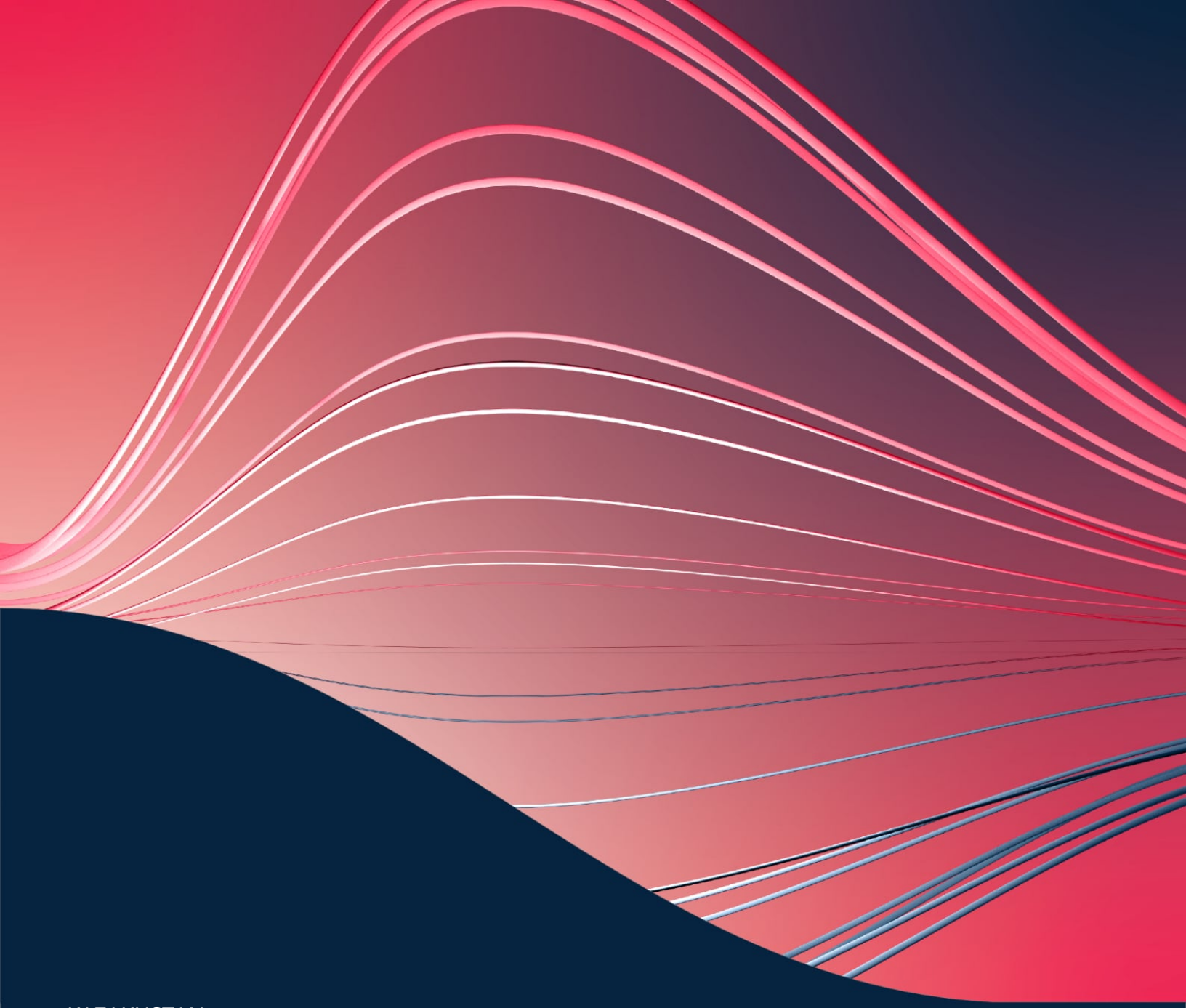


KAZAKHSTAN

Data Protection Laws of the World

DLA PIPER

Introduction

Welcome to the 2025 edition of DLA Piper's Data Protection Laws of the World Handbook. Since the launch of our first edition in 2012, this comprehensive guide has been a trusted resource for navigating the complex landscape of privacy and data protection laws worldwide. Now in its fourteenth edition, the Handbook has grown to provide an extensive overview of key privacy and data protection regulations across more than 160 jurisdictions. As we step into 2025, the global landscape of data protection and privacy law continues to evolve at an unprecedented pace. With new legislation emerging in jurisdictions around the world, businesses face a growing need to stay informed and agile in adapting to these changes. This year promises to bring new developments and challenges, making the Handbook an invaluable tool for staying ahead in this ever-changing field.

Europe

Established data protection laws in Europe continue to evolve through active regulatory guidance and enforcement action. In the United Kingdom, the UK government has proposed reforms to data protection and e-privacy laws through the new Data (Use and Access) Bill ("**DUAB**"). The DUAB follows the previous government's unsuccessful attempts to reform these laws post-Brexit, which led to the abandonment of the Data Protection and Digital Information (No.2) Bill ("**DPDI Bill**"), in the run-up to the general election. Although the DUAB comes with some bold statements from the government that it will *"unlock the power of data to grow the economy and improve people's lives"*, the proposals represent incremental reform, rather than radical change.

United States

In the United States, legislation on the federal and in particular state level continues to evolve at a rapid pace. Currently, the US has fourteen states with comprehensive data privacy laws in effect and six state laws will take effect in 2025 and early 2026. Additionally, at the federal level, the new administration has signaled a shift in enforcement priorities concerning data privacy. Notably, there is a renewed focus on the regulation of artificial intelligence (AI), with an emphasis on steering away from regulation and promoting innovation. This includes the revocation of previous executive orders related to AI and the implementation of new directives to guide AI development and use.

In the realm of children's privacy, many of the new administration's supporters in Congress have indicated a desire to make the protection of children on social media a top priority, and new leadership at the Federal Trade Commission (FTC) appears aligned on this goal, albeit with a willingness to take another look at the recently adopted amendments to the Children's Online Privacy Protection Act (COPPA) Rule. Health data

