TABLE OF CONTENTS

September 2021

GENERAL

1. LEGAL REQUIREMENT | OFFICIAL RECOMMENDATION

Data protection in Kazakhstan is mainly regulated by the Law of 21 May 2013 No. 94-V ZRK on Personal Data and its Protection ('the Personal Data Law'), Law of 24 November 2015 No. 418-V on Informatisation ('the Informatisation Law') and relevant subsidiary laws. The Personal Data Law contains a general legal framework for personal data protection, whereas the Informatisation Law regulates, *inter alia*, the protection of data contained in so-called 'informatisation objects.' Informatisation objects include electronic information resources (e.g. websites), programme software, internet-resources and information and communication infrastructure (Article 1.4 of the Informatisation Law).

The relevant authority in the sphere of personal data protection is the Ministry of Internal Affairs of the Republic of Kazakhstan ('MIA').

The relevant authority in the sphere of information safety is the Committee for Information Safety of the Ministry of Defense and Aerospace Industry of the Republic of Kazakhstan ('MDAI').

The Personal Data Law does not contain a requirement to notify a personal data breach. However, the Informatisation Law contains a general notification requirement about so-called 'information security incidents.' Information security incident means separately or serially occurring failures in the

operation of the information and communication infrastructure or its individual objects, which threaten their proper functioning and/or the conditions for illegally obtaining, copying, distributing, modifying, destroying or blocking electronic information resources.

Our interpretation of the law suggests that a general requirement to notify breaches of information security incidents entails, *inter alia*, a requirement to notify on data breaches.

The Informatisation Law contains the following requirements:

- the Operational Information Security Center ('OISC') (a legal entity or a structural subdivision of a legal entity that carries out activities to protect electronic information resources, information systems, telecommunications networks and other information facilities) shall immediately notify the owner of the information and communication infrastructure and the National Information Security Coordination Center ('NISCC') (a legal entity that coordinates exchange of information among OISCs) about an information security incident (Article 7-2.1.2 of the Informatisation Law);
- the Information Security Incident Response Service ('ISIRS') (a legal entity or a structural subdivision of a legal entity providing analysis of information on information security events in order to provide advisory and technical assistance in eliminating the consequences of information security incidents) shall notify the owners and possessors of information objects and NISCC about known incidents and threats to information security (Article 7-3.1.3 of the Informatisation Law); and
- owners or possessors of 'electronic government'[1] objects or 'critically important'[2] objects of information and communication infrastructure shall take measures ensuring immediate notification to the NISCC of an occurred information security incident (Article 54.2.6 of the Informatisation Law).

To summarise, Kazakh law provides for notification on data breaches (as a part of an information security incident) only in cases where such data is contained in electronic information resources.

2. DEFINITION OF A DATA BREACH

Data breach is, generally, the unauthorised release of protected data.

There is no specific definition of 'data breach' under Kazakh law.

However, as mentioned above, the Informatisation Law contains the broad definition of 'information security incident' that, according to our interpretation of the law, may include illegal release etc. of data.

3. WHO MUST NOTIFY A BREACH?

In most of the cases provided for by the Informatisation Law, the third parties (OISC, ISIRS, NISCC) rather than the data controller/data processor shall notify the data breach.

The data controller/data processor shall notify data breaches only if the relevant object of information and communication infrastructure (where the information security incident occurred) relates to 'electronic government' or is a 'critically important' object.

4. WHO MUST BE NOTIFIED?

4.1. Authorities

Depending on the case, the NISCC and owners of information and communication infrastructure shall be notified.

4.2. Subscribers

Not applicable.

4.3. Others

Not applicable.

5. NOTIFICATION REQUIREMENTS

5.1. Type/content of notice

Not applicable.

5.2. Substitute notice

Not applicable.

5.3. Timeframe

There are certain requirements relating to the timeframe and form of notifications regarding information security incidents mentioned above.

5.4. Exemptions

Not applicable.

6. PENALTIES

Since there is no mandatory requirement under Kazakh law to notify subjects of data breaches, Kazakh law does not establish any sanctions for the failure to notify data breaches.

There are, however, certain administrative sanctions (fines) for the failure to notify the information security incidents mentioned above.

7. HOW TO

Not applicable.

