ICLG

The International Comparative Legal Guide to:

Data Protection 2017

4th Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Affärsadvokaterna i Sverige AB
Bae, Kim & Lee LLC
Bagus Enrico & Partners
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Cuatrecasas
Dittmar & Indrenius
Drew & Napier LLC
Ecija Abogados
ErsoyBilgehan
Eversheds Sutherland
GANADO Advocates
Gilbert + Tobin
GRATA International
Hacohen & Co.
Herbst Kinsky Rechtsanwälte GmbH
Hunton & Williams
Koushos Korfiotis Papacharalambous LLC
Lee and Li, Attorneys-at-Law
LPS L@w
Matheson
Mori Hamada & Matsumoto
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi Attorneys at Law Ltd.
Portolano Cavallo
Rato, Ling, Lei & Cortés Lawyers
Rossi Asociados
Subramaniam & Associates (SNA)
Wikborg Rein Advokatfirma AS

global legal group

global legal group

Contributing Editors
Anita Bapat and Aaron P. Simpson, Hunton & Williams

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Paul Mochalski

Sub Editor
Hollie Parker

Senior Editors
Suzie Levy, Rachel Williams

Chief Operating Officer
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd
May 2017

ISBN 978-1-911367-50-5
ISSN 2054-3786

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

General Chapter:

Country Question and Answer Chapters:

Kazakhstan

Leila Makhmetova

Saule Akhmetova

GRATA International

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The principal data protection laws are described below.

The Constitution of the Republic of Kazakhstan, dated 30 August 1995, declares that everyone has the right to privacy and protection of private and family secrets.

The Law 'On Informatisation', dated 24 November 2015 provides for the measures to prevent illegal access to digital information.

The Law 'On Personal Data and Protection thereof", dated 21 May 2013, provides for the rules on the collection, storage, processing and protection of personal data.

1.2 Is there any other general legislation that impacts data protection?

According to the **Civil Code** of the Republic of Kazakhstan, every citizen has the right to protection of confidentiality of his/her private life, including privacy of his/her correspondence, phone conversations, diaries, notes, messages, intimacy, adoption, birth, medical and client-attorney privilege.

The Civil Procedural Code and **The Criminal Procedural Code** of the Republic of Kazakhstan say that the right to confidentiality of the private life of anyone may be restricted only in cases directly specified by laws.

The Labour Code of the Republic of Kazakhstan requires an employer to protect personal data on its employees, if such data are kept by the employer.

1.3 Is there any sector-specific legislation that impacts data protection?

The Law of the Republic of Kazakhstan "On National Security of the Republic of Kazakhstan", dated 6 January 2012, provides information security that is protecting the information space of the Republic of Kazakhstan, as well as the rights and interests of citizens, society and the state in the information sphere from the real and potential threats.

The Law of the Republic of Kazakhstan "On State Secrets", dated 15 March 1999, envisages protective measures for state secrets, i.e. information, the dissemination of which is restricted by the Government in order to perform effective military, economic, scientific, foreign economic, foreign policy, intelligence, counter-intelligence, investigative and other activities.

The Law of the Republic of Kazakhstan, "On Telecommunications", dated 5 July 2004 provides for the rules on protection of privacy of correspondence, telephone conversations, mailing, telegraph and other messages transmitted by telecommunication networks by network operators except for certain cases established by the laws of the Republic of Kazakhstan.

The Law of the Republic of Kazakhstan "On Investigative Activities", dated 15 September 1994, provides for the rules for the performance of investigative activities by the state authorities listed in the Law (the Ministry of Internal Affairs, the Committee on National Security and some others). In particular, the Law specifies restrictions on the control over correspondence, bugging, obtaining information from communication channels, etc.

The Code on the Nation's Health and the Health Care System, dated 18 September 2009, provides for the rules on protection of privacy of medical patients.

1.4 What is the relevant data protection regulatory authority(ies)?

The relevant data protection regulatory authorities are: The Government of the Republic of Kazakhstan; the Ministry on Information and Communications (**hereinafter – the 'Ministry on Communication'**); the Ministry on Internal Affairs; and various Prosecutors.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"

  This means data fixed in any tangible medium and related to a certain person or a person that can be identified on the basis of the data.
- "**Sensitive Personal Data**"
- Kazakh legislation does not provide for such term.
- "**Processing**"

  This means actions taken for accumulation, storage, amendment, development, updating, use, dissemination, depersonalisation, blockage and abolishment of personal data.