privacy remains a critical concern, with a handful of states following Washington state's lead in enhancing or adopting health data privacy laws. On the international data transfer front, Executive Order (E.O.) 14117 " Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" as supplemented by the DOJ's final Rule will impact companies transferring data into certain jurisdictions, such as China, Iran and Russia. Another area of focus for companies with an EU presence will be the Trump administration's approach to the Privacy and Civil Liberties Oversight Board, as it is a critical pillar of the EU/UK/Swiss-US Data Privacy Framework.

Asia, the Middle East, and Africa

Nowhere is the data protection landscape changing faster – and more fundamentally – than in Asia, with new laws in India, Indonesia, Australia and Saudi Arabia, as well continued new data laws and regulations in China and Vietnam. The ever-evolving data laws, as well as the trend towards regulating broader data categories (beyond personal data), in these regions continue to raise compliance challenges for multi-national businesses.

Emerging trends in data governance

Unlocking data, regulating the relentless advance of AI, creating fairer digital markets and safeguarding critical infrastructure against the ever growing cyber threat, continue to impact and overlap with the world of data protection and privacy. Perhaps most notably, the EU have introduced a raft of new laws forming part of its ambitious digital decade, which will bring huge change to businesses operating within the EU. With the rapid adoption of artificial intelligence enabled solutions and functionality, data protection supervisory authorities have been closely scrutinising the operation of AI technologies and their alignment with privacy and data protection laws. For businesses, this highlights the need to integrate date protection compliance into the core design and functionality of their AI systems. In the midst of this, the privacy community found itself at the centre of an emerging debate about the concept of 'AI governance'. This is not a surprising development – AI systems are creatures of data and the principle-based framework for the lawful use of personal data that sits at the heart of data protection law offers a strong starting point for considering how to approach the safe and ethical use of AI. As AI technologies advance, so will regulatory expectations. It is expected that regulatory scrutiny and activity will continue to escalate and accelerate in tandem with the increase in integration of powerful AI models into existing services to enrich data. Whilst privacy professionals cannot tackle the AI challenge alone, expect them to continue to be on the front lines throughout 2025 and beyond.