TELECOMMUNICATIONS

1. LEGAL REQUIREMENT | OFFICIAL RECOMMENDATION

Law of the Republic of Kazakhstan of 5 July 2004 No.567 on Communications ('the Law on Communication') does not specifically require data breach notification. However, the above mentioned general provisions of the Informatisation Law will apply since objects of information and communication infrastructure (to which the Informatisation Law does apply) include, *inter alia*, telecommunication networks (Article 1.25 of the Informatisation Law).

2. DEFINITION OF A DATA BREACH

The Law on Communication does not include a specific data breach notification provision. There is also no specific definition of personal data in the context of telecommunications. However, the Law on Communication contains a definition of 'service information about subscribers' which includes:

- information on subscriber numbers, including information on individual identification numbers (for individuals) or business identification numbers (for legal entities) of the owners of subscriber numbers;
- information on the identification codes of cellular subscriber units, including information on individual identification numbers (for individuals) or business identification numbers (for legal entities) of owners of cellular subscriber units;
- billing information (information about the services received by the subscriber);
- the location of the subscriber unit in the network in accordance with the requirements of the technical regulations;
- addresses in the data network;
- addresses of access to internet resources in the data network;
- identifiers of the internet resource; and
- data network protocols.

Service information about subscribers is subject to protection by communication operators and/or owners of communication networks (Article 15.1.2 of the Law on Communications).

3. WHO MUST NOTIFY A BREACH?

Please see section 3 in General above.

4. WHO MUST BE NOTIFIED?

4.1. Authorities

Please see section 4 in General above.

4.2. Subscribers

Please see section 4 in General above.

4.3. Others

Please see section 4 in General above.

5. NOTIFICATION REQUIREMENTS

5.1. Type/content of notice

Please see section 5.1 in General above.

5.2. Substitute notice

Please see section 5.2 in General above.

5.3. Timeframe

Please see section 5.3 in General above.

5.4. Exemptions

Please see section 5.4 in General above.

6. PENALTIES

Please see section 6 in General above.

7. HOW TO

Not applicable.

BREACH NOTIFICATION PROVISIONS IN THE FINANCIAL SERVICES AND HEALTH SECTORS

1. HEALTH SECTOR

Code of the Republic of Kazakhstan of 7 July 2020 No. 360-VI on the Public Health and Healthcare System ('the Code on Public Health') defines a medical secret as personal medical data, information on the seeking of medical help, health status of a citizen, the diagnosis of their illness and other information obtained during their examination and/or treatment. A medical secret can generally be disclosed only upon the consent of a relevant subject.

The Code on Public Health does not contain a mandatory provision to report a medical secret breach to any supervisory authority or subject of a medical secret.

However, the above mentioned general provisions of the Informatisation Law will apply (to the extent that relevant data is contained in electronic information resources).

2. FINANCIAL SERVICES SECTOR

Law of the Republic of Kazakhstan of 31 August 1995 No. 2444 on Banks and Banking Activity in the Republic of Kazakhstan ('the Banking Law') contains a definition of bank secret that includes information of availability, owners, numbers of bank accounts of depositors, customers, and correspondents of the bank, of the balance and flow of money on these accounts and accounts of the bank itself, of bank operations (except for general terms of bank operations execution), and information of availability, owners, character and cost of customers' property, kept in safe boxes, boards and premises of the bank. A bank secret does not include information on credits issued by banks being in the process of liquidation. A bank secret can generally be disclosed only upon consent of the relevant subject.

The Banking Law does not contain mandatory provision to report a bank secret breach to any supervisory authority or subject of a bank secret.

However, the above mentioned general provisions of the Law on Informatisation will apply (to the extent that relevant data is contained in electronic information resources).

1. 'Electronic government' is a system of information interaction of state bodies among themselves and with individuals and legal entities, based on automation and optimisation of state functions, as well as being designed to provide services in electronic form.

2. 'Critically important' objects of the information and communication infrastructure are objects of the information and communication infrastructure, the violation or termination of functioning of which leads to an emergency situation of social and/or technogenic nature or to significant negative consequences for defence, security, international relations, the economy, certain spheres of the economy, or for vital activity of the population residing in the respective territory, including infrastructure: heat supply, electricity, gas supply, water supply, industry, healthcare, communications, banking, transport, hydraulic structures, law enforcement, and electronic government.