- "**Data Controller**"
- There is no such term in Kazakh legislation.
- "**Data Processor**"

  There is no such term in Kazakh legislation.
- "**Data Subject**"

  This means the individual whom the relevant personal data are related to.
- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*
  - "**Owner of the Database, which Contains Personal Data**"

    This means a state authority, individual or legal entity, which has the right to own, use and manage of a database that contains personal data.
  - "**Operator of the Database, which Contain Personal Data**"

    This means a state authority, individual or legal entity, which engages in the collection, processing and protection of personal data.

3 Key Principles

3.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

  This principle is not provided by the legislation.
- **Lawful basis for processing**

  This is not applicable in Kazakhstan.
- **Purpose limitation**

  This is not applicable in Kazakhstan.
- **Data minimisation**

  This is not applicable in Kazakhstan.
- **Proportionality**

  This principle is not provided by the legislation.
- **Retention**

  This principle is not provided by the legislation.
- *Other key principles – please specify*
  - **Legitimacy**
    - Respect to human and civil rights provided by the Constitution.
    - Confidentiality of personal data of restricted access.
    - Equal rights of personal data subjects, owners and operators of databases which contain personal data.
    - Maintenance of safety of individuals, the society and the State.

4 Individual Rights

4.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Access to data**

  Personal data subjects have the right to gain access to their personal data upon requests submitted to owners or operators of the databases.
- **Correction and deletion**

  Personal data subjects may require owners or operators of the databases: (1) to correct personal data on reasons confirmed by the relevant documents; or (2) to delete personal data collected or processed in an unlawful way.
- **Objection to processing**

  Collection and processing of personal data is only possible upon the valid consent of the personal data subject. The personal data subject may withdraw his/her consent except in cases specified by the laws of the Republic of Kazakhstan.
- **Objection to marketing**

  Personal data subjects may give or refuse to give their consent to the dissemination of their personal data through publicly available sources.
- **Complaint to relevant data protection authority(ies)**

  Personal data subjects may apply for protection of their rights to prosecutors or courts.

5 Registration Formalities and Prior Approval

5.1 In what circumstances is registration or notification required to the relevant data protection regulatory authority(ies)? (E.g., general notification requirement, notification required for specific processing activities.)

The legislation provides obligatory attestation for internet resources and data systems as follows:

- internet resources and data systems of the state authorities;
- "critically important" data systems (which is to be defined by the Government, but have not been defined yet); and
- non-governmental data systems integrated with governmental ones or destined for development of governmental data systems or internet resources.

Attestation of other non-governmental data systems and internet-resources is not obligatory.

5.2 On what basis are registrations/notifications made? (E.g., per legal entity, per processing purpose, per data category, per system or database.)

Attestation is performed on a internet resource basis as stated in question 5.1 above.

5.3 Who must register with/notify the relevant data protection authority(ies)? (E.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation.)

Attestation is conducted upon an application of the owner of the data system or internet resource.

5.4 What information must be included in the registration/notification? (E.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes.)

The certificate issued as a result of the attestation confirms that the certain data system or internet resource complies with requirements

on informational security and contains the name of the data system, the hardware and software used for the data system and some other information.

5.5 What are the sanctions for failure to register/notify where required?

Failure to perform an obligatory attestation may result in a fine of the amount of up to 100 Months Calculated Indexes ('MCI'). In 2017, 1 MCI is 2,269 tenge, and equates to approximately 7.1 USD as of 3 March 2017.

5.6 What is the fee per registration (if applicable)?

The fee is subject to approval by the Ministry on Investment and Development of the Republic of Kazakhstan. As of 6 March 2017, the amount of the fee is 2,948,967 tenge (which is about 9,303 USD) and trip costs (if any) for experts of the Republican State Enterprise "State Technical Service" which examines information systems.

5.7 How frequently must registrations/notifications be renewed (if applicable)?

The attestation is required again in case of any change (1) in the conditions of operation or functionality of the data system or internet resource, or (2) in hardware-software complex or information and communication technologies used for data processing and protection.

5.8 For what types of processing activities is prior approval required from the data protection regulator?

Implementation of works connected with use of state secrets requires a permit of the Committee of National Security of the Republic of Kazakhstan. In addition, development or sale (or another transfer) of cryptographic tools requires a licence issued by the said authority.