Disclaimer

This handbook is not a substitute for legal advice. Nor does it cover all aspects of the legal regimes surveyed, such as specific sectorial requirements. Enforcement climates and legal requirements in this area continue to evolve. Most fundamentally, knowing high-level principles of law is just one of the components required to shape and to implement a successful global data protection compliance program.

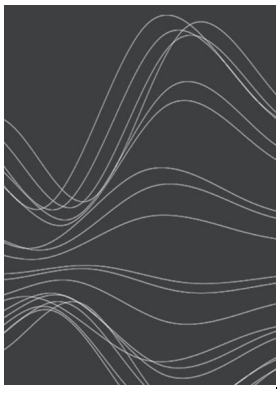
Africa key contact

Monique Jefferson
Director
monique.jefferson@dlapiper.com
Full bio

Americas key contact

Andrew Serwin
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
andrew.serwin@us.dlapiper.com
Full bio

Asia Pacific key contact



Carolyn Bigg
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
carolyn.bigg@dlapiper.com
Full bio

Europe key contacts

Andrew Dyson
Partner
andrew.dyson@dlapiper.com
Full bio

Ewa Kurowska-Tober
Partner
Head of Intellectual Property and Technology, Poland
ewa.kurowska-tober@dlapiper.com
Full bio

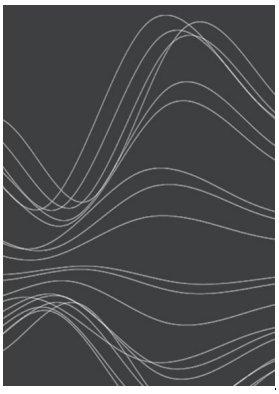
John Magee
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
john.magee@dlapiper.com
Full bio

Middle East key contact

Rami Zayat
Partner
rami.zayat@dlapiper.com
Full bio

Editors

Kate Lucente
Partner
kate.lucente@us.dlapiper.com
Full bio



Lea Lurquin
Associate
lea.lurquin@us.dlapiper.com
Full bio

Kazakhstan

LAST MODIFIED 4 FEBRUARY 2025

Data protection laws

The main legal act regulating personal data in Kazakhstan is the law of the Republic of Kazakhstan No. 94-V dated May 21, 2013 'On Personal Data and Its Protection' (the 'Law').

There are also a number of other laws providing for personal data protection requirements, including:

- The Law on Informatisation;
- The Law on Communication;
- The Labour Code of Kazakhstan;
- The Law on Online Platforms and Online Advertising.

Definitions

Definition of personal data

'**Personal data**' is any information relating to a specific individual (personal data subject) or a personal data subject who can be identified on the basis of such information which is recorded on electronic, paper and / or another tangible medium.

The law divides personal data into:

- '**Generally accessible personal data**', which is personal data that can be accessed freely with the consent of the personal data subject or to which confidentiality requirements do not apply in accordance with Kazakh law; and
- '**Limited access personal data**', which is personal data, access to which is limited by Kazakh law

Definition of sensitive personal data

Kazakh law does not provide for express definition of sensitive personal data.

In certain cases, sensitive personal data may qualify as limited access personal data and, as such, it is additionally regulated by sector-specific laws of Kazakhstan (e.g. medical secrecy, subscriber data). In our replies, we do not consider sector-specific restrictions which may affect personal data regulation (e.g. Kazakh law prohibits transfer of subscriber data, which includes, *inter alia*, personal data of subscribers).

