No. 44-VIII ZRK
[2] Owner of the database containing personal data means the state authority, individual and(or) legal entity implementing in accordance with the laws of the Republic of Kazakhstan the right of possession, use and disposal of the database containing personal data.
[3] operator of the database containing personal data means the state authority, individual and(or) legal entity engaged in the collection, processing and protection of personal data.
[4]Third party means a person, which is not the subject, owner and (or) operator, but having connections or legal relationships with them concerning the collection, processing and protection of personal data.
[5] Article 1.11.4 of the Law 'On the Introduction of Amendments and Supplements to Certain Legislative Acts On Information Security, Informatization, and Digital Assets', dated 11 December 2023, No. 44-VIII ZRK. See also Article 25.2.8 of the Personal Data Law ('Rights and Obligations of the Owner and/or Operator, the Person Responsible for Organisation of Processing of Personal Data').

data security breach to the operator of the information and communication infrastructure of the 'e-government' ('National Information Technologies' JSC) if such a breach entails the risk of violating personal data subjects' rights and legitimate interests. Thus, the new provision introduces a mechanism for alerting the competent authority and the 'e-government' operator about personal data security breaches that risk violating the rights and legitimate interests of the data subjects. The new provision establishes a strictly defined procedure for actions by owners and operators in case of personal data security breaches. Such an approach will enable a prompt response to breaches and minimise potential consequences for data subjects. In addition, the Parliament made corresponding amendments to the Law of the Republic of Kazakhstan 'On Informatisation' dated 24 November 2015.[6]

Please note that the obligation to report data security breaches will only come into effect on 1 July 2024. However, businesses should minimise potential risks and liabilities and implement the obligations stipulated by the Personal Data Law before 1 July 2024. Many companies and enterprises still need to develop and adopt the required legislative documents, procedures, and policies for protecting personal data, have not appointed a person responsible for the organisation of personal data processing, and have not taken other measures to protect personal data. Below, we will indicate what businesses should pay attention to.

3. PROHIBITION OF THE COLLECTION AND PROCESSING OF PHYSICAL COPIES OF IDENTITY DOCUMENTS

The Law prohibits the collection and processing of physical copies of identity documents.[7] The prohibition also applies to documents certifying identity generated by the e-government digital document service, as they are considered equivalent to paper documents.

The Law also establishes cases that do not fall under this prohibition. It is permitted to collect and process paper copies of identity documents if:

- the owner, operator, or third party has no integration with the information systems of state authorities and/or state legal entities;
- the owner, operator, or third party cannot identify the data subject using technical means;
- in other cases, established by laws of the Republic of Kazakhstan.

According to the Law developers, the new provisions regarding the prohibition of collecting

[6] Article 1.12 of the Law 'On the Introduction of Amendments and Supplements to Certain Legislative Acts On Information Security, Informatization, and Digital Assets', dated 11 December 2023, No. 44-VIII ZRK
[7] Article 1.11.2 of the Law 'On the Introduction of Amendments and Supplements to Certain Legislative Acts On Information Security, Informatization, and Digital Assets', dated 11 December 2023, No. 44-VIII ZRK

paper copies of documents will protect personal data and eliminate the causes and conditions for their leakage. However, the above list of exceptions to this requirement (prohibition) raises questions of interpretation and enforcement. In other words, any owner, operator, or third party that does not have integration with the e-government or technological means of identification retains the right to request paper copies of identity documents from individuals. This option may be used, for example, by private employers, landlords, educational institutions (schools, colleges, universities, language training courses, etc.), fitness centres, and other institutions. With this approach, it seems doubtful whether the new provisions prohibiting the collection of paper copies can eliminate the causes of personal data leakage.

It is worth noting that the prohibition does not apply to copies of documents of non-residents and labour migrants.

4. COLLECTION AND PROCESSING OF PERSONAL DATA WITHOUT THE CONSENT OF THE SUBJECT

The list of cases where consent of the data subject is not required for the collection and processing of personal data has been expanded. The law grants the Unified Accumulative Pension Fund the right not to obtain consent from the data subject when opening a pension account, informing them about pension savings and conditional pension accounts.[8] This new provision contributes to the efficiency of the Unified Accumulative Pension Fund's operations, allowing for the reduction of administrative procedures and simplification of interaction with users of the pension system.