5.9 Describe the procedure for obtaining prior approval, and the applicable timeframe.

For obtaining a permit for implementation of works connected with the use of state secrets, a legal entity submits, an application and some other documents including a conclusion of a special examination of the applicant to the Committee of National Security.

A licence for development or sale (or another transfer) of cryptographic tools is issued within 15 business days from the day of submission of an application and other required documents (information on the applicant, information on the availability of employees with the relevant education, etc.).

6 Appointment of a Data Protection Officer

6.1 Is the appointment of a Data Protection Officer mandatory or optional?

Appointment of one or several Data Protection Officers is mandatory for all owners and operators of personal databases and other persons/entities that hold and/or use personal data.

6.2 What are the sanctions for failing to appoint a mandatory Data Protection Officer where required?

Usually, it is a fine in the amount of up to 300 MCI.

6.3 What are the advantages of voluntarily appointing a Data Protection Officer (if applicable)?

This is not applicable.

6.4 Please describe any specific qualifications for the Data Protection Officer required by law.

The laws do not provide for any specific qualifications for the Data Protection Officer.

6.5 What are the responsibilities of the Data Protection Officer, as required by law or typical in practice?

The main responsibilities of the Data Protection Officer include development of a list of personal data to be collected, processed and used, taking measures for personal data protection.

6.6 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

A Data Protection Officer may be an employee or a contractor of the owner or operator of the database. The appointment and liabilities of the employee must be fixed by a written order of the owner or operator of the database. The appointment and liabilities of the contractor are provided by the contract. Registration or notification of state authorities on issue of the order or conclusion of the contract is not required.

7 Marketing and Cookies

7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, email, or SMS text message. (E.g., requirement to obtain prior opt-in consent or to provide a simple and free means of opt-out.)

According to the Rules for Rendering Mobile Communication Services, distribution of marketing messages via mobile communication networks is only allowed upon a subscriber's consent. However, there are no restrictions on sending marketing communications by post, fixed telephone or email.

There are restrictions connected with the content of advertisement (for example, a ban on advertising tobacco and alcohol products; and a restriction on inaccurate advertisement, etc.).

7.2 Is the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The Ministry on Communication is active in enforcement of breaches of the Rules for Rendering Mobile Communication Services. In other cases, the state control over marketing activities is connected with the content of the advertisements, rather than with data protection.

7.3 Are companies required to screen against any "do not contact" list or registry?

Communication operators may not provide access to information, the dissemination of which is prohibited by a court decision or by laws (for example, foreign mass media including internet resources which provide calls for extremism, terrorism, mass disorders, etc.).

7.4 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Such a penalty is 200 MCI (for providing access to information, the dissemination of which is prohibited).

7.5 What types of cookies require explicit opt-in consent, as mandated by law or binding guidance issued by the relevant data protection authority(ies)?

Any type of cookies, which collects personal data, requires opt-in consent of the personal data subject. Such consent may be expressed in writing, in an electronic document or in another way not prohibited by the legislation.

7.6 For what types of cookies is implied consent acceptable, under relevant national legislation or binding guidance issued by the relevant data protection authority(ies)?

If cookies are used for the collection of personal data, no consent of the personal data subject can be implied. In any case, it must be expressed by the personal data subject in a way not prohibited by the legislation.

7.7 To date, has the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

This has not been the case so far.

7.8 What are the maximum penalties for breaches of applicable cookie restrictions?

Kazakh legislation does not provide for any cookies restrictions and, therefore, no penalties are specified for violations of such restrictions.

8 Restrictions on International Data Transfers

8.1 Please describe any restrictions on the transfer of personal data abroad.

Personal data may be transferred to the states, where protection is ensured for such personal data. The personal data transfer to other states is allowed (1) upon the consent of the personal data subject, (2) in cases specified by international agreements, or (3) if such a transfer is required for protection of human rights, health, morality or law enforcement.

8.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions.

Usually, companies obtain written consent of their employees to the collection and processing of their personal data, and subsequently transfer them abroad.

8.3 Do transfers of personal data abroad require registration/notification or prior approval from the relevant data protection authority(ies)? Describe which mechanisms require approval or notification, what those steps involve, and how long they take.