National data protection authority

The main state authority in the field of personal data protection is the Ministry of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan (the 'Ministry'). The Ministry:

- shapes and implements the state policy on personal data and its protection;
- develops the procedure for implementation of personal data protection measures by the owner and / or operator of a personal data database and a third party related to the owner and / or operator of a personal data database;
- develops the rules to be followed by the personal data database owner and (or) operator when determining the scope of personal data necessary and sufficient for the performance of their tasks;
- develops the procedure for determining the list of personal data necessary and sufficient for the performance of tasks by the owner and (or) operator of a personal data database;
- determines the procedure for implementation of personal data protection measures by the owner and (or) operator of a personal data database, as well as by a third party;
- reviews requests of a personal data subject or his / her legal representative on compliance of the content of personal data and methods of its processing with the purpose of its processing and makes a respective decision;
- takes measures on bringing persons who have violated personal data laws of Kazakhstan to liability in accordance with the laws of Kazakhstan;
- requests the owner and / or operator of a personal data database and a third party related to the owner and / or operator of a personal data database to clarify, block or destroy inaccurate or illegally obtained personal data;
- takes measures on improving protection of rights of personal data subjects;
- creates an advisory council on issues of personal data and its protection as well as determines the procedure for its formation and activities;
- approves the rules for collection and processing of personal data;
- approves the rules for conducting a survey in order to assess the security level when storing, processing and distributing limited access personal data contained in electronic information resources and such rules should be agreed with the National Security Committee of the Republic of Kazakhstan;
- approves the rules for the functioning of the state service for control of access to personal data;

- coordinates the integration of non-state informatization entities with the state informatization entities and (or) state legal entities, which involves personal data transfer and (or) provision of access to personal data;
- approves the rules for integration with the state service for control of access to personal data;
- exercises other powers provided by Kazakh law.

The Government of Kazakhstan develops the main directions of state policy on personal data and its protection.

In relation to personal data and its protection, state authorities (each within its competence):

- develop and / or approve regulatory acts;
- consider appeals of individuals and / or legal entities regarding personal data and protection of personal data issues;
- take measures for bringing persons who have violated personal data legislation of Kazakhstan to liability;
- exercise other powers provided for by Kazakh law.

Supervision over observance of Kazakh law in respect of personal data and its protection is carried out by the prosecution authorities of Kazakhstan.

Registration

Under Kazakh law, there is no express registration requirement in relation to personal data and its protection, except the requirement for the personal data database owner and (or) operator as well as a third party related to the owner and / or operator to register and keep a record of the following actions:

- The term or period during which the consent to the collection, processing of personal data is valid;
- Information on whether there is a possibility of transfer of personal data to third parties by the personal data operator or not;
- Information on whether there is a cross-border transfer of personal data as part of the personal data processing;
- Information on dissemination of personal data in publicly resources.

Data protection officers

Under Kazakh law, an owner and / or operator of a personal data database, which is a legal entity, should appoint a person responsible for organizing the processing of personal data. Such person is obliged to:

- exercise internal control over observance by the owner and / or operator of a personal data database and its employees of Kazakh law requirements in relation to personal data and its protection;

- inform the employees of an owner and / or operator of the provisions of Kazakh law in respect of processing and protection of personal data;
- exercise control over receipt and processing of applications from personal data subjects or their legal representatives.

In addition, an owner and / or operator of a database containing personal data and a third party related to the owner and / or operator should, *inter alia*, when collecting and processing personal data, determine list of persons carrying out collection and processing of personal data or having access to it.

Collection and processing

Kazakh law requires to carry out collection and processing of personal data with the consent of a personal data subject or his / her legal representative. Such consent should be given in writing, via the state service, non-state service or other method that allows to confirm the receipt of consent. The consent should be given via the state service when collecting and / or processing personal data contained in the databases of the state bodies and / or state legal entities.

As a general rule, personal data subjects or their representatives may revoke their consent. However, the consent may not be revoked in cases where such revocation contradicts requirements of Kazakh law or there are any unfulfilled obligations.