5. STATE OVERSIGHT OVER COMPLIANCE WITH THE LEGISLATION OF THE REPUBLIC OF KAZAKHSTAN ON PERSONAL DATA AND ITS PROTECTION

The Law has endowed the Digital Development Ministry, the competent authority in personal data protection (hereinafter, the 'Competent Authority'), with additional powers.[9] The critical innovation is state control over compliance with the Republic of Kazakhstan's legislation on personal data and its protection.[10]

[8] Article 1.11.3 of the Law 'On the Introduction of Amendments and Supplements to Certain Legislative Acts On Information Security, Informatization, and Digital Assets', dated 11 December 2023, No. 44-VIII ZRK
[9] Article 1.11.5 of the Law 'On the Introduction of Amendments and Supplements to Certain Legislative Acts On Information Security, Informatization, and Digital Assets', dated 11 December 2023, No. 44-VIII ZRK
[10] Articles 1.2 and 1.11.6 of the Law 'On the Introduction of Amendments and Supplements to Certain Legislative Acts On Information Security, Informatization, and Digital Assets', dated 11 December 2023, No. 44-VIII ZRK.

Furthermore, the new Article 27-2 of the Personal Data Law establishes that businesses and state authorities are subject to control. While the Entrepreneurial Code of the Republic of Kazakhstan regulates the procedure for conducting state control over businesses, Article 27-3 of the Personal Data Law separately establishes the procedure for monitoring compliance with the legislation on personal data protection by state authorities, the National Bank of the Republic of Kazakhstan, and its organisations.

5.1. STATE OVERSIGHT REGARDING STATE AUTHORITIES

Article 27-3 of the Personal Data Law establishes the procedure for conducting state control regarding state authorities through periodic and unplanned inspections. Periodic inspections are performed no more than once a year according to a plan approved by the head of the Competent Authority. Unscheduled inspections are appointed by the Competent Authority and conducted upon receipt of complaints from individuals and legal entities, requests from prosecutors, state authorities, and other cases.

Moreover, Articles 27-3 of the Personal Data Law define the rights and obligations of the subjects of State Control, the deadlines for conducting inspections, and other provisions.

5.2. STATE OVERSIGHT REGARDING BUSINESS ENTITIES

Under the first part of Article 27-2 of the Personal Data Law, the Digital Development Ministry performs state control over owners and operators who are business entities in the form of unscheduled inspections following the Entrepreneurial Code of the Republic of Kazakhstan. It is crucial to note that such inspections require a valid reason - a specific fact or set of circumstances concerning a particular entity (or object) under the oversight. The primary aim of these unscheduled inspections is to prevent or address immediate threats to the lawful interests of individuals. The supervisory authority (the Digital Development Ministry) issues a directive to initiate an unscheduled inspection,[11] which is then mandatorily registered with the Committee on Legal Statistics and Special Records of the General Prosecutor's Office of the Republic of Kazakhstan.[12]

These unscheduled inspections are designed to focus solely on the requirements outlined in the comprehensive inspection checklist.[13] It's crucial to understand that, in accordance with the stipulations of Article 85.2.2 and Article 143 of the Entrepreneurial Code of the Republic of Kazakhstan, a Joint Order of competent authorities has been issued, approving the checklist

[11] Article 145.1 of the Entrepreneurial Code of the Republic of Kazakhstan
[12] Article 146.1 of the Entrepreneurial Code of the Republic of Kazakhstan
13] Article 137.6 of the Entrepreneurial Code of the Republic of Kazakhstan.

for adherence to legislation on personal data.[14] This checklist encompasses 33 essential requirements that are applicable to the activities of owners, operators, and third parties. It's important to note, however, that not all checklist requirements may be relevant to certain owners, operators, and third parties. After the inspection, the supervisory authority will issue a directive detailing checklist items where violations were identified, along with directives for remedial action.[15]

Please note that during an unscheduled inspection, grounds may be found to initiate administrative offence proceedings and impose the appropriate administrative penalty.

[14] Joint Order the Minister of Digital Development, Innovation, and Aerospace Industry of the Republic of Kazakhstan, dated 19 March 2024, No. 149/NK and Order of the Deputy Prime Minister - Minister of National Economy of the Republic of Kazakhstan, dated 19 March 2024, No. 12. 'On the Approval of an Inspection Checklist for Compliance with the Legislation of the Republic of Kazakhstan on Personal Data and Protection Thereof in Relation to Owners, Operators, and Third Parties.' Registered with the Ministry of Justice of the Republic of Kazakhstan on 29 March 2024, No. 34179

[15] Article 152 of the Entrepreneurial Code of the Republic of Kazakhstan