Transfers of personal data abroad do not require any registration/notification or prior approval from state authorities.

9 Whistle-blower Hotlines

9.1 What is the permitted scope of corporate whistle-blower hotlines under applicable law or binding guidance issued by the relevant data protection authority(ies)? (E.g., restrictions on the scope of issues that may be reported, the persons who may submit a report, the persons whom a report may concern.)

The Kazakh legislation does not directly regulate the matters of corporate whistle-blowing, except for the issues of personal data protection. If any third party (other than a reporting person) may obtain access to personal data, this can be only done according to an explicit written consent of the person, whose data are being accessed.

9.2 Is anonymous reporting strictly prohibited, or strongly discouraged, under applicable law or binding guidance issued by the relevant data protection authority(ies)? If so, how do companies typically address this issue?

Anonymous reporting is not recognised as a reason for any kind of criminal, administrative or other investigations by the Kazakh state authorities. The companies usually declare commercially sensible information as a commercial secret and impose the non-disclosure obligations on employees, but this does not deprive the employees of applying with non-anonymous complaints on the employer.

9.3 Do corporate whistle-blower hotlines require separate registration/notification or prior approval from the relevant data protection authority(ies)? Please explain the process, how long it typically takes, and any available exemptions.

No, there is no requirement on obtaining separate registration/notification or prior approval from the relevant data protection authority for corporate whistle-blower hotlines.

9.4 Do corporate whistle-blower hotlines require a separate privacy notice?

No, there is no such requirement, but the company needs to comply with personal data protection requirements.

9.5 To what extent do works councils/trade unions/ employee representatives need to be notified or consulted?

There is no such requirement, unless the relevant obligation is imposed by a collective bargaining or social partnership agreement.

10 CCTV and Employee Monitoring

10.1 Does the use of CCTV require separate registration/ notification or prior approval from the relevant data protection authority(ies)?

No, there is no requirement to obtain registration/notification or prior approval from the relevant data protection authority for the use of CCTV, but consent of an affected employee is to be sought.

10.2 What types of employee monitoring are permitted (if any), and in what circumstances?

The Kazakh legislation is silent on the issue of employee monitoring via video or other remedies. According to the Constitution of Kazakhstan, everyone shall have the right to inviolability of private life, personal or family secrets, protection of honour and dignity. Moreover, records of covert video recording cannot be used as evidence in court proceedings, except by the competent state authorities. It is recommended to get consent of the employees for their monitoring and recording.

10.3 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Written consent of employees are required. The employer shall ask for written consent of the employee before initiating the monitoring. The law does not establish any terms for obtaining the employee's consent, but we recommend to meet the term of three days before the start of monitoring (the standard term as provided by the labour legislation).

10.4 To what extent do works councils/trade unions/ employee representatives need to be notified or consulted?

There is no such requirement in the laws, unless a collective bargaining or a social partnership agreement states otherwise.

10.5 Does employee monitoring require separate registration/notification or prior approval from the relevant data protection authority(ies)?

There is no such requirement.

11 Processing Data in the Cloud

11.1 Is it permitted to process personal data in the cloud? If so, what specific due diligence must be performed, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

The processing of Personal Data in the cloud except for storage is not prohibited. The storage of Personal Data is only allowed through databases located in Kazakhstan.

There is no binding guidance issued by the relevant authority. The law requires obtaining the consent of individuals for data processing.

11.2 What specific contractual obligations must be imposed on a processor providing cloud-based services, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

The legislation allows to process data only upon provision of protection thereof. Therefore, the contract should include obligation of the provider of cloud-based services to protect personal data while processing. Additionally, the provider should:

- segregate personal data from any other information;
- identify mediums, on which personal data are recorded and kept; and
- identify persons engaged in the personal data processing and having access thereto.

12 Big Data and Analytics

12.1 Is the utilisation of big data and analytics permitted? If so, what due diligence is required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Kazakh law does not contain definitions for big data, analytics and utilisation. However, some requirements to i-system, object of informatisation, i-communication services, i-communication technologies, hardware and software complex, and software should be applied. Utilisation as to the use of specific means for data processing is not prohibited by law. Such utilisation should be performed subject to the available valid consent of a person concerned and is prohibited for causing property or moral damages and limitation in the implementation of rights and freedoms.