Consent to the collection and processing of personal data should include:

- full name, business identification number (individual identification number) of the personal data database operator;
- full name of the personal data subject;
- the term and period during which the consent is effective;
- information on whether the operator may transfer the personal data to third parties or not;
- information on whether there is a cross-border transfer of personal date in the process of its processing or not;
- information on dissemination of personal data in public resources;
- list of data being collected on the personal data subject;
- other information as determined by the owner and / or operator.

Kazakh law allows the collection and processing of personal data without the consent of a personal data subject or his / her legal representative in cases explicitly prescribed by Kazakh law. Such cases may include, inter alia:

- implementation of activities of law enforcement bodies and courts;
- implementation of state statistical activities;
- use of depersonalised personal data by the state authorities for statistical purposes;
- implementation of international treaties ratified by Kazakhstan;

- protection of constitutional rights and freedoms of a person, if obtaining the consent of a personal data subject or his / her legal representative is impossible;
- carrying out legal professional activities of a journalist, carrying out tv-channel, radio-channel, news agency, mass media, online media, scientific, literary or other creative activities, subject to compliance with requirements of Kazakh law;
- publication of personal data in accordance with Kazakh law, including personal data of candidates for elective public offices;
- failure by a personal data subject to fulfil its obligation to provide personal data in accordance with Kazakh law;
- receipt by the state authority regulating, controlling and supervising financial market and financial organisations of information from individuals and legal entities in accordance with Kazakh law;
- receipt by the state revenue authorities of information from individuals and legal entities for purposes of tax administering and control;
- storage of a backup copy of electronic information resources containing limited access personal data to a national backupplatform for storing electronic information resources in cases provided for by Kazakh law;
- the use of personal data of entrepreneurs related directly to their business activities to form a register of business partners, subject to compliance with the requirements of Kazakh law;
- the use of personal data of a Kazakhstani national for the purposes of bankruptcy procedure.

Under the Law, processing of personal data should be limited to the achievement of specific, predetermined and legitimate goals. Processing of personal data that is incompatible with the purposes of collecting personal data is not allowed. Personal data, the content and volume of which is excessive in relation to the purposes of its processing, should not be processed.

Under Kazakh law, access to personal data is determined by the terms of consent for collection and processing of personal data, unless otherwise provided by Kazakh law. A person should be denied access to personal data if he / she refuses to assume obligations to ensure compliance with the requirements of the Law or may not ensure it.

Persons having access to limited access personal data should ensure its confidentiality.

Under Kazakh law, accumulation of personal data is carried out by collecting personal data that is necessary and sufficient to fulfil the tasks performed by an owner and / or an operator of a database containing personal data and by a third-party having access to such database.

Personal data should be stored in databases located in Kazakhstan.

The period for retention of personal data is determined by the date of fulfilment of the purpose(s) for collection and processing of the personal data, unless otherwise provided by Kazakh law.

Kazakh law provides for additional requirements in respect of electronic resources containing personal data and integration between personal data databases of private entities and the personal data databases of state bodies and state legal entities via the state service.

Transfer

Transfers of personal data are allowed if they do not violate the rights and freedoms of a personal data subject and do not affect the legitimate interests of other individuals and / or legal entities.

The transfer of personal data in cases that go beyond the previously stated purposes of its collection is permitted if carried out with the consent of a personal data subject or his / her legal representative.

The cross-border transfer of personal data to other countries is carried out only in cases where such countries ensure protection of personal data.

The cross-border transfer of personal data to countries that do not ensure protection of personal data is possible:

- with the consent of the personal data subject or his / her legal representative to the cross-border transfer of his / her personal data;
- in cases stipulated by international treaties ratified by Kazakhstan;
- in cases provided for by Kazakh law, if it is necessary for protecting the constitutional system, public order and public health and morals and rights and the freedoms of a person in Kazakhstan;
- in case of protection of constitutional rights and freedoms of a person, if obtaining the consent of a personal data subject or his / her legal representative is impossible.

Kazakh law may in certain cases prohibit the cross-border transfer of personal data.

Security

Protection of personal data is guaranteed by the state and is carried out in a manner determined by the Ministry.

Collection and processing of personal data is carried out only if its protection is ensured. Kazakh law defines protection of personal data as a set of legal, organization and technical measures.

The owner and / or operator of a personal data database and a third party having access to such database are required to take measures for protecting personal data in a manner determined by the Ministry, which ensure:

- prevention of unauthorized access to personal data;
- timely detection of the facts relating to an incident of unauthorized access to personal data, if such unauthorized access could not be prevented;

- minimizing adverse effects of unauthorized access to personal data;
- the state technical service's access to objects of informatisation that use, store, process and distribute limited access personal data contained in electronic information resources, so that the state technical service could carry out a survey to assess the security level of the processes of storage, processing and distribution of limited access personal data contained in electronic information resources in the manner determined by the authorized body;
- registration of certain operations with the personal data where required by Kazakh law.

The obligations of an owner and / or operator of a database containing personal data and a third party having access to such database to protect personal data arise from the moment of collecting the personal data and remain in force until such personal data is destroyed or depersonalized.

Kazakh law provides for additional requirements with regard to protection of electronic resources containing personal data.

Breach notification

An owner and / or operator of a database containing personal data should notify the authorized state body of security incidents related to an illegal access to the personal datawithin one business day since of detection.

Enforcement

Generally, all state authorities of Kazakhstan, depending on their competences, may consider appeals of individuals and / or legal entities regarding personal data and protection of personal data issues. The Ministry is authorised to take measures against persons who have violated the personal data legislation of Kazakhstan.

Prosecution Authorities of Kazakhstan carry out supervision over compliance with personal data legislation of Kazakhstan and may also take measures on bringing persons who have violated personal data legislation of Kazakhstan to liability. Interested persons may file complaints to the Prosecutor's Office and the Ministry regarding breach of the legislation in relation to personal data and its protection.

Kazakh law provides for administrative and criminal liability for violation of Kazakh law in relation to personal data and its protection.

Electronic marketing

The Law on Online Platforms and Online Advertising provides for certain requirements for personal data protection in relation to the use of online platforms (websites, messengers, etc.) and online advertising.

In particular, it prohibits the profiling of the online-platform's users for the purposes of targeted advertising if such profiling is based on race or nationality, political opinions, biometric or personal data, or information about the users' health. Profiling is defined as a set of algorithms aimed at determining the preferences and (or) interests of users.

Online privacy

Under the Law on Online Platforms and Online Advertising, the owner and (or) legal representative of the relevant online platform should do the following in order to protect personal data on the online platform:

- familiarize users with the privacy policy of the online platform before completing their registration;
- ensure the integrity, safety and confidentiality of personal data;
- prevent the dissemination of personal data without the consent of the user or his / her legal representative;
- immediately notify the user in case of violation of the confidentiality of his / her personal data;
- perform other duties provided for by the Law on Personal Data and Its Protection.

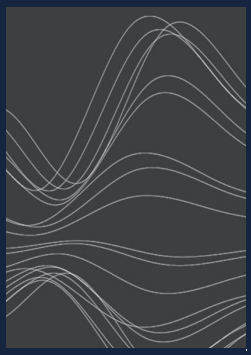
Data protection lawyers

Dinara Jarmukhanova
Partner
Centil Law Firm
dinara.jarmukhanova@centil.law

Dariga Adanbekova
Associate
Centil Law Firm
dariga.adanbekova@centil.law

For more information

To learn more about DLA Piper, visit dlapiper.com or contact:



Carolyn Bigg
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
carolyn.bigg@dlapiper.com
Full bio

John Magee
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
john.magee@dlapiper.com
Full bio

Andrew Serwin
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
andrew.serwin@us.dlapiper.com
Full bio

About us

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa and Asia Pacific, positioning us to help companies with their legal needs around the world.

dlapiper.com