No special guidance or requirements are approved by the Committee of Public Control in the sphere of Communication, Informatisation and Mass Media of the Ministry of Information and Communication of the Republic of Kazakhstan.

13 Data Security and Data Breach

13.1 What data security standards (e.g., encryption) are required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

The law requires the owners/holders of informatisation objects (that includes information resources, software, communication infrastructure) to provide protection thereof in accordance with the relevant standards.

The Unified Requirements in the Field of Information and Communication Technologies and Provision of Information Security was approved by the Governmental Decree No.832 dated 20 December 2016. These requirements supposed to be applicable to informatisation objects related to "E-Government" sector.

At the same time, there is a great number of relevant data security standards approved by different authorities for standardisation purposes. These standards shall be applied depending on particular case, type of data, and holder of informatisation objects.

13.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

Kazakh legislation does not directly provide the reporting obligation in case of data breaching.

The Data Protection authority expects voluntary breach reporting, since such reporting is in the interests of the relevant owner/holder/user of data. Otherwise, an offender who breached data security will not be convicted.

13.3 Is there a legal requirement to report data breaches to individuals? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

Kazakh legislation on informatisation does not contain any requirements to report data breaches to individuals. The Data Protection authorities expect that individuals will be informed if they are recognised as an injured person due to the breach.

13.4 What are the maximum penalties for security breaches?

A maximum penalty for security breaches under the criminal legislation is imprisonment for up to 10 years. This penalty can be applied for:

- Violation of the information system of telecommunication networks.
- Forcing data transmission.
- Creation and use or distribution of harmful computer programs and software.

A maximum penalty for security breaches under the administrative legislation is a fine of 20 MCI for individuals; 50 MCI for officials; and 100 MCI for legal entities. This penalty can be applied for a wide range of actions that can be considered an offence. However, most of these actions relates to the unduly provision of data security by owners/holders.

14 Enforcement and Sanctions

14.1 Describe the enforcement powers of the data protection authority(ies).

Investigatory Power	Please note that in Kazakhstan, there is no one authority that may apply civil, administrative and criminal sanctions. It depends on the particular case and offence. **Administrative investigation**: The following state authorities have the right to consider cases of administrative offences and to impose administrative penalties in the area of informatisation: ■ Prosecutor's Authorities (to initiate investigation in case of breaching personal data). ■ Committee of Public Control in the sphere of Communication, Informatisation and Mass Media of the Ministry of Information and Communication of the Republic of Kazakhstan (to initiate an investigation for certain offences and to impose an administrative penalty). ■ Court (to impose an administrative penalty in certain circumstances and to consider the appeals). **Criminal investigation**: The following government authorities have the right to initiate and investigate criminal offences in the area of informatisation: ■ Ministry of Internal Affairs of the Republic of Kazakhstan (to initiate and to carry out investigation). ■ Committee of National Security (to initiate investigation and to investigate criminal cases connected with interests of national security in the sphere of informatisation). ■ Prosecutor's Authorities (approves the indictment and directs criminal case to court and supervises the process of investigation). ■ Court (to impose a criminal responsibility).
Civil/Administrative Sanction	**Civil law sanction**: Civil law sanction, such as monetary compensation, may be imposed by the court on the basis of a claim from an entity, which is harmed due to breaching. **Administrative sanction**: Administrative sanctions are established by the Administrative Code. Please see below administrative sanctions for data protection breaching. ■ **Article 79** 'A violation of the Law of the Republic of Kazakhstan on personal data and protection thereof'. **Penalty**: a fine in the amount from 30 MCI to 1000 MCI depending on circumstances of the offence. ■ **Article 641** 'A violation of the law of the Republic of Kazakhstan on informatisation'. **Penalty**: this article contains various types of offences in the area of Informatisation, where the minimum sanction is a fine of 10 up to 200 MCI depending on circumstances of the offence.
Criminal Sanction	**Criminal law sanction**: The Criminal Code establishes the following sanctions for data protection breaching: ■ **Article 147** 'Violation of personal privacy and legislation of the Republic of Kazakhstan on personal data and protection thereof'. **Penalty**: fine in the amount from 3,000 MCI or imprisonment for up to seven years depending on circumstances of the crime. ■ **Article 205** 'Illegal access to information, information system or network of telecommunications'. **Penalty**: a fine in the amount from 300 MCI to 2,000 MCI and (or) corrective works in the same amount or restriction of freedom for up to two years, or imprisonment for the same period, with or without the deprivation of the right to hold certain positions or to be engaged in a certain activity for up to three years, depending on circumstances of the crime. ■ **Article 206** 'Illegal destruction or modification of information'. **Penalty**: a fine in the amount from 500 MCI to 2,000 MCI or imprisonment for three to seven years with or without deprivation of the right to hold certain positions or to be engaged in a certain activity for up to three years, depending on circumstances of the crime. ■ **Article 207** 'Disfunction of maintenance of information system or networks of telecommunications'. **Penalty**: a fine in the amount from 3,000 MCI or imprisonment for a period from five to 10 years with or without deprivation of the right to hold certain positions or to be engaged in a certain activity for up to five years, depending on circumstances of the crime. ■ **Article 208** 'Illegal seizure of information'. **Penalty**: a fine in the amount from 200 MCI to imprisonment for a period of three to seven years with or without deprivation of the right to hold certain positions or to be engaged in a certain activity for up to three years, depending on circumstances of the crime. ■ **Article 209** 'Information transfer compulsion'. **Penalty**: a fine in the amount from 2,000 MCI or imprisonment for a period of five to 10 years with or without deprivation of the right to hold certain positions or to be engaged in a certain activity for up to five years, depending on circumstances of the crime. ■ **Article 210** 'Creation, use or distribution of harmful computer applications and software products'. **Penalty**: a fine in the amount to 3,000 MCI or imprisonment for a period of five to 10 years with or without deprivation of the right to hold certain positions or to be engaged in a certain activity for up to five years, depending on circumstances of the crime. ■ **Article 211** 'Illegal distribution of electronic information resources of limited access'. **Penalty**: a fine in the amount up to 200 MCI or imprisonment for a period of three to seven years with or without deprivation of the right to hold certain positions or to be engaged in a certain activity for up to five years, depending on circumstances of the crime.

14.2 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

Unfortunately, there is not a register of initiated administrative cases in Kazakhstan to get a picture of Data Protection Law enforcement.

According to the information provided on the official website of the Supreme Court of the Republic of Kazakhstan, since 1 January 2015, there were only three criminal law cases regarding data protection considered by courts of the Republic of Kazakhstan.

Therefore, Data Protection is not a priority area in Kazakhstan practice and no proper approach of Data Protection authorities have been developed yet.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

15.1 How do companies within your jurisdiction respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

According to the legislation of the Republic of Kazakhstan, companies within our jurisdiction do not have to respond to requests from foreign law enforcement agencies, as foreign law enforcement acts do not have jurisdiction over the territory of the Republic of Kazakhstan. Please note that it is not possible to monitor the way such companies respond to requests of foreign law enforcement agencies, as there is no such database.

However, on the assumption of the Law of the Republic of Kazakhstan "On Prosecutor's office", if there is a (i) convention, or (ii) bilateral treaty on legal cooperation that both the Republic of Kazakhstan and the foreign state are members of, the foreign state law enforcement agency may send a request regarding e-discovery or disclosure to the Prosecutor General's office of the Republic of Kazakhstan, which can be addressed to the companies within our jurisdiction by the Prosecutor General's office of the Republic of Kazakhstan and which is subject to response by the companies.

15.2 What guidance has the data protection authority(ies) issued?

There is not any guidance issued by a data protection authority in Kazakhstan.

16 Trends and Developments

16.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

According to the information provided on the official website of the Supreme Court of the Republic of Kazakhstan, since 1 January 2015, there were only three criminal law cases regarding data protection considered by courts of the Republic of Kazakhstan.

There have not been any administrative or civil law cases regarding data protection considered in the Republic of Kazakhstan since 1 January 2015. Therefore, it is not possible to mark any enforcement trends.

Thus, by the court sentence, dated 14 May 2015, of Semey city, the defendant was called not guilty for committing the crime stipulated by Article 147.2 of the Criminal Code. Article 147.2 of the Criminal Code stipulates criminal liability for illegal collection of information on private life of a person, which include his private or family life without his consent or if such actions cause harm to the rights and (or) legitimate interests of the person as a result of illegal collection and (or) processing of other personal data.

16.2 What "hot topics" are currently a focus for the data protection regulator?

The Informatisation Law is new and came into force in 2016. Therefore, the main "hot topic" is the adoption of relevant secondary legislation such as Unified Rules.

In addition, the Data Protection authority is in the process of the unification of data protection legislation with the Member States of the Eurasian Economic Union.

Moreover, on 29 March 2016, the Republic of Kazakhstan ratified the Protocol on Interaction of Member States of the Collective Security Treaty Organisation on Counteraction of Criminal Activity in the Information Area. According to this Protocol, the parties shall cooperate by the following measures:

- Exchange of information on crimes in information area.
- Execution of request regarding operational search actions.
- Planning and performance of coordinated actions.
- Rendering assistance in professional development.
- Creation of information systems.
- Implementation of joint scientific research.

Leila Makhmetova
GRATA International
104, M. Ospanov Street
Almaty, 050020
Kazakhstan

Tel: +7 727 2445 777
Email: lmakhmetova@gratanet.com
URL: www.gratanet.com

Counsel, Director of Environmental Law Department

Leila has extensive experience in environmental dispute resolution. Her success in representing clients has been constant and consistent. This success has led to her recent promotion to the position of counsel of GRATA Law Firm. Leila's clients include some of the most prominent figures in heavy industry. Previously, Leila was a Senior Lecturer at the Kazakh University of Law and Humanities and a legal expert at the Institute of Legislation governed by the Ministry of Justice of RK. She is a Candidate of Jurisprudence. She speaks Russian and English.

Practice Areas:

- Litigation and Dispute Resolution.
- Environmental Law.
- Health and Safety.

Saule Akhmetova
GRATA International
104, M. Ospanov Street
Almaty, 050020
Kazakhstan

Tel: +7 727 2445 777
Email: sakhmetova@gratanet.com
URL: www.gratanet.com

Partner, Branch Director

Saule graduated with honours from the Kazakh National University named after Al-Farabi. She has been working as a lawyer since 1997.

She has published many papers on tax, investment and subsoil use legislation.

Saule is a member of the Kazakhstan Petroleum Lawyers Association and the Almaty City Bar Association.

She speaks Kazakh, Russian and English.

GRATA INTERNATIONAL

GRATA International is an international law firm, founded on April 22, 1992.

Today, our clients have 200 professionals in 21 countries at their disposal. GRATA International is a global team representing different countries and nationalities, and which has legal advising experience in all areas of law.

GRATA International provides legal services across all cities in Kazakhstan. The firm has offices in Baku (Azerbaijan), Bishkek (Kyrgyzstan), Dushanbe (Tajikistan), Moscow (Russia) and Tashkent (Uzbekistan), as well as country desks in Ashgabat (Turkmenistan), Tbilisi (Georgia) and Ulaanbaatar (Mongolia), and associated offices in Kyiv (Ukraine), Minsk (Belarus), Istanbul (Turkey), Prague (Czech Republic), Riga (Latvia), and Zurich (Switzerland).

In addition to its offices, our firm has representatives in the cities of Amsterdam (Netherlands), Beijing (China), Dubai (United Arab Emirates), London (United Kingdom), New York (United States of America) and Vancouver (Canada).

Our competitive advantages include a wide network of offices mostly covering Eurasia, optimal price and quality ratio, and understanding of the local mentality of doing business.

Clients can gain access to the entire network by enquiring at one of the offices or representatives of GRATA International. The opportunity to utilise resources without regional boundaries enables us to increase the cost-effectiveness and the efficiency of the services provided.

GRATA International has been recognised by leading international ratings: *The Legal 500*; *Chambers Global*; *Chambers Asia-Pacific*; *IFLR1000*; *Who's Who Legal*; and *Asialaw Profiles*.

GRATA International advises clients in the following industries and areas of law around the globe:

- Natural Resources.
- Industry & Trade.
- Banking & Finance.
- Telecommunications & Transport.
- Construction & Infrastructure.
- Corporate Law.
- Contract Law.
- Dispute Resolution.
- Environmental Law.
- Finance & Securities.
- Intellectual Property.
- International Trade, Customs and WTO Law.
- Labour Law.
- Licences & Permits.
- Project Finance and Public-Private Partnership (PPP).
- Real Estate.
- Restructuring and Insolvency.
- Subsoil Use.
- Tax Law.

Other titles in the ICLG series include:

- Alternative Investment Funds
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com